The Emergence of Picard Jacobians in Cryptography

Jorge Estrada-Sarlabous* Jean-Pierre Cherdieu†

Ernesto Reinaldo-Barreiro* Rolf-Peter Holzapfel‡

February 15, 2001

Abstract

In this paper we present a new family of Jacobian Varieties defined over finite fields that provides many elements whose group structure is suitable for cryptosystems based on the intractability of the discrete logarithm problem. Their security against several known attacks and the efficiency (and effectiveness) of the most important algorithms of the corresponding cryptosystems are discussed.

1 Introduction

Most of the cryptosystems based on the intractability of the discrete logarithm problem on the group structure of the Jacobian Varieties of curves defined over finite fields deal with elliptic or hyperelliptic jacobians (see [Ko1], [Ko2], [Ko3], [Fre2] and [DuuSak], for instance). In this paper we present a new family of Jacobian Varieties defined over finite fields that provides many members whose group structure is suitable for cryptosystems based on the discrete logarithm and show that they are a good source for public-key crytosystems.

*ICIMAF, La Habana, Cuba. E-mail: {matdis, ernesto}@cidet.icmf.inf.cu

†UAG, Pointe-a-Pitre, Guadeloupe. E-mail: Jean-Pierre.Cherdieu@univ-ag.fr

‡IRM, Humboldt Uni. zu Berlin, Germany. E-mail: holzapfl@mathematik.hu-berlin.de

[0] **AMS Subject Classification**: 14H45, 14H40, 14H05, 14K22, 14Q05, 14Q20, 11G10, 11T71.

Key Words: Picard Curves, Jacobian Varieties, Addition Law, Discrete Logarithm, Complex Multiplication.

We consider jacobians of curves defined by the equation

$$C_a : Y^3 W = X^4 + aXW^3 \tag{1}$$

with $a \in \mathbb{F}_p$, $a \neq 0$.

Crucial for our approach are the explicit addition law and algebraic structure , the fast addition algorithm for Picard Jacobians, as well as the explicit determination of the Hasse-Witt matrix of curves C_a and the isogeny types of their Jacobians (see [EstReiPi], [EstReiChe] and [Est1]).

Picard Curves are non hyperelliptic genus *three* plane projective curves which have been intensively studied due to their connection with certain Hilbert's problems (cf.[Ho3]). The authors thank heartly Florin Nicolae for his skillful comments and correcture of some places in the last part of this paper.

2 General Facts

Let $k = \mathbb{F}_q$, $q = p^m$ be finite field with $p > 3$ and let $\overline{k}$ denote its algebraic closure. Let C_{p_4} be the k-defined nonsingular genus three plane projective curve with affine model

$$C_{p_4} : y^3 = p_4(x) \tag{2}$$

where $p_4(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is a polynomial in $k[x]$ without multiple roots in $\overline{k}$. In [Est2] it is proved that there is no lost of generality if we suppose $a_3 = 0$. Let's denote by $K_{p_4} = k(x, y)$ the algebraic function field of one variable associated to C_{p_4}. We call C_{p_4} (resp. K_{p_4}) a Picard curve (resp. a Picard function field).

Let C/k and C_1/k be two k-defined plane projective curves. We will say that C/k and C_1/k are k-linearly isomorphic iff there exist $G \in Gl_3(k)$ satisfying $C_1 = G^*(C)$ where

$$G^*(C) = \{(X_1 : Y_1 : W_1)\,|C(X_1, Y_1, W_1) = 0, (X_1, Y_1, W_1) = G(X, Y, W)\}.$$

If $C/\mathbb{F}_q$ is a complete non-singular curve of genus g, one important tool for studying its Jacobian $J(C)$ is Weil's theorem:

Theorem 2.1 *There exist complex numbers $\alpha_1, \alpha_1, \ldots, \alpha_{2g}$ such that,*

$$N_r = \#C(\mathbb{F}_q) = q^r + 1 - \sum_{i=1}^{2g} {\alpha_i}^r \tag{3}$$

for $r > 0$, or equivalently, the power series

$$Z(t) = \exp(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}) \in \mathbb{C}[[t]]$$

represents a rational function, whith numerator

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$$

and denominator $(1-t)(1-qt)$. Moreover, $L(t)$ has integer coefficients and the complex numbers α_i have absolute value $q^{1/2}$.

$Z(t)$ and $L(t)$ are called the zeta function and the L-polynomial of $C/\mathbb{F}_q$, respectively. We have also

$$L(t) = t^g P_\pi(1/t)$$

where $P_\pi(\lambda)$ is the characteristic polynomial of the Frobenius endomorphism π of $J(C)$ relative to $\mathbb{F}_q$. Thus, the computation of $Z(t)$ reduces to the computation of $P_\pi(\lambda)$. It is also well known that the number of $\mathbb{F}_q$-rational points of $J(C)$ is equal to

$$\#J(C)(\mathbb{F}_q) = L(1) = P_\pi(1). \tag{4}$$

Remark 2.2 *For $C_{P_4}/\mathbb{F}_q$, let $P_\pi(p_4;\lambda) = \sum_{i=0}^{6} a_i \lambda^i$ be the charateristic polynomial of the Frobenius endomorphism π of $J(C_{p_4})$ relative to $\mathbb{F}_q$ and let's consider the quantities $\mu_r = N_r - (q^r + 1)$, $r = 1, 2, 3$, where the N_r are defined as in (3). Then, we have:*

1. *$a_6 = 1$ and $a_0 = q^3$*
2. *$a_5 = \mu_1$, $a_4 = \frac{1}{2}(\mu_2 + \mu_1^2)$ and $a_3 = \frac{1}{3}\mu_3 + \frac{1}{2}\mu_2\mu_1 + \frac{1}{6}\mu_1^3$.*
3. *$a_1 = q^2 a_5$ and $a_2 = q a_4$.*

Therefore, $P_\pi(p_4;\lambda)$ is completely determined by the numbers N_r.

3 The Hasse-Witt Matrix of C_{P_4}.

In this section, we will follow the notations and results exposed in [StoVol]. Let $\Omega(K_{p_4})$ be the space of differential forms of degree 1 on K_{p_4} and denote by $d : K_{p_4} \to \Omega(K_{p_4})$ the canonical derivation of K_{p_4}. Let $x \in K_{p_4} \setminus K_{p_4}^p$ be a separably generating element of K_{p_4}. Since $d(x) \neq 0$, any element $\omega \in \Omega(K_{p_4})$ can be uniquely expresed as

$$\omega = zdx = (z_0^p + z_1^p x + \ldots + z_{p-1}^p x_1^p)dx \tag{5}$$

whith $z_j \in K_{p_4}$.

