

A CM CONSTRUCTION FOR CURVES OF GENUS 2 WITH p -RANK 1

LAURA HITT O'CONNOR, GARY MCGUIRE, MICHAEL NAEHRIG,
AND MARCO STRENG

ABSTRACT. We construct Weil numbers corresponding to genus-2 curves with p -rank 1 over the finite field \mathbf{F}_{p^2} of p^2 elements. The corresponding curves can be constructed using explicit CM constructions. In one of our algorithms, the group of \mathbf{F}_{p^2} -valued points of the Jacobian has prime order, while another allows for a prescribed embedding degree with respect to a subgroup of prescribed order. The curves are defined over \mathbf{F}_{p^2} out of necessity: we show that curves of p -rank 1 over \mathbf{F}_p for large p cannot be efficiently constructed using explicit CM constructions.

1. INTRODUCTION

The p -rank of an abelian variety A over a field k of characteristic p is the integer $r = r(A)$ such that the group $A[p](\bar{k})$ of p -torsion points over an algebraic closure \bar{k} of k has order p^r . It satisfies $0 \leq r \leq g$, where g is the dimension of A , and we call A *ordinary* if r is equal to g . If A is *supersingular*, that is, if A becomes isogenous over \bar{k} to a product of supersingular elliptic curves, then we have $r = 0$, and the converse holds for abelian surfaces: if $r = 0$ and $g = 2$, then A is supersingular.

This shows that for an abelian surface A , besides the ordinary and supersingular cases, there is only one *intermediate* case: the case where A has p -rank 1. Most CM constructions of curves of genus two [21, 27, 4, 5] generate curves that are ordinary with probability tending to 1, while another [18] constructs only supersingular curves. We focus on the intermediate case, for which no constructions existed yet.

The p -rank $r(A)$ depends only on the *isogeny class* of A over \bar{k} , and any simple abelian surface A of p -rank 1 over a finite field k is isogenous to the Jacobian of a curve over k of genus 2 (see Section 2). By the p -rank of a curve C , we mean the p -rank of its Jacobian J_C .

Let k be the finite field of order $q = p^n$. The Frobenius endomorphism π of a simple abelian variety over k is a *Weil q -number*, i.e., an algebraic integer π such that $|\pi|^2 = q$ holds for every embedding of the field $K = \mathbf{Q}(\pi)$ into the complex numbers. A theorem of Honda and Tate [24] states that this defines a bijection between the set of isogeny classes of simple abelian varieties over k and the set of Weil q -numbers up to Galois conjugacy.

We characterize those Weil numbers corresponding to abelian surfaces with p -rank 1 in Section 2, show their existence in Section 3 and give algorithms for finding

Research of the first author supported by Science Foundation Ireland Post-Doctoral Grant 07/RFP/ENM123.

Research of the second author supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

them in Section 4. In Section 3 we also explain why curves of p -rank 1 over \mathbf{F}_p for large p cannot be efficiently constructed using explicit CM constructions.

The construction of an abelian variety A corresponding to a given Weil q -number π dates back to Shimura and Taniyama [20] and Honda [12]. It exhibits A as the reduction of a characteristic-0 abelian variety with *complex multiplication (CM)* by $\mathbf{Z}[\pi]$ and is also known as the *CM method*. We explain this explicit CM construction in Section 5. For now, it suffices to say that the computational complexity of this construction grows very rapidly with the size of the field $K = \mathbf{Q}(\pi)$. Therefore, our algorithms will look for Weil q -numbers π only in fixed small input fields K .

Let A be an abelian variety over the finite field k and suppose that $A(k)$ has a subgroup of prime order r . The *embedding degree* of A with respect to r is the degree of the field extension $k(\zeta_r)/k$, where ζ_r is a primitive r -th root of unity. The *Weil* and *Tate* pairings on A with respect to r have their image in $\langle \zeta_r \rangle \subset k(\zeta_r)^*$, and in order to compute these pairings, one needs to work with $k(\zeta_r)$. As the embedding degree is the order of q in $(\mathbf{Z}/r\mathbf{Z})^*$, it is close to r for most curves, while for *pairing-based cryptography*, one wants r to be large and the embedding degree to be small. Algorithm 3 in Section 4 provides curves with p -rank 1 and a prescribed small embedding degree.

We used our algorithms to compute various examples, which we give in Section 8. Each example was computed in a few seconds on a standard PC.

