PAPER

Construction of Secure C_{ab} Curves Using Modular Curves

Seigo ARITA†, *Member*

SUMMARY *This paper proposes a heuristic algorithm which, given a basis of a subspace of the space of cuspforms of weight 2 for $\Gamma_0(N)$ which is invariant for the action of the Hecke operators, tests whether the subspace corresponds to a quotient A of the jacobian of the modular curve $X_0(N)$ such that A is the jacobian of a curve C. Moreover, equations for such a curve C are computed which make the quotient suitable for applications in cryptography. One advantage of using such quotients of modular jacobians is that fast methods are known for finding their number of points over finite fields.*

key words: discrete logarithm, modular curve, hyperelliptic curve, C_{ab} curve

1. C_{ab} curve

We define C_{ab} curve, following Miura[10]. Let C be an algebraic curve defined over a perfect field K with a place P of degree one. Take the ring $L(\infty P)$ of functions on C which are holomorphic away from P:

$$L(\infty P) = \{f \in K(C)^\times \mid v_Q(f) \geqq 0 \ (\forall Q \neq P)\}.$$

All of the pole numbers $-v_P(f)$ at P of $f \in L(\infty P)$ become a monoid M_P:

$$M_P = \{-v_P(f) \mid f \in L(\infty P)\}.$$

Take a minimum system $A = \{a_1, a_2, \ldots, a_t\}$ $(a_1 < a_2 < \cdots < a_t)$ of generators of M_P as a monoid:

$$M_P = \boldsymbol{N}_0 a_1 + \boldsymbol{N}_0 a_2 + \cdots + \boldsymbol{N}_0 a_t = \langle A \rangle.$$

Note $\gcd(a_1, \ldots, a_t) = 1$, since M_P has a finite complement set in $\boldsymbol{N}_0$.

For $A = \{a_1, \ldots, a_t\}$, define a function Ψ_A on $\boldsymbol{N}_0^t$ as

$$\Psi_A(n_1, \ldots, n_t) = \sum_{i=1}^{t} a_i n_i \quad (n = (n_i) \in \boldsymbol{N}_0^t).$$

Definition 1 (C_{ab} order)**:** For $m = (m_1, \ldots, m_t)$, and $n = (n_1, \ldots, n_t) \in \boldsymbol{N}_0^t$, define an order $>_A$, as

$$\begin{aligned} m >_A n \overset{\text{def}}{\iff} & \ \Psi_A(m) > \Psi_A(n) \\ \text{or} \quad & \ \Psi_A(m) = \Psi_A(n), \\ & \ m_1 = n_1, \ldots, m_{i-1} = n_{i-1}, m_i < n_i. \end{aligned}$$

Then, the order $>_A$ becomes a monomial order, called "C_{ab} order of type A". □

We define two sets dependent only on A;

$$\begin{aligned} B(A) = & \{\text{the least } m \in \boldsymbol{N}_0^t \text{ w.r.t } C_{ab} \text{ order of type } A \\ & \text{satisfying } \Psi_A(m) = a \mid a \in \langle A \rangle\}, \\ V(A) = & \{l \in \boldsymbol{N}_0^t \setminus B(A) \mid l = m + n, m \in \boldsymbol{N}_0^t \setminus B(A), \\ & n \in \boldsymbol{N}_0^t \Rightarrow n = (0, 0, \ldots, 0)\}. \end{aligned}$$

Miura[10] showed;

Theorem 2: Let C be an algebraic curve defined over a perfect field K with a place P of degree one. Suppose M_P has a minimum system $A = \{a_1, \ldots, a_t\}$ $(a_1 < \cdots < a_t)$ of generators as a monoid. Then, the curve C has a nonsingular affine model in t-dimensional affine space defined by the equations

$$F_m = X^m + \alpha_l X^l + \sum_n \alpha_n X^n \quad (m \in V(A)), \quad (1)$$

with $n \in B(A)$ satisfying $\Psi_A(n) < \Psi_A(m)$, a unique $l \in B(A)$ satisfying $\Psi_A(m) = \Psi_A(l)$, and $\alpha_l (\neq 0), \alpha_n \in K$. Here, X^m, X^l and X^n are written in multi index notations, for example $X^m = X_1^{m_1} X_2^{m_2} \cdots X_t^{m_t}$.

The above affine curve $F_m = 0$ $(m \in V(A))$ obtained from $A = \{a_1, \ldots, a_t\}$ $(\gcd(a_1, \ldots, a_t) = 1, a_1 < \cdots < a_t)$, is called a "$C_{ab}$ curve of type A".

Example: $C_{3,5,7}$ curve

$C_{3,5,7}$ curve, that is C_{ab} curve of type $\{3, 5, 7\}$, is a space curve defined by three equations of the following form;

$$\begin{aligned} Y^2 = & \ a_0 XZ + a_1 X^3 + a_2 XY + a_3 Z + a_4 X^2 + a_5 Y \\ & + a_6 X + a_7, \\ YZ = & \ b_0 X^4 + b_1 X^2 Y + b_2 XZ + b_3 X^3 + b_4 XY + b_5 Z \\ & + b_6 X^2 + b_7 Y + b_8 X + b_9, \\ Z^2 = & \ c_0 X^3 Y + c_1 X^2 Z + c_2 X^4 + c_3 X^2 Y + c_4 XZ \\ & + c_5 X^3 + c_6 XY + c_7 Z + c_8 X^2 + c_9 Y + c_{10} X \\ & + c_{11}. \end{aligned} \quad (2)$$

2. Security Condition

A discrete-log based cryptosystem using the jacobian group of a curve C over a field $\boldsymbol{F}_q$ will be less secure

Manuscript received
Manuscript revised
†The author is with NEC Co.,Kawasaki-shi,216 Japan.

than a standard 1024 bit RSA system, unless four conditions are satisfied.

1. (Against Pollard's rho algorithm)
   The order h of the Jacobian J_C has a prime factor l of 160 or more bits[11].
2. (Against FR attack)
   The prime factor l does not divide $q^k - 1$ for small k [5].
3. (Against Rück attack)
   l should be coprime with q[13].
4. (Against Gaudry's variant)
   q has $(40 + \log_2(84(g-1)) + \log_2(m))$ or more bits[3], [8].