Definition 3.1 *Let $\omega = zdx$ an element of $\Omega(K_{p_4})$, then with the notation of (5), the* modifed Cartier operator *is defined as*

$$C(zdx) = z_{p-1}dx$$

Let $D_0(K_{p_4})$ be the space of differentials of the first kind on K_{p_4}, it is a k-linear space of dimension $g = 3$ with canonical basis

$$\{\omega_1, \omega_2, \omega_3\} = \left\{ \frac{dx}{y^2}, \frac{xdx}{y^2}, \frac{dx}{y} \right\}.$$

$D_0(K_{p_4})$ is closed under the action of the modified Cartier operator C. Indeed, if we write $\omega = (\omega_1, \omega_2, \omega_3)$, then holds

$$C(\omega) = H_{p_4}^{(1/p)}\omega,$$

where we denote by $H_{p_4}^{(s)}$ the matrix obtained by rising each coefficient of H_{p_4} to the power s. H_{p_4} is called the Hasse-Witt matrix of C_{p_4} defined over k . Moreover, in [Est1] it is shown that:

1. if $p \equiv 1 \bmod 3$

$$H_{p_4} = \begin{pmatrix} c_{p-1,p-1} & c_{2p-1,p-1} & 0 \\ c_{p-2,p-1} & c_{2p-2,p-1} & 0 \\ 0 & 0 & c_{p-1,2p-2} \end{pmatrix} \tag{6}$$

2. if $p \equiv 2 \bmod 3$

$$H_{p_4} = \begin{pmatrix} 0 & 0 & c_{p-1,2p-1} \\ 0 & 0 & c_{p-2,2p-1} \\ c_{p-1,p-2} & c_{2p-1,p-2} & 0 \end{pmatrix} \tag{7}$$

where $c_{i,j}$ is equal to the coefficient of x^i in $p_4(x)^{q-1-\frac{j}{3}}$.
Let $P_\pi(p_4;\lambda)$ be the characteristic polynomial of the Frobenius endomorphism of $J(C_{p_4}/\mathbb{F}_q)$ relative to $\mathbb{F}_q$. Then $P_\pi(p_4;\lambda)$ is connected to the Hasse-Witt matrix H_{p_4} through Manin's congruence ([Man]):

$$P_\pi(p_4;\lambda) \equiv (-1)^g \lambda^g \left|H_\pi - \lambda I_g\right| \mod p \tag{8}$$

where $g = 3 =$ genus(C_{p_4}), $H_\pi = H_{p_4} \cdot H_{p_4}^{(p)} \ldots H_{p_4}^{(p^{m-1})}$ and $\pi\overline{\pi} = q = p^m$.

Definition 3.2 *We call the integer*

$$r_{p_4} = rank \left(H_{p_4} \cdot H_{p_4}^{(p)} \cdot H_{p_4}^{(p^2)} \right)$$

the Hasse-Witt invariant (or the p-rank) of the non-singular curve C_{p_4}.

After (4), if $P_\pi(p_4;\lambda)$ factorizes, then the number $P_\pi(p_4;1)$ factorizes too. Hence, if we wish to obtain secure cryptosystems, it is necessary to find Picard curves $C_{p_4}/\mathbb{F}_p$ with $\mathbb{Q}$-irreducible characteristic polynomial $P_\pi(p_4;\lambda)$.

For a general non-singular curve C, it is well known that $P_\pi(\lambda)$ completely determines the isogeny class of $J(C)$ (cf. [Tat]) and the formal and algebraic structure of $J(C)$ up to isogeny (cf. [Man]). For our family C_a we will consider the following case.

3.1 The case p-rank $= 0$

If p-rank$(J(C_{p_4})) = 0$, after [Yui2] there are only two possible isogeny types:

1. The formal group of type $G_{1,2} + G_{2,1}$, which is called *the symmetric formal group of dimension* 3.
2. The formal group of type $3G_{1,1}$, which is called *the supersingular formal group of dimension* 3

Let be v_p the p-adic valuation of $\mathbb{Q}_p$ and denote by ν_p the unique extension of the p-adic valuation v_p to the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, normalized so that $\nu_p(p) = 1$. In [Yui1] it is shown that p-rank $(J(C)) = 0$ iff $\nu_p(\mu_r) \geq 1$, $r = 1,2,3$. Moreover, $J(C)$ is supersingular iff p-rank$(J(C)) = 0$ and $\nu_p(\mu_3) > 1$. For genus three curves, the symmetric case is very attractive, since it is $\mathbb{F}_q$-simple (any abelian variety A with dimension 3 and p-rank equal to 0, which is the product of strictly lower dimensional abelian varieties may have only supersingular factors, hence A is also supersingular).

4 The Family $C_a : Y^3W = X^4 + aXW^3$

Lemma 4.1 *With the same notation of (6) and (7). The coefficients of the Hasse-Witt matrix $H_a = (c_{i,j})$ for the curve C_a are equal to*

1. *if $p \equiv 4 \bmod 9$: $c_{p-2,p-1} = \binom{\frac{2(p-1)}{3}}{\frac{(5p-2)}{9}} a^{\frac{(5p-2)}{9}}$ and $c_{i,j} = 0$ otherwise.*

2. *if $p \equiv 7 \bmod 9$: $c_{2p-1,p-1} = \binom{\frac{2(p-1)}{3}}{\frac{(2p-5)}{9}} a^{\frac{(2p-5)}{9}}$ and $c_{i,j} = 0$ otherwise.*

Proof. For the polynomial $p_4(x) = x^4 + ax$ it is strightforward to obtain an explicit formula to compute the coefficients of $p_4(x)^N$, $N > 1$. □

Theorem 4.2 *Let be $p \equiv 4, 7 \bmod 9$, $p > 37$. Then, for any curve C_a, $a \neq 0$, the Jacobian $J(C_a)$ is $\mathbb{F}_p$-simple and of symmetric type. Moreover, the polynomial $P_\pi(a; \lambda)$ belongs to the set $S(C_a; {\mu'}_2; {\mu'}_3; p)$ of polynomials*

$$P_\pi(\lambda; {\mu'}_2; {\mu'}_3) = \lambda^6 + {\mu'}_2 p\lambda^4 + {\mu'}_3 p\lambda^3 + {\mu'}_2 p^2\lambda^2 + p^3$$

where ${\mu'}_2 = -3, 0, 3$ and ${\mu'}_3$ is an integer satisfying $|{\mu'}_3| \leq 2\left[p^{\frac{1}{2}}\right] + 1$ and ${\mu'}_3 \equiv 1 \bmod 3$.

Proof. From (8), Lemma 4.1 and Remark 2.2, we obtain

$$\begin{aligned} \mu_1 &\equiv 0 \quad \bmod p \\ \mu_2 + \mu_1^2 &\equiv 0 \quad \bmod 2p \\ 2\mu_3 + 3\mu_2\mu_1 + \mu_1^3 &\equiv 0 \quad \bmod 6p. \end{aligned}$$

Recalling Serre-Weil's bound $|\mu_i| \leq \left[2g\sqrt{p^i}\right]$ we get:

1. $\mu_1 = 0$ for $p > 37$: it is trivial.

2. $\mu_2 = 2p{\mu'}_2$ with $|{\mu'}_2| \leq 3$. The curve C_a has 2 or 5 ramification points, depending on $a \in (\mathbb{F}_q^*)^3$ or not, respectively; and for each point $P_1 = (x_1 : y_1 : z_1) \in C_a$, the points $P_1 = (x_1 : \xi y_1 : z_1)$ and $P_1 = (x_1 : \xi^2 y_1 : z_1)$, ξ a cubic root of unity in $\mathbb{F}_q$, are also points of C_a. Since $p \equiv 1 \bmod 3$, then $q = p^2 \equiv 1 \bmod 3$ and therefore, $N_2 \equiv 2 \bmod 3$. Now, we have

$$2 \equiv N_2 = 2p{\mu'}_2 + p^2 + 1 \equiv 2{\mu'}_2 + 2 \bmod 3.$$

Previous equation holds only if ${\mu'}_2 = -3, 0, 3$.

