GENUS 2 CURVES WITH COMPLEX MULTIPLICATION

EYAL Z. GOREN & KRISTIN E. LAUTER

1. Introduction

While the main goal of this paper is to give a bound on the denominators of Igusa class polynomials of genus 2 curves, our motivation is two-fold: on the one hand we are interested in applications to cryptography via the use of genus 2 curves with a prescribed number of points, and on the other hand, we are interested in construction of class invariants with a view towards explicit class field theory and Stark's conjectures. In the following we give an overview of these motivating problems and explain the contents of the paper.

Some basic protocols in public key cryptography such as key exchange and digital signatures rely on the assumption that the discrete logarithm problem in an underlying group is hard. Current available alternatives favor the use of the group of points on an elliptic curve or the Jacobian of a hyperelliptic genus 2 curve over a finite field as the underlying group. The security of the system depends on the largest prime factor of the group order, so it is crucial to be able to construct curves such that the resulting group order is prime. Also, for applications in pairing-based cryptography, it may be necessary to impose additional divisibility conditions on the group order. Parameterized families of curves satisfying these type of conditions are called pairing friendly curves. Thus algorithms to construct curves with prescribed group orders are required. Currently, typical minimum security requirements require a group size of at least 2^{256} when the best-known attacks are square-root algorithms, giving roughly 128 bits of security. Compared to elliptic curves, Jacobians of genus 2 curves are an attractive alternative because they offer comparable security levels over a field of half the bit size, since the group size of the Jacobian of a genus 2 curve over a finite field $\mathbb{F}_p$ is roughly p^2, whereas elliptic curves have group size roughly p.

In the case of elliptic curves, the polynomial-time point-counting algorithm proposed by Schoof and improved by Elkies and Atkin (or the newer Arithmetic-Geometric mean algorithm) allows the following approach: one can pick elliptic curves over a finite field of cryptographic size and count points until a prime group order is found. This solution will not work for generating pairing-friendly curves however. Also, over prime fields of cryptographic size, it will not work for hyperelliptic curves of genus greater than one, either. Starting with the work of Atkin and Morain on generating elliptic curves with a prescribed group order for primality proving, the standard approach to constructing such curves has been to use the theory of Complex Multiplication in the so-called CM method.

Given a prime number p, and a non-negative group order N lying in the Hasse-Weil interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, the goal is to produce an elliptic curve E over $\mathbb{F}_p$ with N $\mathbb{F}_p$-points: $\#E(\mathbb{F}_p) = N = p+1-t$, where t is the trace of the Frobenius endomorphism of E over $\mathbb{F}_p$. Set $D = t^2 - 4p$. The Frobenius endomorphism of E has characteristic polynomial $x^2 - tx + p$, so it

1991 *Mathematics Subject Classification.* Primary 11G15, 11G16 Secondary 11G18, 11R27.

follows from the quadratic formula that the roots of this polynomial lie in $\mathbb{Q}(\sqrt{D})$. It is standard to associate the Frobenius endomorphism with a root of this polynomial. If E is not supersingular, then R, the endomorphism ring of E, is an order in the ring of integers of $K = \mathbb{Q}(\sqrt{D})$. Now the problem is transformed into one of generating elliptic curves with endomorphism ring equal to an order in K. The correspondance between isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ with endomorphism ring equal to $\mathcal{O}_K$ and primitive, reduced, positive definite binary quadratic forms of discriminant D gives an easy way to run through all such elliptic curves.

Define the Hilbert class polynomial $H_D(X)$ associated to the field K as follows:

$$H_D(X) = \prod \left(X - j\left(\frac{-b + \sqrt{D}}{2a} \right) \right),$$

where the product ranges over the set of $(a, b) \in \mathbb{Z}^2$ such that $ax^2 + bxy + cy^2$ is a primitive, reduced, positive definite binary quadratic form of discriminant D for some $c \in \mathbb{Z}$, and j denotes the modular j-function. The degree of $H_D(X)$ is equal to h_K, the class number of K, and it is known that $H_D(X)$ has integer coefficients. To find an elliptic curve modulo p with N points over $\mathbb{F}_p$, it suffices to find a root j of $H_D(X)$ modulo p. One can then reconstruct the elliptic curve from its j-invariant j. Assuming $j \neq 0, 1728$ and $p \neq 2, 3$, the required elliptic curve is given by the Weierstrass equation $y^2 = x^3 + 3kx + 2k$, where $k = \frac{j}{1728-j}$. The number of points on the elliptic curve is either $p + 1 - t$ or $p + 1 + t$, and one can easily check which one it is by randomly picking points and checking whether they are killed by the group order.

There are at least three approaches to computing the Hilbert class polynomial. The complex analytic approach computes $H_D(X)$ as an integral polynomial by listing all the relevant binary quadratic forms, evaluating the j-function as a floating point integer with sufficient precision, and then taking the product and rounding the coefficients to nearest integers. The Chinese remainder theorem (CRT) approach computes $H_D(X) \bmod \ell$ for sufficiently many small primes ℓ and then uses the Chinese remainder theorem (CRT) to compute $H_D(X)$ as a polynomial with integer coefficients. The p-adic approach uses p-adic lifting to approximate the roots and recognize the polynomial. These algorithms are all satisfactory in practice for small D, and the current world record for the largest D for which $H_D(X)$ has been computed is held by the Explicit CRT method for some $|D| > 10^{13}$ [Sut].

The situation for generating genus 2 curves is more difficult. The moduli space of genus 2 curves is 3-dimensional and so at least 3 invariants are needed to specify a curve up to isomorphism, and, in fact, Igusa's results show that most genus curves are determined by 3 invariants. The CM algorithm for genus 2 is analogous to the Atkin-Morain CM algorithm for elliptic curves just described. But whereas the Atkin-Morain algorithm computes the Hilbert class polynomial of an imaginary quadratic field K by evaluating the modular j-invariants of all elliptic curves with CM by K, the genus 2 algorithm computes *Igusa class polynomials* of a quartic CM field K by evaluating the modular invariants of all the abelian varieties of dimension 2 with CM by K.

For a primitive quartic CM field K we can define Igusa class polynomials

$$h_i(X) = \prod_{\tau} (X - j_i(\tau)), \qquad i = 1, 2, 3,$$

in analogy with the Hilbert class polynomial for a quadratic imaginary field; they depend on the quartic CM field K, but we suppress it in the notation. The roots are CM values of Siegel modular functions, and it is known that these roots generate abelian extensions of the reflex field of K. Again in analogy with the elliptic curve case, CM values of modular functions on the Siegel upper half space can be directly related to the invariants of a binary sextic defining the genus 2

curve associated to the CM point. Note that the j-invariant of an elliptic curve can be calculated in two ways, either as the value of a modular function on a lattice defining the elliptic curve as a complex torus over $\mathbb{C}$, or directly from the coefficients of the equation defining the elliptic curve. Similarly for genus 2 curves, the triple of Igusa invariants of a genus 2 curve can also be calculated in two different ways. Using classical invariant theory over a field of characteristic zero, Clebsch defined the triple of invariants of a binary sextic f defining a genus 2 curve $y^2 = f(x)$. Bolza showed how those invariants could also be expressed in terms of theta functions on the period matrix associated to the Jacobian variety and its canonical polarization over $\mathbb{C}$. Igusa showed how these invariants could be extended to work in arbitrary characteristic, and so the invariants are often referred to as Igusa or Clebsch-Bolza-Igusa invariants. These invariants will be discussed in more detail in § 2 below. To recover the equation of a genus 2 curve given its invariants, Mestre gave an algorithm which works in most cases, and involves possibly passing to an extension of the field of definition of the invariants ([Mes]).

The CM algorithm for genus 2 curves takes as input a quartic CM field K and outputs the Igusa class polynomials with coefficients in $\mathbb{Q}$ and if desired, a suitable prime p and a genus 2 curve over $\mathbb{F}_p$ whose Jacobian has CM by K. The CM algorithm was first implemented by Spallek [Spa], van Wamelen [Wam], and Weng [Wen]. Alternative algorithms for computing Igusa class polynomials have also been proposed and studied, such as the genus 2 Explicit CRT algorithm [EL] and a p-adic approach [GHKRW].

To compute the Igusa polynomials, Spallek [Spa] determined a collection of period matrices which form a set of representatives for isomorphism classes of polarized abelian surfaces with CM by a given field. Determining this set was complicated, and a complete set of representatives in general was not determined until the recent work of Streng [Str]. In [Wen], Weng gave an algorithm for computing the minimal polynomials of Igusa invariants by evaluating Siegel modular forms to very high precision in order to recognize the coefficients of the minimal polynomials as rational numbers. Unfortunately, the polynomials $h_i(X)$ have rational coefficients, not integral coefficients, which makes them harder to recognize from floating point approximations. The large number of floating point multiplications performed in the computation causes loss of precision and makes the algorithm hard to analyze. The running time of the CM algorithm had until recently not yet been analyzed due to the fact that no bound on the denominators of the coefficients of the Igusa class polynomials was known.

Since the polynomials $h_i(X)$ have rational coefficients, we can ask about the prime factorization of the coefficients. In particular, the primes appearing in the denominators are of special interest. In [Lau], it was conjectured that primes in the denominator are bounded by the discriminant of the CM field and satisfy some additional arithmetic conditions. In fact, the primes in the denominator are primes of bad reduction for the associated curve. It was shown in [GL1] that bad reduction of a CM curve at a prime is equivalent to existence of a solution to a certain embedding problem: embedding the ring of integers of the primitive quartic CM field into the endomorphism ring of a product of supersingular elliptic curves in a way which is compatible with the Rosati involution induced by the product polarization. In [GL1], we provided bounds on the primes which can appear in the prime factorization of the denominators. In the present paper, we extend that work to provide bounds on the powers to which those primes appear, thereby proving an absolute upper bound on the size of the denominators. Our bounds have already been used in [Str] to provide a complete running time analysis of the complex analytic CM method for genus 2. The additional arithmetic conditions turn out to be equivalent to superspecial reduction of the abelian surfaces in question and so are essentially covered by [Gor], and in more generality in §3 of this paper. In related work [BY], the factorization of the denominators, when averaged over

the corresponding CM cycle, was studied and a precise conjecture was formulated. In subsequent work of Yang, the conjecture was proved for certain classes of quartic CM fields, thereby giving tight bounds on the size of the denominators in those cases. But a general bound needed for the complexity analysis has not been known until the work of the present paper.

The investigations carried out in this paper also have a completely different motivation, which comes from class field theory and Stark's conjecture. Consider the modular form that we call Θ in this paper (§2.4); it is the unique Siegel cusp form of weight 10 and full level, up to a scalar, and is equal, up to a scalar, to the product of the squares of the 10 even Riemann theta functions of integer characteristics. In many ways Θ is the analogue the elliptic cusp form Δ of weight 12. Because of this analogy, Goren and Deshalit have studied in [DSG] certain algebraic numbers constructed from values of Θ at CM points associated to a primitive quartic CM field K, whose definition parallels the definition of the Siegel units. Certain expressions in such values gave quantities $u(\mathfrak{a}, \mathfrak{b})$ associated to certain ideals in K, that depend also on the choice of CM type. These quantities lie in the Hilbert class field of the reflex field of K and have many appealing properties, such as a nice transformation law under Galois automorphism, and their dependence only on the ideal classes of $\mathfrak{a}$ and $\mathfrak{b}$. Thus, one is justified in calling them class invariants.

A natural question that arose is whether these invariants are actually units, or close to being units, in the sense that one knows their exact prime factorization, and these primes are small relative to, say, the discriminant of the field K. While we do not have complete solutions, several results concerning these have been obtained by the authors in recent years [GL1, GL2]. See also [Val] for numerical data. One of the main reasons to study such quantities is Stark's conjecture.

Recall that for a number field K and $\mathfrak{m}$, a modulus in K divisible by all the infinite primes, Stark's conjecture asserts that if $\zeta(K; \mathcal{A}, 0) = 0$ then there exists a unit $u(\mathcal{A})$ of $K[\mathfrak{m}]$ (the associated ring class field) such that

$$\zeta'(K, \mathcal{A}, 0) = \log |u(A)|,$$

where $\zeta(K; \mathcal{A}, s)$ is the partial zeta function associated to an ideal class $\mathcal{A}$ modulo $\mathfrak{m}$. In spite of much work in this area, it is fair to say that Stark's conjecture is essentially completely open. It is believed that the main obstacle is finding a "good" construction of units, and that was precisely the motivation of [DSG], although the problem of relating the class invariants $u(\mathfrak{a}, \mathfrak{b})$ to L-functions is still outstanding.

Now, as it turns out, the denominators occurring in the coefficients of the Igusa class polynomials h_i have to do with the modular form Θ as well, and essentially both questions - the nature of the denominators and the factorization of the invariants $u(\mathfrak{a}, \mathfrak{b})$ - have the same underlying geometric question, which is whether an abelian surface with CM by K, over some artinian local ring, can be isomorphic to a product of elliptic curves (with additional conditions on polarizations). The main theorem of the paper is the following.

Theorem 7.0.4. *Let $f = g/\Delta^k$ be a modular function of level one on $\mathfrak{H}_2$ where:*

1. *Δ is Igusa's χ_{10}, the product of the squares of the ten Riemann theta functions with even integral chracteristics, normalized to have Fourier coefficients that are integers and of g.c.d. 1.*
2. *g is a level one modular form of weight $10k$ with integral Fourier coefficients whose g.c.d. is 1.*

Then $f(\tau) \in L = NH_{K^*}$ *and*

$$\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq \begin{cases} -4ke\left(\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right)+1\right) & e \leq p-1 \\ -4ke\left(8\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right)+2\right) & \textit{any other case.} \end{cases} \tag{1.0.1}$$

Furthermore, unless we are in the situation of superspecial reduction, namely, we have a check mark in the last column of the tables in § 3, $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq 0$. *The valuation is normalized so that a uniformizer at* $\mathfrak{p}_L$ *has valuation* 1.

Corollaries 7.1.1, 7.1.3, of this theorem give the applications to denominators of Igusa class polynomials and class invariants described above.

In order to prove this theorem, we develop several tools that are of independent interest. The first one is an explicit determination of the reduction of abelian surfaces with complex multiplication. The main invariants of an abelian surface A over a field of characteristic $p > 0$ are its f-number, that determines the size of the étale quotient of $A[p]$, and the a-number that determines the size of the local-local part of that group scheme. These numbers determine, for example, in which Ekedahl-Oort strata the moduli point corresponding to A lies. It turns out, and that was essentially known by [Gor] and [Yu], that these numbers can be read from the prime factorization of p in the normal closure N of K over $\mathbb{Q}$ and the CM type. However, to our knowledge, a complete analysis had not appeared in the literature, and we make this analysis explicit here, dealing also with ramified primes, in a self-contained manner.

For a prime p to appear in the denominators of the h_i, or for $\mathfrak{p}|p$ to appear in the factorization of a $u(\mathfrak{a},\mathfrak{b})$, some abelian surface with CM by K must be isomorphic over $\overline{\mathbb{F}}_p$ to the product of two supersingular elliptic curves $E \times E'$. This gives $f = 0, a = 2$, and so sieves out the "evil primes" according to their factorization in N. A further, and most important condition, is imposed by the fact that the Rosati involution of $E \times E'$ must induce complex conjugation on K. We are able to translate the fact that a prime appears to a certain power in the denominators of the h_i (similarly for the $u(\mathfrak{a},\mathfrak{b})$) to the fact that a similar situation must hold over a certain artinian ring $(R,\mathfrak{m})$ and the index of nilpotency of $\mathfrak{m}$ is proportional to the power of the prime. This requires some results in intersection theory (§5) and the introduction of an auxiliary moduli space (§4).

A certain maneuver, already used in [GL1], allows us to reduce the problem to a question about endomorphisms of elliptic curves over R whose reduction modulo $\mathfrak{m}$ is supersingular. Some special instance of this problem was studied by Gross in [Grs], but his results do not suffice for our purposes. We approach this problem using crystalline deformation theory in §6; in the course of developing the results we need, we provide some more general results that are natural in that context and will, so we believe, be useful for others. Since crystalline deformation theory is only valid under certain restrictions on ramification, we provide an alternative approach that works without any restriction (§6.6) and gives results that are not too much worse than crystalline deformation theory gives.

2. Moduli of curves of genus 2

2.1. **Curves of genus two - Igusa's results.** Let y_1, y_2, y_3 be independent variables and let $y_4 = \frac{1}{4}(y_1y_3 - y_2^2)$. The group of fifth roots of unity μ_5 acts on the ring $\mathbb{Z}[\zeta_5][y_1,y_2,y_3,y_4]$ by

$[\zeta](y_i) := \zeta^i y_i$ (and trivially on the coefficients). The ring of invariants is defined over $\mathbb{Z}$ and we denote it, *by abuse of notation*,

$$\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}.$$

One of Igusa's main results [Igu1, p. 613] is that $\mathscr{M}_2$, the coarse moduli space of curves of genus 2, satisfies

$$\mathscr{M}_2 \cong \mathrm{Spec}(\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}). \tag{2.1.1}$$

This ring of invariant elements is generated over $\mathbb{Z}$ by 10 elements. We remark that outside the prime 2, namely if we work over $\mathbb{Z}[1/2]$, we can dispense with y_4 and conclude that

$$\mathscr{M}_2 \otimes \mathbb{Z}[1/2] \cong \mathrm{Spec}(\mathbb{Z}[1/2][y_1, y_2, y_3]^{\mu_5}).$$

(Same abuse of notation.) Note that to find generators over $\mathbb{Z}[1/2]$ for $\mathbb{Z}[1/2][y_1, y_2, y_3]^{\mu_5}$ amounts to finding vectors $(a, b, c) \in \mathbb{Z}^3_{\geq 0}$ such that $a + 2b + 3c \equiv 0 \pmod 5$ that generate the semigroup $\{(a, b, c) \in \mathbb{Z}^3_{\geq 0} : a + 2b + 3c \equiv 0 \pmod 5\}$ – one associate to the vector (a, b, c) the monomial $y_1^a y_2^b y_3^c$. Such generators are given by the following 8 triples:

$$\{(0, 0, 5), (0, 5, 0), (5, 0, 0), (0, 1, 1), (1, 2, 0), (3, 1, 0), (1, 0, 3), (2, 0, 1)\}. \tag{2.1.2}$$

On the other hand, given a field k of odd characteristic, to find generators for the fraction field $\mathrm{Frac}(k[y_1, y_2, y_3]^{\mu_5})$, one needs generators for the group $\{(a, b, c) \in \mathbb{Z}^3 : a + 2b + 3c \equiv 0 \pmod 5\}$, which one can choose to be the vectors $(2, -1, 0), (3, 0, -1), (5, 0, 0)$ (corresponding to the monomials $y_1^2/y_2, y_1^3/y_3, y_1^5$), for example.

Igusa's construction is based on much earlier work by Clebsch and others on invariants of sextics. A genus 2 curve is hyperelliptic, where a hyperelliptic curve is defined to be a curve which is a double cover of the projective plane. In characteristic different from 2 the situation is very much like over the complex numbers, and one can conclude that such a curve can be written as $y^2 = f(x)$, where $f(x)$ is a separable monic polynomial of degree 6, uniquely determined up to projective substitutions, thus reducing the problems of classifying genus 2 curves to studying when two sextics are equivalent under a projective transformation, or, equivalently, studying the space parameterizing unordered 6-tuples of points in $\mathbb{P}^1$.

2.2. **Igusa's coordinates.** To describe the invariants of sextics we use Igusa's notation. Let

$$y^2 = f(x) = u_0 x^6 + u_1 x^5 + \cdots + u_6,$$

be a hyperelliptic curve and let $x_1, \ldots, x_6$ be the roots of the polynomial $f(x)$. The noation (ij) is a shorthand for the expression $(x_i - x_j)$. Consider then

$$A(u) = u_0^2 \sum_{\text{fifteen}} (12)^2(34)^2(56)^2 \tag{2.2.1}$$

$$B(u) = u_0^4 \sum_{\text{ten}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \tag{2.2.2}$$

$$C(u) = u_0^6 \sum_{\text{sixty}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \tag{2.2.3}$$

$$D(u) = u_0^{10} \prod_{i<j} (ij)^2 \tag{2.2.4}$$

The subscript "fifteen" in A refers to the fact that there are 15 ways to partition 6 objects into 3 groups of 2 elements, the subscript "ten" in B refers to the fact that there are 10 ways to partition 6 objects into 2 groups of 3 elements. The subscript "sixty" refers to partitioning 6

objects into two groups and then finding a matching between these two groups: there are 10 ways to partition into 2 groups and six matching between the two chosen groups. The invariants A, B, C, D are denoted A', B', C', D' in [Mes, p. 319], but we follow Igusa's notation; these invariants are often called now the *Igusa-Clebsch invariants*. Another common notation one finds in the literature is $I_2 = A, I_4 = B, I_6 = C, I_{10} = D$, for example in the Magma help pages on February 2010, but we shall avoid using it, especially since it conflicts with Igusa notation as in [Igu4, p. 848].

The invariants A, B, C, D are homogenous polynomials of weights $2, 4, 6$ and 10, respectively, in $u_0, \ldots, u_6$, thought of as variables. In addition they are invariants of index $6, 12, 18$ and 30, respectively. This means the following: Let $f(x, z)$ be the homogenized form of f, that is,

$$f(x, z) = u_0 x^6 + u_1 x^5 z + \cdots + u_6 z^6.$$

Let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2$ and let

$$x = \alpha x' + \beta z', \qquad z = \gamma x' + \delta z'.$$

Write, by substituting these expressions for x, z, and expanding,

$$f(x, z) = u'_0 x'^6 + u'_1 x'^5 z' + \cdots + u'_6 z'^6.$$

Then, a polynomial $J = J(u_0, \ldots, u_6)$ in the variables $u_0, \ldots, u_6$ is called an *invariant of index* k if

$$J(u'_0, \ldots, u'_6) = \det(M)^k J(u_0, \ldots, u_6).$$

The terminology here is classical and follows, e.g., [Mes]. (An *invariant*, in the terminology of loc. cit, is a covariant of order 0, which means it is an expression in the coefficients of f alone, as is the case here.) An invariant of degree r of a sextic has index $3r$; cf. loc. cit. p. 314.

Note that if we let f' be the polynomial $f'(t) = u'_0 t^6 + \cdots + u'_6$ then the two hyperelliptic curves

$$C : y^2 = f(x), \qquad C' : y'^2 = f'(x),$$

are isomorphic. Indeed, the map

$$(x', y') \mapsto (x, y) := \left(\frac{ax' + b}{cx' + d}, \frac{y'}{(cx' + d)^3} \right)$$

gives an isomorphism $C' \to C$ as $(\frac{y'}{(cx'+d)^3})^2 = f(\frac{ax'+b}{cx'+d})$.

In characteristic 0, every sextic gives a vector (A, B, C, D) with $D \neq 0$ and, vice-versa, every such vector comes from a sextic. Two curves over an algebraically closed field are isomorphic if and only if one curve has invariants (A, B, C, D) and the invariants of the other curve are $(r^2 A : r^4 B : r^6 C : r^{10} D)$ for some $r \neq 0$ in the field [Igu1, Corollary, p. 632] (it would have been more natural to write the powers of r in multiple of 6, but we follow convention here). Thus, it is natural to associate to a sextic a vector $(A : B : C : D)$ in the weighted projective space $\mathbb{P}^3_{2,4,6,10}$. Similar to the case of the usual projective space $\mathbb{P}^3_{1,1,1,1}$, the complement of the hypersurface defined by $D = 0$ is affine. But, where for a usual projective space with coordinates (x_0, x_1, x_2, x_3) the affine variety is $\mathrm{Spec}(\mathbb{Q}[x_0/x_3, x_1/x_3, x_2/x_3])$, for a weighted projective space we need more functions; at the case at hand one needs 10 functions, and these will be given below in terms of the J_{2i}; every regular function on the affine variety $\mathbb{P}^3_{2,4,6,10} \setminus \{D = 0\}$ is a polynomial in these functions.

Define

$$J_2 = 2^{-3}A \qquad J_4 = 2^{-5}3^{-1}(4J_2^2 - B) \qquad J_6 = 2^{-6}3^{-2}(8J_2^3 - 160J_2J_4 - C)$$

$$J_8 = 2^{-2}(J_2J_6 - J_4^2) \qquad J_{10} = 2^{-12}D$$

A calculation shows that these invariants still make sense in characteristic 2.

Let $\mathfrak{R}$ be the ring of homogenous elements of degree zero in the graded ring generated over $\mathbb{Z}$ by $J_2, J_4, \ldots, J_{10}$ and localized at J_{10}. In fact, any absolute invariant, namely any invariant which is the quotient of two invariants of the same index, belongs to $\mathfrak{R}$ ([Igu1, Proposition 3, p. 633]). One can show that there is an isomorphism

$$\mathfrak{R} \xrightarrow{\sim} \mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5},$$

uniquely determined by

$$J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5} \mapsto y_1^{e_1}y_2^{e_2}y_3^{e_4}y_4^{e_4},$$

where the e_i are non-negative integers satisfying the relation $e_1 + 2e_2 + 3e_3 + 4e_4 = 5e_5$ and as before $y_4 = \frac{1}{4}(y_1y_3 - y_2^2)$. Igusa proceeds to show that the ring $\mathfrak{R}$ is generated by 10 elements over $\mathbb{Z}$, and by 8 elements over $\mathbb{Z}[1/2]$, and that is best possible.

Over $\mathbb{Z}$ the generators of $\mathfrak{R}$ can be taken to be the following.

$$\gamma_1 = J_2^5/J_{10} \qquad \gamma_2 = J_2^3J_4/J_{10} \qquad \gamma_3 = J_2^2J_6/J_{10} \qquad \gamma_4 = J_2J_8/J_{10} \qquad \gamma_5 = J_4J_6/J_{10}$$

$$\gamma_6 = J_4J_8^2/J_{10}^2 \qquad \gamma_7 = J_6^2J_8/J_{10}^2 \qquad \gamma_8 = J_6^5/J_{10}^3 \qquad \gamma_9 = J_6J_8^3/J_{10}^3 \qquad \gamma_{10} = J_8^5/J_{10}^4$$

(Over $\mathbb{Z}[1/2]$ a set of generators is

$$g_1 = J_2^5/J_{10} \qquad g_2 = J_2^3J_4/J_{10} \qquad g_3 = J_2J_4^2/J_{10} \qquad g_4 = J_2^2J_6/J_{10}$$

$$g_5 = J_4J_6/J_{10} \qquad g_6 = J_2J_6^3/J_{10}^2 \qquad g_7 = J_4^5/J_{10}^2 \qquad g_8 = J_6^5/J_{10}^3$$

(and the reader will recognize the exponents from (2.1.2).) We call them *the Igusa coordinates of $\mathscr{M}_2$*. Here are some consequences of these results.