3. Construction of Secure C_{ab} curves

For definitions of the congruence subgroup $\Gamma_0(N)$, the modular curve $X_0(N)$, and so on, see [4] or [12].

3.1 Number of points of a simple factor of a modular curve

Let N be a natural number. Let $C(N)$ be a $\boldsymbol{Q}$-vector space with basis $\boldsymbol{P}^1(\boldsymbol{Z}/N\boldsymbol{Z})$, and $B(N)$ be its subspace spanned by all elements of the form

$$(c:d) + (-d:c),$$
$$(c:d) + (c+d:-c) + (d:-c-d).$$

Let $C_0(N)$ be a $\boldsymbol{Q}$-vector space spanned by $\Gamma_0(N)$-cusps. The boundary map $\delta : C(N) \to C_0(N)$ is defined by

$$\delta((c:d)) = [a/c] - [b/d],$$

where integers a and b are chosen so that $ad - bc = 1$, and for example, $[a/c]$ denotes a $\Gamma_0(N)$ equivalent class of a cusp a/c. Set $Z(N) = \ker(\delta)$. As $B(N) \subset Z(N)$, we can define $H(N) = Z(N)/B(N)$, which is a $\boldsymbol{Q}$-vector space of dimension $2g$, where g is the genus of the modular curve $X_0(N)$. Take the eigenspace $H^+(N)$ belonging to $+1$ of the star operator $* : (c:d) \mapsto (-c:d)$ on $H(N)$. Note the star operator is an involution.

Proposition 3 ([4])**:** Let $\boldsymbol{T}$ be the Hecke algebra of level N. As $\boldsymbol{T}$-modules,

$$H^+(N) \otimes_{\boldsymbol{Q}} \boldsymbol{C} \cong S_2(N).$$

For a prime p not dividing N, the operator T_p on $H^+(N)$ is calculated by the set R_p of Heilbronn matrices for p;

$$T_p((c:d)) = \sum_{M \in R_p} (c:d)M.$$

An algorithm for computing Heilbronn matrices is given in page 22 of [4].

A simple factor A of the Jacobian $J_0(N)$ corresponds to a simple $\boldsymbol{T}$-submodule K of $H^+(N)$ one-to-one. The dimension of A as an abelian variety is equal to the dimension of K as a vector space over $\boldsymbol{Q}$. Using Eichler-Shimura relation [12] one finds the formula for the number of points on a factor A over a prime field $\boldsymbol{F}_p$ for a prime p not dividing N,

$$\sharp A/\boldsymbol{F}_p = \mathrm{Det}(x^2 - T_p \mid_K x + p) \mid_{x=1} . \tag{3}$$

In the above, scalars x^2, x and p denotes the scalar multiplication operators. For example, $p = p \cdot \mathrm{Id}$.

3.1.1 Example: level 97

Let $N = 97$. $H^+(97)$ is 7-dimensional over $\boldsymbol{Q}$ with a basis $\{g_1, g_2, \cdots, g_7\}$;

$$\begin{aligned}
g_1 &= (44:1) - (88:1) + (91:1),\\
g_2 &= (70:1) + (87:1) - (88:1) + (91:1) - (92:1)\\
&\quad + (93:1) - (94:1),\\
g_3 &= (78:1) - (92:1) + (93:1) - (94:1),\\
g_4 &= (79:1) + (87:1) - (88:1) + (91:1) - (92:1)\\
&\quad + (93:1) - (94:1),\\
g_5 &= (83:1) - (90:1),\\
g_6 &= (89:1) - (91:1),\\
g_7 &= (95:1).
\end{aligned}$$

Calculating the characteristic polynomial of T_2 using the basis $\{g_1, g_2, \cdots, g_7\}$, and factor it over $\boldsymbol{Q}$, we get

$$(-1 + 3x + 4x^2 + x^3)(-1 + 6x - x^2 - 3x^3 + x^4). \tag{4}$$

This leads to the guess that $J_0(97)$ is isogenous to the product of 3-dimensional simple abelian variety A_3 and 4-dimensional simple abelian variety A_4.

Let K_3 be the $\boldsymbol{T}$-submodule of $H^+(97)$ corresponding to A_3. K_3 is spanned by eigenvectors of the irreducible factor $-1+3x+4x^2+x^3$ of Equation (4). Using this, we can find a basis $\{f_1, f_2, f_3\}$ of K_3 over $\boldsymbol{Q}$;

$$\begin{aligned}
f_1 &= 8\cdot(44:1) + 30\cdot(70:1) - 16\cdot(78:1) + 2\cdot(79:1)\\
&\quad + 20\cdot(83:1) + 32\cdot(87:1) - 40\cdot(88:1) + 35\cdot(89:1)\\
&\quad - 20\cdot(90:1) + 5\cdot(91:1) - 16\cdot(92:1) + 16\cdot(93:1)\\
&\quad - 16\cdot(94:1) + 39\cdot(95:1),\\
f_2 &= -6\cdot(44:1) - 68\cdot(70:1) + 12\cdot(78:1) + 44\cdot(79:1)\\
&\quad - 15\cdot(83:1) - 24\cdot(87:1) + 30\cdot(88:1) - 49\cdot(89:1)\\
&\quad + 15\cdot(90:1) + 19\cdot(91:1) + 12\cdot(92:1) - 12\cdot(93:1)\\
&\quad + 12\cdot(94:1) - 52\cdot(95:1),\\
f_3 &= 50\cdot(44:1) + 142\cdot(70:1) - 9\cdot(78:1) - 124\cdot(79:1)\\
&\quad + 34\cdot(83:1) + 18\cdot(87:1) - 68\cdot(88:1) + 105\cdot(89:1)\\
&\quad - 34\cdot(90:1) - 37\cdot(91:1) - 9\cdot(92:1) + 9\cdot(93:1)\\
&\quad - 9\cdot(94:1) + 130\cdot(95:1).
\end{aligned}$$

If A_3 happens to be a Jacobian variety J_C of some curve C, the basis $\{f_1, f_2, f_3\}$ should give a basis of regular differential forms on the curve C. It turns out

that this is indeed the case.

