p-adic construction of CM-curves

David Kohel & Christophe Ritzenthaler

Abstract

We give a p-adic analytic construction of the invariants of CM curves of genus 2, obtained by the 2-adic AGM lifting algorithm. This construction provides an alternative to the complex analytic approach for reconstructing the invariants of curves. By reduction modulo a suitable large prime, the CM invariants of these curves enable the efficient construction of curves of with known group order suitable for cryptosystems based on the discrete logarithm problem.

1 Introduction

The traditional approach to CM constructions in genus 1 has been through evaluate of the j-function on an upper half complex plane at special points corresponding to lattices with complex multiplication [4] or using special modular functions of higher level as in Yui and Zagier [17] or Enge and Morain [2]. This construction has been extends to genus 2 curves, using theta functions on Siegel upper half plane (see, e.g., van Wamelen [14] and Weng [16]).

The p-adic point counting algorithms of Satoh and generalizations such as Mestre's AGM method determine the number of points on an elliptic or hyperelliptic curves by constructing a p-adic canonical lift. Although conceived for the purpose of point counting these algorithms are in fact p-adic analytic analogues of the complex analytic CM constructions cited above. Couveignes and Henocq [1] developed the theory of this method when applied to the j-function in genus 1.

In the present work, we utilise the AGM construction for genus 2 curves to lift invariants of a hyperelliptic curve over a finite field of characteristic 2 to an extension of $\mathbb{Q}_2$, then use lattice reduction to reconstruct the minimal polynomials of these invariants over $\mathbb{Q}$. The algorithm uses only the elementary recursive construction of the AGM algorithm, applied to curves over small finite fields, together with LLL reduction to rationally reconstruct the invariants.

2 Canonical Lift by the AGM

We recall in this section the principle and the formulas of the AGM algorithm for genus 2 curves. For proofs we refer to Lercier and Lubicz [5], Mestre [6] or Ritzenthaler [12]. Let $q = 2^n$, set $k = \mathbb{F}_q$, let $K = \mathbb{Q}_q$ be the unramified extension of $\mathbb{Q}_2$ of degree n, and let $\mathbb{Z}_q$ be its ring of integers. Then the Galois group $\mathrm{Gal}(K/\mathbb{Q}_2)$ is generated by the Frobenius automorphism which we denote by σ.

The AGM algorithm applies to any ordinary hyperelliptic curve $\tilde{C}$, which we may represent in Weierstrass form:

$$\tilde{C}/k : y^2 + \tilde{v}(x)y = \tilde{u}(x)\tilde{v}(x) \tag{1}$$

where $\tilde{v}$ and $\tilde{u}$ are degree 3 monic polynomials such that $\tilde{v}$ is square-free. Note that for any curve

$$\tilde{C}/k : y^2 + \tilde{v}(x)y = f(x)$$

such that $(v, f) = w$, we can set $c = 1/\sqrt{f/w} \bmod (v/w)$, and set make a change of variables $y \mapsto y + c$ to put $\tilde{C}$ in the form (1).

Such a curve $\tilde{C}$ is a genus 2 curve and is ordinary, i.e the Jacobian $\tilde{J}$ of $\tilde{C}$, has four 2-torsion points defined over some extension field. We know then that there exists a principally polarized abelian surface $(J, \lambda)/K$ which lifts the principally polarized Jacobian $(\tilde{J}, \tilde{\lambda})/k$ together with its ring of endomorphisms: $\mathrm{End}_K(J) \simeq \mathrm{End}_k(\tilde{J})$.

Using the AGM algorithm, we can construct sequences of 2-adic numbers which converge 2-adicly to 'invariants' associated to (J, λ). This is achieved by the following process :

1. Replace k by a finite extension (of degree up to three) such that the roots of $\tilde{v}$ are defined.

2. Lift $\tilde{C}$ over K: Lift $\tilde{v}$ and $\tilde{u}$ to $v(x)$ and $u(x)$ in $K[x]$ and then let

$$C/K : Y^2 = (2y + v(x))^2 = v(x)(v(x) + 4u(x)).$$

   Since $\tilde{v}$ splits in k with distinct roots, we can write in K,

$$C/K : Y^2 = \prod_{i=1}^{3}(x - x_i)\prod_{i=1}^{3}(x - (x_i + 4s_i)).$$

3. Initialization of theta characteristics: Denote by

$$\begin{array}{lll} e_1 = x_1, & e3 = x_2, & e5 = x_3, \\ e_2 = x_1 + 4s_1, & e_4 = x_2 + 4s_2, & e_6 = x_3 + 4s_3 \end{array}$$