(1) Let C_1, C_2, be curves over an algebraically closed field k, and write $C_i : y^2 = f_i(x)$, where $f_i(x) \in k[x]$ is a sextic. Then,

$$C_1 \cong C_2 \iff (\gamma_1(f_1), \ldots, \gamma_{10}(f_1)) = (\gamma_1(f_2), \ldots, \gamma_{10}(f_2)).$$

(2) Let C now be defined over a number field L_0, $C : y^2 = f(x), f(x) \in L_0[x]$, then C has potentially good reduction at a prime $\mathfrak{p}$ of L_0, namely, there exists a finite extension field L/L_0 and an ideal $\mathfrak{P}|\mathfrak{p}$ of L such that C has good reduction modulo $\mathfrak{P}$, if and only if

$$\mathrm{val}_{\mathfrak{p}}(\gamma_i(f)) \geq 0, \qquad i = 1, \ldots, 10.$$

(3) Let C_1, C_2, be curves over a number field L, $C_i : y^2 = f_i(x)$ as above, having good reduction at $\mathfrak{p}$. Then,

$$C_1 \pmod{\mathfrak{p}} \cong_{/\overline{\mathbb{F}}_p} C_2 \pmod{\mathfrak{p}} \iff$$
$$(\gamma_1(f_1), \ldots, \gamma_{10}(f_1)) \equiv (\gamma_1(f_2), \ldots, \gamma_{10}(f_2)) \pmod{\mathfrak{p}}.$$

2.3. **Efficacy of the absolute Igusa invariants.** The so-called *absolute Igusa invariants* are the functions

$$i_1 = A^5/D, \qquad i_2 = A^3B/D, \qquad i_3 = A^2C/D.$$

The choice of terminology is somewhat unfortunate, as it leads one to think that these invariants determine the isomorphism class of the curve; we'll discuss it further below.

Since $D = 2^{12}J_{10}$, the functions i_1, i_2, i_3, belong to $\mathfrak{R}\otimes\mathbb{Z}[1/2]$. It is a consequence of the results mentioned so far that the functions γ_j are rational functions of the functions i_j and vice-versa. This calculation is presented in the following two tables.

TABLE 2.3.1. The absolute Igusa invariants i_1, i_2, i_3 in terms of the generators γ_j

i_1	$8 \cdot \gamma_1$
i_2	$\frac{1}{2} \cdot (\gamma_1 - 24 \cdot \gamma_2)$
i_3	$\frac{1}{8} \cdot (\gamma_1 - 20 \cdot \gamma_2 - 72 \cdot \gamma_3)$

An interesting consequence of this calculation is that the natural map

$$\mathscr{M}_2 \otimes \mathbb{Z}[1/6] = \mathrm{Spec}(\mathfrak{R} \otimes [1/6]) \longrightarrow \mathrm{Spec}(\mathbb{Z}[1/6][i_1, i_2, i_3]) = \mathbb{A}^3_{\mathbb{Z}[1/6]},$$

can be inverted whenever $i_1 \neq 0$. However, given a triple (i_1, i_2, i_3), which is in the image of the map, and such that $i_1 = 0$, we find that $A = 0$ and hence also that $i_2 = i_3 = 0$. Thus, there is a unique point of $\mathbb{A}^3$, which is in the image, for which we cannot invert the map and it corresponds to all the genus 2 curves for which $A = 0$. Thus, the absolute Igusa invariants fail to completely determine the isomorphism class of the curve, but only if $i_1 = 0$.

The vanishing locus of A is a surface in $\mathscr{M}_2$. There is a natural immersion,

$$\rho : \mathscr{M}_2 \longrightarrow \mathscr{A}_{2,1},$$

of the moduli space of curves $\mathscr{M}_2$ to the moduli space of principally polarized abelian surfaces with no level structure $\mathscr{A}_{2,1}$, sending a curve to its canonically polarized Jacobian. The image is the complement of the Humbert surface H_1, which is the divisor of the modular form Θ defined below. Via this map, each of the Igusa invariants is, in a suitable sense, a pull-back via ρ of a meromorphic Siegel modular form whose polls are supported on H_1. These modular forms were calculated by Igusa [Igu3, p. 177-8] and the reader is referred to this reference for details. The invariant D is the pullback of a scalar multiple of Θ, defined in page 12. There is a modular form of weight 12, which Igusa denotes χ_{12}, such that, in a suitable sense, A is a scalar multiple of the weight 2 meromorphic form χ_{12}/Θ. We have thus, as sets,

$$\{A = 0\} = \rho^{-1}\{\chi_{12} = 0\}.$$

The modular form χ_{12} is a cusp form (see [Igu2, p. 195]). However, there does not seem to be any simple interpretation to its vanishing loci. Indeed, the results of [vdG] (see, in particular, §8 there) imply that the divisor of χ_{12} is *not* supported on a union of Humbert surfaces.

TABLE 2.3.2. The generators γ_j in terms of the absolute Igusa invariants i_1, i_2, i_3 (the last column gives the denominator)

γ_1	$2^{-3} \cdot i_1$
γ_2	$2^{-6}3^{-1} \cdot (i_1 - 16 \cdot i_2)$
γ_3	$\frac{1}{3456} \cdot (i_1 + 80 \cdot i_2 - 384 \cdot i_3)$
γ_4	$2^{-11}3^{-3} \cdot \frac{{i_1}^2+416 \cdot i_1 i_2-1536 \cdot i_1 i_3-768 \cdot {i_2}^2}{i_1}$
γ_5	$2^{-10} \cdot 3^{-4} \cdot \frac{(i_1-16 \cdot i_2)(i_1+80 \cdot i_2-384 \cdot i_3)}{i_1}$
γ_6	$2^{-25} \cdot 3^{-7} \cdot \frac{(i_1-16 \cdot i_2)\left({i_1}^2+416 \cdot i_1 i_2-1536 \cdot i_1 i_3-768 \cdot {i_2}^2\right)^2}{{i_1}^3}$
γ_7	$2^{-22} \cdot 3^{-9} \cdot \frac{(i_1+80 \cdot i_2-384 \cdot i_3)^2\left({i_1}^2+416 \cdot i_1 i_2-1536 \cdot i_1 i_3-768 \cdot {i_2}^2\right)}{{i_1}^2}$
γ_8	$2^{-29} \cdot 3^{-15} \cdot \frac{(i_1+80 \cdot i_2-384 \cdot i_3)^5}{{i_1}^2}$
γ_9	$2^{-37} \cdot 3^{-12} \cdot \frac{(i_1+80 \cdot i_2-384 \cdot i_3)\left({i_1}^2+416 \cdot i_1 i_2-1536 \cdot i_1 i_3-768 \cdot {i_2}^2\right)^3}{{i_1}^4}$
γ_{10}	$2^{-52} \cdot 3^{-15} \cdot \frac{\left({i_1}^2+416 \cdot i_1 i_2-1536 \cdot i_1 i_3-768 \cdot {i_2}^2\right)^5}{{i_1}^6}$

Proposition 2.3.1. *Let $V \subseteq \mathscr{A}_{2,1}(\mathbb{C})$ be the support of the divisor of χ_{12}. There are finitely many primitive CM points on V, that is, CM points associated to primitive CM fields of degree four.*

Proof. Let S be the collection of all primitive CM points on V. We note that the description of $\mathscr{M}_2$ implies that V is irreducible. Let C be the Zariski closure of S. If S is infinite then C is either a curve, or V itself. In either case, it follows from the André-Oort conjecture, known to be true under GRH by the work of Klinger-Yafaev [Yaf], that C is either a Shimura curve, or a Shimura surface. It remains to review the possibilities: (i) if C is a Shimura curve then every CM point on C is coming from a bi-quadratic (equivalently, non-primitive) CM field of degree 4; (ii) if $C = V$ then V is a priori in the Hecke orbit of some Humbert surfaces, but that Hecke orbit is a union of Humbert surfaces (this follows easily from the moduli interpretation). Since the Humbert surfaces in $\mathscr{A}_{2,1}$ are irreducible, V is a Humbert surface itself, which is not the case. □

2.4. **Igusa class polynomials.** In [GL1, §5.2] it was explained how the absolute Igusa invariants can also be expressed in terms of Siegel modular functions. We summarize this here for the reader's convenience.

The Igusa functions i_1, i_2, i_3 can be defined as rational functions in Siegel Eisenstein series, ψ_w, of weights $w = 4$, 6, 10, 12. To begin with, the cusp forms Θ and χ_{12}, of weights 10 and 12, introduced above can be expressed in terms of these Eisenstein series as follows ([Igu2, p.195]

and [Igu4, p. 848]):

$$-2^{-2}\Theta = \chi_{10} = \frac{-43867}{2^{12}\cdot 3^5\cdot 5^2\cdot 7\cdot 53}(\psi_4\psi_6 - \psi_{10})$$

and

$$\chi_{12} = \frac{131\cdot 593}{2^{13}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 337}(3^2\cdot 7^2\psi_4^3 + 2\cdot 5^3\psi_6^2 - 691\psi_{12}).$$

Then the *Igusa functions* i_1, i_2, i_3 can be expressed as

$$i_1 = 2\cdot 3^5\frac{\chi_{12}^5}{\chi_{10}^6},\quad i_2 = 2^{-3}\cdot 3^3\frac{\psi_4\chi_{12}^3}{\chi_{10}^4},\quad i_3 = 2^{-5}\cdot 3\frac{\psi_6\chi_{12}^2\chi_{10} + 2^2\cdot 3\psi_4\chi_{12}^3}{\chi_{10}^4}.$$

(These are often called j_1, j_2, j_3 in the literature, but we stick with Igusa's notation.)

Let K be a primitive, i.e. not biquadratic, CM field of degree 4 over $\mathbb{Q}$. We define the *Igusa class polynomials* to be:

$$h_1(x) = \prod_\tau (x - i_1(\tau)),\quad h_2(x) = \prod_\tau (x - i_2(\tau)),\quad h_3(x) = \prod_\tau (x - i_3(\tau)), \tag{2.4.1}$$

where the product is taken over all $\tau \in \mathrm{Sp}(4,\mathbb{Z})\backslash\mathfrak{H}_2$, such that the associated principally polarized abelian variety has CM by $\mathcal{O}_K$. One can define other absolute invariants, called j_1, j_2, j_3, as in [GL1, p. 473], where it is also remarked that $i_1 = 2^{-12}\mathrm{j}_1$ and $i_2 = 2^{-12}\mathrm{j}_2$, and then we define the corresponding class polynomials as follows:

$$\mathfrak{h}_i(x) = \prod_\tau (x - \mathrm{j}_i(\tau)),\qquad i = 1,2,3. \tag{2.4.2}$$

The advantage of using these is that it is clear from their definition that they satisfy the hypotheses of our Main Theorem.

2.5. **Rosenhain normal form.** While Igusa's approach to the moduli of genus 2 curves is through the study of invariants of sextics, we remark that after a finite extension of the base we may always arrange the six ramification points to contain $\{0, 1, \infty\}$ and arrive at an equation of the form

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3), \tag{2.5.1}$$

called the Rosenhain normal form of the curve C. The λ_i's are in a finite field extension of the field of definition of the curve and are determined up to the action of the stabilizer of the triple $\{0, 1, \infty\}$ in PGL_2 a group isomorphic to the symmetric group S_3 on 3 letters. If $\tau \in \mathfrak{H}_2$ is the period matrix of the polarized abelian surface $\mathrm{Jac}(C)$, then, up to projective equivalence we may take the λ_i to be

$$\lambda_1 = \frac{\Theta\begin{bmatrix}1\\1\\0\\0\end{bmatrix}(\tau)^2\,\Theta\begin{bmatrix}1\\0\\0\\0\end{bmatrix}(\tau)^2}{\Theta\begin{bmatrix}0\\1\\0\\0\end{bmatrix}(\tau)^2\,\Theta\begin{bmatrix}0\\0\\0\\0\end{bmatrix}(\tau)^2},\quad \lambda_2 = \frac{\Theta\begin{bmatrix}1\\0\\0\\1\end{bmatrix}(\tau)^2\,\Theta\begin{bmatrix}1\\1\\0\\0\end{bmatrix}(\tau)^2}{\Theta\begin{bmatrix}0\\0\\0\\1\end{bmatrix}(\tau)^2\,\Theta\begin{bmatrix}0\\1\\0\\0\end{bmatrix}(\tau)^2},\quad \lambda_3 = \frac{\Theta\begin{bmatrix}1\\0\\0\\1\end{bmatrix}(\tau)^2\,\Theta\begin{bmatrix}1\\0\\0\\0\end{bmatrix}(\tau)^2}{\Theta\begin{bmatrix}0\\0\\0\\1\end{bmatrix}(\tau)^2\,\Theta\begin{bmatrix}0\\0\\0\\0\end{bmatrix}(\tau)^2}.$$

(See [Igu2, p. 179].) Note that if C is defined over some number field and the equation (2.5.1) is over that field then the λ_i appearing there are algebraic numbers. When obtaining a triple of λ_i from the period matrix the λ_i are in fact algebraic. This is a consequence of the fact that the ratios of the theta functions appearing above are modular functions defined over $\mathbb{Q}(i)$ (say) and full level 2.

The theta functions used here are Riemann's theta functions: Let $\epsilon, \epsilon' \in \mathbb{Q}^g$, $\tau \in \mathfrak{H}_g$, and define the *Riemann theta function* with *characteristic* $\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]$ to be the power series

$$\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau) = \sum_{N\in\mathbb{Z}^g} e\left(\frac{1}{2}{}^t\left(N+\frac{\epsilon}{2}\right)\tau\left(N+\frac{\epsilon}{2}\right) + {}^t\left(N+\frac{\epsilon}{2}\right)\frac{\epsilon'}{2}\right),$$

where $e(x) = e^{2\pi i x}$. It can be shown that this series defines a holomorphic function $\mathfrak{H}_g \to \mathbb{C}$. If $\epsilon, \epsilon' \in \mathbb{Z}^g$ they are called an *integral characteristic*. If ${}^t\epsilon\epsilon' \equiv 0 \pmod 2$ they are called *even*, and else *odd*. It turns out that for an odd characteristic the theta function vanishes identically, and for even characteristic $\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)^2$ depends only on (ϵ, ϵ') modulo $\mathbb{Z}^{2g}$. For $g = 1$ this gives us 3 (squares of) theta functions and for $g = 2$ this gives us ten (squares of) even theta functions.

One can show that each $\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)$ to a large enough even power $2r$ is a Siegel modular form of weight r of some level. For $g = 1$, it goes probably to Jacobi that

$$\Delta = c \prod_{\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right] \text{ even}} \Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)^4,$$

where c is a constant and $\Delta = E_4^3 - E_6^2$ is the classical modular form of weight 12. Recall that the divisor of Δ is the cusp of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. Igusa proved for $g = 2$ that

$$\Theta := 2^{-12} \prod_{\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right] \text{ even}} \Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)^2$$

is a Siegel modular form of level $\mathrm{Sp}(4,\mathbb{Z})$ and weight 10. The factor of 2 is introduced to ensure integral Fourier coefficients with gcd 1. The divisor of Θ is precisely the Humbert divisor H_1 (with multiplicity 2). See §4.

Finally, we make some remarks as the utility of the Rosenhain normal form for generating curves of genus 2 with CM. Given a primitive CM field K, it is an easy matter to enumerate representatives for the ideal classes of K and so to get, by varying over all CM types, the period matrices whose classes modulo $\Gamma(2)$ give all the CM points of level 2 associated to this field. The modular forms used above are of level 2 and so, by evaluating them on these period matrices, we get a collection of equations $C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ defining, in particular, the isomorphism classes of all the curves of genus 2 whose Jacobians have CM by $\mathcal{O}_K$. For a *generic* period matrix $\tau \in \mathfrak{H}_2$ the $\lambda_i(\tau)$ live in a very large extension L of the field of definition, say L_0, of the curve. Let $L' = L(\sqrt{\lambda_1}, \sqrt{\lambda_2}, \sqrt{\lambda_3})$; note that $[L' : L] \le 8$. Implicit in the fact that $\lambda_i \in L$ is that all the 2-torsion of $\mathrm{Jac}(C)$ are defined over L', because under the embedding $C \to \mathrm{Jac}(C)$ (taking the point at infinity as the base point) the images of the Weierstrass points generate the 2 torsion subgroup of $\mathrm{Jac}(C)$. For a generic curve, the extension L'/L_0 has degree $\sharp\,\mathrm{Sp}(4,\mathbb{Z})/\Gamma(2) = 720$. However, in the case of complex multiplication, the field of definition of C can be taken H_{K^*}, the Hilbert class field of the reflex field, and so the λ_i generates the ray class field of conductor 2 of K^*. In fact, since $\mathrm{Sp}(4,\mathbb{Z})/\Gamma(2) \cong \mathrm{Sp}(4,\mathbb{F}_2) \cong S_6$, the symmetric group on 6 letters, and since the maximal abelian subgroups of S_6 have degrees $5, 6, 8, 9$, it follows that $[L' : L_0] | a$ for some $a \in \{5, 6, 8, 9\}$. This can be utilized to construct curves over a number fields whose Jacobians have CM.

2.6. **Ramification locus of $\mathscr{A}_{2,N}(\mathbb{C}) \to \mathscr{A}_{2,1}(\mathbb{C})$.** Let N be a positive integer. We denote by $\mathscr{A}_{2,N}$ the moduli scheme of principally polarized abelian surfaces with symplectic level N structure over $\mathrm{Spec}(\mathbb{Z}[\zeta_N, 1/N])$. $\mathscr{A}_{2,1} \otimes \mathbb{Z}[\zeta_N, 1/N]$ is the quotient of $\mathscr{A}_{2,N}$ by the finite group

$\mathrm{Sp}(4,\mathbb{Z}/N\mathbb{Z})/\{\pm I_4\}$. We denote the by $H_{\Delta,N}$ the Humbert surface of invariant Δ (a discriminant of real quadratic order) in $\mathscr{A}_{2,N}(\mathbb{C})$. It is irreducible for $N=1$, but reducible for $N>1$.

Let $N\geq 3$, so the representation $\mathrm{Aut}(A,\lambda)\to\mathrm{Aut}(A[3])$ is faithful. The ramification locus of $\pi_N:\mathscr{A}_{2,N}\to\mathscr{A}_{2,1}$ is clearly the locus of points x on $\mathscr{A}_{2,1}$ with non-trivial stabilizers, which, by the moduli interpretation, correspond to principally polarized abelian surfaces (A,λ) such that $\mathrm{rAut}(A,\lambda)\neq\{1\}$, where rAut is the reduced automorphism group (namely the automorphisms $\varphi:A\to A$ such that $\varphi^*\lambda=\lambda$, taken modulo $\{\pm 1\}$). Furthermore, in that case, any point in the fibre over x has the same ramification index, equal to the cardinality of $\mathrm{rAut}(A,\lambda)$.

We say that a component of the Humbert divisor $H_{\Delta,N}$ in $\mathscr{A}_{2,N}(\mathbb{C})$ is ramified if it is contained in the ramification locus and otherwise we say it is unramified. If every component of $H_{\Delta,N}$ is unramified then

$$\pi_N^*(H_{\Delta,1})=H_{\Delta,N}.$$

Lemma 2.6.1. *If $\Delta\neq 1,4$ every component of $H_{\Delta,N}$ is unramified. If $\Delta\in\{1,4\}$ the ramification index along each component of $H_{\Delta,N}$ is 2.*

Proof. Suppose first that Δ is not a square. In this case, every abelian variety (A,λ) parameterized by $H_{\Delta,N}$ has real multiplication by a real quadratic order of discriminant Δ and, generically, only by that order. Thus, generically, $\mathrm{Aut}(A,\lambda)=\{\pm 1\}$ (as the Rosati involution is the identity). That resolves this case.

Suppose now that Δ is a square, but $\Delta\neq 1$. Then. except of codimension one subset, the points of $H_{\Delta,N}$ correspond to curves C of genus 2 affording a map of degree Δ, $C\to E$, to an elliptic curve E, that does not factor non-trivially thorough another elliptic curve [FK].

From Igusa's classification of $\mathrm{Aut}(C)$ we deduce that there is only one 2-dimensional family of curves of genus 2 with a non-trivial reduced automorphism group. This family, as one observes, is exactly the curves C of genus 2 allowing a map of degree 2, $C\to E$, to an elliptic curve, ramified at exactly two points of E. This family is the Humbert divisor $H_{4,1}$, and in particular, we have proven the lemma for all cases but $\Delta=1$.

It is easy to see that for a generic pair of elliptic curves E_1,E_2 we have $\mathrm{Aut}(E_1\times E_2,\lambda_1\times\lambda_2)=\{(\pm 1,\pm 1)\}$. Thus, our proof is complete. □

2.7. **Existence of good models for abelian varieties with complex multiplication.** Our purpose is to prove the following lemma.

Lemma 2.7.1. *Let (A,λ) be a g-dimensional principally polarized complex abelian variety with complex multiplication by the ring of integers $\mathcal{O}_K$ of a CM field K of degree $2g$, $\iota:\mathcal{O}_K\to\mathrm{End}(A)$. Let Φ be the associated CM type and K^* the reflex field associated to K and Φ. Assume that Φ is a simple CM type. Let $\mathfrak{p}$ be a prime of K^* and R the completion of the ring of integers of K^* by $\mathfrak{p}$. Then (A,λ,ι) has a model with good reduction over an unramified extension $\mathcal{O}$ of R.*

Proof. As is well known ([Lang1, Ch. 3, Thm. 1.1]), (A,ι,λ) has a model over H_{K^*}, the Hilbert class field of K^*, corresponding to an H_{K^*}-rational point $a\in\mathscr{A}_{g,1}$. In fact, a is defined over the field of moduli M of (A,ι,λ) which is contained in H_{K^*}. Let $N\geq 3$ be an integer prime to p. Let $\tilde{a}$ be a point of $\mathscr{A}_{g,N}$ lying above a. The field of definition of the point $\tilde{a}$ is contained in $H_{K^*}(A[N])$ and is equal to the field of moduli $M[N]$ of $(A,\iota,\lambda,A[N])$, which, since the moduli scheme is a fine moduli scheme, is also the field of definition of $(A,\iota,\lambda,A[N])$.

Let $\mathscr{A}_{g,N}^\dagger$ be a smooth toroidal compactification of $\mathscr{A}_{g,N}$ over $\mathrm{Spec}(\mathbb{Z}[\zeta_N,1/N])$. It carries a semi-abelian variety X over it. Choose a prime $\mathfrak{P}$ of $M[N]$ over $\mathfrak{p}$. Since the morphism $\mathscr{A}_{g,N}^\dagger\to\mathrm{Spec}(\mathbb{Z}[\zeta_N,1/N])$ is proper, the morphism $\mathrm{Spec}(M[N]_{\mathfrak{P}})\to\mathscr{A}_{g,N}\hookrightarrow\mathscr{A}_{g,N}^\dagger$ induces by

the valuative criterion a morphism $\beta : \mathrm{Spec}(\mathcal{O}) \to \mathscr{A}^{\dagger}_{g,N}$, where $\mathcal{O}$ is the valuation ring of $M[N]_{\mathfrak{P}}$. Then $\beta^* X$ is a principally polarized semi-abelian variety over $\mathcal{O}$ whose generic fiber is $(A, \lambda) \otimes M[N]_{\mathfrak{P}}$ (ι extends automatically). As is well known, since $[K : \mathbb{Q}] = 2g > g$, the toric part of the mod $\mathfrak{P}$ reduction of $\beta^* X$ must be trivial and so $A \otimes M[N]$ has good reduction modulo $\mathfrak{P}$.

We claim that the extension $M[N]/K^*$ is unramified at $\mathfrak{p}$ and so $\mathcal{O}$ is an unramified extension of R. This follows from the main theorems of complex multiplication. In fact $M[N]$ is an abelian extension of K^* corresponding to a precisely described group of ideals and has conductor dividing N. See [Lang1], Chapter 5, Theorem 4.3 (use also Theorem 3.3). Thus, the extension $M[N]/K^*$ is unramified at $\mathfrak{p}$. □

Remark 2.7.2. In fact, using more subtle results in complex multiplication due to Shimura, one can conclude the existence of a model over H_{K^*} with good reduction at $\mathfrak{p}$. See [Gor, Proposition 2.1].

Remark 2.7.3. The abelian variety (A, ι, λ) has a model over H_{K^*}, but this model is not unique. In fact, the forms of (A, ι, λ) over H_{K^*} are classified, up to H_{K^*} isomorphism, by the Galois cohomology group $H^1(G_{H_{K^*}}, \mathrm{Aut}(A, \iota, \lambda))$, where $G_{H_{K^*}}$ is the absolute Galois group of H_{K^*} and $\mathrm{Aut}(A, \iota, \lambda)$ are the automorphisms commuting with the action of K and preserving the polarization. It is easy to see that $\mathrm{Aut}(A, \iota, \lambda)$ is equal to μ_K, the group of roots of unity lying in K. Typically this group is $\{\pm 1\}$ and the forms correspond to quadratic twists, but it may be larger. It can be μ_t for any t such that $\varphi(t)|2g$. On the other hand, with accordance with the fine moduli space property $(A, \iota, \lambda, A[N])$ has no forms as $\mathrm{Aut}((A, \iota, \lambda, A[N])) = \{1\}$ for $N \geq 3$.