2. CHARACTERIZATION OF ABELIAN SURFACES OF p -RANK 1

It follows from the definition that the p -rank $r(A)$ of an abelian variety A does not change under extensions of the base field, and that it satisfies $r(A \times B) = r(A) + r(B)$ for any pair of abelian varieties A and B . It is also well-known that the p -rank is invariant under isogeny (see Lemma 2 below). In particular, the non-simple abelian surfaces of p -rank 1 are exactly those isogenous to the product of an ordinary and a supersingular elliptic curve. Both types of elliptic curves are well understood, so we focus on *simple* abelian surfaces. We use the word *isogeny* to mean isogeny defined over the base field k , unless otherwise stated. We use the same convention for the definition of *simple* abelian variety.

Our algorithms are based on a characterization of Weil numbers corresponding to simple abelian surfaces of p -rank 1, which we give in this section. A major part of this characterization can already be found in Goren [9] and Gonzalez [8, proof of Thm. 3.7], but we give a proof, as this result is the foundation of our construction.

Let k be the finite field of $q = p^n$ elements and let π be a Weil q -number. For every embedding of the field $K = \mathbf{Q}(\pi)$ into \mathbf{C} , complex conjugation on K is given by $\pi \mapsto q/\pi$. As this automorphism of K doesn't depend on the choice of the embedding, we denote it by $x \mapsto \bar{x}$ and call it complex conjugation. If we let K_0 be the fixed field of complex conjugation, then K_0 is totally real and K is either equal to K_0 or it is a *CM-field*, that is, a totally imaginary quadratic extension of a totally real number field.

Lemma 1. *A simple abelian variety A over the field k of $q = p^n$ elements has dimension 2 and p -rank 1 if and only if the following three conditions hold for its Frobenius endomorphism π :*

- (1) *the field $K = \mathbf{Q}(\pi)$ is a CM-field of degree 4,*
- (2) *the prime p factors in K as $p\mathcal{O}_K = \mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2^e$, with $e \in \{1, 2\}$, and*
- (3) *we have $\pi\mathcal{O}_K = \mathfrak{p}_1^n\mathfrak{p}_2^{en/2}$ with e as in (2).*

Note that condition (3) implies that en is even.

We prove Lemma 1 using the following formula for the p -rank of an abelian variety.

Lemma 2 ([8, Prop. 3.1]). *Let A be a simple abelian variety over k and let $K = \mathbf{Q}(\pi)$, where π is the Frobenius endomorphism of A . There is an integer m such that $2 \dim(A) = m \deg K$ holds. Suppose that p factors in K as $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$ and let f_i be given by $\#(\mathcal{O}_K/\mathfrak{p}_i) = p^{f_i}$. Then we have $r(A) = \sum m e_i f_i$, where the sum is taken over those i for which $\pi \notin \mathfrak{p}_i$ holds.*

Proof. The degree $\deg g$ and separable degree $\deg_s g$ of an isogeny $g : A \rightarrow B$ of abelian varieties are defined to be the degree and separable degree of the induced embedding of function fields $g^* : k(B) \rightarrow k(A)$. We have $\#(\ker g)(\bar{k}) = \deg_s g$, hence $p^{r(A)}$ is the separable degree of the multiplication-by- p map on A . As the separable degree is multiplicative under composition, we find that the p -rank of A depends only on its isogeny class, hence we can assume that $\text{End}_k A$ contains the maximal order \mathcal{O}_K by [20, Prop. 7 in §7.1].

The existence of m follows from [24, Thm. 1(2)]. The theory in [20, §7] shows how to factor the multiplication-by- p map into multiplication-by- \mathfrak{p}_i maps for prime ideals \mathfrak{p}_i , and that the multiplication-by- \mathfrak{p}_i map has degree $p^{f_i m}$. The Frobenius endomorphism π is totally inseparable by [20, Thm. 1(iii) in §2.8], hence so is multiplication-by- \mathfrak{p}_i if \mathfrak{p}_i contains π . If \mathfrak{p}_i is coprime to π , then [20, Prop. 6 in §2.8] shows that it is separable, hence satisfies $\deg_s \mathfrak{p}_i = \deg \mathfrak{p}_i$. \square

Proof of Lemma 1. If A has dimension 2 and p -rank 1, then Lemma 2 tells us $m = 1$, hence K has degree 4 and exactly one prime $\bar{\mathfrak{p}}_1 | p$ with $\pi \notin \bar{\mathfrak{p}}_1$, which is unramified and has residue degree 1. This implies $p\mathcal{O}_K = \mathfrak{p}_1 \bar{\mathfrak{p}}_1 \mathfrak{q}$, where \mathfrak{q} is prime in the fixed field K_0 of complex conjugation.