   The Thomae formulas give us 4 initial invariants

$$\begin{array}{rcl} A & = & (e_1 - e_3)(e_3 - e_5)(e_5 - e_1)(e_2 - e_4)(e_4 - e_6)(e_6 - e_2) \\ B & = & (e_1 - e_3)(e_3 - e_6)(e_6 - e_1)(e_2 - e_4)(e_4 - e_5)(e_5 - e_2) \\ C & = & (e_1 - e_4)(e_4 - e_5)(e_5 - e_1)(e_2 - e_3)(e_3 - e_6)(e_6 - e_2) \\ D & = & (e_1 - e_4)(e_4 - e_6)(e_6 - e_1)(e_2 - e_3)(e_3 - e_5)(e_5 - e_2) \end{array}$$

   We recall that these numbers are 2-adic analogs of the respective complex values :

$$\vartheta\left[\begin{smallmatrix}00\\00\end{smallmatrix}\right](0)^4,\ \vartheta\left[\begin{smallmatrix}00\\10\end{smallmatrix}\right](0)^4,\ \vartheta\left[\begin{smallmatrix}00\\01\end{smallmatrix}\right](0)^4,\ \vartheta\left[\begin{smallmatrix}00\\11\end{smallmatrix}\right](0)^4.$$

   We initialize $(A_0, B_0, C_0, D_0) := (1, \sqrt{B/A}, \sqrt{C/A}, \sqrt{D/A})$, where the square root of an element of the form $1 + 8\mathbb{Z}_q$ is taken as the unique element of $\mathbb{Z}_q$ of the form $1 + 4\mathbb{Z}_q$.

4. Lifting process: We use the duplication formula to obtain a 4-tuple of invariants

$$(A_n, B_n, C_n, D_n)$$

   as elements of $\mathbb{Z}_q$:

$$A_{n+1} = \frac{A_n + B_n + C_n + D_n}{4} \qquad C_{n+1} = \frac{\sqrt{A_n C_n} + \sqrt{B_n D_n}}{2}$$
$$B_{n+1} = \frac{\sqrt{A_n B_n} + \sqrt{C_n D_n}}{2} \qquad D_{n+1} = \frac{\sqrt{A_n D_n} + \sqrt{B_n C_n}}{2}$$

These invariants do not converge but if we denote the invariants associated to J by $(A_\infty, B_\infty, C_\infty, D_\infty)$, we have

$$(A_n, B_n, C_n, D_n) \equiv (A_\infty, B_\infty, C_\infty, D_\infty)^{\sigma^n} \bmod 2^n,$$

where σ is the Frobenius automorphism of $\mathbb{Z}_q/$. In particular, each of the sequences of invariants

$$(A_{kr+i}, B_{kr+i}, C_{kr+i}, D_{kr+i}),$$

for fixed i in $1 \le i \le r$, does converge as k goes to infinity. But since we may consider any of the Galois conjugates of Igusa invariants, we terminate the algorithm at any step n to obtain a precision of n bits.

Finally, we note that the algorithmic improvements of Lercier and Lubicz [5] to obtain quadratic convergence is applicable here.

3 Computation of the p-adic invariants

The seqeunce of values A_n, B_n, C_n, D_n of the preceding section describe a cycle of Galois conjugate invariants of the canonical lift (J, λ) to K of our original Jacobian $(\tilde{J}, \tilde{\lambda})$ over k. In genus 2 the canonical lift is itself the Jacobian of a genus 2 curve C over K. We now describe how to determine the invariants of the curve C/K, from a set of invariants A_n, B_n, C_n, and D_n.