For $p = 16529$, T_p is represented by the matrix

$$\begin{pmatrix} -36 & 68 & -1 & 67/2 & -55 & 53/2 & 34 \\ 138 & 120 & 29 & 9 & 3 & 20 & -50 \\ -136 & -305 & -185 & -321 & -85 & -322 & -162 \\ 0 & 0 & 0 & 114 & 0 & 17 & 53 \\ -110 & 85 & 82 & 93 & 145 & 95 & 34 \\ 0 & 0 & 0 & 19 & 0 & 171 & -17 \\ 0 & 0 & 0 & 17 & 0 & -2 & 167 \end{pmatrix}$$

with respect to the basis $\{g_1, g_2, \cdots, g_7\}$.

Using the Eichler-Shimura relation, one computes from this the characteristic polynomial f_0 of Frobenius σ_p at p (on l^n torsion for a prime l distinct from p, or on a Tate module of A_3):

$$\begin{aligned} f_0 \;=\; & (x^6 - 452x^5 + 115418x^4 - 17978899x^3 + 1907744122x^2 \\ & - 123489944132x + 4515852403889) \cdot (x^8 - 44x^7 \\ & + 31601x^6 - 1865601x^5 + 749060774x^4 - 30836518929x^3 \\ & + 8633640983441x^2 - 198697505771116x \\ & + 74642524383881281) \end{aligned}$$

So, the characteristic polynomial f of σ_p over K_3 is the irreducible factor of f_0 of sixth degree:

$$\begin{aligned} f \;=\; & x^6 - 452x^5 + 115418x^4 - 17978899x^3 \\ & + 1907744122x^2 - 123489944132x + 4515852403889. \end{aligned}$$

The number h_0 of points of A_3 over $\boldsymbol{F}_p$ is obtained by substituting $x = 1$ for f:

$$h_0 = f(1) = 4394252339947.$$

Since the characteristic polynomial of the fifth power of Frobenius is also easily calculated from T_p, the number h of points over a degree five extension $\boldsymbol{F}_{p^5}$ is obtained similarly:

$$\begin{aligned} h \;=\; & 4394252339947 \times \\ & 427379515481622744216694600721926448140291414819361. \end{aligned}$$

It is immediately verified that $q = p^5$ and h in the above satisfies the security conditions 1,2,3, and 4.

3.2 Defining equation of a simple factor of a modular curve

Using the method of [7], [14], we determine whether or not a given simple factor of $J_0(N)$ is a Jacobian J_C of some algebraic curve, and if it is, we find a defining equation of the corresponding curve C.

First, we give Shimura and Galbraith's result for hyperelliptic modular curves.

Algorithm 1 ([7], [14])**:**
Input: a basis $\{f_1(z), f_2(z), \ldots, f_g(z)\}$ for $S_2(N)$ of a hyperelliptic level N, Output: a defining polynomial $y^2 - x^{2g+2} - a_1x^{2g+1} - \cdots - a_{2g+2}$.

1. Calculate a Fourier expansion of every cusp form $f_i(z)$, and normalize them into the following form;
$$\begin{aligned} f_1(z) &= q^g + s_{1,g+1}q^{g+1} + \cdots + s_{1,g+i}q^{g+i} + \cdots \\ f_2(z) &= q^{g-1} + s_{2,g}q^g + \cdots + s_{2,g+i}q^{g+i} + \cdots \\ &\cdots \\ f_g(z) &= q + s_{g,2}q^2 + \cdots + s_{g,g+i}q^{g+i} + \cdots. \end{aligned} \quad (5)$$
We only need Fourier coefficients of at most $(3g + 3)$-th degree.
2. $$x \leftarrow \frac{f_2}{f_1}, \quad y \leftarrow \frac{q}{f_1}\frac{dx}{dq}$$
3. Calculate coefficients $a_1, a_2, \cdots$ recursively as follows;
$$\begin{aligned} y^2 - x^{2g+2} &= a_1q^{-2g-1} + \cdots \\ y^2 - x^{2g+2} - a_1x^{2g+1} &= a_2q^{-2g} + \cdots \\ &\cdots. \end{aligned}$$

The principle of Algorithm 1 is as follows. As one can see, for example, in tables in [14], when a modular curve $X_0(N)$ is hyperelliptic, the cusp $\infty i \in \boldsymbol{H}$ is not a Weierstrass point. So, $X_0(N)$ has an affine model with the cusp ∞i as one of the two points at infinity:

$$y^2 = x^{2g+2} + a_1x^{2g+1} + \cdots + a_{2g+2}.$$

Let α be one of the roots of the right-hand side, then a basis of regular differential forms on $X_0(N)$ is given by

$$\{\frac{dx}{y}, \frac{(x-\alpha)dx}{y}, \cdots, \frac{(x-\alpha)^{g-1}dx}{y}\}.$$

On the other hand, a basis of regular differential forms on $X_0(N)$ is also given by

$$\{f_1dz, f_2dz, \ldots, f_gdz\}.$$

Therefore, we can suppose

$$x = \frac{f_2}{f_1}, \quad y = \frac{q}{f_1}\frac{dx}{dq}.$$

For a hyperelliptic curve C obtained as a factor of a modular curve, the cusp $\infty i \in \boldsymbol{H}$ may be its Weierstrass point. (For example, the hyperelliptic curve of genus 2 obtained as a factor of $X_0(68)$.) But, also in this case, C has an affine model with the cusp ∞i as a unique point at infinity:

$$y^2 = x^{2g+1} + a_1x^{2g} + \cdots + a_{2g+1}.$$

Putting one of the roots of the right-hand side as α, a basis of regular differential forms on C is given by

$$\{\frac{dx}{y}, \frac{(x-\alpha)dx}{y}, \cdots, \frac{(x-\alpha)^{g-1}dx}{y}\}.$$