To prove that (2) and (3) hold, it now suffices to prove that \mathfrak{q} does not split in K/K_0 . Suppose that it does, say $\mathfrak{q} = \mathfrak{q}_1 \bar{\mathfrak{q}}_1$. Then by [24, Thm. 1(1)], the fact $m = 1$ implies that $\text{ord}_{\mathfrak{q}_1}(\pi)$ is either 0 or equal to the degree $n = \deg k/\mathbf{F}_p$. We also have $\text{ord}_{\mathfrak{q}_1}(\pi) + \text{ord}_{\bar{\mathfrak{q}}_1}(\pi) = \text{ord}_{\mathfrak{q}_1}(\pi \bar{\pi}) = n$, hence one of \mathfrak{q}_1 and $\bar{\mathfrak{q}}_1$ does not divide π , i.e., contradicts uniqueness of $\bar{\mathfrak{p}}_1$.

Conversely, if π satisfies (1), (2), and (3), then Lemma 2 implies $r(A) = m$ with $2 \dim(A) = m \deg K$ and [24, Thm. 1(1)] implies $m = 1$. \square

Corollary 3. *A simple abelian surface A/k of p -rank 1 is absolutely simple, that is, simple over \bar{k} , and is isogenous to the Jacobian of a curve C over k .*

Proof. Suppose that k'/k is an extension of degree d such that we have $A_{k'} \sim E \times F$. The Frobenius endomorphism of $A_{k'}$ is π^d and the characteristic polynomial of its action on the ℓ -adic Tate module of A for $\ell \neq p$ is the product of the (quadratic) characteristic polynomials of the action on the Tate modules of E and F .

On the other hand, part (3) of Lemma 1 implies that $\mathbf{Q}(\pi^d)$ is equal to K , which is a field of degree 4. This is a contradiction, hence A is absolutely simple.

By [15, Theorem 4.3], any absolutely simple abelian surface over a finite field k is isogenous to the Jacobian of a curve. \square

Remark 4. The conditions (1), (2), and (3) of Lemma 1 are equivalent to conditions (M) of Theorem 2.9 of Maisner and Nart [15], i.e., to the characteristic polynomial $f = X^4 - a_1 X^3 + (a_2 + 2q) X^2 - qa_1 X + q^2$ of π satisfying

- (1) f is irreducible,
- (2) $\text{ord}_p(a_1) = 0$,
- (3) $\text{ord}_p(a_2) \geq n/2$,
- (4) and that $(a_2 + 4q)^2 - 4qa_1^2$ is not a square in the ring of p -adic integers \mathbf{Z}_p .

Remark 5. For an elliptic curve E over a finite field k , the rank of the \mathbf{Z} -algebra $\text{End}_{\bar{k}}(E)$ of \bar{k} -endomorphisms is either 2 or 4, and these cases correspond exactly to the cases $r(E) = 1$ and $r(E) = 0$.

For abelian surfaces A , the p -rank $r(A)$ cannot be computed from the \mathbf{Z} -rank of the endomorphism algebra. In fact, for absolutely simple abelian surfaces A , the ring $\text{End}_{\bar{k}}(A) \otimes \mathbf{Q}$ is always a CM-field of degree 4, while both $r(A) = 1$ and $r(A) = 2$ occur (see also [8, Thm 3.7(ii)]).

3. EXISTENCE OF SUITABLE WEIL NUMBERS

Let p be a prime that factors in K as in (2) of Lemma 1. The fact that not all primes over p have the same ramification index or residue degree implies that the degree-4 extension K/\mathbf{Q} is not Galois. As K has a non-trivial automorphism, complex conjugation, the normal closure L of K has Galois group D_4 . We therefore have to restrict to non-Galois quartic number fields K with Galois group D_4 .

In the case $e = 2$, the prime p ramifies in K , hence divides its discriminant. Since explicit CM constructions are feasible only for small fields K , i.e., fields K of small discriminant, this means that we can construct the curve C corresponding to π only for very small values of p . For such small values of p , not only are the curves less interesting, especially from a cryptographic point of view, it also becomes possible to construct them using a more direct approach such as by enumerating all curves C of genus 2 over \mathbf{F}_p and computing the group orders of their Jacobians. Therefore, we will focus on the case $e = 1$. For $e = 1$, condition (3) of Lemma 1 implies $2|n$, so that curves are defined only over fields containing \mathbf{F}_{p^2} . This is the reason why we construct our curves over \mathbf{F}_{p^2} and not over \mathbf{F}_p , and this is why curves of p -rank 1 over \mathbf{F}_p for large p cannot be efficiently constructed using explicit CM constructions.