3. $\mu_3 = 3p\mu'_3$ with $|\mu'_3| \leq 2\left[p^{\frac{1}{2}}\right] + 1$ and $\mu'_3 \equiv 1 \bmod 3$: note first that the cardinality of $J(C_a)$ is always divisible by 3, since the class $\overline{x}$ of $R_0 - P_\infty = (0:0:1) - (0:1:0)$ is a tree torsion of any Jacobian $J(C_a)$. Then, we have

$$\#J(C_a)(\mathbb{F}_p) = p^3 + \mu'_2(p+p^2) + \mu'_3 p + 1 \equiv 2 + \mu'_3 \equiv 0 \bmod 3,$$

whence $\mu'_3 \equiv 1 \bmod 3$.

$\mu'_3 \equiv 1 \bmod 3$ implies $\mu'_3 \neq 0$, and from the Serre-Weil bound, one gets $\nu_p(\mu_3) \leq 1$, then $J(C_a)$ must be symmetric and the corresponding polynomial $P_\pi(\lambda;\mu'_2;\mu'_3)$ is $\mathbb{Q}$-irreducible

4.1 Explicit determination of $P_\pi(a;\lambda)$

Given a fixed curve C_a and a prime $p > 3$, in the previous theorem we have determined the characteristic polynomial $P_\pi(a;\lambda)$ of the Frobenius endomorphism π of $J(C_a)$ up to some *free parameters* μ'_2, μ'_3. Since $P_\pi(a;1)$ gives the cardinality of $J(C_a)(\mathbb{F}_p)$, the number $P_\pi(a;1)$ must kill all the elements of $J(C_a)(\mathbb{F}_p)$. This suggested us the idea of using the addition in $J(C_a)(\mathbb{F}_p)$ to choose among the polynomials in the family $S(C_a;\mu'_2;\mu'_3;p)$, the polynomial corresponding to $P_\pi(\lambda)$. In this way $P_\pi(\lambda)$ could be completely determined. Of course, this procedure is feasible only if you have a very efficient way to add in $J(C_a)$. Fortunately, for Picard Jacobians we have developed in [EstReiChe] a fast addition algorithm. Moreover, since the ramification point $R_0 = (0:0:1)$ belongs to any curve C_a, then the class $[R_0 - P_\infty]$, $P_\infty = (0:1:0)$, is a *three torsion* of $J(C_a)$. Thus, the cardinality of $J(C_a)$ is, necessarily, divisible by 3 and we may discard the polynomials $P(\lambda)$ with $P(1)$ not divisible by 3.

The following algorithm computes for a fixed curve C_a and an inicial prime p_0 the next prime $p_1 \geq p_0$, if there exist any, such that $\#J(C_a)(\mathbb{F}_{p_1})$ is quasiprime and also computes the corresponding characteristic polynomial $P_\pi(a;\lambda)$ of $J(C_a)(\mathbb{F}_{p_1})$.

1. Randomly compute a $\mathbb{F}_p$-rational point $P_1 = (x_1 : y_1 : 1)$, $y_1 \neq 0$, of $C_a/\mathbb{F}_{p_0}$ and set $x =$ class on $J(C_a/\mathbb{F}_{p_0})$ of $P_1 - P_\infty$, $P_\infty = (0:1:0)$.

2. Set $I = S(C_a;\mu'_2;\mu'_3;p_0)$.

3. Choose $P(\lambda) \in I$, set $I := I \setminus \{P(\lambda)\}$.

4. If $P(1) = 3 \cdot m$, m quasiprime, then compute $\overline{x} =$ class of $P(1) \cdot x$ in $J(C_a)$, else go to 3.

5. If $\overline{x} = 0$, then set $P_\pi(a; \lambda) = P(\lambda)$, $p_1 = p_0$ and finish, else if $I \neq \emptyset$ go to 3

6. If the algorithm reaches this point, then the cardinality of $J(C_a)$ is not of the form if $P(1) = 3 \cdot m$, m quasiprime. Then, we set p_0 equal to the next prime greater than p_0 congruent to $4, 7$ mod 9 and go to step 1.

5 Efficient computations on the jacobian

The fast addition algorithm in [EstReiChe] is effectively implemented and the cost of computing a reduced representative of the sum of two divisors D_1 and D_2 is $O(deg(D_1) + deg(D_2))$ additions in $\mathbb{F}_p$. Expressing the number $P(1)$ in base p, it is possible to perform the computation of $\overline{x}$ = class of $P(1) \cdot x$ in $J(C_a)$ with a cost of $O(log\ p)$ additions in $\mathbb{F}_p$.

Example 5.1 *For primes $p \equiv 4, 7 \mod 9$ we obtained for the fixed curve C_2*

p	$P_\pi(2; \lambda)$	$\#J(C_a)(\mathbb{F}_p)$
1001011003	$p^3+51133p\lambda^3+\lambda^6$	3·334345358804874247270637809
1001014177	$p^3+61729p\lambda^3+\lambda^6$	3·334348539236053529996165089
1001015467	$p^3+24421p\lambda^3+\lambda^6$	3·334349831855610365735524057
1001015503	$p^3+52177p\lambda^3+\lambda^6$	3·334349867928771670683522853
1001018209	$p^3+11869p\lambda^3+\lambda^6$	3·334352579434780888214675317
1001023501	$p^3+33541p\lambda^3+\lambda^6$	3·334357882245032482954689181
1001025457	$p^3+63085p\lambda^3+\lambda^6$	3·334359842254857123624024613
1001027947	$p^3+28879p\lambda^3+\lambda^6$	3·334362337370446422564296179
1001028841	$p^3+51367p\lambda^3+\lambda^6$	3·334363233210167887576634323
1001029333	$p^3+50137p\lambda^3+\lambda^6$	3·334363726223310123039312553
1001029669	$p^3+54499p\lambda^3+\lambda^6$	3·334364062915492367641052047

6 Discussed security against known attacks

1. Shank's baby-step giant-step method [Odl] and Pollig-Hellman method [PohHel] can be avoided selecting jacobians with quasiprime cardinality. Our numerical experiments show that in many cases the cardinality of the proposed family of Picard curves is indeed quasiprime, hence the corresponding cryptosystems are secure against these attacks.