3. Reduction type of abelian surfaces with complex multiplication

Our goal in this section is to study the reduction type of an abelian surface with complex multiplication by a field K modulo a prime ideal of the field of definition, lying above p, as a function of the decomposition of the prime p in K

3.1. **Combinatorics of embeddings and primes.** Let K be a number field and N its normal closure over $\mathbb{Q}$. Let G be the Galois group $\mathrm{Gal}(N/\mathbb{Q})$, acting on K by $k \mapsto g(k), g \in G$, and let $H = \mathrm{Gal}(N/K) < G$. Fix inclusions

$$\varphi_{\mathbb{C}} \colon N \to \mathbb{C}, \qquad \varphi_p \colon N \to \overline{\mathbb{Q}}_p.$$

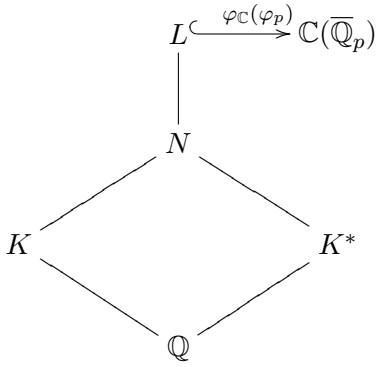
This allows us to make the following identifications:

$$\mathrm{Hom}(K, \mathbb{C}) = \varphi_{\mathbb{C}} \circ G/H, \qquad \mathrm{Hom}(K, \overline{\mathbb{Q}}_p) = \varphi_p \circ G/H,$$

where a left coset gH gives the embeddings $\varphi_{\mathbb{C}} \circ g$ and $\varphi_p \circ g$. We then have an identification

$$\mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, \overline{\mathbb{Q}}_p).$$

Let $L \supseteq N$ be a finite extension and choose an extension of $\varphi_{\mathbb{C}}, \varphi_p$ to L. We have the following diagram:



Let $\mathfrak{P}$ be the maximal ideal of $\overline{\mathbb{Q}}_p$. The choice of φ_p provides us with a prime ideal $\mathfrak{p}_{L,1} := \varphi_p^{-1}(\mathfrak{P})$ of L, and so with prime ideals $\mathfrak{p}_{N,1} = \mathfrak{p}_{L,1} \cap N$ of N and $\mathfrak{p}_{K,1} = \mathfrak{p}_{L,1} \cap K$ of K. Let D be the decomposition group of $\mathfrak{p}_{N,1}$ in N and I its inertia group. Let $e = \sharp\, I$. The primes ideals above p in N are in bijection with the cosets G/D:

$$p\mathcal{O}_N = \prod_{\alpha \in G/D} \mathfrak{p}_{N,\alpha}^e, \qquad \mathfrak{p}_{N,\alpha} = \alpha(\mathfrak{p}_{N,1}).$$

The decomposition (respectively, inertia) group of $\mathfrak{p}_{N,\alpha}$ is $D^\alpha := \alpha D \alpha^{-1}$ (respectively, $I^\alpha := \alpha I \alpha^{-1}$). The primes dividing p in K correspond to the double cosets $H\backslash G/D$. More precisely,

$$p\mathcal{O}_K = \prod_{H\alpha D \in H\backslash G/D} \mathfrak{p}_{K,\alpha}^{e(\alpha)}, \qquad \mathfrak{p}_{K,\alpha} = \alpha(\mathfrak{p}_{N,1}) \cap K,$$

where, by Lemma 3.2.1 below, $e(\alpha) = [I^\alpha : I^\alpha \cap H]$.

Let $\alpha \in G$; it induces a homomorphism $\varphi_p \circ \alpha \colon K \to \overline{\mathbb{Q}}_p$ that depends only on αH. It therefore defines a prime $(\varphi_p \circ \alpha)^{-1}(\mathfrak{P})$ of K, or more precisely $(\varphi_p|_K \circ \alpha)^{-1}(\mathfrak{P})$. We have

$$(\varphi_p|_K \circ \alpha)^{-1}(\mathfrak{P}) = (\alpha^{-1}\varphi_p|_N^{-1}(\mathfrak{P})) \cap K = \alpha^{-1}(\mathfrak{p}_{N,1}) \cap K = \mathfrak{p}_{K,\alpha^{-1}}. \tag{3.1.1}$$

That is, *the coset αH corresponding to an embedding $K \to \overline{\mathbb{Q}}_p$ induces the prime corresponding to the double coset $H\alpha^{-1}D$.* (This "inversion" is a result of our definition of $\mathfrak{p}_{N,\alpha}$ as $\alpha(\mathfrak{p}_{N,1})$, as opposed to $\alpha^{-1}(\mathfrak{p}_{N,1})$, made in order to conform with [Gor].)

Suppose that we are given a finitely generated torsion free $\mathcal{O}_L$-module M on which $\mathcal{O}_K$ acts as endomorphisms. Then $M_{\mathbb{C}} = M \otimes_{\mathcal{O}_L, \varphi_{\mathbb{C}}} \mathbb{C}$ is a finite dimensional vector space over $\mathbb{C}$, which is an $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C} = K \otimes_{\mathbb{Q}} \mathbb{C}$ module. We have then a decomposition

$$M_{\mathbb{C}} = \oplus_{\varphi \in \mathrm{Hom}(K,\mathbb{C})} M_{\mathbb{C}}(\varphi) = \mathrm{Hom}_{\alpha \in G/H} M_{\mathbb{C}}(\alpha), \tag{3.1.2}$$

where $M_{\mathbb{C}}(\varphi)$ is the eigenspace for the character $\varphi \colon K \to \mathbb{C}$, where, using the identifications $\mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, N) = G/H$, we have let $M_{\mathbb{C}}(\alpha) := M_{\mathbb{C}}(\varphi_{\mathbb{C}} \circ \alpha)$. We assume that each eigenspace is either zero or one dimensional and so we get a subset

$$\Phi \subset \mathrm{Hom}(K, N),$$

corresponding to the non-trivial eigenspaces. We call Φ a "CM type", although none of the fields appearing in our discussion so far needs to be CM.

On the other hand, we also have the finite dimensional $\overline{\mathbb{Q}}_p$-vector space $M_p := M \otimes_{\mathcal{O}_L,\varphi_p} \overline{\mathbb{Q}}_p$, grace of the homomorphism $\varphi_p\colon L \to \overline{\mathbb{Q}}_p$, which is an $\mathcal{O}_K \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}_p = K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_p$-module. Since all the homomorphisms $K \to \overline{\mathbb{Q}}_p$ factor as $K \to N \xrightarrow{\varphi_p} \overline{\mathbb{Q}}_p$, we have a decomposition, similar to the one in (3.1.2),

$$M_p = \oplus_{\varphi\in \mathrm{Hom}(K,\overline{\mathbb{Q}}_p)} M_p(\varphi) = \oplus_{\alpha\in G/H} M_p(\alpha). \tag{3.1.3}$$

Moreover, for each $\alpha \in G/H$ there is a one dimensional L-subspace $M_L(\alpha)$ of $M_L := M \otimes_{\mathcal{O}_L} L$ such that

$$M_{\mathbb{C}}(\alpha) = M_L(\alpha) \otimes_{L,\varphi_{\mathbb{C}}} \mathbb{C}, \qquad M_p(\alpha) = M_L(\alpha) \otimes_{L,\varphi_p} \overline{\mathbb{Q}}_p.$$

And so, in the obvious sense, Φ becomes a "p-adic CM type" as well.

Now, the decomposition in (3.1.3) can be packaged as follows: We have $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \oplus_{\mathfrak{p}|p} \mathcal{O}_{K_{\mathfrak{p}}}$ and thus $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_p = \oplus_{\mathfrak{p}|p}(K_{\mathfrak{p}} \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p)$, or

$$K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_p = \oplus_{\alpha\in H\backslash G/D}(K_{\mathfrak{p}_{K,\alpha}} \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p).$$

This decomposition induces a decomposition

$$M_p = \oplus_{\alpha\in H\backslash G/D} M_{p,\alpha}. \tag{3.1.4}$$

Note that, due to (3.1.1), the relation between (3.1.3) and (3.1.4) is (sic!)

$$M_p(\alpha) \subseteq M_{p,\alpha^{-1}}. \tag{3.1.5}$$

3.2. **The case of quartic fields and Dieudonné modules.** Let K be a CM field of degree four over the rational numbers and let A be a principally polarized abelian surface with complex multiplication by $\mathcal{O}_K$, CM type Φ, defined over a field L and having everywhere good reduction. Let K^* be the reflex field. We assume that L contains a normal closure N of K and let $G = \mathrm{Gal}(N/\mathbb{Q})$. Thus, our notation conforms with the one in the previous section.

Let K^+ be the totally real subfield of K. Let p be a prime number. Our purpose is to determine the reduction $\bar{A}$ of A modulo a prime ideal $\mathfrak{p}_L$ of L. It follows from results of C.-F. Yu [Yu] that the Dieudonné module of $\bar{A}$ is determined uniquely by Φ and the prime decomposition of p in K (and not just in the case of surfaces). A fortiori, the Ekedahl-Oort strata in which it falls is determined. In the case of surfaces, the complete information is contained in two numbers

$$a(\bar{A}) = \dim \mathrm{Hom}_{\overline{\mathbb{F}}_p}(\alpha_p, \bar{A} \otimes \overline{\mathbb{F}}_p), \qquad f(\bar{A}) = \log_p \sharp A[p](\overline{\mathbb{F}}_p),$$

the a-number and f-number.

We the situation more explicit that in loc. cit., and provide a self-contained proof in our case. We will have several fields to consider N, K, K^* (the reflex field determined by K and Φ), and their totally real subfields K^+ and K^{*+}, respecively. The basic information is the factorization of p in N. As above, we fix a prime ideal $\mathfrak{p} = \mathfrak{p}_{N,1} = \mathfrak{p}_L \cap N$ of N. The decomposition of p in each field is determined by the pair of subgroups (I, D), where I is the inertia group of $\mathfrak{p}$ in N and D is its decomposition group. The pair of subgroups (I, D) of $\mathrm{Gal}(N/\mathbb{Q})$ must satisfy the two restrictions:

- $I \lhd D$;
- D/I is a cyclic group.

As explained above, having chosen $\mathfrak{p}$, we may index the primes dividing p in N by coset representatives for D in G. If these coset representatives are $a, b, c, \dots$ (so $G = aD \sqcup bD \sqcup cD \sqcup \dots$) then we write $p\mathcal{O}_N = \mathfrak{p}_{N,a}^e \mathfrak{p}_{N,b}^e \mathfrak{p}_{N,c}^e \cdots$, where $e = \sharp I$ and $\mathfrak{p}_{N,a} := a(\mathfrak{p}_N)$ (and in particular, $\mathfrak{p}_{N,1} = \mathfrak{p}$). If the primes appearing in the decomposition of p in N are determined by G/D then the primes appearing in the decomposition of p in a subfield N^H of N, corresponding to a subgroup H of G, are determined by $H\backslash G/D$. As above, we shall denote such primes by $\mathfrak{p}_{N^H,x}$ where x is a representative for a double coset HxD. (This is consistent with the previous notation for $H = \{1\}$.) The following lemma is used to determine ramification in subfields.

Lemma 3.2.1. *Let $Q \subset B \subset N$ be three number fields where N/Q is Galois with Galois group G. Let B correspond to a subgroup H of G. Let $\mathfrak{p}_N$ be a prime ideal of N, $\mathfrak{p}_B = \mathfrak{p}_N \cap B$ and $\mathfrak{p}_Q = \mathfrak{p}_N \cap Q$. Let $I(\mathfrak{p}_N)$ be the inertia group in G. Then,*

$$e(\mathfrak{p}_B/\mathfrak{p}_Q) = [I(\mathfrak{p}_N) : I(\mathfrak{p}_N) \cap H]$$

and

$$e(\mathfrak{p}_N/\mathfrak{p}_B) = \sharp\, I(\mathfrak{p}_N) \cap H.$$

Proof. This is Lemma 3.3.29 in [Coh]. □

The main tool for studying the reduction $\bar{A} = A \pmod{\mathfrak{p}_L}$ of the abelian surface A is the following. Let $\mathbb{D}$ be the Dieudonné module of $\bar{A}[p]$ over $\overline{\mathbb{F}}_p$. The formalism of the previous section will be applied to the algebraic first de Rham cohomology of A/L, serving as M in the previous section, which by base change gives us the complex de Rham cohomology of A as well as the crystalline cohomology of $\bar{A}$, of which $\mathbb{D}$ is the reduction modulo p.

The a-number and f-number of $\bar{A}$ can of course be read from $\mathbb{D}$. The Dieudonné module has a decomposition relative to the $\mathcal{O}_{K^+}$ action and a refined decomposition relative to the $\mathcal{O}_K$ action. Using $\mathfrak{p}_{K^+}$ to denote a prime ideal of $\mathcal{O}_{K^+}$ above p and similarly for $\mathfrak{p}_K$, we have, by virtue of the decompositions $\mathcal{O}_{K^+} \otimes \mathbb{Z}_p = \oplus_{\mathfrak{p}_{K^+}} \mathcal{O}_{K^+,\mathfrak{p}_{K^+}}$, $\mathcal{O}_K \otimes \mathbb{Z}_p = \oplus_{\mathfrak{p}_K} \mathcal{O}_{K,\mathfrak{p}_K}$, induced decompositions

$$\mathbb{D} = \oplus_{\mathfrak{p}_{K^+}} \mathbb{D}(\mathfrak{p}_{K^+}), \qquad \mathbb{D}(\mathfrak{p}_{K^+}) = \oplus_{\mathfrak{p}_K | \mathfrak{p}_{K^+}} \mathbb{D}(\mathfrak{p}_K).$$

Here each $\mathbb{D}(\mathfrak{p}_{K^+})$ is a self-dual Dieudonné module of dimension $2e(\mathfrak{p}_{K^+}/p)f(\mathfrak{p}_{K^+}/p)$, which is then decomposed in Dieudonné modules $\mathbb{D}(\mathfrak{p}_K)$ of dimension $e(\mathfrak{p}_K/p)f(\mathfrak{p}_K/p)$. On $\mathbb{D}(\mathfrak{p}_{K^+})$ there is an action of $\mathcal{O}_{K^+,\mathfrak{p}_{K^+}} \otimes \overline{\mathbb{F}}_p \cong \oplus_\alpha \overline{\mathbb{F}}_p[t]/(t^e)$, where the summation is over embeddings α of the maximal unramified subring $\mathcal{O}^{\mathrm{ur}}_{K^+,\mathfrak{p}_{K^+}}$ of $\mathcal{O}_{K^+,\mathfrak{p}_{K^+}}$ into $W(\overline{\mathbb{F}}_p)$ and $e = e(\mathfrak{p}_{K^+}/p)$. There is a similar and compatible decomposition of $\mathcal{O}_{K,\mathfrak{p}_K} \otimes \overline{\mathbb{F}}_p$. These decompositions induce decompositions of the Dieudonné modules $\mathbb{D}(\mathfrak{p}_{K^+}), \mathbb{D}(\mathfrak{p}_K)$, such that $\mathbb{D}(\mathfrak{p}_{K^+}) = \oplus_\alpha \mathbb{D}(\mathfrak{p}_{K^+}, \alpha), \mathbb{D}(\mathfrak{p}_K) = \oplus_\alpha \mathbb{D}(\mathfrak{p}_K, \alpha)$. $\mathbb{D}(\mathfrak{p}_{K^+}, \alpha)$ is a vector space of dimension $2e(\mathfrak{p}_{K^+}/p)$, which is a free rank 2 module over $\overline{\mathbb{F}}_p[t]/(t^e)$ on which $\mathcal{O}_{K^+,\mathfrak{p}_{K^+}} = \mathcal{O}^{\mathrm{ur}}_{K^+,\mathfrak{p}_{K^+}}[\pi]$ acts via the map $\bar{\alpha} : \mathcal{O}^{\mathrm{ur}}_{K^+,\mathfrak{p}_{K^+}} \to \overline{\mathbb{F}}_p$ and π, which is an Eisenstein element, acts via t. A similar and compatible description is obtained for $\mathbb{D}(\mathfrak{p}_K, \alpha)$. Frobenius induces maps $\mathbb{D}(\mathfrak{p}_{K^+}, \alpha) \to \mathbb{D}(\mathfrak{p}_{K^+}, \sigma \circ \alpha)$.

Implicit in our considerations is the identification of $\mathrm{Hom}(K, N)$ with $\mathrm{Hom}(K, \overline{\mathbb{Q}}_p)$, where N is a normal closure of K. This identification is done as discussed in detail above. In particular, we note that the subspace $\mathbb{D}(\mathfrak{p}_K, \alpha)$ is associated with the prime ideal $\mathfrak{p}_{K,\alpha^{-1}}$. Since $H^0(\bar{A}, \Omega^1_{\bar{A},\overline{\mathbb{F}}_p}) \subset \mathbb{D}$, any $\alpha \in \Phi$ contributes 1 to the dimension of the kernel of Frobenius on $\mathbb{D}(\mathfrak{p}_{K,\alpha^{-1}})$. This often allows us to conclude that $\mathrm{Fr}^2 = 0$ on $\mathbb{D}$, which implies $a = 2, f = 0$ and, so, superspecial reduction.

TABLE 3.3.1. Reduction in the cyclic case.

	I	D	decomposition of p in $K=K^*$	decomposition of p in K^+	a	f	super-special?
i	$\{1\}$	$\{1\}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,g}\mathfrak{p}_{K,g^2}\mathfrak{p}_{K,g^3}$	$\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,g}$	0	2	×
ii	$\{1\}$	$\{1,g^2\}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,g}$	$\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,g}$	2	0	√
iii	$\{1\}$	G	$\mathfrak{p}_{K,1}$	$\mathfrak{p}_{K^+,1}$	1	0	×
iv	$\{1,g^2\}$	$\{1,g^2\}$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,g}^2$	$\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,g}$	2	0	√
v	$\{1,g^2\}$	G	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K^+,1}$	2	0	√
vi	G	G	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K^+,1}^2$	2	0	√

Another useful tool to quickly decide some properties of the reduction is the following relation. Let K^* be the reflex field defined by the CM type of the abelian variety under consideration and let Φ^* be the reflex type. Let $\mathfrak{p}_{K^*,1}=\mathfrak{p}_{N,1}\cap K^*$. Then some power of $\mathrm{Norm}_{\Phi^*}(\mathfrak{p}_{K^*,1})$ is equal to a power of Fr, viewed as endomorphisms of the reduction. One can be more precise (see [Lang1]), but we note that this suffices to calculate the f-number of the reduction.

3.3. K **cyclic Galois.** In this case $K=N=K^*$. The Galois group is cyclic of order 4, generated by g, say, where g^2 is complex conjugation. The CM types are either $\{1,g\},\{g,g^2\},\{g^2,g^3\}$ or $\{g^3,1\}$. Since the reduction type does not depend on the way K is embedded in A, namely we can compose with an automorphism $K\to K$, we may assume that the CM type is $\{1,g\}$. The reflex CM field K^* is K and $\Phi^*=\{1,g^{-1}\}$. We have the following possibilities.

The unramified case appears in [Gor], but we shall do one case to illustrate our method. Consider the case ii. We have a decomposition

$$\mathbb{D}=\mathbb{D}(\mathfrak{p}_{K^+,1})\oplus\mathbb{D}(\mathfrak{p}_{K^+,g}),$$

and $\mathbb{D}(\mathfrak{p}_{K^+,i})$, $i=1,g$, is a two dimensional $\overline{\mathbb{F}}_p$-vector space that does not decompose further relative to the $\mathcal{O}_{K^+}$ action. However, $\mathbb{D}(\mathfrak{p}_{K^+,i})=\mathbb{D}(\mathfrak{p}_{K,i})$, because $\mathfrak{p}_{K^+,i}$ is inert in K, and

$$\mathbb{D}(\mathfrak{p}_{K,i})=\mathbb{D}(\mathfrak{p}_{K,i},\alpha)\oplus\mathbb{D}(\mathfrak{p}_{K,i},\sigma\circ\alpha).$$

Frobenius takes $\mathbb{D}(\mathfrak{p}_{K,i},\alpha)$ to $\mathbb{D}(\mathfrak{p}_{K,i},\sigma\circ\alpha)$, and vice-versa. The CM type is $\{1,g\}$ and we note that g switches $\mathfrak{p}_{K,1}$ and $\mathfrak{p}_{K,g}$. This means that the cotangent space, or rather $H^0(A,\Omega^1_{A/\overline{\mathbb{F}}_p})\otimes_{\overline{\mathbb{F}}_p,\sigma}\overline{\mathbb{F}}_p=\mathbb{D}(\mathrm{Ker\ Fr})$, which is an $\mathcal{O}_K$-module, is not contained completely in any of $\mathbb{D}(\mathfrak{p}_{K,i})$. Thus, Frobenius has a kernel on each of $\mathbb{D}(\mathfrak{p}_{K,i})$. It follows that Fr^2 is zero on each $\mathbb{D}(\mathfrak{p}_{K,i})$ and hence on $\mathbb{D}$ and that implies that $a(\bar{A})=2$, by a well known and elementary argument and $f(\bar{A})=0$.

In case iv we again have

$$\mathbb{D}=\mathbb{D}(\mathfrak{p}_{K^+,1})\oplus\mathbb{D}(\mathfrak{p}_{K^+,g}),$$

and $\mathbb{D}(\mathfrak{p}_{K^+,i})$ is a two dimensional $\overline{\mathbb{F}}_p$-vector space that does not decompose further relative to the $\mathcal{O}_{K^+}$ action. However, $\mathbb{D}(\mathfrak{p}_{K^+,i})=\mathbb{D}(\mathfrak{p}_{K,i})$ and $\mathbb{D}(\mathfrak{p}_{K,i})$ becomes a rank 1 module over $\overline{\mathbb{F}}_p[t]/(t^2)$ by using the $\mathcal{O}_K$ action and Frobenius is a module homomorphism. Once more, since g permutes $\mathfrak{p}_{K^+,1}$ and $\mathfrak{p}_{K^+,g}$, it follows that Frobenius has a kernel on each of $\mathbb{D}(\mathfrak{p}_{K^+,i})$ and since the dimension of the kernel of Frobenius is two, it follows that the kernel Frobenius must be $(t)\oplus(t)\subset D(\mathfrak{p}_{K,1})\oplus D(\mathfrak{p}_{K,g})$ and $\mathrm{Fr}^2=0$.

In case v, after a similar analysis we reach the conclusion that $\mathbb{D}=\overline{\mathbb{F}}_p[t]/(t^2)\oplus\overline{\mathbb{F}}_p[t]/(t^2)$ and that Frobenius, which commutes with the $\overline{\mathbb{F}}_p[t]/(t^2)$ structure, permutes the components. Whether the kernel of Frobenius is one of the components, or the submodule $(t)\oplus(t)$, we have

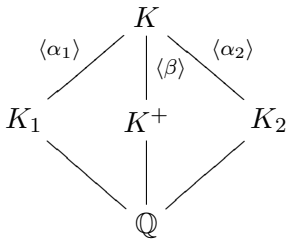
TABLE 3.4.1. Reduction in the bi-quadratic case.

	I	D	decomposition of p in $K = K^*$	decomposition of p in K^+	a	f	super-special?
i	$\{1\}$	$\{1\}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}\mathfrak{p}_{K,\beta}\mathfrak{p}_{K,\alpha_2}$	$\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,\alpha_1}$	0	2	×
ii	$\{1\}$	$\{1,\alpha_1\}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,\beta}$	$\mathfrak{p}_{K^+,1}$	0	2	×
iii	$\{1\}$	$\{1,\beta\}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}$	$\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,\alpha_1}$	2	0	√
iv	$\{1\}$	$\{1,\alpha_2\}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,\beta}$	$\mathfrak{p}_{K^+,1}$	2	0	√
v	$\{1,\alpha_1\}$	$\{1,\alpha_1\}$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,\beta}^2$	$\mathfrak{p}_{K^+,1}^2$	0	2	×
vi	$\{1,\alpha_1\}$	G	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K^+,1}^2$	2	0	√
vii	$\{1,\beta\}$	$\{1,\beta\}$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,\alpha_1}^2$	$\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,\alpha_1}$	2	0	√
viii	$\{1,\beta\}$	G	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K^+,1}$	2	0	√
ix	$\{1,\alpha_2\}$	$\{1,\alpha_2\}$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,\beta}^2$	$\mathfrak{p}_{K^+,1}^2$	2	0	√
x	$\{1,\alpha_2\}$	G	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K^+,1}^2$	2	0	√
xi	G	G	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K^+,1}^2$	2	0	√

$\mathrm{Fr}^2 = 0$ (in fact, taking into consideration the CM type we must have the kernel is $(t) \oplus (t)$, but this is not important at present).

In case vi we conclude that $\mathbb{D} = \overline{\mathbb{F}}_p[t]/(t^4)$ and that Frobenius acts as a $\overline{\mathbb{F}}_p[t]/(t^4)$-module homomorphism. It follows that the kernel of Frobenius, being an $\overline{\mathbb{F}}_p[t]/(t^4)$-module is (t^2) and so is the image. Hence $\mathrm{Fr}^2 = 0$ again.

3.4. K **biquadratic.** In this case $K = N$ is the compositum K_1K_2 where K_i are quadratic imaginary fields. Let K^+ be the totally real subfield of K. Write the Galois group is $\{1, \alpha_1, \alpha_2, \beta\}$ where K_i is fixed by α_i and β is complex conjugation. We have the following diagram:



The possible CM types are $\{1, \alpha_i\}, \{\beta, \alpha_i\}$ and twisting the action of $\mathcal{O}_K$ by an automorphism we may assume the CM type is $\{1, \alpha_1\}$ or $\{1, \alpha_2\}$. The situation being symmetric we assume w.l.o.g that the CM type is $\{1, \alpha_1\}$. The reflex CM field is K_1 and the reflex CM type is $\{1\}$. In this case A is isogenous to $E \otimes_{\mathbb{Z}} \mathcal{O}_L$, or equivalently to $E \otimes_{K_1} K$, where E is an elliptic curve with CM by $\mathcal{O}_{K_1}$. Thus, $\bar{A}$ is ordinary if p is split in K_1 and supersingular otherwise (and in that case one still needs to figure out its a number). Now, p is split in K_1 if and only if $\langle D, \alpha_1 \rangle \neq G$.

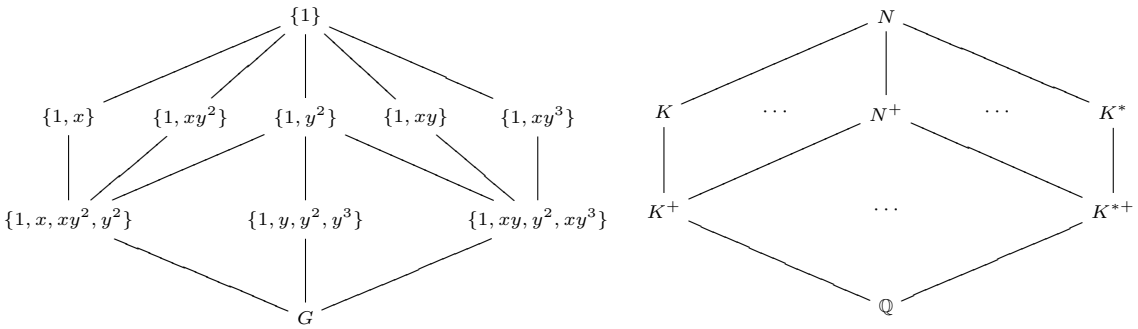
Consider for example case vi. After the usual analysis we find that $\mathbb{D} \cong \overline{\mathbb{F}}_p[t]/(t^2) \oplus \overline{\mathbb{F}}_p[t]/(t^2)$, where Fr is $\overline{\mathbb{F}}_p[t]/(t^2)$ σ-linear and switches the components. Its kernel is then either one of the components, or the submodule $(t) \oplus (t)$. In any case, $\mathrm{Fr}^2 = 0$ and so $a = 2$. Cases vii, viii and x lead exactly to the same setting.