We proceed in two steps as described by van Wamelen [14]. Recall that over $\mathbb{C}$, if C is given by the Rosenhain normal form

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

then the λ_i are given by the following expressions :

$$\lambda_1 = -\frac{\vartheta_1^2\vartheta_3^2}{\vartheta_6^2\vartheta_4^2}, \quad \lambda_2 = -\frac{\vartheta_2^2\vartheta_3^2}{\vartheta_6^2\vartheta_5^2}, \quad \lambda_3 = -\frac{\vartheta_2^2\vartheta_1^2}{\vartheta_4^2\vartheta_5^2}$$

where

$$\vartheta_1 = \vartheta[\begin{smallmatrix}00\\10\end{smallmatrix}](0), \quad \vartheta_2 = \vartheta[\begin{smallmatrix}00\\11\end{smallmatrix}](0), \quad \vartheta_3 = \vartheta[\begin{smallmatrix}01\\10\end{smallmatrix}](0),$$

$$\vartheta_4 = \vartheta[\begin{smallmatrix}10\\00\end{smallmatrix}](0), \quad \vartheta_5 = \vartheta[\begin{smallmatrix}10\\01\end{smallmatrix}](0), \quad \vartheta_6 = \vartheta[\begin{smallmatrix}11\\00\end{smallmatrix}](0).$$

We then use 2-adic analogues that we can compute by means of the general duplication formulas (see Mumford [10], and [11]), namely we set

$$\vartheta_1^2 = B_n, \qquad \vartheta_2^2 = D_n,$$

$$\vartheta_3^2 = \frac{\sqrt{A_{n-1}B_{n-1}} - \sqrt{C_{n-1}D_{n-1}}}{2}, \quad \vartheta_4^2 = \frac{A_{n-1} - B_{n-1} + C_{n-1} - D_{n-1}}{4},$$

$$\vartheta_5^2 = \frac{\sqrt{A_{n-1}C_{n-1}} - \sqrt{B_{n-1}D_{n-1}}}{2}, \quad \vartheta_6^2 = \frac{A_{n-1} - B_{n-1} - C_{n-1} + D_{n-1}}{2}.$$

Given λ_i we can then compute the Igusa invariants I_2, I_4, I_6, and I_{10} (for details we refer to van Wamelen [14]) and define the absolute invariants

$$i_1 = I_2^5/I_{10}, \; i_2 = I_2^3 I_4/I_{10}, \; i_3 = I_2^2 I_6/I_{10}.$$

4 Rational reconstruction of the invariants

From the p-adic invariants it remains to determine a set of defining relations over $\mathbb{Z}$. For this purpose it is desirable to predetermine the degree of relations among the absolute invariants. This degree can be explicitly determined, from the data of a CM type for K. However, in the case that K/Q defines a cyclic or non-normal quartic extension, that the totally real subfield L of K has class number one, and the only roots of unity in K are $\{\pm 1\}$, we have the following theorem of Weng [15, Theorem 3.1].

Theorem 1. *The number of classes of Igusa invariants of a CM type for the maximal order of K equals the class number h_K of K if K is cyclic and $2h_K$ if K is a non-normal quartic extension.*

From these absolute invariants, we use LLL on the space of p-adic relations among the powers $1, i_k, i_k^2 \dots, i_k^n$ of degree n to solve for

$$H_1(i_1) = H_2(i_2) = H_3(i_3) = 0. \tag{2}$$

Such relations appear as short vectors in the space of all relations over $\mathbb{Z}_p$ to some precision p^N. In addition, we reconstruct additional relations

$$L_1(i_1, i_2, i_3) = L_2(i_1, i_2, i_3) = 0, \tag{3}$$

in order to record the dependencies among the diffferent invariants. This removes the problem of combinatorial matching of up to n^3 possible combinations of roots over some finite field $\mathbb{F}_p$.

We note that the polynomials H_1, H_2, and H_3 are not in general monic. The possible prime divisors of the leading coefficient are characterised by Goren and Lauter [9]. Although the exact powers of these leading coefficients are not known, it is possible to clear denominators in the absolute invariants and reconstruct first the leading coefficients using a much smaller precision.

A more critical issue is the identification of a representative curve whose Jacobian has maximal endomorphism ring. It is necessary to have a mechanism to distinguish and discard curves associated to the nonmaximal orders. The following theorem provides such as test.