2. In many cases we have obtained cyclic quasiprime symmetric jacobians, hence the embedding of $J(\mathbb{F}_p)$ in $J(\mathbb{F}^*_{p^k})$ via the Tate-pairing for supersingular curves (see [FreRue]) does not apply

3. Our curves have low genus, hence any attack analogous to the smooth divisor attack (see [AdlDeMHua]) is not applicable

4. The order of the group of automorphisms is small, hence the speeding up factor for the discrete log computation proposed in [MorDuuGau] is not substantial

The authors found fascinating to be able to present a short exposition of the picture that one obtains, when the special families of curves are considered from the complex point of view. In their beautiful paper [LewRau], Lewittes and Rauch determined the (normalized) period matrix of the Klein curve $X^3Y + Y^3Z + Z^3X = 0$. Up to isomorphy, this plane projective complex curve is characterized as compact Riemann surface of genus 3 with the maximal possible number of $168 = 84(g-1)$ automorphisms. In analogy, we want to determine the (normalized) period matrix of the special Picard curve with projective equation $Y^3Z = X^4 - XZ^3$. Moreover, up to isomorphy, we characterize this (complex) curve by the quality of the corresponding Picard moduli point: the only orbitally isolated surface singularity. Most interesting is the characterization of the curve by the endomorphism ring of its Jacobian threefold: the ring of 9-th unit roots. We extend our considerations also to the Picard curve $Y^3Z = X^4 - Z^4$ corresponding to the second singularity of the modular surface of Picard curves. Nowadays the Klein quartics over finite fields are used for the construction of error correcting codes, see [Pre]. This should be done also for special Picard curves.

7 Simultaneous CM-Lifting of the Jacobians

Let F be a number field and A a complex abelian variety of dimension g. We say that A has *F-multiplication*, if there is a $\mathbb{Q}$-algebra embedding ι of F into the endomorphism algebra $End^\circ A = \mathbb{Q} \otimes End\, A$ of A. If, moreover, the (total) degree of F is equal to $2g$ and ι is an isomorphism, then A is called an abelian CM-*variety*. It is well- known that in this case that A is simple and F is a CM-field, which is, by definition, a totally imaginary quadratic field extension of a totally real number field, see [Lan]. A CM-curve is a (smooth complex) projective curve C whose Jacobian variety $J(C)$ is an abelian CM-variety.

A *Picard curve* is the projective closure of an affine plane curve of equation type $Y^3 = p_4(X)$, where $p_4(X)$ is a polynomial of degree 4. We exclude all polynomials $p_4(X)$ with only one zero. So one avoids unstable curves in order to get a compact algebraic moduli space $\hat{M}$ of (isomorphy classes of semistable) Picard curves, which we choose in a very canonical way (see below). Smooth Picard curves have genus 3. They correspond to a Zariski-open part $M^{\#}$ of $\hat{M}$. There Jacobians are (principally polarized) abelian threefolds. Via period matrices they are represented by points in the generalized Siegel upper half plane

$$\mathbb{H}_3 = \{\Omega \in Mat_3(\mathbb{C});\ {}^t\Omega = \Omega\,,\ Im\,\Omega\, positive\, definit\},$$

uniquely up to $\mathbb{S}p(6, \mathbb{Z})$-equivalence, where

$$\mathbb{S}p(6, \mathbb{Z}) = \{G \in \mathbb{G}l_6(\mathbb{Z});\ {}^tG \cdot \left(\begin{smallmatrix} O & E_3 \\ -E_3 & O \end{smallmatrix}\right) \cdot G = \left(\begin{smallmatrix} O & E_3 \\ -E_3 & O \end{smallmatrix}\right)\},$$

$E_3 := diag(1, 1, 1)$, denotes the symplectic group acting on $\mathbb{H}_3$ in the well-known manner. By Torelli's theorem there is a canonical algebraic embedding $M^{\#} \hookrightarrow \mathfrak{A}_3$ into the moduli space $\mathfrak{A}_3 = \mathbb{H}_3/\mathbb{S}p(6, \mathbb{Z})$ of principally polarized abelian threefolds. Restricting to the Zariski-open subspace $\mathfrak{A}_3^{\#} \subset \mathfrak{A}_3$ corresponding to Jacobians of smooth genus 3 curves one gets a closed embedding $M^{\#} \hookrightarrow \mathfrak{A}_3^{\#}$, which determines $M^{\#}$ uniquely, up to isomorphy.

Obviously, our special Picard curves

$$C_{aX} : Y^3 = X^4 - aX\,,\ C_b : Y^3 = X^4 - b,\ a, b \in \mathbb{C}^*,$$

are isomorphic over $\mathbb{C}$ to

$$C_X : Y^3 = X^4 - X \text{ or } C_1 : Y^3 = X^4 - 1,$$

respectively.

Proposition 7.1 . *The Picard curves C_{aX} are CM-curves with $\mathbb{Q}(\rho)$-multiplication, where ρ is a primitive 9-th unit root. The endomorphism ring $End\, J(C_{aX})$ is isomorphic to $\mathbb{Z}[\rho]$. Up to isomorphy, C_X is the only Picard CM-curve with a cyclotomic maximal order as endomorphism ring.*

Proposition 7.2 . *The moduli points of C_X and of C_1 are the only surface singularities on $M^{\#}$ and also on $\hat{M}$.*

Proposition 7.3 . *Let $\omega = \rho^3$ be the primitive third unit root $e^{2\pi i/3}$. A period matrix of the Jacobian $J(C_X)$ is:*

$$
\Pi = \begin{pmatrix} -\rho+1 & 0 & -2\rho^2-2\rho & -\rho^2-1 & 1 & 2\rho^2+\rho \\ \rho^2-1 & 0 & -\rho^2+2\rho & -\rho^2+\rho+1 & -1 & \rho^2-2\rho \\ -\rho+1 & 0 & -2\rho^2-2\rho & -\rho^2-1 & 1 & 2\rho^2+\rho \end{pmatrix} \cdot \omega
$$

$$
+ \begin{pmatrix} 2\rho^2+\rho+1 & 1 & -\rho+1 & -2\rho^2-\rho & 0 & \rho^2+\rho-1 \\ -\rho^2+2\rho & 1 & -2\rho^2+2\rho+1 & -\rho+1 & -1 & \rho^2-\rho-1 \\ 2\rho^2+\rho+1 & 1 & -\rho+1 & -2\rho^2-\rho & 0 & \rho^2+\rho-1 \end{pmatrix}.
$$

The closed algebraic embedding $M^{\#} \hookrightarrow \mathfrak{A}_3^{\#}$ can be *uniformized* in the following sense. In the analytic category there is a commutative *Shimura diagram*

$$
\begin{tikzcd}
\mathbb{B} \arrow[rrr, hook] \arrow[ddd] & & & \mathbb{H}_3 \arrow[ddd] \\
& \mathbb{B}^{\#} \arrow[ul] \arrow[r, hook] \arrow[d] & \mathbb{H}_3^{\#} \arrow[ur] \arrow[d] & \\
& M^{\#} \arrow[r, hook] \arrow[dl] & \mathfrak{A}_3^{\#} \arrow[dr] & \\
M \arrow[rrr, hook] & & & \mathfrak{A}_3
\end{tikzcd}
\tag{9}
$$

where $\mathbb{B}$ is the two-dimensional complex unit ball

$$
\mathbb{B} = \{z = (z_1, z_2) \in \mathbb{C}^2;\ |z|^2 := |z_1|^2 + |z_2|^2 < 1\}, \tag{10}
$$

$\mathbb{H}_3 \longrightarrow \mathfrak{A}_3$ the $\mathbb{S}p(6,\mathbb{Z})$-quotient morphism, $\mathbb{H}_3^{\#}$ the preimage of $\mathfrak{A}_3^{\#}$ in $\mathbb{H}_3$, $\mathbb{B} \hookrightarrow \mathbb{H}_3$ is a closed embedding, $\mathbb{B}^{\#} = \mathbb{B} \cap \mathbb{H}_3^{\#}$ and $\mathbb{B} \longrightarrow M$ is the analytic quotient morphism of the arithmetic group

$$
\Gamma = N_{\mathbb{S}p(6,\mathbb{Z})}(\mathbb{B}) := \{G \in \mathbb{S}p(6,\mathbb{Z});\ G(\mathbb{B}) = \mathbb{B}\} \tag{11}
$$

acting on $\mathbb{B}$.