We have found that all fields with p -rank-1 Weil p^2 -numbers are quartic non-Galois CM-fields. However, not all quartic non-Galois CM-fields have p -rank-1 Weil p^2 -numbers, and we give a complete characterization in Section 6.

For now, we give two lemmas that put a condition on the CM-fields K that is slightly too strong, but is easy to check and is satisfied by ‘most’ non-Galois quartic CM-fields.

Lemma 6. *Let K be a quartic CM-field and let p be a prime that factors in K as $p\mathcal{O}_K = \mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2$. Suppose that $\mathfrak{p}_1 = \alpha\mathcal{O}_K$ is principal. Then $\pi = \alpha\bar{\alpha}^{-1}p$ is a Weil p^2 -number that satisfies the conditions of Lemma 1.*

Proof. The number π satisfies $\pi\bar{\pi} = p^2$, hence is a Weil p^2 -number. Conditions (1) and (2) of Lemma 1 are satisfied by assumption. Moreover, we have $\mathfrak{p}_2 = p(\mathfrak{p}_1\bar{\mathfrak{p}}_1)^{-1} = p(\alpha\bar{\alpha})^{-1}\mathcal{O}_K$, so that we have $\pi\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$, i.e., condition (3) is also satisfied. \square

The condition on p of Lemma 6 is stronger than the condition that there exists a Weil p^2 -number in K with $e = 1$. The following lemma gives a necessary and sufficient criterion on K for the existence of primes p satisfying this stronger condition.

For a non-Galois quartic CM-field K , let L be its normal closure over \mathbf{Q} and let d be the discriminant of the real quadratic subfield K_0 of K . Then we have $K = K_0(\sqrt{r})$ for a totally negative element $r \in K_0$, and $s = N_{K_0/\mathbf{Q}}(r) \in \mathbf{Q}$ is not a square, because K is non-Galois. Let d^r be the discriminant of the real quadratic field $K_0^r = \mathbf{Q}(\sqrt{s})$. Note that this field is independent of the choice of r . Indeed, the element r is well-defined up to squares in K_0^* , hence s is well-defined up to squares in \mathbf{Q}^* .

A *prime discriminant* is a number that is -4 or ± 8 or is $\pm p \equiv 1 \pmod{4}$ for an odd prime p . The discriminant of a quadratic field can be written uniquely as a product of distinct prime discriminants in which at most one even factor occurs.

Lemma 7. *Let K be a non-Galois quartic CM-field. The following are equivalent*

- (1) *there exists a prime p that factors in K as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ with \mathfrak{p}_1 principal;*
- (2) *the Dirichlet density of the set of primes p as in (1) is $(4h_K)^{-1}$, where h_K is the class number of K ;*
- (3) *there is a prime that ramifies in L/K ;*
- (4) *not all prime discriminants in the discriminant factorization of d^r occur in that of d .*

Proof. The implication (2) \Rightarrow (1) is trivial. Now suppose that (1) holds, so the decomposition group of \mathfrak{p}_1 in $\text{Gal}(L/\mathbf{Q})$ is $\text{Gal}(L/K)$ and the ideal class of \mathfrak{p}_1 is trivial. By the Artin isomorphism $\text{Cl}_K \rightarrow \text{Gal}(H/K)$, this implies that the decomposition group of \mathfrak{p}_1 in $\text{Gal}(H/K)$ is trivial for the Hilbert class field H of K . As the decomposition group of \mathfrak{p}_1 in $\text{Gal}(L/K)$ is non-trivial, this implies that L is not contained in the maximal unramified abelian extension H of K , so L/K ramifies at some prime and (3) holds.