In case ix, once again $\mathbb{D} \cong \overline{\mathbb{F}}_p[t]/(t^2) \oplus \overline{\mathbb{F}}_p[t]/(t^2)$ but now Fr acts on each component separately. $\bar{A}$ is ordinary if the kernel of Fr is one of the components and is superspecial if the kernel is $(t) \oplus (t)$. Since ordinary is not possible, because p is inert in K_1 (or, we can argue by using the CM type that Frobenius has a kernel on each component), we are in the superspecial case.

In case xi we find that $\mathbb{D} \cong \overline{\mathbb{F}}_p[t]/(t^4)$ and we must have that the kernel of Frobenius is the submodule (t^2). It follows that $\mathrm{Fr}^2 = 0$.

3.5. K **non-Galois.** In this case the normal closure of K is a Galois extension $N/\mathbb{Q}$ of degree 8 and Galois group D_4. As above, we view N as embedded in $\mathbb{C}$. K is the fixed field of a non-central involution we call x. Let y be an element of order 4, then y^2 is complex conjugation and $xyx = y^{-1} = y^3$. We identify $\mathrm{Hom}(K, \mathbb{C})$ with $\{1, y, y^2, y^3\}$ and the CM types are $\{1, y\}, \{y^2, y^3\}, \{1, y^3\}$ and $\{y^2, y^3\}$. We may twist the action of K by complex conjugation and so assume that the CM type is $\{1, y\}$ or $\{1, y^3\}$. If it is $\{1, y^{-1}\}$ we can change the presentation of our group by using the generator y^{-1} instead of y. We can therefore assume that K is fixed by x, the Galois group is $\langle x, y | x^2, y^4, xyxy\rangle$ and the CM type is $\{1, y\}$. The reflex CM field K^* is then fixed by $\{1, xy^3\}$ (follow the recipe in [Lang1, Ch. 1, Theorem 5.1]) and the reflex CM type is $\{1, y^{-1}\}$.

We have the following diagrams of fields and subgroups:



The analysis of the reduction of A proceeds along the same lines as above. Namely, one considers the decomposition of the Dieudonné module as a module over $\mathcal{O}_K \otimes \overline{\mathbb{F}}_p$ and the induced action of Frobenius, which is $1 \otimes \sigma$-linear, so to say. In most cases, this suffices to determine the a and f numbers, but in certain cases one needs to decide between two possibilities, and there the CM type matters. The interpretation of the CM type mod p is done through the formalism of §3.1.

For example, referring to the table, in case viii we find that $\mathbb{D} \cong \overline{\mathbb{F}}_p[t]/(t^2) \oplus \overline{\mathbb{F}}_p[t]/(t^2)$ and Frobenius acts σ-$\overline{\mathbb{F}}_p[t]/(t^2)$ linearly (meaning, it acts σ-linearly on $\overline{\mathbb{F}}_p$ and commutes with t) on each component. The kernel, a-priori could be one of the components or the submodule $(t) \oplus (t)$. Taking the CM type into consideration, we see that Frobenius has a kernel in each component and so its kernel is $(t) \oplus (t)$. It follows that $\mathrm{Fr}^2 = 0$. Case x is the same.

Case ix is easier as in this case $\mathbb{D} \cong \overline{\mathbb{F}}_p[t]/(t^2) \oplus \overline{\mathbb{F}}_p[t]/(t^2)$, where Fr is acting σ-$\overline{\mathbb{F}}_p$-linearly, but permutes the components. The kernel is either one of the components or the submodule $(t) \oplus (t)$ and, regardless, $\mathrm{Fr}^2 = 0$. Case xi is the same.

TABLE 3.5.1. Reduction in the non Galois case.

	I	D	decomposition of p in N	decomposition of p in K	decomposition of p in K^+	decomposition of p in K^*	decomposition of p in K^{*+}	$N_{\Phi^*}(\mathfrak{p}_{K^*,1})$	a	f	ss?
i	$\{1\}$	$\{1\}$	$\prod_{\alpha\in G}\mathfrak{p}_{N,\alpha}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^2}\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^2}\mathfrak{p}_{K^*,y^3}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	0	2	$\times$
ii	$\{1\}$	$\langle x\rangle$	$\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y^2}$	$\mathfrak{p}_{K^*+,1}$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}$	1	1	$\times$
iii	$\{1\}$	$\langle xy\rangle$	$\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{K+,1}$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^3}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	p	2	0	$\surd$
iv	$\{1\}$	$\langle xy^2\rangle$	$\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}$	$\mathfrak{p}_{K^*+,1}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}^2$	1	1	$\times$
v	$\{1\}$	$\langle xy^3\rangle$	$\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{K+,1}$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^2}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	$\mathfrak{p}_{K,1}^2$	0	2	$\times$
vi	$\{1\}$	$\langle y^2\rangle$	$\mathfrak{p}_{N,1}\mathfrak{p}_{N,x}\mathfrak{p}_{N,y}\mathfrak{p}_{N,xy}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	p	2	0	$\surd$
vii	$\{1\}$	$\langle y\rangle$	$\mathfrak{p}_{N,1}\mathfrak{p}_{N,x}$	$\mathfrak{p}_{K,1}$	$\mathfrak{p}_{K+,1}$	$\mathfrak{p}_{K^*,1}$	$\mathfrak{p}_{K^*+,1}$	p^2	1	0	$\times$
viii	$\langle y^2\rangle$	$\langle y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,x}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,xy}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y}^2$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	2	0	$\surd$
ix	$\langle y^2\rangle$	$\langle y\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,x}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K+,1}$	$\mathfrak{p}_{K^*,1}^2$	$\mathfrak{p}_{K^*+,1}$	p	2	0	$\surd$
x	$\langle y^2\rangle$	$\langle x,y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^2$	$\mathfrak{p}_{K^*+,1}$	p	2	0	$\surd$
xi	$\langle y^2\rangle$	$\langle xy,y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K+,1}$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y}^2$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	p	2	0	$\surd$
xii	$\langle x\rangle$	$\langle x\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y^2}^2$	$\mathfrak{p}_{K^*+,1}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	1	1	$\times$
xiii	$\langle x\rangle$	$\langle x,y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^2$	$\mathfrak{p}_{K^*+,1}^2$	p	2	0	$\surd$
xiv	$\langle xy^2\rangle$	$\langle xy^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y}^2$	$\mathfrak{p}_{K^*+,1}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}\triangle$	1	1	$\times$
xv	$\langle xy^2\rangle$	$\langle x,y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^2$	$\mathfrak{p}_{K^*+,1}^2$	p	2	0	$\surd$
xvi	$\langle xy\rangle$	$\langle xy\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y^3}^2$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^3}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}\triangle$	2	0	$\surd$
xvii	$\langle xy\rangle$	$\langle xy,y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K*,y}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	p	2	0	$\surd$
xviii	$\langle xy^3\rangle$	$\langle xy^3\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}^2\mathfrak{p}_{K^*,y^2}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	$\mathfrak{p}_{K,1}^2\triangle$	2	0	$\surd$
xix	$\langle xy\rangle$	$\langle xy,y^2\rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y}$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	p	2	0	$\surd$
xx	$\langle y\rangle$	$\langle y\rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,x}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^4$	$\mathfrak{p}_{K^*+,1}^2$	$\mathfrak{p}_{K,1}^2$	2	0	$\surd$
xxi	$\langle y\rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^4$	$\mathfrak{p}_{K^*+,1}^2$	p	2	0	$\surd$
xxii	$\langle x,y^2\rangle$	$\langle x,y^2\rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{K+,1}\mathfrak{p}_{K+,y}$	$\mathfrak{p}_{K^*,1}^4$	$\mathfrak{p}_{K^*+,1}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	2	0	$\surd$
xxiii	$\langle x,y^2\rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{K+,1}$	$\mathfrak{p}_{K^*,1}^4$	$\mathfrak{p}_{K^*+,1}^2$	p	2	0	$\surd$
xxiv	$\langle xy,y^2\rangle$	$\langle xy,y^2\rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^2\mathfrak{p}_{K^*,y}^2$	$\mathfrak{p}_{K^*+,1}\mathfrak{p}_{K^*+,y}$	$\mathfrak{p}_{K,1}^2$	2	0	$\surd$
xxv	$\langle xy,y^2\rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^2$	$\mathfrak{p}_{K^*+,1}$	p	2	0	$\surd$
xxvi	G	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{K+,1}^2$	$\mathfrak{p}_{K^*,1}^4$	$\mathfrak{p}_{K^*+,1}^2$	p	2	0	$\surd$

3.6. **Examples.** Take a curve C of genus 2 over $\mathbb{Q}$ (to simplify). Given a prime p at which C has good reduction $\bar{C}$, one has a simple method of writing down the Hasse Witt matrix M of $\bar{A} = Jac(\bar{C})$ and so deciding the a number and f number of $\bar{A}$: The f number is the rank of $M^{(p)}M$ and the a-number is the co-rank of M. In general it is hard to decide the reduction type by examining M, but in certain cases we can do that and compare our results with the results above when $A = \mathrm{Jac}(C)$ has complex multiplication.

Let $C : y^2 = f(x)$, where $f(x) = x^5 + a_4x^4 + \cdots + a_0$ be a hyperelliptic curve and write

$$f(x)^{(p-1)/2} = \sum_{j\geq 0} c_j x^j.$$

Then the Hasse-Witt matrix M is given by

$$\begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix},$$

and $M^{(p)}$ is

$$\begin{pmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{pmatrix}.$$

Exactly the same recipe works if $f(x)$ is a sextic. See [IKO, p. 129]

3.6.1. Let $C : y^2 = x^5 + 1$. The curve has good reduction outside $2 \cdot 5$. The Jacobian has complex multiplication by $\mathbb{Q}(\zeta_5)$ and the automorphism group of the curve in characteristic zero is μ_{10}. The coefficient of x^n in $f(x)^{(p-1)/2}$ is 0 if $5 \nmid n$ and, for n not larger than $5(p-1)/2$ such that $5|n$, is $\binom{(p-1)/2}{n/5}$. We divide the analysis to several cases:

- If $p \equiv 1 \pmod 5$, $M = \begin{pmatrix} \binom{(p-1)/2}{(p-1)/5} & 0 \\ 0 & \binom{(p-1)/2}{(2p-2)/5} \end{pmatrix}$ has rank 2 and we conclude that $\bar{A}$ is ordinary. Note that p splits completely in this case. Namely we are in case i of the cyclic Galois case.
- If $p \equiv 2 \pmod 5, p > 2$, $M = \begin{pmatrix} 0 & \binom{(p-1)/2}{(p-2)/5} \\ 0 & 0 \end{pmatrix}$ has rank 1 and $M^{(p)}M = 0$. Thus, $f = 0$ and $a = 1$. This is a supersingular, but not superspecial reduction, in accordance to case iii.
- If $p \equiv 3 \pmod 5$, $M = \begin{pmatrix} 0 & 0 \\ \binom{(p-1)/2}{(2p-1)/5} & 0 \end{pmatrix}$ has rank 1 and $M^{(p)}M = 0$. Thus, $f = 0$ and $a = 1$. This is a supersingular, but not superspecial reduction, in accordance to case iii again.
- If $p \equiv -1 \pmod 5$, $M = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ has rank 0 and we have superspecial reduction, in accordance with case ii.
- $p = 5$. It follows from Igusa's classification of genus 2 curves with many automorphisms [Igu1, §8] that the reduction of a stable model of $y^2 = x^5 + 1$ modulo 5 is isomorphic, possibly after base change, to the curve $y^2 = f(x)$, where $f(x) = x(x-1)(x+1)(x-2)(x+2)$. That is, since the characteristic is 5, $f(x) = x^5 - x$. Then $f(x)^2 = x^{10} - 2x^6 + x^2$ and the Hasse-Witt matrix is the zero matrix, giving us superspecial reduction. This agrees with case v.
- In characteristic 2, Igusa's classification gives us the model $y^2 - y = x^5$. According to our table, since we are in case iii, this curve should be supersingular, but not superspecial. The fact that the curve is supersingular, which in genus 2 is equivalent to $f = 0$, follows from the theory of Artin-Schreier coverings, c.f. [PZ, Lemma 2.6]. According to [IKO, Theorem 3.3] there are no superspecial non-singular curves of genus 2 in characteristic 2. Therefore, we have supersingular and not superspecial reduction.

3.6.2. Consider the curve $y^2 = -8x^6 - 64x^5 + 1120x^4 + 4760x^3 - 48400x^2 + 22627x - 91839$, which has complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-65 + 26\sqrt{5}})$ by [Wam]. The field is a cyclic Galois extension with a totally real field $K^+ = \mathbb{Q}(\sqrt{5})$. Its discriminant is $5^3 \cdot 13^2$. The prime 5 decomposes as $\mathfrak{p}_{K^+}^2 = \mathfrak{p}_K^4$ and belongs to case vi, the prime 13 decomposes as $\mathfrak{q}_{K^+} = \mathfrak{q}_K^2$ and belongs to case v. In any case, we have superspecial reduction. And, indeed, in both cases one finds that the Hasse-Witt matrix is identically zero modulo the corresponding prime. For example, for $p = 5$ we have $f(x)^2 = 64x^{12} + 1024x^{11} - 13824x^{10} - 219520x^9 + 1419520x^8 + 16495568x^7 - 87185232x^6 - 398328128x^5 + 2352249680x^4 - 3064600880x^3 + 9401996329x^2 - 4156082106x + 8434401921$ and the Hasse-Witt matrix is $\left(\begin{smallmatrix} 2352249680 & -3064600880 \\ -219520 & 1419520 \end{smallmatrix}\right) \equiv 0 \pmod 5$.

3.6.3. *Cases (v) and (vi) in Table 3.3.1 for Galois cyclic fields.* Examples 1 and 2 below demonstrate cases (v) and (vi) in the table for Galois cyclic fields. For both, we take the Galois cyclic field $K = \mathbb{Q}[x]/(x^4 + 238x^2 + 833)$, with real quadratic subfield $\mathbb{Q}(\sqrt{17})$. It can be constructed by adjoining $\sqrt{-119 + 28\sqrt{17}}$ to $\mathbb{Q}$. The class number of K is 2 and the field discriminant is $7^2 17^3$.

The three Igusa Class polynomials are:

$$h_1(x) = x^2 + \frac{3^{16} \cdot 11 \cdot 163 \cdot 4801 \cdot 712465984819 \cdot 1521601757530149022573056491434222390219848955 43}{2^{23} \cdot 7^6 \cdot 43^{12} \cdot 179^{12}} x - \frac{3^{30} \cdot 62273^5 \cdot 173166943^5}{2^{22} \cdot 7^{12} \cdot 43^{12} \cdot 179^{12}}$$

$$h_2(x) = x^2 + \frac{3^{11} \cdot 5 \cdot 967 \cdot 19976366524956829638494908885597306960507 3}{2^9 \cdot 7^3 \cdot 43^8 \cdot 179^8} x - \frac{3^{22} \cdot 5^2 \cdot 19^2 \cdot 191 \cdot 62273^3 \cdot 173166943^3}{2^6 \cdot 7^8 \cdot 43^8 \cdot 179^8}$$

$$h_3(x) = x^2 + \frac{3^9 \cdot 1823 \cdot 819734099639522362577121888804614972466874 9}{2^{11} \cdot 7^3 \cdot 43^8 \cdot 179^8} x - \frac{3^{18} \cdot 359 \cdot 1667 \cdot 1811 \cdot 228122997426508267522036684197215571753 7}{2^{10} \cdot 7^8 \cdot 43^8 \cdot 179^8}$$

Example 1 (Case v) The prime 7 decomposes in K as the square of an inert prime with inertia degree 2. Modulo 7 the class polynomials reduce badly, since 7 is in the denominator. The two CM curves each reduce to a product of elliptic curves with product polarization modulo 7, and the Galois action takes one curve to the other. Both have superspecial reduction.

Example 2 (Case vi) The prime 17 is totally ramified in K. Modulo 17 the reduction of the Igusa class polynomials is:

$$h_1(x) = (x + 13)^2 \pmod{17}, \quad h_2(x) = (x + 12)^2 \pmod{17}, \quad h_3(x) = (x + 2)^2 \pmod{17}.$$

Taking the absolute Igusa invariants $[i_1, i_2, i_3] = [-13, -12, -2]$ modulo 17, we recover a 4-tuple of Igusa-Clebsch invariants $[I_2, I_4, I_6, I_{10}] = [1, 14, 8, 13]$ via the formulas: $I_2 = 1$, $I_{10} = I_2^5/i_1$, $I_4 = i_2 \cdot I_{10}/I_2^3$, $I_6 = i_3 \cdot I_{10}/I_2^2$. Using Magma's implementation of Mestre's algorithm, we obtain a genus 2 curve $C : y^2 = x^6 + 16$ with these invariants over $\mathbb{F}_{17}$. Taking $f(x) = x^6 + 16 \pmod{17}$, we compute the $(p-1)/2 = 8^{th}$ power and compute the Hasse-Witt matrix. The only non-zero coefficients of f are for terms whose degree is 0 (mod 6), so the Hasse-Witt Matrix is zero and the reduction is superspecial.

3.6.4. *Cases (xii), (xiv), (xvii) and (xix) in Table 3.5.1 for non-Galois fields.* In Examples 3 and 4 below we deal with cases (xii) and (xiv) (Example 4) and cases (xvii) and (xix) (Example 3) in the table for non-Galois fields. We work with a non-Galois quartic CM field, given by $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ with reflex field given by $K^* = \mathbb{Q}[x]/(x^4 + 268x^2 + 17600)$. The class number of K is 4 and the discriminant is $2^4 11^2 89$.

For typographical reasons we list the class polynomials in modified form. To get the class polynomials $h_i(x)$ from the polynomials $h_i^*(x)$ listed below, divide by the leading coefficient in each case.

$$
\begin{aligned}
h_1^* = {} & 467861685000827419831582500859570065480089664861245464225306306576334606367462143339253088925033807754516601562 5 \cdot x^8 + \\
& 55544914984551752820183085463077470228846020683654003234780668955704468066812106738036411695702554425224661827087402343750000 0 \cdot x^7 + \\
& 18403368676473300391621439332312217593072665716535882120977793742786451616170252466041678857284459287923047251104058697819709777832031250000000 \cdot x^6 - \\
& 18532528196713610966248735059989496921744294218655209931046129134295796866360219594850246272816241093321185745310256539534492913064849853515625000000000 \cdot x^5 - \\
& 14951761577386221607707550178552615664390163794144774072964515539112873485 \\
& 17794686579946784109717502195174755425822553736877872571144391143148905722300000000000 \cdot x^4 - \\
& 27450021278778632036317492245198741865628889556425416852671533372575037558 5 \\
& 56384959106460164764658831329000379776543259072657572814515177392240269322428312127339426217984 \cdot x^3 - \\
& 1297531069082446204942804872389223658522300816123923232354502537340424218996 55 \\
& 80593001771951508989819214516847958284764562224480102456678890713123681109259524813544942909521920000 0 \cdot x^2 + \\
& 75816198120430164253210000030177809833640567679756337667150872417366816696541 \\
& 96164395918854519565530006696018114343272004390698210911241524053337213250547824282545177808076800000000000 \cdot x - \\
& 16656107625921887452438039161862781245920062995237772854060296102410270027835 2 \\
& 47550412464024850182603102460369557884286225502239544621426526599134047332382519936843117913702400000000000000000 0 \\
\\
h_2^* = {} & 12262099322453399085426697957216858990040719509124755855937500 00 \cdot x^8 + \\
& 74859292699910714365190193192134728726759194326538186885028839111328125000 00 \cdot x^7 + \\
& 12791159057342942976406125242262664790963503623354664862360417676311258231837768554687500 0 \cdot x^6 - \\
& 43280146930239897012056393411434863079486256354344323252772261688698955439431510858034378897460937 50 \cdot x^5 - \\
& 70989757220371345897539040783507004210240989969604889311893737913941059181926255577325566490374971604296562 5 \cdot x^4 + \\
& 14121458395374925874619003891297821593782870891378302331148263540097878729488802928890913822935905126587220991510912 \cdot x^3 - \\
& 32473097442534731491748805085721565503853990994944181119931887975608935788334464574063164679998777171297279904405132800 00 \cdot x^2 + \\
& 28782588004841469734963132748357993072457690496417175213541663608846266436741262222738002055112157673052941309023744000000000 \cdot x - \\
& 875776675051081603171574386294121650913389467088993679908740136586915776656894551107952370791602330470602373237659904000000000000
\end{aligned}
$$

$$
\begin{aligned}
h_3^* = {} & 313909742654807016586923467704751590145042419433593750000000000000 \cdot x^8 + \\
& 49334832389339251232218788220183648065719090972122115456623535156250000000000 \cdot x^7 + \\
& 21684439654189899860384926880674030457109419610359893724091288770677724553115234375000000 \cdot x^6 - \\
& 2302525585957788818152082352653829396337430793844914883168947610481921539535736987830563608984375000 \cdot x^5 - \\
& 152380762091374020434799837277117715974184875809865052975561585447684346918113356183254740900302324932628125 \cdot x^4 + \\
& 10126109533827119049053068717187006903486316579619512203213100610192022688776977601251774144342956667543232947564 8 \cdot x^3 - \\
& 82394230890068050809147635660557623685629965618893227966125666811860080407429030642077770538444660191227910486571712000 \cdot x^2 - \\
& 19264091315676614841969614988160005311744110600313352222208130788571940203903715353966189818913274713356215878346240000000 \cdot x - \\
& 1870374669751414608923737345184889994628232369194056109733545677638411383291159282002508930826987969131561815775577216000000000
\end{aligned}
$$

Example 3 (cases xvii, xix) The prime decomposition of 11 in K is such that it is ramified in K^+ and the prime above it in K^+ is inert in K. Further, 11 is split in K^{*+}, and mixed in K^* (one degree-one prime ideal with ramification index 2, and one unramified prime ideal of degree 2). The prime 11 appears in the denominator, so at least one of the curves with CM by K is superspecial.

Example 4 (cases xii and xiv) The prime decomposition of 89 in K is mixed: one ramified prime of degree 1 and two unramified primes of degree 1. It is split in K^+, ramified in $K^{*,+}$, and that prime in $K^{*,+}$ then splits in K^*. Modulo 89 the class polynomials factor as a product of the squares of two degree-2 polynomials:

$$h_1 = (x^2 + 17x + 9)^2(x^2 + 18x + 25)^2 \pmod{89}$$

$$h_2 = (x^2 + 37x + 67)^2(x^2 + 69x + 57)^2 \pmod{89}$$

$$h_3 = (x^2 + 83x + 83)^2(x^2 + 85x + 45)^2 \pmod{89}.$$

Note that in this case, it is not obvious from the polynomials how to match up roots of the three polynomials to form triples of Igusa invariants. A common approach has been to use the knowledge of the CM field to determine the possible group orders of the Jacobian of the curve, and then to run through all possible triples of roots of these polynomials until the correct triples and the corresponding curves are found. In the case that the prime p splits completely in the field K (case (i) in Table 3.5.1), a method for determining the possible group orders was given in [Wen] and [EL, Proposition 4], and the resulting CM curves constructed there were indeed ordinary. For other possible decompositions of the prime p in K, alternative algorithms are needed to compute the possible group orders. In the case of p-rank 1, a solution was given in [HMNS]. In some of the other examples, we show how to determine the group orders for other cases below.

The possible group orders in the case for Example 3 are $\#J(C)(\mathbb{F}_{89^2}) = 62045284$ or 63439556, for a genus 2 curve C over $\mathbb{F}_{89^2}$ with CM by K. This can be seen as follows: let $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$. In this case it can be verified using Magma or pari that both of the ideals $\mathfrak{p}_1\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3$ are principal, generated by π and $\overline{\pi}$, and $\pi\overline{\pi} = p$. As in the algorithm explained in [HMNS], we find the Weil p^2-numbers $\beta = \pm\pi\overline{\pi}^{-1}p$. Then the corresponding group orders for these Weil p^2-numbers are $N = \prod_\sigma(1 - \beta^\sigma)$, where σ ranges over the complex embeddings of K.

Represent $\mathbb{F}_{89^2} = \mathbb{F}_{89}[\alpha]$, where α satisfies $\alpha^2 + 82\alpha + 3 = 0$. The four curves are

$$y^2 = f_1(x) = \alpha^{5245}x^6 + \alpha^{2244}x^5 + \alpha^{7129}x^4 + \alpha^{1567}x^3 + \alpha^{2060}x^2 + \alpha^{5783}x + \alpha^{3905}$$

$$y^2 = f_2(x) = \alpha^{2667}x^6 + \alpha^{795}x^5 + \alpha^{1956}x^4 + \alpha^{5619}x^3 + \alpha^{5331}x^2 + \alpha^{7272}x + 52$$

$$y^2 = f_3(x) = \alpha^{6464}x^6 + \alpha^{795}x^5 + \alpha^{4574}x^4 + \alpha^{2946}x^3 + \alpha^{1544}x^2 + \alpha^{6684}x + \alpha^{803}$$

$$y^2 = f_4(x) = \alpha^{132}x^6 + \alpha^{3403}x^5 + \alpha^{2326}x^4 + \alpha^{3493}x^3 + \alpha^{5184}x^2 + \alpha^{1943}x + \alpha^{4418}$$

Calculating the Hasse-Witt matrix for the first curve, one computes f_1^{44} and finds $c_{88} = \alpha^{7555}$, $c_{87} = \alpha^{7787}$, $c_{177} = \alpha^{950}$, $c_{176} = \alpha^{1182}$, and that both M and $M^{(p)}M$ have rank 1, so both the f-number and the a-number equal 1. The same is true for the other three curves as well.

3.6.5. *Cases (ii) and (iv) in Table 3.5.1 for non-Galois fields.* We still refer to the field $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ and the class polynomials given above.