The other morphisms in Diagram 9 are open dense embeddings or restrictions, which should be clear. For proofs and more explicit details, which are needed below, we refer to [Ho3].

Identifying for a moment the ball with its image in $\mathbb{H}_3$ we call $\mathbb{B}$ the *period space of Picard curves* and its points are called *Picard period points* (of the family of Picard curves). An element $\gamma \in \Gamma$ is called *elliptic*, iff γ has an isolated fixed point $P \in \mathbb{B}$.

Let Γ' be a subgroup of Γ. We call the elliptic element γ *purely* Γ'-*elliptic*, iff all non-trivially on $\mathbb{B}$ acting elements of the stationary group Γ'_P are elliptic. The images of purely Γ'-elliptic points on $\mathbb{B}/\Gamma'$ are isolated (cyclic quotient) singularities. Notice that the fixed point P is uniquely determined by the elliptic element γ because the group of biholomorphic automorphisms of $\mathbb{B}$ coincides with $\mathbb{PU}((2,1),\mathbb{C})$, so γ has only one negative eigenline in $V = (\mathbb{C}^3, < .\,, . >)$ with respect to the hermitian metric $< .\,, . >$ of signature $(2,1)$ on $\mathbb{C}^3$, namely

$$\mathbb{B} = \mathbb{P}V_- \,,\ V_- = \{\mathfrak{a} \in V;\ < \mathfrak{a}, \mathfrak{a} > < 0\}.$$

Proposition 7.4 . *The set of Picard period points of C_X coincides with the set of purely Γ-elliptic points on $\mathbb{B}$. It coincides with the Γ-orbit of*

$$P_\rho := (\rho^4 - \rho^2 \,:\, 1 \,:\, \rho^5 + \rho^4 - 1) \in \mathbb{B}.$$

Proposition 7.5 . *The set of $\mathbb{H}_3$-(Siegel-)period points of (Jacobians of) the curves C_{aX} coincides with the $\mathbb{S}p(6,\mathbb{Z})$-orbit of*

$$\begin{pmatrix} \frac{-2ac-1}{3a^2} & \frac{1}{a} & \frac{ac-1}{3a^2} \\ \frac{1}{a}, -1, 0 & & \\ \frac{ac-1}{3a^2} & 0 & \frac{-2ac+2}{3a^2} \end{pmatrix} \cdot \omega + \begin{pmatrix} \frac{2ac-2}{3a^2} & \frac{1}{a} & \frac{-ac+1}{3a^2} \\ \frac{1}{a} & -1 & \frac{-1}{a} \\ \frac{-ac+1}{3a^2} & \frac{-1}{a} & \frac{2ac+1}{3a^2} \end{pmatrix}$$

with

$$a = -\rho^4 + \rho^3 + 2\rho^2 + \rho + 1 \,,\ c = -(\rho^5 + \rho^3 + 2\rho^2 + \rho)$$

Proof of Proposition 7.2. Let $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ be the field of Eisenstein numbers. The cyclic group Z_3 of order 3 acts via $(x,y) \mapsto (x, \omega y)$ on each Picard curve C. If C is smooth, we get $\mathbb{P}^1$ as quotient curve C/Z_3 with Z_3 as Galois group of $C\,/\,\mathbb{P}^1$. The action of Z_3 induces a K-multiplication on $J(C)$ of type $(2,1)$, which means that the diagonalized representation group of Z_3 on the tangent space $T_0J(C)$ of $J(C)$ is generated by $\left(\begin{smallmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \bar{\omega} \end{smallmatrix}\right)$. The moduli space of abelian threefolds with K-multiplication of type $(2,1)$ is the Shimura surface $\mathbb{B}/\Gamma$, $\Gamma = \mathbb{U}((2,1),\mathfrak{O})$, $\mathfrak{O} = \mathfrak{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ the ring of Eisenstein integers. In [Ho3] we proved that this ball lattice Γ coincides with Γ defined in (11). We define the congruence subgroup $\Gamma(\sqrt{-3})$ by the exact group sequence

$$1 \longrightarrow \Gamma(\sqrt{-3}) \longrightarrow \Gamma \longrightarrow \mathbb{U}((2,1), \mathfrak{O}/(1-\omega\mathfrak{O}) \longrightarrow 1$$

and know that $\mathbb{U}((2,1),\mathbb{F}_3) \cong S_4$, the symmetric group of four letters, see [Ho1]. In the same monograph, see ch. I, Prop. 3.2.3, we proved the following central

Theorem 7.6 . *The Baily-Borel compactification $\widehat{\mathbb{B}/\Gamma(\sqrt{-3})}$ coincides with the projective plane $\mathbb{P}^2$. The compactifying cusp points are four points*

$K_1, K_2, K_3, K_4 \in \mathbb{P}^2$ in general position. The open part $\mathbb{P}_2^{\#} \subset \mathbb{P}^2$ coming from smooth Picard curves is precisely the complement of the six projective lines $L_{ij} = L_{ji}$ going through pairs K_i, K_j of different cusp points.

It turns out that

$$M^{\#} = \mathbb{P}_2^{\#}/S_4 \ , \ \hat{M} = \mathbb{P}^2/S_4 \ , \ M = \mathbb{P}_2^{*}/S_4,$$

where $\mathbb{P}_2^{*} := \mathbb{P}^2 \setminus \{K_1, K_2, K_3, K_4\}$. Now identify $\mathbb{P}^2$ with

$$\mathbb{P}_0^3 = \{(t_1 : t_2 : t_3 : t_4) \in \mathbb{P}^3;\ t_1 + t_2 + t_3 + t_4 = 0\},$$

and introduce projective coordinates such that

$$\begin{gathered} K_1 = (-3 : 1 : 1 : 1),\ K_2 = (1 : -3 : 1 : 1), \\ K_3 = (1 : 1 : -31 : 1),\ K_4 = (1 : 1 : 1 : -3). \end{gathered}$$

Theorem 7.7 *(see [Ho1] I, Prop. 3.4.4). The only singularities of $\hat{M}$ are the image points of $S := (0 : 1 : \omega : \omega^2)$ and $N := (1 : i : -1 : -i)$, along the S_4-quotient morphism.*

This is a simple application of a theorem of Chevalley stating that the singularities of a finite (more generally: locally finite) Galois quotient X/H of a smooth complex manifold X come precisely from points $x \in X$ with isotropy group G_x not generated by reflections at x, where reflections at x are defined as elements of G_x acting trivially on a submanifold of X through x of codimension 1. Looking at finite subgroups of S_4 and their fixed points on $\mathbb{P}^2$ one finds up to S_4-equivalence the points S, N as only singular possibilities. The S_4-isotropy group of S is generated by the cyclic permutation (234) of order 3. The S_4-isotropy group of N is generated by the cyclic permutation (1234) of order 4. The (13)(24)-reflection line on $\mathbb{P}^2$ contains N.