On the other hand, regular differential forms is also spanned by

$$\{f_1 dz, f_2 dz, \ldots, f_g dz\},$$

where $\{f_1, \cdots, f_g\}$ is a basis of $\boldsymbol{T}$-submodule of $S_2(N)$ corresponding to C. Therefore, normalizing $\{f_1, \cdots, f_g\}$ as

$$\begin{aligned} f_1(z) &= q^{2g-1} + s_{1,g+1} q^{2g} + \cdots \\ f_2(z) &= q^{2g-3} + s_{2,g} q^{2g-2} + \cdots \\ &\cdots \\ f_g(z) &= q + s_{g,2} q^2 + \cdots, \end{aligned}$$

we can also suppose

$$x = \frac{f_2}{f_1}, \quad y = \frac{q}{f_1}\frac{dx}{dq}.$$

Note that when the cusp ∞i is a Weierstrass point, x has a pole of order two at a unique point at infinity, which corresponds to the cusp ∞i. So, q-expansion of x begins at q^{-2}. This is the reason why q-expansion of f_{i+1} begins at two lower degree than that of f_i.

Thus, we get

Algorithm 2 (with cusp ∞i as a Weierstrass point)**:** Input: a basis $\{f_1(z), f_2(z), \ldots, f_g(z)\}$ of a $\boldsymbol{T}$-submodule of $S_2(N)$, Output: a defining polynomial $y^2 - 4x^{2g+1} - a_1 x^{2g} - \cdots - a_{2g+1}$.

1. Calculate a Fourier expansion of every cusp form $f_i(z)$, and normalize them into the following form;

$$\begin{aligned} f_1(z) &= q^{2g-1} + s_{1,g+1} q^{2g} + \cdots \\ f_2(z) &= q^{2g-3} + s_{2,g} q^{2g-2} + \cdots \\ &\cdots \\ f_g(z) &= q + s_{g,2} q^2 + \cdots. \end{aligned}$$

2. $$x \leftarrow \frac{f_2}{f_1}, \quad y \leftarrow \frac{q}{f_1}\frac{dx}{dq}$$

3. Calculate coefficients $a_1, a_2, \cdots$ recursively as follows:

$$\begin{aligned} y^2 - 4x^{2g+1} &= a_1 q^{-4g} + \cdots \\ y^2 - 4x^{2g+1} - a_1 x^{2g} &= a_2 q^{-4g+2} + \cdots \\ &\cdots. \end{aligned}$$

In general, for an algebraic curve C which is not hyperelliptic, letting a basis of space of regular differential forms $H^0(\Omega^1_C)$ be $\{\omega_1, \cdots, \omega_g\}$, the map

$$\begin{aligned} \Phi : C &\longrightarrow \boldsymbol{P}^{g-1} \\ P &\mapsto \left(1 : \frac{\omega_2}{\omega_1}(P) : \cdots : \frac{\omega_g}{\omega_1}(P)\right) \end{aligned}$$

is an embedding morphism, and its image $\mathrm{Im}(\Phi)$ is a nonsingular algebraic curve in $\boldsymbol{P}^{g-1}$, called a "canonical curve" of C.

In the case of modular curve or its factor, its canonical curve is just an algebraic curve in $\boldsymbol{P}^{g-1}$ defined by the relations among $\{f_1, \cdots, f_g\}$ which is a basis of the corresponding $\boldsymbol{T}$-submodule of $S_2(N)$.

A canonical curve of genus three is a plane quartic curve. As pointed out in [7], [14], the following Theorem 4 is useful for a canonical curve of genus four or more.

Theorem 4 (Petri's Theorem [1])**:** Let C be a canonical curve of genus four or more. Then C is an intersection of some quadratic hypersurfaces, or an intersection of some quadratic and cubic hypersurfaces.

By Theorem 4, for a curve C obtained as a factor of a modular curve, we only need to find quadratic or cubic relations among $f_1, \cdots, f_g$ in order to obtain a canonical curve of C. Shimura estimates the number of relations as in Table 1 [14].

Table 1 Number of equations for canonical curves

genus	equations
3	one quartic relation
4	one quadratic and one cubic relations
...	...

Each explicit relation is obtained easily using the Fourier expansions of a basis $\{f_1(z), f_2(z), \ldots, f_g(z)\}$.

Take an abelian variety A obtained as a simple factor of $J_0(N)$. Let K be a $\boldsymbol{T}$-submodule of $S_2(N)$ corresponding to A, and $\{f_1, \ldots, f_g\}$ be its basis over $\boldsymbol{Q}$.

Now, we can heuristically determine whether A is a Jacobian J_C of some algebraic curve or not, and if it is, we can find a defining equation of the corresponding curve C, as follows:

Algorithm 3: Input: a basis $\{f_1, \ldots, f_g\}$ of a $\boldsymbol{T}$-submodule of $S_2(N)$ over $\boldsymbol{Q}$ corresponding to a simple factor A of $J_0(N)$, Output: 'null' or a defining polynomial F of an algebraic curve C with Jacobian $J_C \cong A$.

1. Calculate a Fourier expansion of every cusp form $f_i(z)$, and determine the cusp ∞i is a Weierstrass point or not. That the cusp ∞i is not a Weierstrass point is equivalent to the fact that $\{f_1, \ldots, f_g\}$ are expanded just as in Equation (5) in Algorithm 1.

2. Assume A is a Jacobian of some hyperelliptic curve. Calculate a defining polynomial $F(x, y)$ of the hyperelliptic curve, using Algorithm 1 when the cusp ∞i is not a Weierstrass point, or Algorithm 2 when the cusp ∞i is a Weierstrass point.

3. Check the validity of the polynomial $F(x, y)$. That is, substitute $x = \frac{f_2}{f_1}$, and $y = \frac{q}{f_1}\frac{dx}{dq}$ for $F(x, y)$, and see whether the resulting Fourier coefficients vanish, more precisely check whether the coefficients of $q^{-4g-2}, q^{-4g-1}, \ldots, q^{-1}, 1, q$ vanish. If it is, output $F(x, y)$ and terminate.