Example 5 To give an example for cases (ii) and (iv) in Table 3.5.1 for non-Galois fields, we let $p = 313$. The prime $p = 313$ decomposes in K as the product of two prime ideals of degree 1 and one prime ideal with residue degree 2. Modulo 313, the class polynomials factor as a product of four degree-two polynomials:

$$h_1(x) = (x^2 + 25x + 273)(x^2 + 137x + 39)(x^2 + 200x + 108)(x^2 + 312x + 249) \pmod{313},$$
$$h_2(x) = (x^2 + 20x + 121)(x^2 + 90x + 119)(x^2 + 138x + 297)(x^2 + 173x + 78) \pmod{313},$$
$$h_3(x) = (x^2 + 105x + 276)(x^2 + 133x + 230)(x^2 + 232x + 183)(x^2 + 289x + 91) \pmod{313}.$$

The two possible group orders are $\#J(C)(\mathbb{F}_{89^2}) = 9607909136$ or 9588315136, for a genus 2 curve C over $\mathbb{F}_{313^2}$ with CM by K. This can be seen because both of the prime ideals of K of degree 1 lying above p are principal, and letting π and $\overline{\pi}$ be the generators, we find the Weil p^2-numbers $\beta = \pm\pi\overline{\pi}^{-1}p$ (this is also explained in [HMNS]). Then the corresponding group orders for these Weil p^2-numbers are $N = \prod_\sigma(1 - \beta^\sigma)$, where σ ranges over the complex embeddings of K. Represent $\mathbb{F}_{313^2} = \mathbb{F}_{313}[\alpha]$, where α satisfies $\alpha^2 + 310\alpha + 10 = 0$. We find eight curves defined over $\mathbb{F}_{313^2}$. For example, the first one is the hyperelliptic curve defined over $\mathbb{F}_{313^2}$ by

$$y^2 = f(x) = \alpha^{20046}x^6 + \alpha^{18815}x^5 + \alpha^{77496}x^4 + \alpha^{26504}x^3 + \alpha^{19266}x^2 + \alpha^{53721}x + \alpha^{1332}.$$

Calculating $f(x)^{156}$, one finds that the coefficients of the Hasse-Witt matrix M are: $c_{p-1} = \alpha^{91834}$, $c_{p-2} = \alpha^{18900}$, $c_{2p-1} = \alpha^{62990}$, $c_{2p-2} = \alpha^{88024}$. The determinant of both M and $M^{(p)}M$ is 0 and the rank is 1. The same is true for all 8 curves: they all have $a = 1$ and $f = 1$.

3.6.6. *Cases (iii) and (v) in Table 3.5.1.* This next set of cases is very interesting, because we can see here that the decomposition of the prime in K only determines the reduction of the abelian surface in combination with the CM type. This is the first time we have an example of both superspecial and ordinary reduction modulo the same prime (of CM abelian surfaces with CM by the same field K, but different CM type). This phenomenon does not occur in genus 1.

We again work with the primitive quartic CM field $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ and the class polynomials given above. Let $p = 47$. As in cases (iii) and (v) in Table 3.5.1, the prime $p = 47$ decomposes in K as a product of two prime ideals of degree 2: p is inert in K^+, the real quadratic subfield of K, and then splits in K. The class polynomials factor modulo 47 as

$$h_1(x) = (x^2 + 18)^2(x^2 + 22x + 12)(x^2 + 33x + 19)(x^2 + 37x + 6) \pmod{47},$$
$$h_2(x) = (x^2 + 23)^2(x^2 + 10x + 46)(x^2 + 6x + 17)(x^2 + 9x + 39) \pmod{47},$$
$$h_3(x) = (x^2 + 2)^2(x^2 + 42x + 26)(x^2 + x + 19)(x^2 + 27x + 7) \pmod{47}.$$

Example 6 (case (v)) Both degree-2 prime ideals lying over $p = 47$ are principal in this case, and we denote the generators by π and $\overline{\pi}$. In this case, $\pi\overline{\pi} = 47u$, where u is a unit. Setting $\beta = \pm p^2/u$, gives two possible Weil p^2-numbers. The two possible group orders are $\#J(C)(\mathbb{F}_{47^2}) = \prod_\sigma(1 - \beta^\sigma) = 4901092$ or 4865732, where σ ranges over the complex embeddings of K. There are 4 ordinary CM points corresponding to these possible group orders.

Represent $\mathbb{F}_{47^2} = \mathbb{F}_{47}[\alpha]$, where α satisfies $\alpha^2 + 45\alpha + 5 = 0$. Then the four curves with these group orders are:

$$y^2 = \alpha^{829}x^6 + \alpha^{1842}x^5 + \alpha^{622}x^4 + \alpha^{1262}x^3 + \alpha^{956}x^2 + \alpha^{398}x + \alpha^{1255}$$
$$y^2 = \alpha^{929}x^6 + \alpha^{1219}x^5 + \alpha^{1483}x^4 + \alpha^{1511}x^3 + \alpha^{251}x^2 + \alpha^{224}x + \alpha^{1437}$$

$$y^2 = \alpha^{1852}x^6 + \alpha^{2038}x^5 + \alpha^{1790}x^4 + \alpha^{1078}x^3 + \alpha^{1166}x^2 + \alpha^{1634}x + \alpha^{1518}$$
$$y^2 = \alpha^{1783}x^6 + \alpha^{892}x^5 + \alpha^{1454}x^4 + \alpha^{665}x^3 + \alpha^{1014}x^2 + \alpha^{871}x + \alpha^{1754}.$$

For all four curves, we checked that the Hasse-Witt matrix M and $M^{(p)}M$ both have rank 2, so these curves are indeed all ordinary.

Example 7 (case (iii)) Each of the three class polynomials has one linear factor modulo 47. The curve over $\mathbb{F}_{47}$ with those $\mathbb{F}_{47}$-rational invariants is the hyperelliptic curve defined by

$$y^2 = 40x^6 + 22x^5 + 43x^4 + x^3 + 29x^2 + 8x + 28.$$

Its Jacobian has $\#J(C)(\mathbb{F}_{47}) = p^2 + 2p + 1 = 2304$ points and $\#C(\mathbb{F}_{47}) = p + 1 = 48$. The Hasse-Witt matrix M is identically 0 modulo 47, so the curve is superspecial. This curve occurs "with multiplicity two" modulo 47.

The other two CM abelian surfaces reduce to curves defined over $\mathbb{F}_{47^2}$. They are the hyperelliptic curves defined by

$$y^2 = \alpha^{487}x^6 + \alpha^{977}x^5 + \alpha^{1698}x^4 + \alpha^{1530}x^3 + \alpha^{1790}x^2 + \alpha^{1618}x + \alpha^{1063}$$
$$y^2 = \alpha^{809}x^6 + \alpha^{1759}x^5 + \alpha^{318}x^4 + \alpha^{1254}x^3 + \alpha^{226}x^2 + \alpha^{974}x + \alpha^{1385}.$$

They both have $\#J(C)(\mathbb{F}_{47^2}) = p^4 - 2p^2 + 1 = 4875264$ points and $\#C(\mathbb{F}_{47^2}) = p^2 + 1 = 2210$. They both have the property that the Hasse-Witt matrix M is identically 0 modulo 47, so the curves are both superspecial.

3.6.7. *Case (vii) in Table 3.5.1: totally inert.* We again work with the non-galois quartic CM field $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ and the class polynomials given above. The prime $p = 13$ is totally inert in K. Modulo 13, the class polynomials are:

$$h_1(x) = (x^2 + 2x + 9)(x^2 + 6x + 1)(x^4 + 8x^3 + 10x^2 + 12) \pmod{13},$$
$$h_2(x) = (x^2 + 5x + 1)(x^2 + 8x + 1)(x^4 + 7x^3 + 6x^2 + 7x + 8) \pmod{13},$$
$$h_3(x) = (x^2 + 2)(x^2 + 11)(x^4 + 6x^3 + 4x^2 + 5) \pmod{13}.$$

We look for curves over $\mathbb{F}_{13^2}$ with $\#J(C)(\mathbb{F}_{13^2}) = (p^4+2p^2+1) = 28900$. Represent $\mathbb{F}_{13^2} = \mathbb{F}_{13}[\alpha]$, where α satisfies $\alpha^2 + 12\alpha + 2 = 0$. We find 4 curves over $\mathbb{F}_{13^2}$, for example the first one is:

$$y^2 = \alpha^{99}x^6 + \alpha^{47}x^5 + \alpha^{156}x^4 + \alpha^{75}x^3 + \alpha^{27}x^2 + x + \alpha^{148}.$$

Its Hasse-Witt matrix M has rank 1 and the rank of $M^{(p)}M$ is 0, so $a = 1$ and $f = 0$ as predicted in the tables. The same is true of the other 3 curves as well.

4. The moduli space of pairs of elliptic curves

Let N be a positive integer. Consider the functor $\mathbb{B}_N$ on schemes associating to a scheme S the isomorphism class of triples

$$(E_1, E_2, \gamma),$$

where $\pi_i : E_i \to S, i = 1, 2$, are elliptic curves over S and γ is a full level structure on $E_1[N] \times E_2[N]$, namely, an isomorphism,

$$\gamma : E_1[N] \times E_2[N] \to (\mathbb{Z}/N\mathbb{Z})^4,$$

which is symplectic relative to the Weil pairing on $E_1 \times E_2$ (obtained as the product of the Weil pairings on each elliptic curve, or, equivalently, associated to the product polarization on $E_1 \times E_2$) and the standard pairing on $(\mathbb{Z}/N\mathbb{Z})^4$ given by the matrix $\begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & \\ & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \end{pmatrix}$.

An isomorphism $\varphi\colon (E_1, E_2, \gamma) \to (E_1', E_2', \gamma')$ of two such triples over S is a pair of isomorphisms of S schemes, $\varphi_i : E_i \to E_i'$, such that $\gamma = \gamma' \circ (\varphi_1 \times \varphi_2)$.

The functor $\mathbb{B}_N$ is naturally equivalent to the functor parameterizing isomorphism classes of quadruples (A, λ, e, γ) over S, where (A, λ) is a principally polarized abelian surface over S, e is a non-trivial idempotent, fixed under the λ-Rosati involution, and γ is a symplectic level N structure. Indeed, given a triple (E_1, E_2, γ) associate to it $(E_1 \times E_2, \lambda_1 \times \lambda_2, e, \gamma)$, where λ_i are the canonical principal polarizations on E_i and e is the idempotent endomorphism $(x, y) \mapsto x$. The converse construction associates to A the triple (E_1, E_2, γ), where $E_1 = \mathrm{Ker}(1 - e), E_2 = \mathrm{Ker}(e)$. It is not hard to verify that these constructions give a natural equivalence between the functors.

Lemma 4.0.1. *For $N \geq 3$ the moduli problem is rigid. Namely, any automorphism φ of a triple (E_1, E_2, γ) is the identity.*

Proof. Such an automorphism induces an automorphism of (A, λ, γ), where $A = E_1 \times E_2$. It is well known that such an automorphism must be the identity. □

It follows then from standard techniques that for $N \geq 3$ the functor $\mathbb{B}_N$ is representable by a quasi-projective scheme $\mathscr{B}_N$ over $\mathbb{Z}[\zeta_N, N^{-1}]$.

Proposition 4.0.2. *Let $N \geq 2$. Let J be the automorphism of $\mathscr{B}_N$ whose effect on points is*

$$(E_1, E_2, \gamma) \mapsto (E_2, E_1, \gamma \circ s),$$

where s is the natural "switch", $s : E_1[N] \times E_2[N] \to E_2[N] \times E_1[N]$. We have a commutative diagram,

$$\begin{array}{ccc} \mathscr{B}_N & & \\ \downarrow & \searrow^{\beta} & \\ \mathscr{B}_N/\langle J\rangle & \xrightarrow{\beta_J} & \mathscr{A}_{2,N}, \end{array}$$

where the diagonal arrow β is the natural morphism $(E_1, E_2, \gamma) \mapsto (E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma)$, the vertical arrow is an étale Galois cover with Galois group $\mathbb{Z}/2\mathbb{Z}$ and the bottom arrow β_J is a closed immersion, induced by β, whose image is the Humbert surface $\mathscr{H}_{1,N}$ in $\mathscr{A}_{2,N}$, the Zariski closure of $H_{1,N} \subset \mathscr{A}_{2,N}(\mathbb{C})$.

Proof. We first show that the morphism $\mathscr{B}_N \to \mathscr{B}_N/\langle J\rangle$ is unramified. Suppose that $J(E_1, E_2, \gamma) = (E_2, E_1, \gamma \circ s)$ is isomorphic to (E_1, E_2, γ). There are then isomorphisms $\varphi_1 : E_2 \to E_1$, $\varphi_2 : E_1 \to E_2$ such that $\gamma \circ s = \gamma \circ (\varphi_1 \times \varphi_2)$ and so $s = \varphi_1 \times \varphi_2$ on $E_1[N] \times E_2[N]$. But, for $(a, b) \in E_1[N] \times E_2[N]$ we have $s(a, b) = (b, a)$, while $\varphi_1 \times \varphi_2(a, b) = (\varphi_1(a), \varphi_2(b))$, which obviously cannot hold for every pair (a, b) if $N \geq 2$.

The morphism $\mathscr{B}_N \to \mathscr{B}_N/\langle J\rangle$, being a quotient by a finite group, is a finite morphism. We conclude that it is a finite étale cover with Galois group $\mathbb{Z}/2\mathbb{Z}$. The natural morphism $\beta : \mathscr{B}_N \to \mathscr{A}_N$ clearly factors through $\mathscr{B}_N/\langle J\rangle$ and we denote the induced morphism

$$\beta_J : \mathscr{B}_{N,J} \to \mathscr{A}_{2,N}.$$

We claim that this is a geometrically injective morphism. Suppose that

$$(E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma) \cong (E_1' \times E_2', \lambda_1' \times \lambda_2', \gamma').$$

By a theorem of Weil, after possibly switching E_1' with E_2' , we may assume that $E_1 \cong E_1', E_2 \cong E_2'$ and so, under these identifications, that $\gamma = \gamma'$. Namely, up to applying J, every point in the image has a unique pre-image.

The morphism β_J is also proper. This follows from the valuative crietrion of properness. As we shall see below the scheme $\mathscr{B}_N$ is a union of products of modular curves, in particular it is noetherian and so we can use discrete valuation rings in the criterion. To apply it, we must show that if R is a discrete valuation ring with field of fractions K, $(A, \lambda, \gamma)/R$ is an abelian scheme whose generic fiber is isomorphic over K to $(E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma)$ then the elliptic curves E_i extend to elliptic curves over R and then so does the isomorphism. The fact that the elliptic curves extend follows from the theory of Néron models (since $E_1 \times E_2 = A \otimes_R K$ obviously has good reduction). The extension of the isomorphism follows from the fact that $\mathscr{A}_{2,N}$ has a toroidal compactification which is proper over $\mathbb{Z}[\zeta_N, N^{-1}]$. Since both $\mathscr{B}_N/\langle J\rangle$ and $\mathscr{A}_{2,N}$ are reduced and the morphism β_J is proper and injective (hence quasi-finite), β_J is a finite injective morphism. We will conclude it is an isomorphism onto its image, the Humbert surface $\mathscr{H}_{1,N}$ by showing that for a geometric point x of $\mathscr{B}_N/\langle J\rangle$ and its image y in $\mathscr{A}_{2,N}$ the completed local rings are isomorphic. Note that the Humbert divisor $\mathscr{H}_{1,N}$ is the image of β_J, since they have the same generic fiber and both are the closure of their generic fiber.

Indeed, suppose that y is the image of the k-geometric point (y_1, y_2) of $\mathscr{B}_N$. The completed local ring on $\mathscr{B}_N$ is then just isomorphic to $W(k)[\![t_1, t_2]\!]$, as $\mathscr{B}_N$ is a product of smooth curves. Moreover, if E_i is the elliptic curve corresponding to y_i, then t_i is the parameter arising via the local deformation theory for elliptic curves (the level structure need not be a product level structure; regardless it extend uniquely by étaleness). On the other hand, the completed local ring on $\mathscr{A}_{2,N}$ of the point y corresponding to $(A, \lambda, \gamma) = (E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma)$ is isomorphic to the ring $W(k)[\![t_{11}, t_{1,2}, t_{2,1}, t_{2,2}]\!]/(t_{1,2} - t_{2,1})$ and $\mathscr{H}_{1,N}$ contains locally the closed formal subscheme defined by the ideal $(t_{1,2}, t_{2,1})$, as is clear from the interpetation of the variables through local deformation theory. Since $\mathscr{B}_N/\langle J\rangle$ is locally irreducible and the morphism is geometrically injective also $\mathscr{H}_{1,N}$ is locally irreducible. It follows that $\mathscr{H}_{1,N}$ is defined locally by the ideal $(t_{1,2}, t_{2,1})$ and that the morphism is an isomorphism on every completed local ring, which is sufficient to conclude the proof.

Another way to conclude the proof is to prove that the morphism β_J is universally injective (or a monomorphism) and then use EGA IV, §8.11, Proposition (8.11.5). Since $\mathscr{B}_N/\langle J\rangle$ is the categorical quotient of $\mathscr{B}_N$, we know it as a functor of points and so injectivity boils down to the following statement: Given elliptic curves $E_1, \ldots, E_4$ over a connected scheme S such that $E_1 \times E_2 \cong E_3 \times E_4$ as principally polarized abelian schemes over S then, either $E_1 \cong E_3$ and $E_2 \cong E_4$, or $E_1 \cong E_4$ and $E_2 \cong E_3$. Note that to identify E_1 in $E_3 \times E_4$ is equivalent to giving an endomorphism. Choose a geometric point x of S and use Weil's theorem as above together with Grothendieck's theorem $\mathrm{End}_S(E_3 \times E_4) \hookrightarrow \mathrm{End}_{k(x)}((E_3 \times E_4) \otimes k(x))$. □

We next discuss the complex uniformization of $\mathscr{B}_N$. Recall the classical construction of the modular curves: Given $\tau \in \mathfrak{H}$ one lets $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ be the corresponding elliptic curve, and we get a symplectic isomorphism $E_\tau[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ by sending $1/N$ to $(1, 0)$ and τ/N to $(0, 1)$. We call this level structure γ_0. Let $\sigma = M\tau$, where $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the isomorphism $E_\sigma \to E_\tau$ is given by multiplication by $j(M, \tau) = c\tau + d$. Since $\gamma_0(A + B\sigma)/N = {}^t(A, B)$ and $1/N$ is sent to $(d + c\tau)/N$, while σ/N is sent $(b + a\tau)/N$, we find that (E_σ, γ_0) is isomorphic to $(E_\tau, \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right) \circ \gamma_0)$. We remark that $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto M^\dagger := \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$ is an outer automorphism of $\mathrm{SL}_2(\mathbb{Z})$ given by conjugating by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z})$.

Consider the space

$$\mathfrak{H} \times \mathfrak{H} \times \mathrm{Sp}_4(\mathbb{Z}/N\mathbb{Z}).$$

(Here the symplectic group is relative to the pairing fixed above.) To a point (τ_1, τ_2, γ) of this space we associate the triple $(E_{\tau_1}, E_{\tau_2}, \gamma \circ (\gamma_0 \times \gamma_0))$. The group $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ acts on the space by

$$(M_1, M_2) * (\tau_1, \tau_2, \gamma) = (M_1\tau_1, M_2\tau_2, \mathrm{diag}(M_1^\dagger, M_2^\dagger) \circ \gamma).$$

The space of orbits is isomorphic to $\mathscr{B}_N(\mathbb{C})$. Furthermore, choose a complete set of representatives $\gamma_1, \ldots, \gamma_t$ $(t = t(N))$ for $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\backslash \mathrm{Sp}_4(\mathbb{Z}/N\mathbb{Z})$. Then,

$$\mathscr{B}_N(\mathbb{C}) \cong \coprod_{i=1}^{t} (\Gamma(N)\backslash\mathfrak{H})^2 = \coprod_{i=1}^{t} Y(N) \times Y(N).$$

Via this identification, we associate to a pair (τ_1, τ_2) in the i-th (or γ_i-th, if one prefers) component of $\mathscr{B}_N(\mathbb{C})$ the triple $(E_{\tau_1}, E_{\tau_2}, \gamma_i \circ (\gamma_0 \times \gamma_0))$.

The involution J takes the γ_i-component to γ_j-component where γ_j is determined by $\gamma_i \circ (\gamma_0 \times \gamma_0) \circ s \in (\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))\gamma_j \circ (\gamma_0 \times \gamma_0)$. Typically, $\gamma_j \neq \gamma_i$. In fact, the components of $\mathscr{B}_N$ are parameterized by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\backslash \mathrm{Sp}_4(\mathbb{Z}/N\mathbb{Z})$, while the components of $\mathscr{B}_J/\langle N \rangle$ are parameterized by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\backslash \mathrm{Sp}_4(\mathbb{Z}/N\mathbb{Z})/H$, where $H = \{1, \left(\begin{smallmatrix} 0 & I_2 \\ I_2 & 0 \end{smallmatrix}\right)\}$.

Remark 4.0.3. Here is a typical example illustrating the difference between $\mathscr{H}_{1,N}$ and $\mathscr{B}_N$. Let K be a field, L a quadratic Galois extension of K and σ the non-trival automorphism of L over K. Let E_1 be an elliptic curve defined over L and not over K. Let E_2 be the curve obtained by σ to the equation of E_1 (and so $j(E_2) = \sigma(j(E_1))$). The point (E_1, E_2) of $\mathscr{B}_1$ is defined over L, but not over K. On the other hand, its image, $A = (E_1 \times E_2, \lambda_1 \times \lambda_2)$ is defined over K. A quadratic extension is needed to define the elliptic curves E_1, E_2 such that $A \cong E_1 \times E_2$. To study the situation more precisely, we must include level N structure.

From a scheme theoretic point of view we have the following cartesian diagram,

$$\begin{array}{ccccc} \mathrm{Spec}(K) \times_{\mathscr{A}_{2,N}} \mathscr{B}_N & \longrightarrow & \mathscr{B}_N & & \\ \downarrow & & \downarrow & \searrow & \\ \mathrm{Spec}(K) & \longrightarrow & \mathscr{A}_{2,N} & \hookleftarrow & \mathscr{B}_{N,J} \end{array}$$

The morphism $\mathrm{Spec}(K) \times_{\mathscr{A}_{2,N}} \mathscr{B}_N \to \mathrm{Spec}(K)$ is finite étale (being a base change of the morphism $\mathscr{B}_N \to \mathscr{A}_{2,N}$) and so $\mathrm{Spec}(K) \times_{\mathscr{A}_{2,N}} \mathscr{B}_N = \mathrm{Spec}(L')$, where L'/K is a separable quadratic K-algebra.

5. A lemma in arithmetic intersection theory

Let R be a Dedekind ring, finite over $\mathbb{Z}_p$, $\mathfrak{p} \lhd R$ a prime ideal. Let $\pi : S \to \mathrm{Spec}(R)$ be a smooth scheme of finite type over $\mathrm{Spec}(R)$. Let $x \in S$ be a closed point of characteristic p lying over $\mathfrak{p}$. Then $\mathcal{O}_S^{\wedge x}$, the completed local ring at S is isomorphic to $\tilde{R}[\![x_1, \ldots, x_n]\!]$ where n is the relative dimension of S over R and $\tilde{R} = R \otimes_{R_0} W(R/\mathfrak{p})$, where R_0 the maximal unramified subring of R. See [CohI]. In particular, $\mathcal{O}_S^{\wedge x}$ is a noetherian unique factorization domain. As a consequence, every divisor on $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$ is principal. (We remark that in fact this latter fact follows directly from the Auslander-Buchsbaum theorem without need for Cohen's theorem.)

Lemma 5.0.4. *Let $S \to \mathrm{Spec}(R)$ be a smooth integral scheme of finite type over a Dedekind ring R containing $\mathbb{Z}$. Let B be a Dedekind ring containing R, K its field of fractions and η be the generic point. Let*

$$\iota : \mathrm{Spec}(B) \to S,$$

be a morphism of schemes over R. Let f be a rational function on S such that the divisor of f intersects the image of ι properly (in particular, $f(\eta) = \iota^* f$ is a well defined element of K). Let the divisor of f equal $(f)_0 - (f)_\infty = \sum m_i D_i$, where the m_i are non-zero integers and D_i irreducible reduced effective divisors. Let Z be the closed reduced subscheme which is the support of $\mathrm{div}(f)_0$.

Let $\mathfrak{p}$ be a prime ideal of B and x its image under ι. Suppose that $\mathrm{val}_{\mathfrak{p}}(f(\eta)) = \alpha > 0$. *Then* $d = \max\{m_i : x \in D_i\} > 0$. *Let* $a = \lceil \alpha/d \rceil$. *Then $a > 0$ and the morphism $\iota : \mathrm{Spec}(B/\mathfrak{p}^a)$ factors through* $\mathrm{div}(f)_0$*:*

$$\begin{array}{ccccc} \mathrm{Spec}(B/\mathfrak{p}^a) & \longrightarrow & \mathrm{Spec}(B) & \xrightarrow{\iota} & S \\ & \searrow & & & \uparrow \\ & & & & Z \end{array} \tag{5.0.1}$$

Remark 5.0.5. We shall apply this Lemma later, in the following context: S will be the modular scheme $\mathscr{A}_{2,N}$, f will be a function such that $f = \Theta^k/g$, where g is a modular form of weight $10k$ with rational Fourier coefficients, the morphism ι will be such that $\iota(\eta)$ is a CM point and our assumption will be that $\mathrm{val}_{\mathfrak{p}}(f) = a > 0$.

Proof. We first argue that we may replace S by the $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$. Indeed, on the one hand, diagram (5.0.1) gives by passing to completions at x a diagram

$$\begin{array}{ccc} \mathrm{Spec}(B/\mathfrak{p}^a) & \longrightarrow & \mathrm{Spf}(\mathcal{O}_S^{\wedge x}) \\ & \searrow & \uparrow \\ & & Z \cap \mathrm{Spf}(\mathcal{O}_S^{\wedge x}) \end{array} \tag{5.0.2}$$

On the other hand, diagram (5.0.2) is coming from unique continuous morphisms $\mathcal{O}_S^{\wedge x} \to B/\mathfrak{p}^n$ etc., that arise uniquely from morphisms $\mathcal{O}_S \to B/\mathfrak{p}^n$, etc.