Now we need the precise correspondence of Picard curves with their moduli space $\hat{M} = \mathbb{P}^2/S_4$. Each of them is isomorphic to a *normal form* representative

$$C_{\mathfrak{t}} :\ Y^3 = (X - t_1)(X - t_2)(X - t_3)(X - t_4),\ t_1 + t_2 + t_3 + t_4 = 0.$$

The correspondence

$$C_{\mathfrak{t}} \mapsto \mathfrak{t} = (t_1, t_2, t_3, t_4) \mapsto (t_1 : t_2 : t_3 : t_4) \in \mathbb{P}_2^{*}$$

restricted to $\mathbb{P}_2^{\#}$ and composed with the S_4- quotient map yields the precise parametrisation of isomorphy classes, see [Ho1] I, Prop.5.2.3. Especially, the moduli point of

$$C_X : Y^3 = X(X-1)(X-\omega)(X-\omega^2)$$

is the image of S. Proposition 2 is proved.

Proof of Proposition 7.4. For an arbitrary group G we denote by G_{tor} the set of elements of finite order of G (torsion elements), and G_{k-tor} denotes the subset of elements of precise order $k \in \mathbb{N}_+$. G acts on G_{k-tor} and on G_{tor} via conjugations.

Lemma 7.8 . *For $\Gamma = \mathbb{U}((2,1),\mathfrak{O})$ the set Γ_{9-tor} is not void. It consists of precisely six Γ-conjugation classes. They are projecteded onto two $\mathbb{P}\Gamma$-conjugation classes in $(\mathbb{P}\Gamma)_{3-tor}$.*

Proof. For the first statement we consider the element

$$\varphi_1 := \begin{pmatrix} -\omega^2 & -1 & \omega^2 \\ \omega & 1 & 1 \\ 1 & -1 & \omega^2-1 \end{pmatrix}$$

with

$$det\,\varphi_1 = \omega\ ,\ \varphi_1^3 = \omega E_3.$$

found by Feustel in [Feu]. It is easy to check that φ_1 belongs to Γ. The eigenvalues are ρ, ρ^4, ρ^7. The powers φ_1^k, $k = 1,2,4,5,7,8$, yield six different conjugation classes in Γ_{9-tor} (compare determinants and eigenvalues) and two conjugation classes in $(\mathbb{P}\Gamma)_{3-tor}$.

Now let φ be an arbitrary element of Γ_{9-tor} with eigenvalues ρ, ρ^j, ρ^k, say. The Galois group of $F := K(\rho)$ over K is generated by $\sigma : \rho \mapsto \rho^4$. The characteristic polynomial of $\chi_\varphi(T)$ of φ belongs to $K[T]$. Looking at trace and determinant of φ, which must belong to K, it is easy to see, that φ has three different eigenvalues. They must be conjugated over K, hence $\rho^j = \rho^4 = \sigma(\rho)$, $\rho^k = \rho^7 = \sigma^2(\rho)$. The eigenvectors $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ of ρ, $\sigma(\rho)$, $\sigma^2(\rho)$, respectively, can be choosen in F^3. They form an orthogonal basis of F^3 endowed with our hermitian $(2,1)$-metric because of different eigenvalues. From $\varphi(\mathfrak{a}) = \rho\cdot\mathfrak{a}$ it follows that

$$\sigma(\varphi(\mathfrak{a})) = \sigma(\rho)\sigma(\mathfrak{a}) = \rho^4\sigma(\mathfrak{a})$$

because φ belongs to $Mat_3(K)$. Therefore

$$\mathfrak{a},\ \mathfrak{b} = \sigma(\mathfrak{a}),\ \mathfrak{c} = \sigma^2(\mathfrak{a}) \in F^3, \tag{12}$$

satisfying

$$< \mathfrak{a}, \mathfrak{a} > < 0, \quad < \mathfrak{b}, \mathfrak{b} > > 0, \quad < \mathfrak{c}, \mathfrak{c} > > 0,$$

(without loss of generality) is an orthogonal φ-eigenbasis of $\mathbb{C}^3$. The elliptic element φ has the unique elliptic fixed point $P = \mathbb{P}\mathfrak{a} \in \mathbb{B}$. We show that P is a purely Γ-elliptic point. With $\Gamma' := \Gamma(\sqrt{-3})$ we have a commutative diagram of quotient morphisms

$$\begin{tikzcd}
\mathbb{B} \arrow[d, "p'"'] \arrow[dr, "p"] & \\
\mathbb{B}/\Gamma' = \mathbb{P}_2^* \arrow[r, "\pi"] & \mathbb{P}_2^*/S_4 = \mathbb{B}/\Gamma
\end{tikzcd}$$

In [Ho1] I, Prop. 3.4.4, we listed on $\mathbb{P}_2^*$ the p'- images of all Γ-elliptic points $Q \in \mathbb{B}$ together with their (abstract) isotropy groups Γ_Q. Our P cannot be an intersection point of two Γ-reflection discs because the reflections have eigenvalues only in K. Otherwise $P \in \mathbb{B} \subset \mathbb{P}^2$ would be the intersection point of two projective lines (the projectivized orthogonal complements of the one-dimensional eigenspaces) defined over K. This leads to $\mathbb{P}\mathfrak{a} = P = \mathbb{P}\mathfrak{a}'$, $\mathfrak{a}' \in K^3$, $\sigma(P) = P$, which contradicts to $\sigma(P) \notin \mathbb{B} = \mathbb{P}V_-$, see (12). There are precisely two Γ-obits $\Gamma\tilde{N}$, $\Gamma\tilde{S}$ of Γ-elliptic points which isotropy groups are not generated by reflections. The projective isotropy groups $\mathbb{P}\Gamma_{\tilde{N}}$ or $\mathbb{P}\Gamma_{\tilde{S}}$ are cyclic of order 4 or 3, respectively. Since $\mathbb{P}\varphi \in \mathbb{P}\Gamma_P$ is elliptic of order 3 the point P must belong to the second orbit. The image $p(\tilde{S})$ coincides with $p'(S)$, which is an orbitally isolated singularity with respect to Γ. This means that $\tilde{S}$ is a purely Γ-elliptic point, hence $\mathbb{P}/\Gamma_{\tilde{S}} \cong < \mathbb{P}\varphi >$ of order 3.

□

Proof of Proposition 7.1. Our special Picard curve $C_X : Y^3 = X(X^3 - 1)$ has an obvious non-trivial automorphism of 9-th order:

$$(x, y) \mapsto (\omega x,\ \rho y)\ ,\ (\rho^3 = \omega).$$

It extends to the Jacobian threefold of C_X. Therefore $\mathbb{Z}[\rho] \subseteq End\, J(C_X)$. We have embeddings

$$\mathbb{Z}[\rho] \hookrightarrow End\, J(C_X)\ ,\ F \hookrightarrow End\, J(C_X). \tag{13}$$

So the endomorphism algebra of $J_X(C)$ contains a field of degree $2 \cdot dim\, J_X(C) = 2g(C_X) = 6$ over $\mathbb{Q}$ $2 \cdot dim\, J_X(C) = 2g(C_X) = 6$ over $\mathbb{Q}$. It follows that $J_X(C)$ is an abelian DCM- variety, which means that it has an isogeny decomposition into simple abelian CM-varieties (see e.g. [Lan], ch.I). The coordinate field $K(P_\rho)$ of the period point $P_\rho \in \mathbb{B}$ has degree 3 over K. The following criterion (iii) shows that $J(C_X)$ must be a (simple) CM-variety.