For the proof of (3) \Rightarrow (2), we use again that the primes p as in (1) are those for which there exists a prime in L over p with decomposition group $\text{Gal}(L/K)$ in L/\mathbf{Q} and trivial decomposition group H/K . Let $M \supset H$ be Galois over \mathbf{Q} . Since (3) implies $L \cap H = K$, we find $\text{Gal}(HL/K) = \text{Gal}(H/K) \times \text{Gal}(L/K)$ and hence that exactly 1 in every $8h_K$ elements $\sigma \in \text{Gal}(M/\mathbf{Q})$ satisfies $\langle \sigma|_L \rangle = \text{Gal}(L/K)$ and $\sigma|_H = 1$. The conjugation class of $\text{Gal}(L/K)$ in $\text{Gal}(L/\mathbf{Q})$ has two elements, hence the set of all σ yielding the appropriate factorization is twice as large, i.e., consists of 1 in every $4h_K$ elements of $\text{Gal}(M/\mathbf{Q})$. By Chebotarev's density theorem [17, Theorem 13.4], this implies that the density of primes with this factorization is $(4h_K)^{-1}$, which proves (2).

Now, it remains to prove (3) \Leftrightarrow (4). Let L_0 be the compositum of K_0 and K_0^r in L . A prime $q \in \mathbf{Z}$ ramifies in L/K if and only if its inertia group in $\text{Gal}(L/\mathbf{Q})$ contains $\text{Gal}(L/K)$ or its conjugate. This is equivalent to q ramifying in L_0/K_0 , that is, to the prime discriminant in d^r corresponding to q not occurring in the prime discriminant factorization of d . \square

Example 8. The field $K = \mathbf{Q}[X]/(X^4 + 12X^2 + 2)$ does not satisfy the conditions of Lemma 7, because it has $d = 8 \cdot 17$ and $d^r = 8$.

For ‘most’ non-Galois quartic CM-fields K , the discriminant d^r does not divide d , in which case the conditions of Lemma 7 hold. This means that if we try to find our Weil numbers by taking random primes p and checking if there exists a Weil p^2 -number $\pi \in K$ as in Lemma 1, then we have a probability $(4h_K)^{-1}$ of success.

4. THE ALGORITHMS

The discussion in Section 3 leads to the following algorithm.

Algorithm 1.

Input: A non-Galois CM-field K of degree 4 and a positive integer ℓ .

Output: A prime p of ℓ bits and a Weil p^2 -number π corresponding to the Jacobian J_C of a curve of genus 2 over \mathbf{F}_{p^2} such that $\#J_C(\mathbf{F}_{p^2})$ is prime.

- (1) Take a random positive integer p of ℓ bits.
 - (2) If p is prime, continue. Otherwise, go to Step 1.
 - (3) If $p\mathcal{O}_K$ factors as $\mathfrak{p}_1\mathfrak{p}_2$, continue. Otherwise, go to Step 1.
 - (4) If $\mathfrak{p}_1^2\mathfrak{p}_2$ is principal, let π_0 be a generator and let $v = \pi_0\bar{\pi}_0p^{-2} \in \mathcal{O}_{K_0}^*$. Otherwise, go to Step 1.
 - (5) If we have $v = N_{K/K_0}(w)$ for some $w \in \mathcal{O}_K^*$, then put $\pi = w^{-1}\pi_0$. Otherwise, go to Step 1.
 - (6) If $N(u\pi - 1)$ is prime for some $u \in \{\pm 1\}$, then replace π by $u\pi$. Otherwise, go to Step 1.
 - (7) **return** p, π .
-

Note that the group order $N(\pi - 1)$ of J_C has about 4ℓ bits since we have $N(\pi - 1) \approx N(\pi) = p^4$.

Theorem 9. *If Algorithm 1 terminates, then the output is correct.*

Fix the input field K and assume that it satisfies the conditions of Lemma 7. If K has no prime ideal of norm 2, and no prime above 2 is ramified in K/K_0 , then the heuristic expected runtime of the algorithm is polynomial in ℓ .

Proof. The output π is a Weil p^2 -number satisfying the conditions of Lemma 1, and the corresponding abelian surface A has $\#A(\mathbf{F}_{p^2}) = N(\pi - 1)$ rational points, which proves that the output is correct.

All numbers encountered have logarithmic absolute values and heights that are bounded linearly in ℓ , while the field K is fixed. This shows that, using the algorithms of [2], all steps, including the primality and principality tests, as well as finding a generator of $\mathfrak{p}_1^2\mathfrak{p}_2$ and trying to extract a square root of v , take time polynomial in ℓ . It therefore suffices to prove that the heuristic expected number of iterations of Step 1 is quadratic in ℓ .

The number p has a heuristic probability $1/(\ell \log 2)$ to be prime by the Prime Number Theorem. This shows that for each time Step 3 is reached, one expects to run Step 1 about $\ell \log 2$ times.