Theorem 2. *Let χ be the minimal polynomial of the Frobenius endomorphism $Frob_q$ on the Jacobian J of a genus 2 curve $C/\mathbb{F}_q$. Let π be any root of this polynomial and set $K = \mathbb{Q}(\pi)$ and $\bar{\pi} = q/\pi$. If the set*

$$\left\{ \frac{f_1(\pi)}{m_1}, \dots, \frac{f_t(\pi)}{m_t} \right\}$$

for $(m_i, q) = 1$ generates the maximal order O_K over $\mathbb{Z}[\pi, \bar{\pi}]$, then $\mathrm{End}(J) = O_K$ if and only if $f_i(Frob_q)$ is the zero map on $J[m_i]$ for all i.

N.B In practice it suffices to check only for each maximal prime power $p_i^{e_i}$ dividing each m_i.

5 Algorithm and Examples

Strategy:

1. For a given field $k = \mathbb{F}_{2^n}$, choose curve defined by u, v in $k[x]$, hence with field of moduli equal to k, then determine theta constants over some extension.

2. Determine the index of $\mathbb{Z}[\pi, \bar{\pi}]$ in the maximal order O_K, and the group structure of quotient $A = O_K/\mathbb{Z}[\pi, \bar{\pi}]$.

3. Let $f_1(\pi)/m_1, \dots, f_t(\pi)/m_t$ generate O_K over $\mathbb{Z}[\pi, \bar{\pi}]$. For each m_i determine the action of π on $J[m_i]$ and reject the curve if the restriction of $f_i(\pi)$ to $J[m_i]$ is nonzero.

4. Lift the theta constants and reconstruct by LLL the defining relations for the CM igusa invariants defining those curves whose Jacobian J has O_K embedded in $\mathrm{End}(J)$.

Note that by choosing a curve over its field of moduli, rather than the extension field over which the Weierstrass points are defined, we select a curve whose Jacobian is more likely to be in the class of the maximal endomorphism ring. Such a curve minimizes both the degree and the size of coefficients in the relations for the Igusa invariants.

Examples. Here we provide a few examples of canonical lifts of the Igusa invariants of hyperelliptic curves of the form

$$C : y^2 + v(x)y = v(x)u(x)/\mathbb{F}_{2^n},$$

and their application to explicit constructions of Jacobians suitable for cryptography.

1. For the curve $C/\mathbb{F}_2$ with $v = x^3 + 1$ and $u = x^2$, we find relations for the canonical lifts fo the Igusa invariants:

$$\begin{array}{l} i_1^2 - 531441 i_1 + 55788550416, \\ i_2^2 - 426465 i_2 - 68874753600, \\ i_3^2 - 216513 i_3 - 221011431552, \\ 140 i_1 - 243 i_2 + 135 i_3, \\ 69 i_1 - 119 i_2 + 66 i_3 - 104976. \end{array}$$

The minimal polynomial of Frobenius in $\mathrm{End}(J)$ is equal to

$$x^4 + 2x^3 + 3x^2 + 4x + 4,$$

defining an imaginary quadratic extension of the real quadratic field $\mathbb{Q}(\sqrt{2})$.

2. For the curve $C/\mathbb{F}_2$ with $v = x^3 + x^2 + 1$ and $u = x^2 + 1$ we find relations for the canonical lifts fo the Igusa invariants:

$$\begin{array}{l} 4 i_1^2 + 8218017 i_1 + 146211169851, \\ i_2^2 + 1008855 i_2 - 342014432400, \\ i_3^2 + 1368387 i_3 - 240090131376, \\ 4480 i_1 + 7499 i_2 - 12255 i_3, \\ 716 i_1 + 1212 i_2 - 1971 i_3 - 1666737 \end{array}$$

The minimal polynomial of Frobenius in $\mathrm{End}(J)$ is equal to

$$x^4 + x^3 + x^2 + 2x + 4,$$

defining an imaginary quadratic extension of the real quadratic field $\mathbb{Q}(\sqrt{13})$.