4. Assume C is a Jacobian of some non-hyperelliptic curve C, and calculate the canonical curve of C.

That is, find all the quadratic or cubic relations F among $\{f_1, \dots, f_g\}$. And see whether the curve defined by F is nonsingular. If it is, output F and terminate. Else A is supposed to be not a Jacobian variety, and output 'null'.

Algorithm 3 is just a heuristic one. It is not proved that the output of Algorithm 3 defines an algebraic curve with Jacobian A, or Algorithm 3 may reject an A which is in fact a Jacobian. However, remember that our aim is to construct secure C_{ab} curves. We see later that there are many cases in which the output of Algorithm 3 is useful to give a secure C_{ab} curve.

3.2.1 Example: level 97

In section 3.1.1, we guessed that Jacobian $J_0(97)$ has a three-dimensional simple factor A_3. Also, we obtained the basis $\{f_1, f_2, f_3\}$ of the corresponding $\boldsymbol{T}$-submodule K_3 of $S_2(N)$. Here, we perform Algorithm 3 with the basis $\{f_1, f_2, f_3\}$ as an input.

1. Calculating and normalizing Fourier expansions of $\{f_1, f_2, f_3\}$, we get

$$\begin{aligned} f_1 &= q^3 - q^4 - 2q^5 - q^6 + q^7 + 4q^8 - 2q^9 + 3q^{10} + q^{12} \\ &\quad - q^{14} - 7q^{16} - q^{17} + q^{18} + \cdots \\ f_2 &= q^2 - 3q^4 - q^5 - 2q^6 + 5q^8 + q^9 + 2q^{10} + q^{11} + 5q^{12} \\ &\quad - q^{13} - 3q^{14} - 8q^{16} + q^{17} + \cdots \\ f_3 &= q - 4q^4 - 5q^5 - 3q^6 - q^7 + 9q^8 - q^9 + 8q^{10} - q^{11} \\ &\quad + 7q^{12} - 2q^{13} - 3q^{14} - q^{15} - \cdots. \end{aligned}$$

   Coefficients are calculated up to 80-th degree. From this, we know the cusp ∞i is not a Weierstrass point.

2. Assuming A_3 is a Jacobian of some hyperelliptic curve, we calculate a defining equation of the hyperelliptic curve, using Algorithm 1.

   a. Fourier expansions of $\{f_1, f_2, f_3\}$ was already computed at 1°.

   b. We obtain

$$\begin{aligned} x &= \frac{f_2}{f_1} = 1 + q^{-1} + 2q^2 - q^4 + 4q^5 - 2q^7 \\ &\quad + 7q^8 + q^9 - 5q^{10} + 13q^{11} - 9q^{13} + \cdots \\ y &= \frac{q}{f_1}\frac{dx}{dq} = -8 - q^{-4} - q^{-3} - 3q^{-2} - 2q^{-1} \\ &\quad - 14q - 7q^2 - 28q^3 - 57q^4 - \cdots. \end{aligned} \tag{6}$$

   Actually, coefficients are calculated up to 75-th degree.

   c. We obtain the defining polynomial

$$\begin{aligned} &-23 + 182x - 241x^2 + 210x^3 - 136x^4 \\ &+ 62x^5 - 21x^6 + 6x^7 - x^8 + y^2. \end{aligned} \tag{7}$$

3. Substituting Equation (6) for Polynomial (7), we encounter

$$70q + 14q^2 - 300q^3 + 398q^4 + 174q^5 + \cdots.$$

   As coefficients does not vanish, we determine A_3 is not a Jacobian of any hyperelliptic curve.

4. Assuming A_3 is a Jacobian of some non-hyperelliptic curve C, we calculate the canonical curve of C. As the genus of C is three, the defining polynomial is a single quartic equation F among $Z = f_1, Y = f_2, X = f_3$. Using the above Fourier expansion of X, Y, Z, we obtain the unique relation

$$\begin{aligned} F = &-2X^4 - X^3Y - 3X^2Y^2 + 6X^3Z \\ &+ 3X^2YZ + XY^2Z + Y^3Z - 5X^2Z^2 \\ &- Y^2Z^2 + XZ^3. \end{aligned}$$

   As $F = 0$ defines a nonsingular curve, we determine the simple factor A_3 is a Jacobian of the curve $F = 0$.

3.3 C_{ab} model of a simple factor of a modular curve

In the last section, we got an explicit defining equation of a simple factor of a modular curve. Here we translate it into a C_{ab} curve.

In the hyperelliptic case, we obtain the equation of the form

$$y^2 = x^{2g+2} + a_1 x^{2g+1} + \cdots + a_{2g+2},$$

besides C_{ab} curve of type $\{2, 2g+1\}$. Factoring the right-hand side, we get

$$y^2 = (x + \lambda_1)(x + \lambda_2) \cdots (x + \lambda_{2g+2}),$$

and dividing two sides by $(x + \lambda_1)^{2g+2}$, we get

$$\frac{y^2}{(x + \lambda_1)^{2g+2}} = 1 \cdot \prod_{i=2}^{2g+2} (1 + \frac{\lambda_i - \lambda_1}{x + \lambda_1}).$$

So, putting

$$X = \frac{1}{x + \lambda_1}, Y = \frac{y}{(x + \lambda_1)^{g+1}},$$

we get

$$Y^2 = \prod_{i=2}^{2g+2} (1 + (\lambda_i - \lambda_1)X)$$

This is a C_{ab} curve of type $\{2, 2g+1\}$.

We now consider the non-hyperelliptic case. For a non-hyperelliptic simple factor, we obtained its canonical curve C. By Theorem 2, in order to translate C

into a C_{ab} curve, we only need to find the generator $A = \langle a_1, a_2, \cdots, a_t \rangle$ of the monoid M_Q and to find the function $f_i \in L(\infty Q)$ $(i = 1, 2, \cdots, t)$ with pole order a_i at Q , for some rational point Q on C. Therefore, all we have to do is to find a basis $L(mQ)$ for some rational point Q on C $(3 \leqq m \leqq a_t)$.