We will ‘prove’ that the heuristic bound holds even if we restrict in Step 3 to \mathfrak{p}_1 principal and generated by α . By Lemma 7, the density of the set of primes p that factor in the appropriate way and for which α exists is $(4h_K)^{-1}$, so we arrive at Step 4 (with $\mathfrak{p}_1 = (\alpha)$) with probability $(4h_K)^{-1}$.

Note that $\pi = -\alpha\bar{\alpha}^{-1}p$ is a generator of $\mathfrak{p}_1^2\mathfrak{p}_2$, so we pass Step 4 with $\pi_0 = w\pi$ for some unit $w \in \mathcal{O}_K^*$.

Note that we have $p^2 = \pi\bar{\pi}$, hence $v = w\bar{w}$, proving that we pass Step 5 as well.

We now only need to show that $N(\pi - 1)$ is prime with sufficiently high probability. Treating α as a random element of $\mathcal{O} = \mathcal{O}_K$, we wish to know the probability that $X = N(\pi - 1)$ is prime, i.e., not divisible by any prime $q < X$. For each such

q , we consider the homomorphism

$$\varphi : (\mathcal{O}/q\mathcal{O})^* \rightarrow (\mathcal{O}/q\mathcal{O})^* : x \mapsto x\bar{x}^{-1}N(x),$$

which sends $(\alpha \bmod q)$ to $(-\pi \bmod q)$. Now we have $q|N(\pi - 1)$ if and only if $\pi \equiv 1 \pmod{q}$ for some prime $\mathfrak{q}|q$ of K . Let $\varphi_{\mathfrak{q}}$ be the composition of φ with the natural map $(\mathcal{O}/q\mathcal{O})^* \rightarrow (\mathcal{O}/\mathfrak{q})^*$. Note that we have $\pi \equiv 1 \pmod{\mathfrak{q}}$ if and only if α is an element of $\varphi_{\mathfrak{q}}^{-1}(-1)$. If we define

$$P_q = 1 - \frac{\#\bigcup_{\mathfrak{q}|q} \varphi_{\mathfrak{q}}^{-1}(-1)}{\#(\mathcal{O}/q\mathcal{O})^*},$$

then the heuristic probability of $q \nmid N(\pi - 1)$ equals P_q . As the homomorphism φ sends 1 to 1, we find $P_q > 0$ for all $q > 2$.

For $q = 2$, note that we have $N(x) = 1$. Then for all $\mathfrak{q} | q$ with $\bar{\mathfrak{q}} = \mathfrak{q}$, take $(x \bmod \mathfrak{q}) \in (\mathcal{O}/\mathfrak{q})^*$ with $x \neq \bar{x}$, which is possible, because 2 is unramified in K/K_0 . For $\mathfrak{q} | q$ with $\bar{\mathfrak{q}} \neq \mathfrak{q}$, take exactly one of $(x \bmod \mathfrak{q})$ and $(x \bmod \bar{\mathfrak{q}})$ equal to 1, which is possible because \mathfrak{q} has norm ≥ 4 . Then $x\bar{x}^{-1} \not\equiv 1 \equiv -1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} | q$, which proves $P_2 > 0$.

We use the lower bound $P_q > 0$ for $q \leq 17$.

For $q \geq 19$, note that we have

$$P_q \geq 1 - \sum_{\mathfrak{q}|q} \frac{\#\ker \varphi_{\mathfrak{q}}}{\#(\mathcal{O}/q\mathcal{O})^*} \geq 1 - \sum_{\mathfrak{q}|q} \frac{1}{\#\text{im } \varphi_{\mathfrak{q}}}$$

and that $\text{im } \varphi_{\mathfrak{q}} \supset \varphi_{\mathfrak{q}}(\mathbf{F}_q^*) = (\mathbf{F}_q^*)^4$ has order $\geq (q - 1)/4$, hence we have

$$P_q \geq 1 - 4 \frac{4}{q - 1} > 1 - \frac{17}{q}.$$

We thus find heuristically that $N(\pi - 1)$ is prime with probability at least a positive constant times

$$Y = \prod_{\substack{19 \leq q < X \\ \text{prime}}} \left(1 - \frac{17}{q}\right).$$

We find $\log(Y) > -\sum_q \frac{17}{q}$, and the right hand side, by Mertens' theorem [10, Thm. 427 in 22.7], is $17 \log \log X$ plus something that converges to a constant if X tends to infinity. In particular, we find that $1/Y$ is at most polynomial in $\log X \approx 4\ell$, which is what we needed to prove. \square

Remark 10. For more detailed heuristics on prime order Jacobians of curves of genus 2 than what is in the proof of Theorem 9, see [26, §5.2.2].