3. For the curve $C/\mathbb{F}_2$ with $v = x^3 + x^2 + 1$ and $u = x^2$ we find relations for the canonical lifts fo the Igusa invariants:

$$\begin{aligned}
&4i_1^2 + 115322697i_1 - 10896201253125,\\
&i_2^2 + 9073863i_2 - 2152336050000,\\
&i_3^2 + 14410143i_3 - 1214874126000,\\
&896i_1 + 369i_2 - 2025i_3,\\
&300i_1 + 122i_2 - 677i_3 + 273375
\end{aligned}$$

The minimal polynomial of Frobenius in $\mathrm{End}(J)$ is equal to

$$x^4 + x^3 + 3x^2 + 2x + 4,$$

defining an imaginary quadratic extension of the real quadratic field $\mathbb{Q}(\sqrt{5})$.

6 Conclusion

The AGM provides a relatively elementary and effective alternative to the complex analytic construction of complex multiplication for genus 2 curves. We note that not all CM orders arise in this way, but those curves that do have good reduction at 2 and small class number appear among the curves over small fields $\mathbb{F}_2^n$. The approach through p-adic lifting also permits us to treat curves whose Jacobians are not absolutely simple. In order to capture additional orders, corresponding to Jacobians with bad reduction at 2, it would be desirable to extend the algorithmic theory of canonical lifts to curves of genus 2 in odd characteristic.

References

[1] J.-M. Couveignes and T. Henocq, Action of modular correspondences around CM points, *Algorithmic Number Theory (ANTS V, Sydney)*, 234–243, *Lect. Notes in Comp. Sci.*, **2369**, Springer, Berlin, 2002.

[2] A. Enge and François Morain, Comparing invariants for class fields of imaginary quadratic fields, *Algorithmic number theory (Sydney, 2002)*, 252–266, *Lect. Notes in Comput. Sci.*, **2369**, Springer, Berlin, 2002.

[3] J. I. Igusa, Arithmetic variety of moduli for genus two. *Ann. of Math.*, **72** (3), (1960) 612–649.

[4] E. Kaltofen and N. Yui, Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction, *Number theory (New York, 1989/1990)*, 149–202, Springer, New York, 1991.

[5] R. Lercier and D. Lubicz, A quasi quadratic time algorithm for hyperelliptic curve point counting, *Journal of the Ramanujan Mathematical Society*, 2004.

[6] J.-F. Mestre, Algorithmes pour compter des points en petite caractéristique en genre 1 et 2, `http://www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps`.

[7] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, *Effective methods in algebraic geometry*, 313–334, *Progress in Mathematics*, **94**, Birkhäuser, Boston, 1991.

[8] J.-B. Bost and J.-F. Mestre, Moyenne arithmetico-geometrique et periodes des courbes de genre 1 et 2, *Gaz. Math.* **38**, (1988), 36–64.

[9] E. Goren and K. Lauter, Class invariants for quartic CM fields, `http://au.arxiv.org/-abs/math.NT/0404378`

[10] D. Mumford, Tata Lectures on Theta I, *Progress in Mathematics*, **28**, Birhäuser, 1983.

[11] D. Mumford, Tata Lectures on Theta II, *Progress in Mathematics*, **43**, Birhäuser, 1984.

[12] C. Ritzenthaler, *Problèmes arithméthiques relatifs à certaines familles de courbes sur les corps finis*, PhD thesis, Université Paris 7, 2003.

[13] G. Shimura, *Abelian varieties with complex multiplication and modular forms*, Princeton University Press, NJ, 1998.

[14] P. van Wamelen, Examples of genus two CM curves defined over the rationals, *Math. Comp.*, **68** (1999), no. 225, 307–320.

[15] A. Weng, Extensions and improvements for the CM method for genus two, Fields Institute Communications, **42**, 2003a.

[16] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography, *Math. Comp.*, **72** (2003), no. 241, 435 - 458.

[17] N. Yui and D. Zagier, On the singular values of Weber modular functions, *Math. Comp.* **66** (1997), no. 220, 1645–1662.