As the canonical curve C is nonsingular, it is not difficult to find a basis of $L(D)$ for any divisor D [9]:

Proposition 5: Let $D = \sum n_i P_i - \sum m_j Q_j$ be a divisor on a nonsingular affine curve C with non-negative integers n_i, m_j. Let $I_1 = \cap I_{P_i}^{n_i}, I_2 = \cap I_{Q_j}^{m_j}$, where I_P denotes the maximum ideal of the coordinate ring R of C, corresponding to a point P. Fix any nonzero element f belonging to I_1. Then, we have

$$L(D) = \{\frac{g}{f} \mid g \in fI_2 : I_1\}.$$

Proof: Although the proposition is a well known fact, we could not find the written proof. So, we show a proof for convenience to readers.

As C is nonsingular, R is a normal ring. So, any element in $L(D)$ can be written as $\frac{g}{f}$ for some $g \in R$. Then,

$$\begin{aligned} & \frac{g}{f} \in L(D) \\ \Leftrightarrow\ & \frac{g}{f} I_1 \subset I_2 \\ \Leftrightarrow\ & g \in fI_2 : I_1 \quad \square \end{aligned}$$

The number of equations for a C_{ab} curve becomes the smallest when we take a Weierstrass point as the base point. So, it is desirable to choose a Weierstrass point as the point Q in the above. When the genus is three, Weierstrass points of a canonical curve are easily found.

Let C be a canonical curve of genus three. Let K be a canonical series of C. As $\dim(K) = 2$, that a point Q is a Weierstrass point is equivalent to the fact that the tangent line at the point Q meets the curve C with the multiplicity three or more. So, a Weierstrass point Q is obtained as a common zero of

$$\begin{aligned} f(x, y) &= 0 \\ D_{a,b} f(x, y) &= 0 \\ D_{a,b}^{(2)} f(x, y) &= 0, \end{aligned}$$

where

$$D_{a,b} f(x, y) = a\partial f/\partial x + b\partial f/\partial y,$$

and $D_{a,b}^{(2)}(f) = D_{a,b}(D_{a,b}(f))$.

3.3.1 Example: level 97

We saw that the Jacobian $J_0(97)$ of the modular curve $X_0(97)$ has a simple factor A_3 of dimension three, and guessed that A_3 is a Jacobian of an algebraic curve C(ref. section 3.2.1). The equation of the canonical curve of C was given by

$$\begin{aligned} f \ =\ & -2x^4 - x^3y - 3x^2y^2 + 6x^3 + 3x^2y + xy^2 + y^3 \\ & -5x^2 - y^2 + x. \end{aligned}$$

Take the prime $p = 16529$ as in 3.1.1. As equations $f(x, y)$, $D_{a,b} f(x, y)$, and $D_{a,b}^{(2)} f(x, y)$ over $\boldsymbol{F}_p$ has a common zero

$$a = 12900, x = 13695, y = 14705,$$

$Q = (13695, 14705)$ is a Weierstrass point of C over $\boldsymbol{F}_p$.

Calculating $l(m) = \dim L(mQ)$ $(m = 3, 4, 5, 6, 7)$ by Prop. 5, we have

$$l(3) = 2,\ l(4) = 2,\ l(5) = 3,\ l(6) = 4,\ l(7) = 5.$$

So, gap sequences at the point Q is 1,2,4, and we know

$$M_Q = \langle 3, 5, 7 \rangle.$$

The curve C is a $C_{3,5,7}$ curve.

The function $X \in L(3Q)$ with $v_Q(X) = -3$, the function $Y \in L(4Q)$ with $v_Q(Y) = -4$, and the function $Z \in L(5Q)$ with $v_Q(Z) = -5$ are given by

$$\begin{aligned} X \ =\ & (12855 + 11167x + 5996x^2 + x^3 + 9720y + 10529xy + 4636x^2y \\ & + 10496y^2 + 10744xy^2)/(13280 + 13941y + 5472y^2 + y^3) \\ Y \ =\ & (8608 + 6182x + 8423x^2 + 15577x^3 + 13719y + 7604xy \\ & + 424x^2y + 8263x^3y + 7442y^2 + 9157xy^2 + 7894x^2y^2 \\ & + 4131x^3y^2 + 14194y^3 + 12726xy^3 + 9702x^2y^3 + 15348y^4 + \\ & 5202xy^4)/(9403 + 5617y + 568y^2 + 13412y^3 + 9120y^4 + y^5) \\ Z \ =\ & (10644 + 13291x + 7571x^2 + 8617x^3 + 2836y + 15714xy \\ & + 1350x^2y + x^3y + 667y^2 + 3987xy^2 + 11840x^2y^2 \\ & + 2036x^3y^2 + 1947y^3 + 1150xy^3 + 12002x^2y^3 + 6207x^3y^3 \\ & + 15337y^4 + 7047xy^4 + 8184x^2y^4 + 13431x^3y^4 + 8564y^5 \\ & + 5258xy^5 + 14541x^2y^5 + 9149y^6 + 7639xy^6)/(9594 \\ & + 7377y + 15644y^2 + 6261y^3 + 1988y^4 + 14942y^5 \\ & + 12768y^6 + y^7). \end{aligned} \tag{8}$$

A general form of defining equations of $C_{3,5,7}$ curve is given by Equation (2). In this case, we have

$$\begin{aligned} 0 \ =\ & 11654X + 6133X^2 + 10293X^3 + 3017Y + 463XY \\ & + Y^2 + 7669Z + 15127XZ \\ 0 \ =\ & 15687X + 8029X^2 + 10416X^3 + 9882X^4 + 14252Y \\ & + 6982XY + 9150X^2Y + 4600Z + 6150XZ + YZ \\ 0 \ =\ & 1362X + 11237X^2 + 3867X^3 + 95X^4 + 8346Y \\ & + 9761XY + 10084X^2Y + 5949X^3Y + 1677Z \\ & + 7169XZ + 831X^2Z + Z^2. \end{aligned}$$

By the result of section 3.1.1, we guess that the above $C_{3,5,7}$ curve has a Jacobian of the order

$$\begin{aligned} h \ =\ & 4394252339947 \times \\ & 427379515481622744216694600721926448140291414819361 \end{aligned}$$

over the finite field $\boldsymbol{F}_{p^5}$ for $p = 16529$. In fact, it is verified using the addition algorithm in [2] that h times a random rational point of the curve over $\boldsymbol{F}_{p^5}$ is equal to the unit element of the Jacobian, but any proper factor of h doesn't have a such property.