Remark 11. The conditions of Lemma 7 are sufficient in Theorem 9 and, as we said before, they hold for 'most' non-Galois quartic CM-fields. They are however not necessary, and we give strictly weaker conditions in Section 6.

The following lemma shows that the conditions on the decomposition of 2 in K are necessary in Theorem 9, and that these conditions are not specific to p -rank 1, or even to abelian surfaces. These conditions vanish however if one allows the group order to be 'almost prime' in the sense that it is a prime times a 'small' (say ≤ 16) positive integer.

Lemma 12. *Let π be the Frobenius endomorphism of an abelian variety A over a finite field k of odd characteristic, and let $K = \mathbf{Q}(\pi)$. If one of the following conditions holds, then the order of $A(k)$ is even.*

- (1) K has a prime ideal \mathfrak{q} of norm 2,
- (2) K is totally real, or
- (3) K is a CM-field with totally real subfield K_0 and K has a prime ideal $\mathfrak{q}|2$ that is ramified in K/K_0 .

Proof. If \mathfrak{q} has norm 2, then we have $\pi \not\equiv 0 \pmod{\mathfrak{q}}$, hence $\pi - 1 \equiv 0 \pmod{\mathfrak{q}}$, which implies $2|N(\pi - 1)$.

In the other two cases, complex conjugation is trivial on the group $(\mathcal{O}/\mathfrak{q})^*$ of odd order. Note that $\pi\bar{\pi} \in \mathbf{Q}$ implies that $\pi^2 = \pi\bar{\pi}$ is trivial in that group, hence so is π . We see again that $\pi - 1 \equiv 0 \pmod{\mathfrak{q}}$ implies $2|N(\pi - 1)$. \square

Our second algorithm is a modification of Algorithm 1 in which we start with an element $\alpha \in \mathcal{O}_K$, instead of with a prime p , and check if $p = N(\alpha)$ is a prime that decomposes in the appropriate manner. We use Algorithm 2 as a stepping stone towards Algorithm 3, which allows one to prescribe the embedding degree of the output by imposing congruence conditions on α .

Algorithm 2.

Input: A non-Galois CM-field K of degree 4 and a positive integer ℓ .

Output: A prime p of ℓ bits and a Weil p^2 -number corresponding to the Jacobian J_C of a curve C of genus 2 over \mathbf{F}_{p^2} such that J_C has p -rank 1 and a prime number of \mathbf{F}_{p^2} -rational points.

-
- (1) Take a random element α of \mathcal{O}_K of which the norm $N(\alpha)$ has ℓ bits.
 - (2) If $p = N(\alpha)$ is prime in \mathbf{Z} , continue. Otherwise, go to Step 1.
 - (3) If the prime $\beta = p\alpha^{-1}\bar{\alpha}^{-1}$ of \mathcal{O}_{K_0} remains prime in \mathcal{O}_K , then let $\pi = \alpha^2\beta$. Otherwise, go to Step 1.
 - (4) If $N(u\pi - 1)$ is prime for some $u \in \{\pm 1\}$, then replace π by $u\pi$. Otherwise, go to Step 1.
 - (5) **return** p, π .
-

Theorem 13. *If Algorithm 2 terminates, then the output is correct.*

Fix the input field K and assume that it satisfies the conditions of Lemma 7. If K has no prime ideal of norm 2, and no prime above 2 is ramified in K/K_0 , then the heuristic expected runtime of the algorithm is polynomial in ℓ .

Proof. By Lemma 6, the output π is a Weil p^2 -number satisfying the conditions of Lemma 1, and the corresponding abelian surface A has $\#A(\mathbf{F}_{p^2}) = N(\pi - 1)$ rational points, which proves that the output is correct.

Lemma 7 shows that among the elements α of \mathcal{O}_K of prime norm, at least about 1 in every $4h_K$ has the appropriate factorization, so if we treat $N(\alpha)$ and $N(\pi - 1)$ as random integers as we did in the proof of Theorem 9, then we find again that the heuristic expected runtime is polynomial in ℓ . \square

Remark 14. Actually, the heuristic probability of passing from Step 3 to Step 4 in Algorithm 2 is $1/2$ instead of only $(4h_K)^{-1}$ as can be seen by applying Chebotarev's density theorem to the quadratic extension LH/H from the proof of Lemma 7.