Theorem 7.9 *(see [Ho2], 7). Let*

$$\tau = (\tau_1, \tau_2) = (\tau_1 : \tau_2 : 1) \in \mathbb{B} \subset \mathbb{P}^2 = \mathbb{P}V$$

be a period point of the abelian DCM-3-fold A_τ with K-multiplication of type $(2,1)$, K an arbitrary imaginary quadratic number field. Then the following equivalences hold:

(i) $[K(\tau) : K] = 1 \Longleftrightarrow$
$A_\tau \sim E \times E \times E$, *$E$ elliptic curve with K-multiplication;*

(ii) $[K(\tau) : K] = 2 \Longleftrightarrow$
$A_\tau \sim E \times E'^2$, *$E'$ an elliptic CM-curve not isogeneous to E, or*
$A_\tau \sim E \times B$, *B a (simple) abelian CM- surface;*

(iii) $[K(\tau) : K] = 3 \Longleftrightarrow$
A_τ is a (simple) abelian CM-threefold with $K(\tau)$- multiplication,

where $\sim$ means "isogeneous".

The endomorphism ring of any abelian CM-variety is an order in the corresponding CM-field. Each order of a number field L is contained in the maximal order, the ring $\mathfrak{O}_L$ of integers in L. The maximal order of a cyclotomic field $L = \mathbb{Q}(\zeta)$ is equal to $\mathbb{Z}[\zeta]$, ζ a generating unit root, see e.g. [Neu], I, Prop. 10.2. So the embeddings (13) must be isomorphisms, especially

$$\mathfrak{O}_F = \mathbb{Z}[\rho] \cong EndJ(C_a) \subseteq EndJ(C_a) \cong F. \tag{14}$$

The first two parts of Proposition 7.1 are proved. F is the only cyclotomic field of degree 3 over K. Therefore the Jacobian threefolds of CM-Picard curves C with cyclotomic endomorphism algebra $EndJ(C)$, which must be isomorphic to F, have to be isogeneous. There is a bijective correspondence between the ideal classes of $\mathfrak{O}_F$ and the isomorphy classes of principally polarized abelian CM-threefolds A (of same multiplication type) with endomorphism algebra $\mathfrak{O}_F$, see e.g. [Lan], III.2, Cor. 2.7. It is well- known that the class number of F is equal to 1, see e.g. [Hasse], III, end of 29. Therefore, up to isomorphy, there is only one such A. Then, by Torelli's theorem, also the isomorphy class of Picard CM-curves $EndJ(C) \cong \mathfrak{O}_F$ is uniquely determined. This completes the proof of Proposition 7.1.

□

Remark 7.10 . *The* type *of F-multiplication is a lift (F-extension) from the type* $(2,1)$ *of K-multiplication on $J(C_X)$. This lifted type is unique by [Lan], I.3, Theorem 3.6.*

Proof of Propositions 7.3 and 7.5. In [Ho3], sections 2.4-2.5, we described the procedure to receive the period matrices starting from the coordinates of the fixed point P_ρ. First one has to move the "diagonal ball" (10) $\mathbb{B} \subset \mathbb{P}^2$ by a plane projective linear transformation to the "Picard ball" (Siegel domain) $\mathbb{B}' \subset \mathbb{P}^2$. This is done by the inverse of

$$\begin{pmatrix} \omega & 0 & -1 \\ 0 & 1 & 0 \\ -\omega^2 & 0 & -1 \end{pmatrix},$$

(see [Ho3], p. 28) acting on row-vectors from the right. Let $P' := (a : b : c) \in \mathbb{B}'$ be the image point of $P_\rho \in \mathbb{B}$. Setting $b = 1$ one gets a, $c \in \mathbb{Z}[\rho]$, explicitly written down in Proposition 7.5. From the vector $(a, 1, c)$ one gets the period matrices of Propositions 7.3 and 7.3 via orthogonal fillings and $*$-procedure coming from Picard period integrals, all described in [Ho3], around Lemma 2.22. The numbers a, c appear in the period matrix Π (see 7.3) as $\Pi_{1,1}$ or $\Pi_{1,4}$, respectively.

□

For the understanding of Jacobian splittings of the Picard curves C_b : $Y^3 = X^4 - b$, $b \neq 0$, we need a refinement of Theorem 7.3. A ball point $\mathbb{P}\mathfrak{a}$, $\mathfrak{a} \in V_-$, is called *exceptional* iff the ring $End_K(\mathfrak{a}, \mathfrak{a}^\perp)$ of K-endomorphisms of V with eigenvector $\mathfrak{a}$ and invariant subspace $\mathfrak{a}^\perp$ is bigger than K. If, moreover, $\mathfrak{a}$ is eigenvector of a simple eigenvalue of an element $\varphi_1 \in End_K(\mathfrak{a}, \mathfrak{a}^\perp)$, then we say that $\mathbb{P}\mathfrak{a}$ is an *isolated exceptional* point. Elliptic points of a Picard modular group are obviously simple exceptional.

Theorem 7.11 *(see [Ho2], section 7). The endomorphism algebra of the Jacobian variety $J_\tau \cong J(C_t)$ of a Picard curve with period point $\tau \in \mathbb{B}$ and moduli point $t = (t_1 : t_2 : t_3 : t_4) \in \mathbb{P}_2^*$ is greater than K if and only if τ is exceptional. J_τ splits up to isogeny into abelian CM- subvarieties if and only if τ is an isolated exceptional point. Thereby Jacobians with CM-field F (of degree 3 over K) correspond to isolated exceptional points of K-degree 3 and $F \cong K(\tau)$. All other isolated exceptional points (of K-degree 2 or 1) ly on K-discs on $\mathbb{B}$ (defined as non-empty intersections $L \cap \mathbb{B}$, L projective lines on $\mathbb{P}^2$ defined over K). Thereby $\tau \in \mathbb{B}(K)$ if and only if J_τ splits into $E \times E \times E$. The degree 2 case happens if and only if J_τ splits into $E \times (E'^2)$, where E is an elliptic CM-curve with K-multiplication and E' elliptic CM with imaginary quadratic multiplication field $L \neq K$. Moreover, it holds that $K(L) = K(\tau)$ in the latter case.*