3.4 Numerical examples

We computed modular algebraic curves of genus two or three obtained as simple factors of modular curves $X_0(N)$ for N up to 109, using Algorithm 3. Table 2 shows the result.

Table 2 modular algebraic curves of genus 2 or 3

level	genus	defining polynomial
23	2	$7-10X+11X^2-2X^3-2X^4+8X^5-X^6+Y^2$
29	2	$7-8X-8X^2-2X^3+12X^4+4X^5-X^6+Y^2$
31	2	$3+14X+11X^2-18X^3-6X^4+8X^5-X^6+Y^2$
35	2	$76+64X+27X^2+32X^3-2X^4+4X^5-X^6+Y^2$
39	2	$-9+48X-64X^2+6X^3+20X^4-X^6+Y^2$
41	3	$4-16X+27X^2+8X^3-60X^4+82X^5-48X^6+12X^7-X^8+Y^2$
63	2	$27+26X^3-X^6+Y^2$
67	2	$-9+14X-9X^2+6X^3-6X^4+4X^5-X^6+Y^2$
68	2	$64X+112X^2+108X^3+24X^4-4X^5+Y^2$
73	2	$-1-10X+15X^2-2X^3-6X^4+4X^5-X^6+Y^2$
81	2	$27+18X^3-X^6+Y^2$
85	2	$-25+40X-32X^2+22X^3-12X^4+4X^5-X^6+Y^2$
87	2	$3+6X+11X^2+6X^3+2X^4-X^6+Y^2$
88	2	$28-4X+56X^2+104X^3+12X^4-4X^5+Y^2$
93	2	$-9+18X-5X^2-14X^3+10X^4-X^6+Y^2$
95	3	$-5+10X-19X^2-4X^3+27X^4-12X^5-7X^6+6X^7-X^8+Y^2$
97	3	$-2X^4-X^3Y-3X^2Y^2+6X^3Z+3X^2YZ+XY^2Z+Y^3Z-5X^2Z^2-Y^2Z^2+XZ^3$
103	2	$-1-6X+19X^2-22X^3+10X^4-X^6+Y^2$
104	2	$-48-64X+20X^2+84X^3+12X^4-4X^5+Y^2$
107	2	$-1+10X-17X^2+18X^3-10X^4+4X^5-X^6+Y^2$
109	3	$5X^3Y-10X^2Y^2+6XY^3-Y^4-3X^3Z+6X^2YZ-6XY^2Z+Y^3Z+X^2Z^2+2XYZ^2-XZ^3$

Using curves in Table 2, we construct secure C_{ab} curves. In the below, h denotes the order of the Jacobian of the secure C_{ab} curve $f=0$ over the extension field $\boldsymbol{F}_{p^m}$, and is shown in the form of factored integer.

N	23
p	16567
m	7
h	$2^4 \cdot 5 \cdot 11^2 \cdot 29 \cdot 59 \cdot 479 \cdot 1478949453271396634623564653053032399567134121166 9$
f	$16566+15542X+13715X^2+4742X^3+14710X^4+12816X^5+Y^2$

N	29
p	16871
m	7
h	$2^4 \cdot 3^2 \cdot 7^4 \cdot 41 \cdot 977 \cdot 109279445667315168277598629101367041591695540549 29$
f	$16870+7012X+11557X^2+2335X^3+1941X^4+245X^5+Y^2$

N	31
p	17011
m	7
h	$2^2 \cdot 5^2 \cdot 2946341 \cdot 576679900472116403581455711323281551165118232514241$
f	$17010+16566X+6818X^2+3587X^3+5840X^4+9875X^5+Y^2$

N	35
p	16607
m	7
h	$2^6 \cdot 5^2 \cdot 13 \cdot 17 \cdot 43 \cdot 769 \cdot 10379335436561642005421252250170857467716516066227$
f	$16606+10X+16570X^2+100X^3+16471X^4+140X^5+Y^2$

N	39
p	16447
m	7
h	$2^3 \cdot 7^2 \cdot 1871 \cdot 2593 \cdot 55725159807738715149597805100129070377980044358567$
f	$16446+18X+16332X^2+306X^3+16194X^4+16339X^5+Y^2$

N	41
p	16831
m	5
h	$2^4 \cdot 5^4 \cdot 13 \cdot 921142907 \cdot 205768283732802473628126035036899477798787041780 21$
f	$16830+14511X+1555X^2+10454X^3+3718X^4+14734X^5+7923X^6+6221X^7+Y^2$

N	63
p	16451
m	7
h	$2^2 \cdot 3^3 \cdot 829 \cdot 3023 \cdot 392894364814918539379824982487271001442574571988761$
f	$16450+6X+16436X^2+46X^3+16358X^4+84X^5+Y^2$

N	67
p	16433
m	7
h	$2^4 \cdot 5 \cdot 109 \cdot 211 \cdot 30881 \cdot 184308632947437014931259832405196945480967036065 1$
f	$16432 + 9210X + 14964X^2 + 6934X^3 + 2579X^4 + 11767X^5 + Y^2$

N	68
p	16417
m	7
h	$2^4 \cdot 3 \cdot 5572907 \cdot 38618032310739276166039212739670075477292706756396 9$
f	$64X + 112X^2 + 108X^3 + 24X^4 - 4X^5 + Y^2$

N	73
p	16979
m	7
h	$2^4 \cdot 5 \cdot 19 \cdot 29 \cdot 89 \cdot 2131 \cdot 19794952976921028986123564187282451849038043880381$
f	$16978 + 10354X + 2868X^2 + 14127X^3 + 1387X^4 + 2370X^5 + Y^2$

N	81
p	16871
m	7
h	$2^7 \cdot 3 \cdot 741253 \cdot 53170882372404906234124314758320619539509653043648 1$
f	$16870 + 14967X + 13507X^2 + 3209X^3 + 528X^4 + 2754X^5 + Y^2$