In $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$ every divisor is principal and so we may write there $D_i' = (f_i)$ where $f_i \in \mathcal{O}_S^{\wedge x}$, and D_i' is the induced divisor on $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$. D_i' may be reducible, but it is reduced. If $x \notin D_i$ then f_i is a unit in $\mathcal{O}_S^{\wedge x}$. Via the morphism $\mathrm{Spec}(B_{\mathfrak{p}}) \to \mathrm{Spec}(B) \to S$, that induces a morphism $\mathrm{Spec}(B_{\mathfrak{p}}) \to \mathrm{Spf}(\mathcal{O}_S^{\wedge x})$, we may view $f(\eta)$ as an element of $K_{\mathfrak{p}}$, which is equal, up to a unit, to $\prod_i f_i(x)^{m_i}$ and so:

$$\begin{aligned} \alpha = \mathrm{val}_{\mathfrak{p}}(f(\eta)) &= \sum_{\{i : x \in D_i\}} m_i \cdot \mathrm{val}_{\mathfrak{p}}(f_i(\eta)) \\ &= \sum_{\{i : x \in D_i, m_i > 0\}} m_i \cdot \mathrm{val}_{\mathfrak{p}}(f_i(\eta)) + \sum_{\{i : x \in D_i, m_i < 0\}} m_i \cdot \mathrm{val}_{\mathfrak{p}}(f_i(\eta)). \end{aligned} \tag{5.0.3}$$

We note that if $x \in D_i$ then $\mathrm{val}_{\mathfrak{p}}(f_i) \geq 1$ (it may be strictly bigger, of course). In particular, $d > 0$. Consider $\alpha' = \sum_{\{i : x \in D_i, m_i > 0\}} \mathrm{val}_{\mathfrak{p}}(f_i(\eta))$; clearly $\alpha' \cdot d \geq \alpha$ and so $\alpha' \geq \lceil \alpha/d \rceil$ and so it will be enough to prove that diagram (5.0.2) holds with α'. Consider the function $f_Z = \prod_{\{i : x \in D_i, m_i > 0\}} f_i$ which defines $Z \cap \mathrm{Spf}(\mathcal{O}_S^{\wedge x})$. To show diagram (5.0.2) holds is equivalent to show

that f_Z, when pulled back to $\mathrm{Spec}B_{\mathfrak{p}}$ has valuation at least α'. But the valuation is precisely $\sum_{\{i:x\in D_i, m_i>0\}} \mathrm{val}_{\mathfrak{p}}(f_i(\eta))$ and we are done. □

5.0.8. *Examples.* The whole theory is developed precisely to deal with situations where one cannot just "write down everything explicitly", and so our examples are a bit artificial.

- Consider the scheme $S = \mathrm{Spec}(\mathbb{Z}[x])$ and the function $f(x) = x^2 - 1$. The divisor of f is
$$D_1 + D_2, \qquad D_1 = \mathrm{div}(x-1), D_2 = \mathrm{div}(x+1).$$
Let $\tau = 3$ corresponding the the point determined by the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}, x \mapsto 3$. We have $\mathrm{val}_2(f(\tau)) = \mathrm{val}_2(8) = 3$. We examine the situation on the completed local ring of the point $(2, x-3) = (2, x-1) = (2, x+1)$ (the reduction of τ modulo 2). Also at this completed local ring the divisor of f is given by $D_1 = \mathrm{div}(x-1), D_2 = \mathrm{div}(x+1)$ (with a slight abuse of notation). It follows from our lemma that the morphism $\mathrm{Spec}(\mathbb{Z}) \to \mathrm{Spec}(\mathbb{Z}[x])$ corresponding to τ induces a morphism
$$\mathrm{Spec}(\mathbb{Z}/2^3\mathbb{Z}) \to D_1 \cup D_2,$$
where by $D_1 \cup D_2$ we mean the closed reduced subscheme whose support is $D_1 \cup D_2$, namely $\mathrm{Spec}(\mathbb{Z}[x]/(x^2-1)$. Indeed, this is nothing but saying that there is indeed a well defined homomorphism $\mathbb{Z}[x]/(x^2-1) \to \mathbb{Z}/2^3\mathbb{Z}$ taking x to 3.

  An interesting feature of this example is that the morphism $\mathrm{Spec}(\mathbb{Z}) \to \mathrm{Spec}(\mathbb{Z}[x])$ only induces a well defined morphism $\mathrm{Spec}(\mathbb{Z}/2^i\mathbb{Z}) \to D_i$ (where D_i is the reduced closed scheme supported on D_i, namely $\mathrm{Spec}(\mathbb{Z}[x]/(x-1))$ for $i = 1$ and $\mathrm{Spec}(\mathbb{Z}[x]/(x+1))$ for $i = 2$). Moreover, the divisors D_1 and D_2 intersect transversely, the intersection being $(x-1, x+1)$. The subtlety is in the scheme structure on $D_1 \cup D_2$ and in particular in the fact that $\mathbb{Z}[x]/(x^2-1) \subsetneqq \mathbb{Z}[x]/(x-1) \oplus \mathbb{Z}[x]/(x+1)$.
- Once more $S = \mathrm{Spec}(\mathbb{Z}[x])$ but now $f(x) = x^2 + 1$, which is irreducible. The point $\tau = 2$ corresponds to the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}, x \mapsto 2$. We have $\mathrm{val}_5(f(\tau)) = \mathrm{val}_5(5) = 1$. We have an induced morphism $\mathrm{Spec}(\mathbb{Z}/5\mathbb{Z}) \to \mathrm{Spec}(\mathbb{Z}[x]/(x^2+1))$, which amount to the fact that there is a homomorphism $\mathbb{Z}[x]/(x^2+1) \to \mathbb{Z}/5\mathbb{Z}$ taking x to 2.

  In the completed local ring of the point $(5, x-2)$ the function f decomposes as $f(x) = (x-i)(x+i)$ where i is an element of $\mathbb{Z}_5$ whose square is -1 and whose reduction is 2 modulo 5. Thus, the function $x-i$ vanishes to first order at this point, while the function $x+i$ is a unit. The divisor of f is locally $D_1 = \mathrm{div}(x+i)$ and the lemma states that we have an induced morphism $\mathrm{Spec}(\mathbb{Z}/5\mathbb{Z}) \to \mathrm{Spf}(\mathbb{Z}_5[\![(x-2)]\!]/(x-i))$, which amounts to the fact that there is a well defined continuous homomorphism $\mathbb{Z}_5[\![(x-2)]\!]/(x-i) \to \mathbb{Z}/5\mathbb{Z}$ taking x to 2.
- Consider $\mathrm{Spec}(\mathbb{Z}[1/6][x,y]/(y^2-(x^3-1)))$ and the function $f(x) = x-1$ whose divisor is $2[(1,0)]$, and we note that the divisor $[(1,0)]$ is not principal . We have $x^3 - 1 = (x-1)(x^2+x+1)$ and we let S' be the open subscheme whose complement is given by x^2+x+1. The divisor of f on S' is still $2[(1,0)]$ but now $[(1,0)]$ is locally principal; it is the divisor $D = [(1,0)]$ of $(x-1)/y$. The divisor of f is $2D$. Finally, let S be the base change of S' to $\mathbb{Z}[1/6, \sqrt{215}]$.

  We consider the point $\tau = (6, \sqrt{215})$ of S, corresponding to the homomorphism
$$\mathbb{Z}[1/6, \sqrt{215}, x, y, 1/(x^2+x+1)]/(y^2 - x^3 + 1) \to \mathbb{Z}[1/6, \sqrt{215}],$$
given by
$$(x, y) \mapsto (6, \sqrt{215}).$$

Let $\mathfrak{p}$ be the prime ideal above 5 in $\mathbb{Z}[1/6, \sqrt{215}]$. We have $f(\tau) = 5$ and $\mathrm{val}_{\mathfrak{p}}(f(\tau)) = 2$. We deduce from our lemma that we have an induced morphism $\mathrm{Spec}(\mathbb{Z}/5\mathbb{Z}) \to D$, corresponding to the fact that there is a well defined homomorphism

$$\mathbb{Z}[1/6, \sqrt{215}, x, y, 1/(x^2+x+1)]/(y^2 - x^3 + 1, (x-1)/y) \to \mathbb{Z}[1/6, \sqrt{215}]/(\mathfrak{p}) \cong \mathbb{Z}/5\mathbb{Z},$$

where $(x, y) \mapsto (6, \sqrt{215})$.

6. A problem in deformation theory

6.1. **Deforming endomorphisms.** Let A be an abelian variety of dimension g over a perfect field k of characteristic p and let r be the rank over $\mathbb{Z}$ of $\mathrm{End}_k(A)$ (it is finite and at most $4g^2$). Let $(R, \mathfrak{m}_R)$ be a local artinian ring with residue field $k = R/\mathfrak{m}_R$ of characteristic p. Let n_R be the minimal positive integer such that $\mathfrak{m}_R^{n_R} = 0$. Let t_R be the least positive integer such that $p^{t_R} \in \mathfrak{m}_R^{p-1}$.

Let $\mathbb{A}/R$ be a deformation of A. By that we mean that $\mathbb{A} \to \mathrm{Spec}(R)$ is an abelian scheme and that there are given closed immersions:

$$\begin{array}{ccc} \mathbb{A} & \hookleftarrow & A \\ \downarrow & & \downarrow \\ \mathrm{Spec}(R) & \hookleftarrow & \mathrm{Spec}(k) \end{array}$$

By a fundamental result of Grothendieck, we have an inclusion of rings

$$\mathrm{End}_R(\mathbb{A}) \hookrightarrow \mathrm{End}_k(A).$$

Let us define the magnitudes (a-priory possibly infinite)

$$i(\mathbb{A}/R) = [\mathrm{End}_k(A) : \mathrm{End}_R(\mathbb{A})],$$

and

$$\mathfrak{i}(R) = \inf\{i(\mathbb{A}/R) : \mathbb{A}/R \text{ a deformation of } A\}, \tag{6.1.1}$$

$$\mathfrak{I}(R) = \sup\{i(\mathbb{A}/R) : \mathbb{A}/R \text{ a deformation of } A\}. \tag{6.1.2}$$

These depend on A but we suppress that from the notation. We are interested in studying $i(\mathbb{A}/R), \mathfrak{i}(R)$ and $\mathfrak{I}(R)$. Although we provide below some general results, our focus later is on the case of elliptic curves. The general case certainly deserves further study, but it will not be carried out here.

Proposition 6.1.1. *The quantity $i(\mathbb{A}/R)$ is finite and is a power of p. So are $\mathfrak{i}(R)$ and $\mathfrak{I}(R)$. The following inequalities hold.*

$$1 \leq \mathfrak{i}(R) \leq \mathfrak{I}(R) \leq p^{(r-1)t_R\lceil (n_R-1)/(p-1)\rceil}.$$

Corollary 6.1.2. *Let K be a CM field and $\mathcal{O}$ an order of K. Let $A \to \mathrm{Spec}(R)$ be an abelian scheme over a dvr $(R, \mathfrak{m}_R)$ whose residue field is a perfect field k of characteristic p, and suppose that we are given an optimal embedding $\mathcal{O} \hookrightarrow \mathrm{End}_R(A)$. Let $\mathcal{O}' \supseteq \mathcal{O}$ be the optimally embedded order of K in $\mathrm{End}_k(A \otimes k)$. Then $[\mathcal{O}' : \mathcal{O}]$ is a power of p.*

Example 6.1.3. Suppose that E is an elliptic curve over a number field M with complex multiplication by an optimally embedded order $\mathcal{O}$ of a quadratic imaginary field K. Let $\mathfrak{p}$ be a prime ideal of M of residue characteristic p, and assume that E has good reduction modulo $\mathfrak{p}$, denoted E', and that the conductor of $\mathcal{O}$ is prime to p. Then $\mathcal{O}$ is optimally embedded in $\mathrm{End}(E')$.

On the other hand, the conductor always becomes smaller when it is divisible by p. Suppose that E has supersingular reduction, $\mathcal{O}_K = \mathbb{Z}[\delta]$ and $\mathcal{O} = \mathbb{Z}[pr\delta]$, where $r \in \mathbb{Z}$. One verifies that $pr\delta$ has degree divisible by p^2. Since E' is supersingular any isogeny of degree p^2 vanishes on $E'[p]$ and it follows that $r\delta$ is also an isogeny of E'. It is an interesting situation. Because $\mathcal{O}$ is optimally embedded in $\mathrm{End}(E)$, the kernel of the multiplication-by-p map on the finite flat group scheme $\mathrm{Ker}[pr\delta]$ has order p generically, but order p^2 modulo p. The same happens in the ordinary case; see § 6.4.1. This example is well-known but is usually proven by other techniques. See, for example [Lang2, Theorem 5, § 13.2].

Proposition 6.1.4. *Let A be an abelian variety over an algebraically closed field k of characteristic p.*

1. *Let $\mathcal{O} \subset \mathrm{End}(A)$ be a set. Let R^u be the universal formal deformation space of A. There is closed subscheme $Z_{\mathcal{O}}$ which is universal for the property of extending $\mathcal{O}$ to a deformation.*
2. *Let n be an integer. There is a closed subscheme that is universal for deformations $\mathbb{A}$ of A such that $[\mathrm{End}(A) : \mathrm{End}(\mathbb{A})] | p^n$. (The same holds true if we wish to work with elementary divisors for the quotient abelian group $\mathrm{End}(A)/\mathrm{End}(\mathbb{A})$.)*

Proposition 6.1.4 is folklore. The first assertion is proven in [Dok, Lemma 4.3.5]. The proof consists of verifying Schlessinger's criteria for pro-representability. The second assertion follows immediately from the first given that there are only finitely many subrings of a given index (let alone of given elementary divisors) and they are all finitely generated as $\mathbb{Z}$-modules.

The proof of Proposition 6.1.1 is given below, after we review Grothendieck's crystalline deformation theory.

6.2. **Crystalline deformation theory.** Our main reference here is Grothendieck's monograph [Gro]. First recall the notion of *divided power structure (d.p.)* on a pair (R, I) consisting of a ring R and an ideal $I \lhd R$ (loc. cit. Chapitre IV, §1.1). These are functions $\gamma_n : I \to I, n = 1, 2, 3, \ldots$ that "behave like" $x^n/n!, n = 1, 2, 3, \ldots$, that is, the following properties hold true:

1. $\gamma_1(x) = x$;
2. $\gamma_n(x + y) = \gamma_n(x) + \sum_{i=1}^{n-1} \gamma_{n-i}(x)\gamma_i(y) + \gamma_n(y)$;
3. $\gamma_n(xy) = x^n\gamma_n(y)$ for $x \in R, y \in I$;
4. $\gamma_m(\gamma_n(x)) = \frac{(mn)!}{(n!)^m m!}\gamma_{mn}(x)$;
5. $\gamma_m(x)\gamma_n(x) = \frac{(m+n)!}{m!n!}\gamma_{m+n}(x)$.

The axioms imply the identities

$$x^n = n!\gamma_n(x), \qquad x \in I,\ n = 1, 2, 3 \ldots.$$

Hence, if R is an integral domain, whose quotient field is of characteristic 0, there is at most one d.p. structure on I. It is given by $\gamma_n(x) = x^n/n!$. This d.p. structure is well defined if $x^n/n! \in I$ for all $x \in I, n = 1, 2, 3, \ldots$. A divided powers structure is called *nilpotent* if there is an N, such that for any positive integers $a_1, \ldots, a_r$ with $\sum_{i=1}^r a_i \geq N$ and elements $x_1, \ldots, x_r$ of I, we have $\gamma_{a_1}(x_1)\gamma_{a_2}(x_2) \cdots \gamma_{a_r}(x_r) = 0$.

Example 6.2.1. Let p be a prime. Suppose that $I^p = 0$ and that $1, 2, 3, \dots p-1$ are invertible in R, then we may define $\gamma_n(x) = x^n/n!, n = 1, 2, \dots, p-1$ and $\gamma_n(x) = 0, n \geq p$. This is a nilpotent d.p. structure with $N = p$.

Example 6.2.2. Let (R, I) be a discrete valuation ring of mixed characteristic $(0, p)$ and uniformizer π. We assume that $\mathrm{val}(p) = 1$ and $\mathrm{val}(\pi) = 1/e$. We have $\pi^n/n! \in I$ if and only if $n/e \geq (n - s_n)/(p-1)$, where s_n is the sum of the digits in the p-adic development of n. See loc. cit. IV §1.3.) That is, $\pi^n/n! \in I$ for all $n \geq 1$ iff $e \leq p-1$.

If R has a d.p. structure, i.e. $e \leq p-1$, then we have an induced d.p. structure on $(R/I^N, I/I^N)$, which is nilpotent of level N if $e < p-1$. We say then that the d.p. structure on (R, I) is topologically nilpotent. The condition $e < p-1$ is necessary for that.

The theorem that we need is in loc. cit. V §4. Following the notation there, we use $\mathbb{D}^*(A)_S$ to denote the relative de Rham cohomology $\mathbb{H}^1_{\mathrm{dR}}(A/S)$. It will take us too long to define the notions of the crystalline site and crystals in general. For that see loc. cit.. We just note a particular example of the theorem: Let $S \hookrightarrow S'$ be a closed immersion of affine schemes, $\mathrm{Spec}(R) \to \mathrm{Spec}(R')$, where $R' \to R$ is a surjective ring homomorphism with kernel I, such that I is equipped with nilpotent d.p.. This is an example of a nilpotent thickening of S by S'. For instance, in Schlessinger's theory one considers the case where the rings R, R', are local rings with maximal ideals $\mathfrak{m}, \mathfrak{m}'$, respectively, $R' \to R$ is a local homomorphism whose kernel is principle, say equal to (t) and $\mathfrak{m}'t = 0$. Note that this implies that $t^2 = 0$. One then has a canonical nilpotent d.p. structure on (t) given by $\gamma_1(x) = x$ and $\gamma_n(x) = 0, n = 2, 3, \dots$.

Theorem 6.2.3. *Let S be a scheme and S' nilpotent thickening of S with d.p. which is locally nilpotent. Consider the natural functor from abelian schemes over S' to the category of couples (A, Fil^1) of an abelian scheme A over S and a submodule, locally a direct summand, Fil^1 of $\mathbb{D}^*(A)_{S'}$, which is a prolongation of $\mathrm{Fil}^1\mathbb{D}^*(A)_S = \underline{\omega}_A$. This functor is an equivalence of categories.*

Example 6.2.4. Let K be a quadratic imaginary field and $\mathcal{O}_{K,m}$ be the order of conductor m in K and say $p^a \| m$, $m = p^a n$. Let E be a superspecial elliptic curve over $\bar{\mathbb{F}}_p$ with an action of $\mathcal{O}_{K,n}$. One may wish to calculate the deformations of E to which the action of the subring $\mathcal{O}_{K,m}$ of $\mathcal{O}_{K,n}$ extends. (Note that this is the general situation by Example 6.1.3.) Unfortunately, such a calculation is not accessible via crystalline deformation theory. For example, consider such deformations to characteristic zero that are defined over a d.v.r. R with d.p.. Every such deformation $\mathbb{E}$ defines then a submodule of $H^1_{crys}(E/R) = H^1_{crys}(E/W(\overline{\mathbb{F}}_p)) \otimes R$, which is a direct summand of rank 1 extending the Hodge-de Rham filtration on $H^1_{\mathrm{dR}}(E/\overline{\mathbb{F}}_p)$. We assume such a deformation exists, which means that there are two embeddings $\iota_1, \iota_2 : \mathcal{O}_{K,n} \to R$, the first induced from the action of $\mathcal{O}_{K,n}$ on the tangent space and the second is its Galois twist. We have $H^1_{crys}(E/R) = \mathcal{O}_{K,n} \otimes_{\mathbb{Z}} R \hookrightarrow R \oplus R$ by $(\iota_1 \otimes 1, \iota_2 \otimes 1)$. If $p \neq 2$ is unramified this is an isomorphism of rings and under this isomorphism the order of conductor m is sent to the subring $\mathcal{O}_a := \{(x, y) \in R \oplus R : x \equiv y \pmod{p^a}\}$, generated as an R-module by $(1, 1), (p^a, -p^a)$. A direct summand R-module of rank 1 of R^2 is given by (x, y) with either x or y a unit. To be preserved under $\mathcal{O}_a$ we must have $x = 0$ or $y = 0$. Thus, we see that there is a unique deformation for which the action of $\mathcal{O}_a$ extends, and then also $\mathcal{O}_0$ acts. The conclusion is that elliptic curves over a finite extension of $\mathbb{Q}_p$ on which $\mathcal{O}_{K,m}$ acts optimally are not defined over a base affording d.p.. That is, the ramification index is at least p. Of course the theory of complex multiplication and class field theory give more precise results. It remains an interesting problem to actually calculate the closed subscheme of the deformation space of E to which the action of $\mathcal{O}_{K,m}$ extends.

6.3. **Proof of Proposition 6.1.1.** We remark that there are many cases where $\mathfrak{i}(R) = 1$. An obvious example is when $R = k[\epsilon]$ and we take the constant deformation $\mathbb{A} = A \otimes_k k[\epsilon]$. A more interesting example can be given in the case of ordinary abelian varieties, see §6.4.

Let $(R, \mathfrak{m}_R)$ be a local artinian ring with residue field $k = R/\mathfrak{m}_R$. Let n_R be the minimal positive integer such that $\mathfrak{m}_R^{n_R} = 0$, as before. We define successively rings

$$R_0 = R/\mathfrak{m}_R, \quad R_1 = R/\mathfrak{m}_R^{1+(p-1)}, \quad R_2 = R/\mathfrak{m}_R^{1+2(p-1)}, \cdots, \quad R_\ell = R/\mathfrak{m}_R^{1+\ell(p-1)},$$

where $\ell = \lceil (n_R - 1)/(p-1) \rceil$. There are canonical surjections

$$R_\ell \twoheadrightarrow R_{\ell-1} \twoheadrightarrow \ldots \twoheadrightarrow R_1 \twoheadrightarrow R_0,$$

and we let $I_j = \mathfrak{m}_R^{1+(j-1)(p-1)}/\mathfrak{m}_R^{1+j(p-1)}$, $j = 1, 2, \ldots, \ell$, be the kernel of the surjection $R_j \to R_{j-1}$. We note that $I_j^p = 0$ in R_j and hence the morphism

$$\mathrm{Spec}(R_{j-1}) \hookrightarrow \mathrm{Spec}(R_j),$$

is a nil-immersion with canonical divided powers structure as in Example 6.2.1. Let t_R be the minimal power of p such that $p^{t_R} \in \mathfrak{m}_R^{p-1}$. Then $p^{t_R} I_j = 0$ in R_j.

Now, by arguing inductively on j, we reduce to the following situation. Let $A \to \mathrm{Spec}(R_{j-1})$ be an abelian scheme of relative dimension g and let $\mathbb{A} \to \mathrm{Spec}(R_j)$ a deformation of it. We need to show that $[\mathrm{End}(\mathbb{A}) : \mathrm{End}(A)]$ is finite and is equal to a power of p. By crystalline deformation theory, the closed immersion of abelian schemes $A \hookrightarrow \mathbb{A}$ corresponds functorially to a diagram

$$\begin{array}{ccc} R_j^{2g} & \twoheadrightarrow & R_{j-1}^{2g} = \mathbb{H}^1_{\mathrm{dR}}(A/R_{j-1}) \\ \cup & & \cup \\ \omega_j & \twoheadrightarrow & \omega_{j-1} = H^0(A, \Omega^1_{A/R_{j-1}}) \end{array}$$

where ω_{j-1}, ω_j are free R-modules that are rank g direct summands of R_{j-1}^{2g} and R_j^{2g}, respectively. In particular, an endomorphism $f \in \mathrm{End}(A)$ acts canonically and compatibly on R_{j-1}^{2g} and R_j^{2g} and preserves ω_{j-1}. It extends to an endomorphism of $\mathbb{A}$ if and only if it preserves ω_j. Consider then $p^{t_R} f$. Let $x \in \omega_j$ and choose a $y \in \omega_j$ such that $f(x) = y \pmod{I_j}$, i.e. equality holds between the images of $f(x)$ and y in ω_{j-1}. Then $f(x) - y$ is in the kernel of the homomorphism $\omega_j \to \omega_{j-1}$, which is certainly contained in $I_j R_j^{2g}$. Since $p^{t_R} I_j = 0$, we conclude that $p^{t_R} f(x) - p^{t_R} y = 0$ and so $p^{t_R} f(x) \in \omega_j$.

We note that the same reasoning gives that if $s \cdot f$ extends to an endomorphism of $\mathbb{A}$ and $(p, s) = 1$ then f also extends, because s is invertible in R. This can also be concluded from the Serre-Tate theory that gives $\mathrm{End}(\mathbb{A}) = \{f \in \mathrm{End}(\mathbb{A}[p^\infty]) : f|_{A[p^\infty]} = g|_{A[p^\infty]} \text{ for some } g \in \mathrm{End}(A)\}$, namely, the endomorphisms of $\mathbb{A}$ are the endomorphisms of its p-divisible group whose restriction to the p-divisible group of A is induced from a bona fide endomorphism of A.

We have $r - 1$ appearing in the power of p in the statement of the proposition, namely there is "a saving of 1", because $\mathbb{Z} \subseteq \mathrm{End}(\mathbb{A})$ and is a direct summand in it (as an abelian group).

6.4. **Ordinary abelian varieties.** Strictly speaking, the following is not needed for the main results of our paper, as we shall need to consider supersingular abelian varieties. It is included here for the sake of completeness. Our main reference is Katz's paper [Kat].

Let k be an algebraically closed field of characteristic p and let A be an ordinary abelian variety over k. We let $T_p(A) = \varprojlim A[p^n](\overline{\mathbb{F}}_p)$ and $V_p(A) = T_p(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then the deformations of A are pro-represented by a formal torus over the Witt vectors of k, $\widehat{\mathbb{G}}_m^{g^2} \to \mathrm{Spf}(W(k))$. One

fixes isomorhisms $T_p(A) \cong \mathbb{Z}_p^g$ and $T_p(A^t) \cong \mathbb{Z}_p^g$. The deformations $\mathbb{A} \to \mathrm{Spec}(R)$ of A to a local artinian ring R with residue field k are in functorial bijection with

$$\mathrm{Hom}(T_p(A) \otimes_{\mathbb{Z}_p} T_p(A^t), \widehat{\mathbb{G}_m}(R)) = \mathrm{Hom}(\mathbb{Z}_p^g \otimes_{\mathbb{Z}_p} \mathbb{Z}_p^g, 1 + \mathfrak{m}_R),$$

and so can viewed as bilinear forms on $\mathbb{Z}_p^g \times \mathbb{Z}_p^g$ with values in the multiplicative group $1 + \mathfrak{m}_R$. We denote the bilinear form corresponding to a deformation $\mathbb{A} \to \mathrm{Spec}(R)$ of A by $\langle\ ,\ \rangle_{\mathbb{A}}$. In particular, an endomorphism $f\colon A \to A$ extends to $\mathbb{A}$ if and only if

$$\langle fx, y\rangle_{\mathbb{A}} = \langle x, f^t y\rangle_{\mathbb{A}},$$

where we use f to denote also the endomorphism of $\mathbb{Z}_p^g$ induced from f via the chosen identification $\mathbb{Z}_p^g \cong T_p(A)$, and similarly for $f^t\colon A^t \to A^t$.