Example Finale. Let $C : y^2 + v(x)y = u(x)v(x)$ be the hyperelliptic curve over $\mathbb{F}_{2^3} = \mathbb{F}_2[w]$ where $w^3 + w + 1 = 0$ where u and v are given by

$$
\begin{aligned}
u &= (w^2 + w + 1)x^2 + w^2 x + w^2, \\
v &= x^3 + (w^2 + w + 1)x^2 + x + w + 1.
\end{aligned}
$$

The minimal polynomial of Frobenius on the Jacobian of C is

$$x^4 - 3x^3 + 3x^2 - 24x + 64,$$

defining an imaginary quadratic extension of the real quadratic field $\mathbb{Q}(\sqrt{61})$. The defining relations of canonical lifts of the Igusa invariants are given below.

$$
\begin{aligned}
&2^6 3^{42} i_1^6 - 2344912105503116116288576047953057125392 i_1^5 \\
&-112639584390304238456172276845130150039402556586283156 i_1^4 \\
&-21774151033958540600412467485347176632247848315607009342854830510 75 i_1^3 \\
&-15936419940544408709376306530703638369363662226923214713038080125439887 02 i_1^2 \\
&-77232882710173372962531506548540432736193603391160944219774880180377797557 2191 i_1 \\
&+32299720850335379144290409627740329840675572467939277123595091705537581712591977043, \\
&3^{18} i_2^6 + 30345890982308051019805350 i_2^5 \\
&-2881361916498328939170620773887109083 75 i_2^4 \\
&+75311083251582136774909699089942702936936785265637 5 i_2^3 \\
&-6491273094759205393124004826875979142556588855515628300 00 i_2^2 \\
&+51206524459199223335885868122872603853991501852764644768080 0000 i_2 \\
&-24272920155156909628661627097113112044952744390034202392223340800 0000, \\
&3^{24} i_3^6 + 274374611813847636940118813 46 i_3^5 \\
&-35204080604931845265596273380705748924033 1 i_3^4 \\
&+11789221533340810664841739684807257004447396394229660 03 i_3^3 \\
&+50992879098264551485642755853537750581665889092002072268721 6 i_3^2 \\
&+228130282826174574878551565831919365949825510821776329730159434 24 i_3 \\
&-19462770713272722403628597313320440103400790281734382852129885861194547 2, \\
&633895738920000 i_1^3 + 8517595035131037 i_1^2 i_2 - 2422318926838275 i_1^2 i_3 \\
&+52888701255649776 0 i_1^2 - 2671415018933342 i_1 i_2^2 + 10103099744994882 i_1 i_2 i_3 \\
&+4980682705166674 79 i_1 i_2 - 3168582718927297 5 i_1 i_3 + 18498687096353030 60 i_1 \\
&+110024157843386 74 i_2^3 - 1619524775083390 4 i_2^2 i_3 + 8001648464907740 71 i_2^2 \\
&+2286226402382531 45 i_2 i_3, \\
&5258604005092224 0 i_1^3 + 3480461332006314 78 i_1^2 i_2 + 1978897208105781 0 i_1^2 i_3 \\
&+2623630964591332 9728 i_1^2 - 1611043809046282 405 i_1 i_2 i_3 - 3753782789770657 910 i_1 i_2 \\
&+1519575925397564 523 i_1 i_3^2 + 2446649956939951 033 i_1 i_3 - 1746640058954627 936 i_1 \\
&+1153484491100961 901 i_2 i_3^2 - 6729087358177501 571 i_2 i_3 - 3413986566072687 702 i_2 \\
&-158509055831845 9827 i_3^3 - 1037783410918613 0040 i_3^2 - 1238523812063934 3570 i_3, \\
&1428316341357006 2 i_1 i_2^2 - 2196521724202653 0 i_1 i_2 i_3 - 9110050391167390 6 i_1 i_2 \\
&+8753819554156320 i_1 i_3^2 + 7414107877502670 i_1 i_3 - 85097670432239360 i_1 \\
&+3160028075123540 i_2^3 - 19415412647408141 i_2^2 i_3 - 11227855503503951 i_2^2 \\
&+28513098102060099 i_2 i_3^2 - 10104997618986857 3 i_2 i_3 - 10890112918608090 i_3^3 \\
&+42818455041104040 i_3^2
\end{aligned}
$$