N	85
p	16529
m	7
h	$2^3 \cdot 3^2 \cdot 7^4 \cdot 17 \cdot 4519 \cdot 85553187744765518983331106305233864287969606019 69$
f	$16528 + 4409X + 11901X^2 + 14694X^3 + 6566X^4 + 3680X^5 + Y^2$

N	87
p	16421
m	7
h	$2^2 \cdot 5 \cdot 11 \cdot 1219489 \cdot 38636150333000870275487822681787320934488039528601$
f	$16420+9194X+7839X^2+957X^3+2017X^4+10708X^5+Y^2$

N	88
p	16729
m	7
h	$2^6 \cdot 3^2 \cdot 19 \cdot 281 \cdot 25601 \cdot 17078133431474158263353194426598619893033324165 21$
f	$28-4X+56X^2+104X^3+12X^4-4X^5+Y^2$

N	93
p	16433
m	7
h	$2^2 \cdot 5 \cdot 29 \cdot 13317071 \cdot 13558113484642137701074437643375140664178224756229$
f	$16432 + 8977X + 12711X^2 + 1170X^3 + 7043X^4 + 7680X^5 + Y^2$

N	95
p	16879
m	5
h	$2^8 \cdot 5^2 \cdot 311 \cdot 11972309 \cdot 10791514968310675958367014873329114490915564480236 1$
f	$16878 + 6199X + 4692X^2 + 12173X^3 + 15252X^4 + 2933X^5 + 231X^6 + 11611X^7 + Y^2$

N	97
p	16529
m	5
h	$4394252339947 \cdot 42737951548162274421669460072192644814029141481936 1$
f	$11654X + 6133X^2 + 10293X^3 + 3017Y + 463XY + Y^2 + 7669Z + 15127XZ$, $15687X + 8029X^2 + 10416X^3 + 9882X^4 + 14252Y + 6982XY + 9150X^2Y + 4600Z + 6150XZ + YZ$, $1362X+11237X^2+3867X^3+95X^4+8346Y+9761XY+10084X^2Y+5949X^3Y+1677Z+7169XZ+831X^2Z+Z^2$

N	103
p	16519
m	7
h	$2^4 \cdot 5^2 \cdot 11 \cdot 29 \cdot 109 \cdot 569 \cdot 14235840246803888917775510659947714351866859614261$
f	$16518 + 9756X + 3989X^2 + 13979X^3 + 14949X^4 + 3150X^5 + Y^2$

N	104
p	16453
m	7
h	$2^4 \cdot 16788437 \cdot 396552890596328576150858894149680432844146536258509$
f	$16449X + 72X^2 + 16033X^3 + 992X^4 + 15621X^5 + Y^2$

N	107
p	16427
m	7
h	$19 \cdot 31 \cdot 71 \cdot 445541 \cdot 559183413901156790993361525407279304757313746721$
f	$16426 + 10810X + 16010X^2 + 10222X^3 + 5870X^4 + 6942X^5 + Y^2$

N	109
p	16691
m	5
h	$41 \cdot 116437 \cdot 955781 \cdot 476433290691397249169126591183003315415665729352671$
f	$4100 + 16591X + 13954X^2 + 12553X^3 + 3552Y + 8086XY + Y^2 + 4Z + 4XZ$, $8882+10969X+8344X^2+1170X^3+1388X^4+ 8148Y + 1039XY + 13453X^2Y + 583Z + 11930XZ + YZ$, $14826+1004X+11X^2+6341X^3+10099X^4+ 8635Y+5843XY+15154X^2Y+16344X^3Y+ 14580Z + 3575XZ + 4073X^2Z + Z^2$

References

[1] E.Arbarello, M.Cornalba, P.A.Griffiths, and J.Harris, "Geometry of Algebraic Curves Volume I," Springer-Verlag, 1984.

[2] S. Arita, "Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log-based public key cryptosystems," Conference on The Mathematics of Public Key Cryptography, Toronto, 1999.

[3] S. Arita, "Gaudry's variant against C_{ab} curve," LNCS 1751, Proceedings of PKC 2000, pp. 58-67

[4] J.E.Cremona, "Algorithms For Modular Elliptic Curves", Cambridge University Press, 1997.

[5] G.Frey and H.-G.Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", Mathematics of Computation, 62 (1994), 865-874.

[6] G.Frey and M. Müller, "Arithmetic of Modular Curves and Applications", preprint, 1998.

[7] S.D.Galbraith, "Equations For Modular Curves", Doctor thesis, University of Oxford, 1996.

[8] P.Gaudry, "A variant of the Adleman-DeMarris-Huang algorithm and its application to small genera," Conference on The Mathematics of Public Key Cryptography, Toronto, 1999.

[9] D.Grayson, M.Stillman, "Macaulay 2 – a system for computation in algebraic geometry and commutative algebra", http://math.uiuc.edu/Macaulay2.

[10] S. Miura, "Linear Codes on Affine Algebraic Curves", Trans. of IEICE, vol. J81-A, No. 10, 1398-1421, Oct. 1998.

[11] J.M.Pollard, "Monte Carlo methods for index computation mod p," Math. Comp.,32(143),pp.918-924,1978.

[12] G.Cornell, J.H.Silverman, G.Stevens (ed), "Modular Forms and Fermat's Last Theorem", Springer, 1997.

[13] H.-G.Rück, "On the discrete logarithm in the divisor class group of curves," Math. Comp.,68(226),pp.805-806,1999.

[14] M. Shimura, "Defining Equations of Modular Curves $X_0(N)$", Tokyo J. Math., Vol. 18, No. 2 (1995), pp.443-456.

[15] X.Wang, "2-dimensional simple factors of $J_0(N)$", Manuscripta Math. 87 (1995), pp. 179-197.

[16] H-J. Weber, "Hyperelliptic Simple Factors of $J_0(N)$ with Dimension at Least 3", Experimental Mathematics 6:4 (1997), pp. 273-287.

Seigo Arita Since 1990, he has been with Internet Systems Research Laboratories, NEC. He is a member of IEICE and JMS.