The canonical lift of A to R is the deformation $\mathbb{A}$ such that $\langle\ ,\ \rangle_{\mathbb{A}}$ is the trivial pairing (identically 1) and we see the well-known fact that for this deformation $\mathrm{End}(A) = \mathrm{End}(\mathbb{A})$ and so $\mathfrak{i}(R) = 1$. We also see that if p^a is the exponent of the multiplicative group $1 + \mathfrak{m}_R$ then if $f \in \mathrm{End}(A)$ then $p^a f$ extends to any deformation of A to R.

Let us assume that A is a simple ordinary abelian variety with complex multiplication. This is the case for example if A is simple and defined over $\overline{\mathbb{F}}_p$. In this case, $\mathrm{End}^0(A)$ is a CM field K; let $\mathcal{O} \subset K$ be the order optimally embedded in $\mathrm{End}(A)$. Since the action of $\mathcal{O}$ lifts to the canonical lift of A and so to characteristic zero, it follows from the theory of complex abelian varieties that f^t is just given by $\bar{f}$ (complex conjugation applied to f) if one chooses any polarization to identify $V_p(A)$ with $V_p(A^t)$. We find that f extends to a deformation $\langle\ ,\ \rangle_{\mathbb{A}}$ if and only if

$$\langle fx, y\rangle_{\mathbb{A}} = \langle x, \bar{f}y\rangle_{\mathbb{A}}.$$

For a fixed f this is a linear equation in the matrix coefficients of $\langle\ ,\ \rangle_{\mathbb{A}}$. In general, this can be used to explicitly determined the closed subscheme $Z_{\mathcal{O}}$ and one sees that they come out formal sub-tori. To illustrate we consider the one-dimensional case.

6.4.1. *Ordinary elliptic curves.* In this case $\langle\ ,\ \rangle_{\mathbb{A}}$ is just an element $\langle 1, 1\rangle_{\mathbb{A}} = q_{\mathbb{A}} \in 1 + \mathfrak{m}_R$. We claim that since p is split in K, the identification of f with an element of $\mathbb{Z}_p$ (viewed as a homomorphism of $\mathbb{Z}_p \cong T_p(A)$) is just viewing f as an element of $\mathbb{Z}_p$ via the embedding $K \to \mathbb{Q}_p$ determined by one of the prime ideals of K above p (it would not matter which). An endomorphism f extends to this deformation if and only if $q_{\mathbb{A}}^{f-\bar{f}} = 1$. If the order of $q_{\mathbb{A}}$ is p^a then this says that $f - \bar{f}$ is divisible by p^a. Thus, $\mathrm{End}(\mathbb{A})$ is the intersection of $\mathrm{End}(A)$ with the order of conductor p^a in K.

In particular, we see that if $\mathrm{End}(A) = \mathcal{O}_K$ and the exponent of $1 + \mathfrak{m}_R$ is p^b then for every $0 \leq a \leq b$ there is a deformation $\mathbb{A}$ with $\mathrm{End}(A)$ the order $\mathcal{O}_{K,p^a}$ of conductor p^a. Conversely, the set of $q \in 1 + \mathfrak{m}_R$ to which $\mathcal{O}_{K,p^a}$ extend is defined by the equation $q^{p^a} = 1$. These are the closed sets appearing in Proposition 6.1.4. This is of interest: if R is a dvr of mixed characteristic and we are trying to find a deformation $\mathbb{A}$ of A to R such that $\mathrm{End}(\mathbb{A}) = \mathcal{O}_{K,p}$, say, then we must introduce ramification. We need a p-th root of unity. In fact, a closer look reveals that for an elliptic curve $E/\overline{\mathbb{F}}_p$ with CM by $\mathcal{O}_K$, there are precisely $p^a - p^{a-1}$ deformations $\mathbb{E}$ to characteristic zero such that $\mathcal{O}_{K,p^a}$ is optimally embedded in $\mathrm{End}(\mathbb{E})$. They are provided by the primitive p^a-roots of unity. The fact that there is a unique deformation for which we get an action of $\mathcal{O}_K$ implies that no two singular moduli for $\mathcal{O}_K$ are congruent modulo p. The relation between the class numbers h, h_{p^a}, of $\mathcal{O}_K$ and $\mathcal{O}_{K,p^a}$ respectively, is (assume for simplify that $K \neq \mathbb{Q}(i), \mathbb{Q}(\omega)$): $h_{p^a} = h \times (p^a - p^{a-1})$ (cf. [Lang2, Theorem 7, §8.1]) and so we conclude that for every elliptic curve $\mathbb{E}$ over a p-adic ring with action of $\mathcal{O}_{K,p^a}$ the reduction has action by $\mathcal{O}_K$,

as in the supersingular case. This is classical (see [Lang2, Theorem 5, § 13.2]). Note also that we get very precise information about the p-adic completion of the field generated by the singular moduli for $\mathcal{O}_{K,p^a}$ and so about the ramification at p of this field.

6.5. **Supersingular elliptic curves.** Let $k = \overline{\mathbb{F}}_p$. Let V be a complete dvr containing the completion of the maximal unramified extension $W(k)$ of $\mathbb{Z}_p$ and of ramification index $e_V < p-1$. Then $V \to k$ has topologically nilpotent divided powers coming from $\gamma_n(x) = x^n/n!$ in V. In fact, using results of Zink (see remarks on page 6 of [Zink]), it is enough to assume that $e_V \leq p-1$ and so that V has divided powers structure (not necessarily nilpotent). The advantage is that $p = 2$ is allowed too, as long as it is unramified.

Let E/k be a supersingular elliptic curve. Recall that $\mathrm{End}(E)$ is a maximal order in the rational quaternion algebra $B_{p,\infty}$ ramified only at p and ∞. We apply Grothendieck's crystalline deformation theory to study for a deformation $\mathbb{E}/R$ of E the index $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})]$.

Lemma 6.5.1. *The following holds:*

(1) $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] = [\mathrm{End}(E) \otimes \mathbb{Z}_p : \mathrm{End}(\mathbb{E}) \otimes \mathbb{Z}_p]$.
(2) $\mathrm{End}(E) \otimes \mathbb{Z}_p \cong \left\{ \left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in W(\mathbb{F}_{p^2}) \right\} =: D$, *where σ is the Frobenius automorphism.*
(3) *There is a basis $\{e_1, e_2\}$ of $H^1_{\mathrm{crys}}(E/W(k))$ with respect to which the action of $\mathrm{End}(E)$ is given as matrices as in* (2).

Proof. The first claim holds, because by Proposition 6.1.1 the index is a power of p. To prove the rest, we note that E can be defined over $\mathbb{F}_{p^2}$ and so $H^1_{\mathrm{crys}}(E/W(k))$ has a basis e_1, e_2 defined over $\mathbb{F}_{p^2}$ such that the σ-linear Frobenius map is given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)$ with respect to this basis. Now, we have $\mathrm{End}(E) \otimes \mathbb{Z}_p \cong \mathrm{End}(E[p^\infty])$ (this uses Tate's theorem at p plus the fact that the Galois action, being in the commutant of the quaternion algebra $\mathrm{End}^0(E)$ is central), which is in turn isomorphic to the endomorphisms of $H^1_{\mathrm{crys}}(E/W(k))$ commuting with $\left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)$. The condition then comes out

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \begin{pmatrix} a^\sigma & b^\sigma \\ c^\sigma & d^\sigma \end{pmatrix},$$

i.e.,

$$\begin{pmatrix} pb & a \\ pd & c \end{pmatrix} = \begin{pmatrix} c^\sigma & d^\sigma \\ pa^\sigma & pb^\sigma \end{pmatrix},$$

from which now both (2) and (3) follow. □

Proposition 6.5.2. *In the basis $\{e_1, e_2\}$ the Hodge filtration on $H^1_{\mathrm{dR}}(E/k)$ is given by the image of the span of e_1 in $H^1_{\mathrm{crys}}(E/W(k))$.*

Let n be a positive integer. A deformation $\mathbb{E}$ of E to $R := V/\mathfrak{m}_V^n$, equipped with its canonical divided powers structure is given by the span of a vector in $R^2 = H^1_{\mathrm{dR}}(E/R)$ of the form $(1, y)$ with $y \in \mathfrak{m}_R$ and so we denote it $\mathbb{E}_y$. In particular, an element $\left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right)$ in $\mathrm{End}(E) \otimes \mathbb{Z}_p$ extends to the deformation $\mathbb{E}_y$ if and only if

$$\left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right) \in \mathrm{Span}_R\langle \left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right) \rangle.$$

(The proof is straightforward.)

Theorem 6.5.3. *Let V be as in Proposition 6.5.2. Then*

$$p^{2(\lceil n/e_V \rceil - 1)} \leq \mathfrak{i}(V/\mathfrak{m}_V^n) \leq \mathfrak{I}(V/\mathfrak{m}_V^n) \leq p^{3(n-1)}.$$

Furthermore, these bounds are optimal.

Proof. Let $R = V/\mathfrak{m}_V^n$ and $D_y = \left\{ \left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in W(\mathbb{F}_{p^2}), by^2 + (a - a^\sigma)y - pb^\sigma \equiv 0 \pmod{\mathfrak{m}_V^n} \right\}$. Note that

$$\left(\begin{smallmatrix} a & b \\ pb^\sigma & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right) \in \mathrm{Span}_R\langle \left(\begin{smallmatrix} 1 \\ y \end{smallmatrix}\right)\rangle \Leftrightarrow by^2 + (a - a^\sigma)y - pb^\sigma \equiv 0 \pmod{\mathfrak{m}_V^n},$$

and so D_y is a ring, identified with $\mathrm{End}(\mathbb{E}_y) \otimes \mathbb{Z}_p$. We note that the map

$$\varphi : D \to R, \qquad \left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right) \mapsto by^2 + (a - a^\sigma)y - pb^\sigma,$$

is a $\mathbb{Z}_p$-linear map whose kernel is D_y. We shall give a lower bound on $[D : D_y]$ by bounding $\sharp D/D_y = \sharp\varphi(D)$ from below.

Suppose that $p \neq 2$. Let $\{1, \alpha\}$ be a $\mathbb{Z}_p$ basis to $W(\mathbb{F}_{p^2})$ such that $\alpha^\sigma = -\alpha$ and α is a unit. We normalize the p-adic valuation so that $\mathrm{val}(p) = 1$. If $A, B \in \mathbb{Z}_p$ then $\mathrm{val}(A + B\alpha) = \mathrm{val}(A - B\alpha) = \min\{\mathrm{val}(A), \mathrm{val}(B)\}$. We note that

$$\varphi(D) = \mathrm{Span}_{\mathbb{Z}_p}\{y^2 - p, \alpha(y^2 + p), \alpha y\}.$$

Consider the linear combination

$$C(A, B) = A(y^2 - p) + B\alpha(y^2 + p), \qquad A, B \in \mathbb{Z}_p.$$

We note that

$$\mathrm{val}(C(A, B)) < \gamma := \frac{n}{e_v} \implies C(A, B) \neq 0 \quad (\text{in } R = V/\mathfrak{m}_V^n).$$

Let y denote also some lift of $y \in R$ to V. We distinguish cases:

(1) $\mathrm{val}(y) > 1/2$. We write

$$C(A, B) = y^2(A + B\alpha) - p(A - B\alpha).$$

Since $\mathrm{val}(A + B\alpha) = \mathrm{val}(A - B\alpha)$ and $\mathrm{val}(y^2) > 1$, we find that

$$\mathrm{val}(C(A, B)) = 1 + \min\{\mathrm{val}(A), \mathrm{val}(B).$$

It follows that as long as either $\mathrm{val}(A)$ and $\mathrm{val}(B)$ are both less than $\gamma - 1$, or, equivalently, less or equal to $\lceil\gamma\rceil - 2$, we have $C(A, B) \neq 0$. Equivalently, the group homomorphism

$$\mathbb{Z}/p^{\lceil\gamma\rceil-1} \times \mathbb{Z}/p^{\lceil\gamma\rceil-1} \longrightarrow R, \qquad (A, B) \mapsto C(A, B),$$

is injective. We conclude that $\sharp\varphi(D) \geq p^{2(\lceil\gamma\rceil-1)}$.

(2) $\mathrm{val}(y) < 1/2$. In this case $\mathrm{val}(y^2) < 1$ and so we find that $\mathrm{val}(C(A, B)) = \mathrm{val}(y^2) + \min\{\mathrm{val}(A), \mathrm{val}(B)\} < 1 + \min\{\mathrm{val}(A), \mathrm{val}(B)\}$ and we get the same estimate (we do not bother with improving it).

(3) $\mathrm{val}(y) = 1/2$. In this case we note that either $\mathrm{val}(y^2 - p) = 1$ or $\mathrm{val}(y^2 + p) = 1$. So, either $\mathrm{val}(y^2 - p) = 1$ or $\mathrm{val}(\alpha(y^2 + p)) = 1$. We assume that $\mathrm{val}(y^2 - p) = 1$, as the other case is entirely similar. In this case we consider the linear combination

$$D(A, B) = A(Y^2 - p) + B\alpha y, \qquad A, B \in \mathbb{Z}_p.$$

Since $\mathrm{val}(A(y^2 - p)) = \mathrm{val}(A) + 1$ and $\mathrm{val}(B\alpha y) = \mathrm{val}(B) + 1/2$ and, in particular, are never equal, we find that

$$\mathrm{val}(D(A, B)) = \min\{1 + \mathrm{val}(A), 1/2 + \mathrm{val}(B)\},$$

and, as long as $\mathrm{val}(A) < \gamma - 1$ or $\mathrm{val}(B) < \gamma - 1/2$, $D(A, B) \neq 0 \in R$. Weakening the conclusion to $\mathrm{val}(A) < \gamma - 1$ and $\mathrm{val}(B) < \gamma - 1$, we find the previous estimate.

Next consider the case $p = 2$. Represent $W(\mathbb{F}_{p^2})$ as $W(\mathbb{F}_p)[t]/(t^2 + t - 1)$. A key point turn out to be that $\alpha = t - t^\sigma$ is a unit and for $A, B \in \mathbb{Z}_p$ we have

$$\mathrm{val}(A + Bt) = \mathrm{val}(A + Bt^\sigma) = \min\{\mathrm{val}(A), \mathrm{val}(B)\}.$$

One checks that

$$\varphi(D) = \mathrm{Span}_{\mathbb{Z}_p}\{y^2 - p, ty^2 - pt^\sigma, \alpha y\}.$$

We let now

$$C(A, B) = A(y^2 - p) + B(ty^2 - pt^\sigma), \qquad D(A, B) = A(y^2 - p) + B\alpha y, \qquad A, B \in \mathbb{Z}_p.$$

As before the analysis is divided into three cases: (i) $\mathrm{val}(y) > 1/2$, (ii) $\mathrm{val}(y) > 1/2$ and $\mathrm{val}(y) = 1/2$, which are treated in an entirely similar manner. In cases (i) and (ii) it is helpful to write $C(A, B) = y^2(A + Bt) - p(A + Bt^\sigma)$ and in case (iii) first one argues that we can not have both $\mathrm{val}(y^2 - p) > 1$ and $\mathrm{val}(ty^2 - pt^\sigma)$; assuming without loss of generality that $\mathrm{val}(y^2 - p) = 1$, one uses $D(A, B)$ for the estimate, as before.

The upper bound on $\mathfrak{I}(V/\mathfrak{m}_V^n)$ follows using the same technique as in the proof of Proposition 6.1.1, which itself gives a slightly weaker exponent $(3 \cdot \lceil \frac{p-1}{e_V} \rceil \cdot \lceil \frac{n-1}{p-1} \rceil)$.

We now show that the bounds in Theorem 6.5.3 are optimal.

In [Grs] Gross studies the deformations of a supersingular elliptic curve for which an action of a ring of integer of some fixed quadratic imaginary field extends K. He obtains that the endomorphism ring of such a deformation over $W(\overline{\mathbb{F}}_p)$ is precisely $\mathcal{O}_K + p^{n-1}\mathrm{End}(E)$ and, in particular, of index $p^{2(n-1)}$ in $\mathrm{End}(E)$. This conforms nicely with our theorem that states this is the best possible.

A concrete case of a deformation where this bound is achieved is the case when $y = p > 2$ and $n = 2$. Note that in that case the target of the map φ is $W(\mathbb{F}_{p^2})/(p^2)$, which has cardinality p^4. It is also easily verified that $\varphi(D)$ is generated in this case over $\mathbb{Z}_p/(p^2)$ by p and αp and so has cardinality p^2. We conclude that D_y has index p^2. In fact, D_y are the matrices in D defined by the condition $a - a^\sigma = b^\sigma \pmod p$. Thus D_y contains pD and modulo pD it is given by the basis $(a, b) = (1, 0)$ and $(a, b) = (\alpha, -2\alpha^\sigma)$. If we take any quadratic imaginary field $K = \mathbb{Q}(\sqrt{-d})$ (d square-free integer) in which p is inert and let $\alpha = \sqrt{-d}$ then we find one of the deformations considered by Gross for K.

Now consider again the case of a general $(V, \mathfrak{m}_V)$ but which is unramified over $\mathbb{Q}_p$, where $p > 2$. Suppose that there are $A, B, C \in \mathbb{Z}_p$ such that

$$A(y^2 - p) + B\alpha(y^2 + p) + C\alpha y = (B\alpha + A) \cdot y^2 + C\alpha \cdot y + p(B\alpha - A) \equiv 0 \pmod{\mathfrak{m}_V^n} \tag{6.5.1}$$

Choose y to have valuation 1, equal to the valuation of p. If $\mathrm{val}(B\alpha + A) < n - 1$, Equation (6.5.1) implies that $\mathrm{val}(C) = \mathrm{val}(B\alpha - A) = \mathrm{val}(B\alpha + A)$. We get an equation

$$y^2 + \frac{C\alpha}{B\alpha + A}y + p\frac{B\alpha - A}{B\alpha + A} \equiv y(y + \frac{C\alpha}{B\alpha + A}) \equiv 0 \pmod{\mathfrak{m}_V},$$

which is an equation with integral coefficients that holds in $V/\mathfrak{m}_V$. By Hensel's lemma it follows that the polynomial $Y^2 + \frac{C\alpha}{B\alpha+A}Y + p\frac{B\alpha-A}{B\alpha+A}$ in the variable Y has a solution, say y_0, in $W(\mathbb{F}_{p^2})$ lifting 0. Moreover, if y_0' is the other solution (so that $f(Y) = Y^2 + \frac{C\alpha}{B\alpha+A}Y + p\frac{B\alpha-A}{B\alpha+A} = (Y - y_0)(Y - y_0'))$ then $\mathrm{val}(y_0 - y_0') = 0$, as y_0' reduces to a unit modulo the maximal ideal. Now, let us choose y so that in addition $y \notin \mathbb{W}(\mathbb{F}_{p^2})$ and for every Galois conjugate y' of y the difference $y - y'$ is a unit. For example, y could be $p\zeta$ where ζ is an ℓ-t root of unity where $\ell \neq p$ is a large enough prime. Note that $f(y) = (y - y_0)(y - y_0') \equiv 0 \pmod{\mathfrak{m}_V^2}$. Since $\mathrm{val}(y) = 1$, $y - y_0'$ is a

unit and so $\mathrm{val}(y - y_0) \geq 0$. It follows that y_0 is closed to y than any of y's conjugates and so, by Krasner's lemma, $y \in \mathbb{Q}_p(y_0) = W(\mathbb{F}_{p^2}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and that is a contracdiction.

Thus, $\mathrm{val}(B\alpha + A) \geq n - 1$. We get then that $\min\{\mathrm{val}(A), \mathrm{val}(B)\} = n - 1$ and then Equation (6.5.1) give that $\mathrm{val}(C) \geq n - 1$ as well. This shows that for such a choice of y we get that $\sharp\, \varphi(D) \pmod{p^n}$ is $3(n-1)$ and so the upper bound in the theorem can be achieved. This shows that the bounds are optimal. □

6.6. **Bound in the case of high ramification.** As above, let V be a discrete valuation ring, which is a finite extension of $\mathbb{W}(\overline{\mathbb{F}}_p)$ with absolute ramification index e_V. As before, let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. The purpose of this section is to provide a lower bound on $\mathfrak{i}(V/\mathfrak{m}_V^n)$ (defined relative to deformations $\mathbb{E}$ of E to $V/\mathfrak{m}_V^n$) which is valid regardless of whether the ramification index e_V is smaller than p or not. The proof uses different techniques than the ones used above.

Consider a deformation $\mathbb{E}$ over R where $R = V/\mathfrak{m}_V^n$. The Hodge filtration

$$0 \to H^0(\mathbb{E}, \Omega^1_{\mathbb{E}/R}) \to \mathbb{H}^1_{\mathrm{dR}}(\mathbb{E}/R),$$

is stable under $\mathrm{End}(\mathbb{E})$ and so there is a resulting ring homomorphism

$$\varphi : \mathrm{End}(\mathbb{E}) \to T(R),$$

where $T(R)$ are the upper triangular matrices with entries in R,

$$T(R) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in R \right\}.$$

Let $\mathcal{O}' = \mathrm{End}(\mathbb{E}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. As we have proved above, $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] = [\mathcal{O} : \mathcal{O}']$, where $\mathcal{O}$ is the maximal order of $B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ obtained as the p-completion of $\mathrm{End}(E)$.

There is an induced ring homomorphism

$$\varphi : \mathcal{O}' \to T(R).$$

Let $K = \mathrm{Ker}(\varphi)$, let $I(R) = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : a, b, d \in R \right\}$, and let $P = \varphi^{-1}(I(R))$. Note that $I(R)$ is the kernel of the ring homomorphism

$$T(R) \to R \oplus R, \qquad \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in R \right\} \mapsto (a, d).$$

It follows that $I(R)$ is a two-sided ideal, such that $T(R)/I(R)$ is a commutative ring. Moreover, $I(R)^2 = 0$. As consequence P is a two sided ideal of $\mathcal{O}'$ such that $P^2 \subset K$, where $K = \ker(\varphi)$ and $\mathcal{O}'/P$ is commutative.

The following lemmas will be proven in the next subsection.

Lemma 6.6.1. *Let*

$$\mathcal{O}_N = \mathbb{Z}_p + p^N \mathcal{O}.$$

Then $\mathcal{O}_N$ is an order of $\mathcal{O}$. In the situation above, suppose that $\mathcal{O}' = \mathcal{O}_N$, then, in the ring R,

$$p^{4N+2} = 0.$$

Lemma 6.6.2. *For an order $\mathcal{O}' \subseteq \mathcal{O}$, let*

$$\mathrm{Ind}(\mathcal{O}') = \log_p([\mathcal{O} : \mathcal{O}']), \qquad \mathrm{App}(\mathcal{O}') = \min\{N : \mathcal{O}' \supseteq \mathcal{O}_N\}.$$

*(*Ind *is for index and* App *is for approximation.) Then,*

$$\mathrm{App}(\mathcal{O}') \leq \mathrm{Ind}(\mathcal{O}').$$

Assume the Lemmas. Given an order $\mathcal{O}'$, we have $\mathcal{O}' \supseteq \mathcal{O}_N$ where $N = \mathrm{App}(\mathcal{O}')$ and so the homomorphism φ induces a homomorphism $\varphi : \mathcal{O}_N \to T(R)$, which implies by Lemma 6.6.1 that $p^{4N+2} = 0$. Since the minimal power of p which is zero in R is $\lceil n/e_V \rceil$ we conclude that $(4{\cdot}\mathrm{App}(\mathcal{O}')+2) \geq \lceil n/e_V \rceil$. Combining it with Lemma 6.6.2, we find that $\mathrm{Ind}(\mathcal{O}') \geq \frac{1}{4}(\lceil n/e_V \rceil - 2)$. To summarize, we have proven the following theorem.

Theorem 6.6.3. *With the above notation,*

$$p^{\frac{1}{4}(\lceil n/e_V \rceil - 2)} \leq \mathfrak{i}(V/\mathfrak{m}_V^n).$$

6.6.1. *Proof of the Lemmas.* We use the presentation for the maximal order $\mathcal{O}$ given above,

$$\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix} : a, b \in W(\mathbb{F}_p^2) \right\}.$$

Consider the situation where $\mathcal{O}' = \mathcal{O}_N = \mathbb{Z}_p + p^N\mathcal{O}$. We have a homomorphism $\varphi : \mathcal{O}_N \to T(R)$ with kernel K and the ideal $P = \varphi^{-1}(I(R))$. As we have noted $P^2 \subseteq K$. Let $[x, y] := xy - yx$. Since $\mathcal{O}_N/P$ is commutative, we must have $[x, y] \in P$ for all $x, y \in \mathcal{O}_n$, and so $[x, y]^2 \in K$ for all $x, y \in \mathcal{O}_N$. Consider the elements $x = p^N \begin{pmatrix} & 1 \\ p & \end{pmatrix}, y = p^N \begin{pmatrix} & t \\ pt^\sigma & \end{pmatrix}$, where for $p \neq 2$ we choose t to be a unit in $W(\mathbb{F}_{p^2})$ such that $t^\sigma = -t$ and for $t = 2$ we choose $t \in W(\mathbb{F}_{p^2})$ such that $t^2 + t - 1 = 0$. In both cases $t - t^\sigma$ is a unit whose square is a unit in $\mathbb{Z}_p$, hence in $\mathcal{O}_N$. Now,

$$[x, y] = p^{2N+1} \begin{pmatrix} t^\sigma - t & \\ & t - t^\sigma \end{pmatrix}.$$

We conclude that $p^{4N+2} \begin{pmatrix} (t^\sigma - t)^2 & \\ & (t - t^\sigma)^2 \end{pmatrix} \in K$ and so that $p^{4N+2} = 0$ in R. Lemma 6.6.1 follows.

Lemma 6.6.2 is in fact trivial. The abelian group $\mathcal{O}/\mathcal{O}'$ has order $p^{\mathrm{Ind}(\mathcal{O}')}$ and thus, if $a \in \mathcal{O}$ then $p^{\mathrm{Ind}(\mathcal{O}')} \cdot a = 0$ in $\mathcal{O}/\mathcal{O}'$, namely, $p^{\mathrm{Ind}(\mathcal{O}')} \cdot \mathcal{O} \subseteq \mathcal{O}'$.