For the sake of completion we give a hint for finding the period matrices of $C_1 : Y^3 = X^4 - 1$ in the same manner. The moduli point is $M = (1 : i : -1 : i)$. The corresponding period points on $\mathbb{B}$ are $\Gamma(\sqrt{-3})$-elliptic points on $\mathbb{B}$, because the permutation $(1234) \in S_4 \cong \Gamma/\Gamma(\sqrt{-3})$ fixes M. In [Ho1], I, Proposition 3 we proved that the $\Gamma(\sqrt{-3})$-orbit of $\tilde{M}$ can be represented by points $\tilde{M}$ on the diagonal disc $\mathbb{D} = \{(z,z) \in \mathbb{C}^2;\ 2|z|^2 < 1\} \cap \mathbb{B}$, which is a K-disc. Moreover, the projective isotropy group $\mathbb{P}\Gamma(\sqrt{-3})_{\tilde{M}}$ is cyclic of order 4. Therefore the coordinates of $\tilde{M} = \mathbb{P}\mathfrak{a}$ belong to $K(i) \setminus K$. Each elliptic point is obviously an isolated exceptional point. Now Theorem 7.11 shows that the Jacobians of $J(C_b) \cong J(C_1)$ have splitting type $E \times E' \times E'$, E' the elliptic CM-curve with Gauß number multiplication. By the way, it is easy to see that the elliptic CM-curve $E : T^2 = Y^3 + 1$ with Eisenstein multiplication is an isogeny factor of C_1 because of the double covering $C_1 \longrightarrow E'$, $(x,y) \mapsto (x^2, y)$, which extends to the Jacobian. We proved

Proposition 7.12 . *The Jacobians of the Picard curves*

$$C_b : Y^3 = X^4 - b,\ b \neq 0,$$

split into $E \times E' \times E'$, where E, E' are elliptic CM-curves with fields $K = \mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(i)$, respectively.

□

The procedure for finding a representative period point of C_1 has been worked out in Feustel's paper [Feu]. The explicit determination of a period matrix is left to the reader as exercise.

References

[AdlDeMHua] Adleman, L.M., DeMarrais, J., Huang, M., A Subexponential Algorithm for Discrete Logarithm over the Rational Subgroup of Large Genus Hyperelliptic Curves over Finite Fields, Proc. ANTS1, LNCS. vol. 877, Springer-Verlag (1994), pp. 28-40

[Car] Cartier, P., *Questions de rationalité des diviseurs en géométrie Algébrique*, Bull. Soc. Math. France 86 (1958), 177-251.

[DuuSak] Duursma, I., Sakurai, K., Hyperelliptic cryptosystems from curves $y^2 = x^p - x + 1$ over finite fields of characteristic p, Preprint 1998.

[Est1] Estrada Sarlabous. J, *On the Jacobian Varieties of Picard Curves Defined over Fields of Characteristic p,*. Math. Nachr. 152 (1991), 329-340.

[Est2] Estrada Sarlabous. J., *A finiteness theorem for Picard curves with good reduction,*. Appendix I of *Ball models and some Hilbert Problems* by R.-P. Holzapfel. Lectures in Mathematics. Birkhäuser-Verlag, (1995).

[EstReiPi] Estrada Sarlabous. J, Reinaldo Barreiro. E, Piñeiro Barceló. J.A., *On the Jacobian Varieties of Picard curves: explicit Addition Law and Algebraic Structure,* Math. Nachrichten 208 (1999), pp. 149-166

[EstReiChe] Estrada-Sarlabous, J., Reinaldo-Barreiro, E., Cherdieu, J-P. *Efficient Reduction on the Jacobian Variety of Picard Curves* in: Coding Theory, Cryptography and Related Areas*Proceedings of the ICCC-98*, J. Buchmann, T. Hohold, H. Stichtenoth, H. Tapia-Recillas (eds.), pp.13-28, Springer-Verlag, 2000.

[Feu] Feustel, J.M.: Kompaktifizierung und Singularitten des Faktorraumes einer arithmetischen Gruppe, die in der zweidimensionalen Einheitskugel wirkt, Diplomarbeit, Humboldt-Univ. Berlin, 1976 (unpublished)

[FreRue] Frey, G., Rueck, H.G., A Remark Concerning the m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves, Math. Comp. 62, No.206 (1994), pp. 865-874

[Fre2] Frey, G., Aspects of DL-systems based on hyperelliptic curves, in: Proc. Conference on the Mathematics of Public Key Cryptography, A. Odlyzko, G. Walsh, H. Williams (eds.), Toronto, 1999.

[Has] Hasse, H,: Zahlentheorie, Akademie Verlag, Berlin, 1963

[Ho1] Holzapfel, R.-P.: Geometry and Arithmetic around Euler partial differential equations, Dt. Verlag d. Wiss., Berlin/Reidel Publ. Comp., Dordrecht, 1986

[Ho2] Holzapfel, R.-P.: Hierarchies of endomorphism algebras of abelian varieties corresponding to Picard modular surfaces, Schriftenreihe Komplexe Mannigfaltigkeiten **190**, Univ. Erlangen, 1994

[Ho3] Holzapfel, R.-P.: The ball and some Hilbert problems, Lect. in Math. ETH Zrich, Birkhuser, Basel-Boston-Berlin, 1995

[Ko1] Koblitz, N., A Family of Jacobians Suitable for Discrete Log Cryptosystems, Advances in Cryptology, Crypto'88, Springer-Verlag (1992), pp. 94-99

[Ko2] Koblitz, N., Hyperelliptic Cryptosystems, J. Cryptology 1 (1989), pp. 139-150.

[Ko3] Koblitz, N., A Very Fast Way to Generate Curves over Prime Fields for Hyperelliptic Cryptosystems, Crypto'97 Rump Talk (1997)

[Lac] Lachaud,G., *Courbes diagonales et courbes de Picard.* Prétirage N. 97-30. IML-France. (1997).

[Lan] Lang, S.: Complex multiplication, Grundl. Math. Wiss. **255**, Springer, 1983

[LewRau] Lewittes, J., Rauch, H.E.: The Riemann surface of Klein with 168 automorphisms. In: Problems in Analysis, a symposion in honor of Solomon Bochner, 297 - 308, Princeton Univ. Press, 1970

[Man] Manin, Yu. I., *The theory of commutative formal groups over fields of finite characteristic.* Russian Math. Surveys 18 (1963), 3-90.

[MorDuuGau] Morain, F., Duursma, I., Gaudry, P., Speeding up the discrete log computation on curves with automorphisms, in: Proc. Conference on the Mathematics of Public Key Cryptography, A. Odlyzko, G. Walsh, H. Williams (eds.), Toronto, 1999.

[Neu] Neukirch, J.: Algebraische Zahlentheorie, Springer, Berlin-Heidelberg, 1992

[Odl] Odlyzko, A., Discrete logarithms and their cryptographic significance, Advances in Cryptology, Eurocrypto'84, Springer-Verlag (1993), pp. 333-344.

[PohHel] Pohlig, S.C., Hellman, M.E., An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Trans. on IT. 24 (1978), pp. 106-110.

[Pre] Pretzel, O.: Codes and algebraic curves, Clarendon Press, Oxford, 1998

[StoVol] Stöhr, K., Voloch, J.F., *Weierstrass points and curves over finite field*, Proc. London Math. Soc. (3), 52 (1986) 1-9.

[Tat] Tate, J.,*Endomorphisms of Abelian Varieties over Finite Fields.* Inventiones math. 2, 134-144. 1966.

[Yui1] Yui, N., *On the Jacobian varieties of Algebraic Curves over Fields of Characteristic* $p > 2$. Uni. of Copenhagen. Math. Inst. Preprint Ser. No. 42 (1977).

[Yui2] Yui, N., *On the Jacobian varieties of Hyperelleiptic Curves over Fields of Characteristic* $p > 2$. J. of Algebra 52 (1978) 378-410.