6.6.2. *Scholium.* One may ask if the bound in Lemma 6.6.2 can be improved. The answer to that is *no*. The reader is referred to the paper by Brzezinski [Brz]. In particular, in Proposition (5.6) of that paper we find the classification of all Gorenstein orders in $\mathcal{O}$. Examination of the classification shows that our Lemma cannot be improved; More precisely, in cases (a), (b) and (c_1) one actually finds that $\mathrm{App}(\mathcal{O}') \leq \lceil \mathrm{Ind}(\mathcal{O}')/2 \rceil$ (and the passage to non-Gorenstein order is not a problem using Proposition (1.4) of that paper), but this does not persist in case (c_2).

7. The main theorem

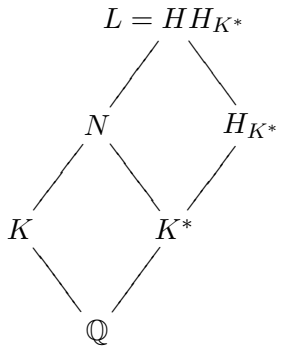
Let K be a primitive CM field of degree four over $\mathbb{Q}$. Let $K^+ = \mathbb{Q}(\sqrt{d})$ where d is a positive square-free integer. Write

$$K = \mathbb{Q}(\sqrt{d})(\sqrt{r}), \qquad r = \alpha + \beta\sqrt{d} \ll 0, \qquad \alpha, \beta \in \mathbb{Z}.$$

(That is, r is negative under both embeddings of K^+ into $\mathbb{R}$.)

Let $\tau \in \mathrm{Sp}(4, \mathbb{Z})\backslash\mathfrak{H}_2$ be a point such that the associated principally polarized abelian variety A_τ has CM by $\mathcal{O}_K$. Let $L = NH_{K^*}$, where N is the normal closure of K over $\mathbb{Q}$ and let $\mathfrak{p}_L$ be

a prime of L above the rational prime p. We fix the notation as in § 3. In particular the CM type is Φ as given there and we have prime ideals $\mathfrak{p}_{N,1} = \mathfrak{p}_L \cap N, \mathfrak{p}_{K,1} = \mathfrak{p}_L \cap K, \mathfrak{p}_{K^*,1} = \mathfrak{p}_L \cap K^*$ and p, corresponding to the fields in the diagram:



Let $e = e(\mathfrak{p}_{N,1}/p)$ be the ramification index of $\mathfrak{p}_{N,1}$ over p.

Theorem 7.0.4. *Let τ be a CM point, as above. Let $f = g/\Theta^k$ be a modular function of level one on $\mathfrak{H}_2$ where:*

1. *Θ is Igusa's $4 \cdot \chi_{10}$, the product of the squares of the ten Riemann theta functions with even integral chracteristics, normalized to have Fourier coefficients that are relatively prime integers.*
2. *g is a level one modular form of weight $10k$ with relatively prime integral Fourier coefficients.*

Then $f(\tau) \in L = NH_{K^*}$ and

$$\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq \begin{cases} -4ke\left(\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right)+1\right) & e \leq p-1 \\ -4ke\left(8\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right)+2\right) & \textit{else.} \end{cases} \tag{7.0.1}$$

Furthermore, unless we are in the situation of superspecial reduction, namely, unless we have a check mark in the last column of the tables in § 3, $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq 0$. The valuation is normalized so that a uniformizer at $\mathfrak{p}_L$ has valuation 1.

Proof. Let $v = \mathrm{val}_{\mathfrak{p}_L}(f(\tau))$. We may assume that $v < 0$. To conceptualize the proof, we divide it into steps.

Step 1: Adding level structure. Let $N \geq 3$ be an integer prime to p. We abuse notation and identify $\mathscr{A}_{2,N}(\mathbb{C})$ with $\Gamma(N)\backslash\mathfrak{H}_2$, where $\Gamma(N) \subseteq \mathrm{Sp}(4,\mathbb{Z})$ is the principal congruence subgroup of matrices congruent to 1 modulo N. Let $\tau_N \in \mathscr{A}$ such that

$$\pi_N(\tau_N) = \tau,$$

where $\pi_N \colon \mathscr{A}_{2,N} \to \mathscr{A}_{2,1}$ is the natural projection. The point τ_N is defined over the field $\mathfrak{p}_{L_N}$, where $L_N = L(A_\tau[N])$ is the field obtained from L by adjoining the N-torsion points of A_τ. The extension L_N/L is unramified at p (c.f. proof of Lemma 2.7.1). We let $\mathfrak{p}_{L_N}$ be a prime of L_N such that $\mathfrak{p}_{L_N} \cap L = \mathfrak{p}_L$.

Lemma 7.0.5. *Let $f_N = f \circ \pi_N$. Then,*

$$\mathrm{val}_{\mathfrak{p}_{L_N}}(f_N(\tau_N)) = \mathrm{val}_{\mathfrak{p}_L}(f(\tau)).$$

Proof. This is clear: $f_N(\tau_N) = f(\tau)$ and the extension L_N/L is unramified at $\mathfrak{p}_L$. □

It is therefore enough to prove the same bound given in (7.0.1) but for $\mathrm{val}_{\mathfrak{p}_{L_N}}(f_N(\tau_N))$.

Step 2: Reducing to a geometric problem.

Lemma 7.0.6. *Let (f_N) be the divisor of f_N on $\mathscr{A}_{2,N}$. Let $(f)_\infty$ be its polar part. Let $\mathscr{H}_{1,N}$ be the Humbert divisor of invariant 1 on $\mathscr{A}_{2,N}$. Then,*

$$(f)_\infty = 4k \cdot \mathscr{H}_{1,N}.$$

Proof. It is well-known that Θ vanishes to order 2 on $\mathscr{H}_{1,1}$. The Lemma then follows immediately from Lemma 2.6.1. □

By Lemma 2.7.1, the abelian variety A_{τ_N} has good reduction at $\mathfrak{p}_{L_N}$. Let Λ be the ring of integers of $\widetilde{L}_N$ (the completion of L_N at $\mathfrak{p}_{L_N}$) and $\mathfrak{P}$ its maximal ideal. Then there is a morphism

$$\iota : \Lambda \to \mathscr{A}_{2,N},$$

corresponding to A_{τ_N}.

Proposition 7.0.7. *Let $A := A_{\tau_N}$. There is an unramified field extension M of $\widetilde{L}_N$ of degree at most 2, with ring of integers V, such that*

$$A \otimes (V/\mathfrak{m}_V^w) \cong \mathbb{E} \times \mathbb{E}',$$

as polarized abelian varieties, where $\mathbb{E}, \mathbb{E}'$ are elliptic curves over $V/\mathfrak{m}_V^w$, and where

$$w = \lceil -v/4k \rceil.$$

Proof. By Lemma 5.0.4, applied to $1/f$, the morphism ι induces a morphism

$$\iota : \Lambda/\mathfrak{P}^w \to \mathscr{H}_{1,N}.$$

In the notation of Proposition 4.0.2, we have $\mathscr{H}_{1,N} = \beta(\mathscr{B}_N)$.

Consider the cartesian diagram

$$\begin{array}{ccc} S & \longrightarrow & \mathscr{B}_N \\ \downarrow & \square & \downarrow \beta \\ \mathrm{Spec}(\Lambda/\mathfrak{P}^w) & \longrightarrow & \mathscr{H}_{1,N} \end{array}$$

Since $\beta\colon \mathscr{B}_N \to \mathscr{H}_{1,N}$ is étale of degree 2, the morphism $S \to \mathrm{Spec}(\Lambda/\mathfrak{P}^w)$ is étale and affine, and so S is an affine scheme, possibly disconnected. We can then choose a field M, as in the statement of the proposition, such that $\mathrm{Spec}(V/\mathfrak{m}_V^w)$ is equal to S (or one of its connected components). We therefore get a point

$$\mathrm{Spec}(V/\mathfrak{m}_V^w) \to \mathscr{B}_N,$$

lifting ι, and that means precisely that $A \otimes V/\mathfrak{m}_V^w$ is isomorphic, as a polarized abelian variety with level N structure, to a product of elliptic curves over $V/\mathfrak{m}_V^w$, with the natural product polarization and some level N structure. □

Note that $\mathrm{val}_{\mathfrak{m}_V}(f_N(\tau_N)) = \mathrm{val}_{\mathfrak{p}_{L_N}}(f_N(\tau_N))$ and so it is enough to show that (7.0.1) holds for $\mathrm{val}_{\mathfrak{m}_V}(f_N(\tau_N))$. Let us reset our notation and recall that at this point we have a principally polarized abelian surface $A = A_{\tau_N} \otimes V$ with CM by $\mathcal{O}_K$, having good reduction at $\mathfrak{m}_V$ and such that

$$A \otimes V/\mathfrak{m}_V^w \cong (\mathbb{E} \times \mathbb{E}', \lambda_1 \times \lambda_2),$$

where $\mathbb{E}, \mathbb{E}'$, are elliptic curves over $V/\mathfrak{m}_V^w$. Recall also that V is an unramified extension of the completion of $L = NH_{K^*}$ at the prime $\mathfrak{p}_L$.

Step 3: Reduction to a statement about $\mathrm{End}(\mathbb{E})$. Our notation for the field $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$ is precisely as in [GL1]. As in loc. cit., one argues that $\mathbb{E}$ and $\mathbb{E}'$ have supersingular reduction, denoted E, E', respectively. One writes

$$\sqrt{d} \mapsto \begin{pmatrix} a & b \\ b^\vee & -a \end{pmatrix}, \qquad \sqrt{r} \mapsto \begin{pmatrix} x & y \\ -y^\vee & w \end{pmatrix},$$

as elements of

$$\mathrm{Hom}(\mathbb{E} \times \mathbb{E}') = \begin{pmatrix} \mathrm{End}(\mathbb{E}) & \mathrm{Hom}(\mathbb{E}', \mathbb{E}) \\ \mathrm{Hom}(\mathbb{E}, \mathbb{E}') & \mathrm{End}(\mathbb{E}') \end{pmatrix}.$$

(We are using $\vee$ to denote the dual isogeny.) Note that $b \in \mathrm{Hom}(\mathbb{E}', \mathbb{E})$ is an isogeny of degree $bb^\vee \leq d$. Using b, we may view $\mathrm{End}(\mathbb{E} \times \mathbb{E}')$ as a subring of $M_2(\mathrm{End}^0(\mathbb{E}))$ by

$$\begin{pmatrix} 1 & \\ & b^{\vee,-1} \end{pmatrix} (\varphi_{ij}) \begin{pmatrix} 1 & \\ & b^\vee \end{pmatrix}.$$

Appying this to the matrices defining $\sqrt{d}, \sqrt{r}$, we find the matrices

$$\begin{pmatrix} a & bb^\vee \\ 1 & -a \end{pmatrix}, \qquad \begin{pmatrix} x & yb^\vee \\ -\frac{1}{bb^\vee} by^\vee & \frac{1}{bb^\vee} bwb^\vee \end{pmatrix}.$$

As in [GL1], the integral(!) elements $1, x, yb^\vee, xyb^\vee$ must be linearly independent over $\mathbb{Z}$ (one shows that otherwise they generate a quadratic imaginary subfield K_1 of $B_{p,\infty}$ such that we have $K \hookrightarrow M_2(K_1)$, leading to a contraction). As in [GL1, p. 464], one finds that the norms of these elements are bounded, respectively, by

$$1, \delta_2, d\delta_1, d\delta_1\delta_2,$$

where

$$\delta_1 = |\alpha| - |\beta| \cdot |a|, \qquad \delta_2 = |\alpha| + |\beta| \cdot |a|.$$

It follows that

$$[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] \leq [\mathrm{End}(E) : \mathbb{Z}[1, x, yb^\vee, xyb^\vee]] \leq 4d^2(\delta_1\delta_2)^2.$$

(Cf. [GL1, p. 460] for the last inequality.)

Step 4: Input from deformation theory. We now utilize the results of § 6 to bound the index $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})]$ from below. Recall that $\mathbb{E}$ is an elliptic curve over $V/\mathfrak{m}_V^w$ and V is an unramified extension of the completion of $L = NH_{K^*}$, hence of N completed at the prime $\mathfrak{p}_{N,1}$. Thus, e_V – the absolute ramification index of V – is equal to $e = e(\mathfrak{p}_{N,1}/p)$.

(1) **Small ramification.** Suppose that $e \leq p - 1$. By Theorem 6.5.3,

$$[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] \geq p^{2(\lceil w/e \rceil - 1)},$$

and so $2(\lceil w/e \rceil - 1) \leq \log_p(4d^2(\delta_1\delta_2)^2)$. Since $\delta_1\delta_2 = \alpha^2 - \beta^2 a^2 \leq \alpha^2 = \frac{1}{4}(\mathrm{Tr}(r))^2$, we find that $w/e \leq \lceil w/e \rceil \leq \frac{1}{2}\log_p(4d^2(\delta_1\delta_2)^2) + 1 \leq \log_p(\frac{d \cdot \mathrm{Tr}(r)^2}{2}) + 1$. Since $w = \lceil -v/4k \rceil$, it follows that $-v \leq 4kw \leq 4ke\left[\log_p(\frac{d \cdot \mathrm{Tr}(r)^2}{2}) + 1\right]$.

(2) **High ramification.** Suppose that $e > p-1$. By Theorem 6.6.3 ,

$$[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] \geq p^{\frac{1}{4}(\lceil w/e \rceil - 2)}.$$

Similar computations yield $-v \leq 4ke\left[8\log_p(\frac{d\cdot \mathrm{Tr}(r)^2}{2}) + 2\right]$.

□

7.1. **Factorization of class invariants and denominators of Igusa class polynomials.** We derive several consequences of Theorem 7.0.4.

Corollary 7.1.1. *Let K be a quartic primitive CM field, as in the beginning of § 7 and let $\mathfrak{h}_i(x)$, $i = 1, 2, 3$, be the class polynomial defined using the function $f_i/\Theta^{k(i)}$ as in §2.4, equation (2.4.2), where $k(i) = 6, 4, 4$ for $i = 1, 2, 3$, respectively. In the notation of Theorem 7.0.4, the coefficient of $x^{\deg(h_i)-a}$ in $h_i(x)$, which is a rational number, has valuation val_p greater or equal to*

$$\begin{cases} -4a \cdot k(i)\left(\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 1\right) & e \leq p-1 \\ -4a \cdot k(i)\left(8\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 2\right) & \textit{else.} \end{cases}$$

Proof. Straightforward from Theorem 7.0.4. □

Remark 7.1.2. We remark that this corollary is crucial in bounding the complexity of construction of CM curves of genus 2, by the methods currently used. The Corollary is proven for the invariants that we find convenient; with little effort one can deduce easily such bound for the Igusa class polynomials appearing in equation 2.4.1, which are often used in the literature. Further, we could have equally proven the Corollary for class polynomials formed out of the Igusa coordinates γ_i (see §2.3). In principle, this is "the right thing to do", on the other hand, given Proposition 2.3.1, in practice it suffices to deal only with (some set of) the absolute Igusa invariants.

Corollary 7.1.3. *Let $u(\Phi; \mathfrak{a}, \mathfrak{b})$ be the class invariant defined in* [DSG]*, associated to fractional ideals $\mathfrak{a}, \mathfrak{b}$ of K. Let $\mathfrak{p}_L$ be a prime of L, as in Theorem 7.0.4 and $\mathfrak{p}_{H_{K^*}} = \mathfrak{p}_L \cap H_{K^*}$. We note that $u(\Phi; \mathfrak{a}, \mathfrak{b}) \in H_{K^*} \subseteq L$. We have*

$$|\mathrm{val}_{\mathfrak{p}_{H_{K^*}}}(u(\Phi; \mathfrak{a}, \mathfrak{b}))| \leq \begin{cases} 8e^*\left(\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 1\right) & e \leq p-1 \\ 8e^*\left(8\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 2\right) & \textit{else,} \end{cases}$$

where e^* is the ramification index of $\mathfrak{p}_{K^*} = \mathfrak{p}_{K^*,1}$ over p.

Proof. We refer to [DSG] for the detailed definitions. We have

$$u(\Phi, \mathfrak{a}) = \frac{\Theta(\Phi(\mathfrak{a}^{-1}))}{\Theta(\Phi(\mathcal{O}_K))},$$

which may also be written as

$$u(\Phi, \mathfrak{a}) = \left(\frac{\Theta|_\gamma}{\Theta}\right)(\tau),$$

where τ is a period matrix for $\Phi(\mathcal{O}_K)$ and, for $\mathfrak{a}^{-1}$ an integral ideal, $\gamma \in \mathrm{Sp}(4, \mathbb{Q})$ is a matrix with integral entries and determinant $\mathrm{Norm}(\mathfrak{a})$ (cf. [DSG] p. 786 and §3.2). We remark that we may also write

$$u(\Phi, \mathfrak{a}) = \left(\frac{\Theta}{\Theta|_{\gamma^{-1}}}\right)(\tau'),$$

where τ' is a period matrix corresponding to $\mathfrak{a}^{-1}$.

Now fix a prime ideal $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above the rational prime p. Assume $\mathfrak{a}^{-1}$ is an integral ideal of norm $N \geq 3$, which is relatively prime to $\mathfrak{P}$. We note that both $\frac{\Theta|_\gamma}{\Theta}$ and $\frac{\Theta}{\Theta|_{\gamma^{-1}}}$ are modular functions of level N, defined over $\mathbb{Q}(\zeta_N)$, and $u(\Phi, \mathfrak{a})$ is obtained by evaluating them at a point with CM by $\mathcal{O}_K$. We can therefore apply Theorem 7.0.4, or, more precisely, the result we have obtained in its proof by passing to level N. We consider both $\left(\frac{\Theta|_\gamma}{\Theta}\right)(\tau)$ and $\left(\frac{\Theta}{\Theta|_{\gamma^{-1}}}\right)(\tau')$ to get from one a bound on the denominator of $u(\Phi, \mathfrak{a})$ at $\mathfrak{P}$ and, from the other, a bound on the numerator. The points τ, τ' correspond to abelian varieties with CM by $\mathcal{O}_K$ defined over the compositum L' of L and $\mathbb{Q}(\zeta_N)$, which does not increase the ramification index e of p at $\mathfrak{p}_L = \mathfrak{P} \cap L$. We may then consider the valuation at $\mathfrak{p}_{L'} = \mathfrak{P} \cap L'$. We conclude that

$$|\mathrm{val}_{\mathfrak{p}_{L'}}(u(\Phi, \mathfrak{a}))| \leq \begin{cases} 4e\left(\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 1\right) & e \leq p-1 \\ 4e\left(8\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 2\right) & \text{else.} \end{cases}$$

However, the algebraic number $u(\Phi, \mathfrak{a})$ actually lies in H_{K^*} and so we get

$$|\mathrm{val}_{\mathfrak{p}_{H_{K^*}}}(u(\Phi, \mathfrak{a}))| \leq \begin{cases} 4e^*\left(\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 1\right) & e \leq p-1 \\ 4e^*\left(8\log_p\left(\frac{d\mathrm{Tr}(r)^2}{2}\right) + 2\right) & \text{else,} \end{cases}$$

where $e^* = e(\mathfrak{p}_{K^*}/p)$.

Let us now consider $u(\Phi; \mathfrak{a}, \mathfrak{b})$. The class invariant $u(\Phi; \mathfrak{a}, \mathfrak{b})$ depends only on the ideal class of $\mathfrak{a}$ and $\mathfrak{b}$ in the class group of K. Having fixed $\mathfrak{P}$, we may assume therefore that $\mathfrak{a}^{-1}, \mathfrak{b}^{-1}$ are integral and of norm prime to p. We note the expressions:

$$u(\Phi; \mathfrak{a}, \mathfrak{b}) = \frac{u(\Phi, \mathfrak{a}\mathfrak{b})}{u(\Phi, \mathfrak{a})u(\Phi, \mathfrak{b})} = \frac{\Theta(\Phi(\mathfrak{a}^{-1}\mathfrak{b}^{-1}))\Theta(\Phi(\mathcal{O}_K))}{\Theta(\Phi(\mathfrak{a}^{-1}))\Theta(\Phi(\mathfrak{b}^{-1}))}.$$

Instead of using directly our bound above, we note that for $\mathfrak{a}^{-1}, \mathfrak{b}^{-1}$ integral ideals, we may write

$$u(\Phi; \mathfrak{a}, \mathfrak{b}) = \left(\frac{\Theta|_\gamma}{\Theta}\right)(\tau')/\left(\frac{\Theta|_\beta}{\Theta}\right)(\tau),$$

where τ is a period matrix for $\Phi(\mathcal{O}_K)$, τ' is a period matrix for $\Phi(\mathfrak{a}^{-1})$, $\beta, \gamma \in \mathrm{Sp}(4, \mathbb{Q})$ are matrices with integral entries and determinants prime to p. Thus, repeating the consideration above, we conclude the bound in the corollary. □

References

[BY] Bruinier, J. H.; Yang, T.: CM-values of Hilbert modular functions. Invent. Math. 163 (2006), no. 2, 229–288.

[Brz] Brzezinski, J.: On orders in quaternion algebras. Comm. Algebra 11 (1983), no. 5, 501–522.

[Coh] Cohen, H.: Number theory. Vol. I. Tools and Diophantine equations. Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[CohI] Cohen, I. S.: On the structure and ideal theory of complete local rings. Trans. Amer. Math. Soc. 59, (1946). 54–106.

[DSG] De Shalit, E.; Goren, E. Z.: On special values of theta functions of genus two. Ann. Inst. Fourier (Grenoble) 47 (1997), no. 3, 775–799.

[Dok] Dokchitser, T.: Deformations of p-divisible groups and p-descent on elliptic curves. Ph.D. Thesis. Utrecht 2000.

[FK] Frey, G.; Kani, E.: Curves of genus 2 covering elliptic curves and an arithmetical application. Arithmetic algebraic geometry (Texel, 1989), 153–176, Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991.

[EL] Eisentraeger, K.; Lauter, K.: A CRT algorithm for constructing genus 2 curves over finite fields, Arithmetic, Geometry and Coding Theory (AGCT 2005), Séminaires et Congrés 21 (2009), 161–176.

[vdG] van der Geer, G.: On the geometry of a Siegel modular threefold. Math. Ann. 260 (1982), no. 3, 317–350.

[GHKRW] Gaudry P.; Houtmann T.; Kohel D.; Ritzenthaler C.; Weng, A.: The 2-adic CM method for genus 2 curves with application to cryptography. Advances in Cryptology, ASIACRYPT 2006, Springer-Verlag, LNCS 4284, 114-129, 2006.

[Gor] Goren, E. Z.: On certain reduction problems concerning abelian surfaces. Manuscripta Math. 94 (1997), no. 1, 33–43.

[GL1] Goren, E. Z.; Lauter, K. E.: Class invariants for quartic CM fields. Ann. Inst. Fourier (Grenoble) 57 (2007), no. 2, 457–480.

[GL2] Goren, E. Z.; Lauter, K. E.: Evil primes and superspecial moduli. Int. Math. Res. Not. 2006, Art. ID 53864, 19 pp.

[Grs] Gross, B. H.: On canonical and quasicanonical liftings. Invent. Math. 84 (1986), no. 2, 321–326.

[Gro] Grothendieck, A.: Groupes de Barsotti-Tate et cristaux de Dieudonné. Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970). Les Presses de l'Université de Montréal, Montreal, Que., 1974.

[HMNS] Hitt O'Connor, L.; McGuire, G.; Naehrig, M.; Streng, M.: CM construction of genus 2 curves with p-rank 1, Preprint 2008. http://arxiv.org/abs/0811.3434v2

[Igu1] Igusa, J.-I.: Arithmetic variety of moduli for genus two. Ann. of Math. (2) 72, 1960, 612–649.

[Igu2] Igusa, J.-I.: On Siegel modular forms of genus two. Amer. J. Math. 84 (1962), 175–200.

[Igu3] Igusa, J.-I.: On the ring of modular forms of degree two over Z. Amer. J. Math. 101 (1979), no. 1, 149–183.

[Igu4] Igusa, J.-I.: Modular forms and projective invariants. Amer. J. Math. 89 (1967), 817–855.

[IKO] Ibukiyama, T.; Katsura, T.; Oort, F.: Supersingular curves of genus two and class numbers. Compositio Math. 57 (1986), no. 2, 127–152.

[Kat] Katz, N.: Serre-Tate local moduli. Algebraic surfaces (Orsay, 1976–78), pp. 138–202, Lecture Notes in Math., 868, Springer, Berlin-New York, 1981.

[Lang1] Lang, S.: Complex multiplication. Grundlehren der Mathematischen Wissenschaften 255. Springer-Verlag, New York, 1983.

[Lang2] Lang, S.: Elliptic functions. With an appendix by J. Tate. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.

[Lau] Lauter, Kristin E.: Primes in the denominators of Igusa class polynomials. Preprint, arXiv:math.NT/0301240, 2003.

[Mes] Mestre, J.-F.: Construction de courbes de genre 2 à partir de leurs modules. Effective methods in algebraic geometry (Castiglioncello, 1990), 313–334, Progr. Math., 94, Birkhäuser Boston, Boston, MA, 1991.

[PZ] Pries, R.; Zhu, H. J.. The p-rank stratification of Artin-Schreier curves. Preprint. http://front.math.ucdavis.edu/0609.5657

[Spa] Spallek, Anne-Monika. Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen. Ph.D. Thesis. Universität Gesamthochschule Essen, 1994.

[Str] Streng, M.: Computing Igusa Class Polynomials. Preprint, http://arxiv.org/abs/0903.4766, 2009.

[Sut] Sutherland, A.: Computing Hilbert class polynomials with the Chinese Remainder Theorem. Preprint, http://arxiv.org/abs/0903.2785, 2009.

[Val] Vallieres, D.: *Class Invariants*. McGill M.Sc. thesis, 2005. http://www.math.mcgill.ca/goren

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

[Wen] Weng, A.: Constructing hyperelliptic curves of genus 2 suitable for cryptography. Math. Comp. 72 (241):435–458, 2003.

[Yaf] Yafaev, A.: Private communication. July, 2009.

[Yu] Yu, C.-F.: The isomorphism classes of abelian varieties of CM-type. J. Pure Appl. Algebra 187 (2004), no. 1-3, 305–319.

[Zink] Zink, Th.: The display of a formal p-divisible group. Cohomologies p-adiques et applications arithmétiques I. Astérisque No. 278 (2002), 127–248.

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. W., Montreal H3A 2K6, QC, Canada.

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA.
E-mail address: goren@math.mcgill.ca; klauter@microsoft.com