Algorithm 3 constructs p -rank-1 curves with prescribed embedding degree by imposing congruence conditions on α in a way that is similar to what is done in the algorithm of Freeman, Stevenhagen, and Streng [5].

Algorithm 3.

Input: A non-Galois CM-field K of degree 4, a positive integer κ and a prime number $r \equiv 1 \pmod{2\kappa}$ that splits completely in K .

Output: A prime p and a Weil p^2 -number π corresponding to the Jacobian J_C of a curve C of genus 2 over \mathbf{F}_{p^2} that has p -rank 1 and embedding degree κ with respect to a subgroup of order r .

- (1) Let \mathfrak{r} be a prime of K dividing r , let $\mathfrak{s} = r\mathfrak{r}^{-1}\bar{\mathfrak{r}}^{-1}$ and compute a basis b of \mathcal{O}_K .
 - (2) Take a random element x of \mathbf{F}_r^* and a primitive 2κ -th root of unity $\zeta \in \mathbf{F}_r^*$.
 - (3) Take the ‘small’ $\alpha \in \mathcal{O}_K$ such that $\alpha \bmod \mathfrak{r} = x$, $\alpha \bmod \bar{\mathfrak{r}} = x\zeta$ and $\alpha \bmod \mathfrak{s} = x^{-1}$. Here ‘small’ means that the coordinates with respect to the basis b are $\leq r/2$, and x^{-1} is interpreted with respect to the natural inclusion of \mathbf{F}_r^* into $\mathcal{O}_K/\mathfrak{s}$.
 - (4) If $p = N_{K/\mathbf{Q}}(\alpha)$ is prime in \mathbf{Z} , continue. Otherwise, go to Step 2.
 - (5) If the prime $\beta = p\alpha^{-1}\bar{\alpha}^{-1}$ of \mathcal{O}_{K_0} remains prime in \mathcal{O}_K , let $\pi = \alpha^2\beta$. Otherwise, go to Step 2.
 - (6) **return** p, π .
-

Theorem 15. *If Algorithm 3 terminates, then the output is correct. If the input field K is fixed and satisfies the conditions of Lemma 7, then the heuristic expected runtime of the algorithm is polynomial in r .*

Proof. The facts that the output has p -rank 1 and a Jacobian of order $N(\pi - 1)$ are proven as in the proof of Theorem 13.

If r divides the group order $N(\pi - 1)$, then the embedding degree is the order of $(p^2 \bmod r)$ in the group \mathbf{F}_r^* (see also [5, Proposition 2.1]). So to prove that J_C has embedding degree κ with respect to r , it suffices to prove that $p^2 \bmod r$ is a primitive κ -th root of unity in \mathbf{F}_r^* and that r divides $N(\pi - 1)$.

Let ϕ be the non-trivial automorphism of K_0 . Then we have $\beta = \phi(\alpha\bar{\alpha})$, hence $\pi \bmod \mathfrak{r} = (\alpha \bmod \mathfrak{r})^2(\phi(\alpha\bar{\alpha}) \bmod \mathfrak{r})$. Inside \mathbf{F}_r , we have

$$\begin{aligned} (\phi(\alpha\bar{\alpha}) \bmod \mathfrak{r}) &= (\alpha\bar{\alpha} \bmod \mathfrak{s}) = (\alpha \bmod \mathfrak{s})(\alpha \bmod \bar{\mathfrak{s}}) \\ &= (\alpha \bmod \mathfrak{s})^2 = x^{-2}, \end{aligned}$$

hence we have $(\pi \bmod \mathfrak{r}) = 1$, so r divides $N(\pi - 1)$. Moreover,

$$\begin{aligned} (p^2 \bmod r) &= (p^2 \bmod \mathfrak{r}) = (\alpha \bmod \mathfrak{r})^2(\bar{\alpha} \bmod \mathfrak{r})^2(\phi(\alpha\bar{\alpha}) \bmod \mathfrak{r})^2 \\ &= (\alpha \bmod \mathfrak{r})^2(\alpha \bmod \bar{\mathfrak{r}})^2 x^{-4} = \zeta^2 \end{aligned}$$

is a primitive κ -th root of unity.

This finishes the proof of the correctness of the output. Next we prove the heuristic runtime. As r splits completely, α is a lift of some element modulo r . We treat its norm $p = N(\alpha)$ as a random integer of $4 \log_2 r$ bits. The rest of the proof is as the proof of Theorem 13. \square

Remark 16. Actually, the prime r does not need to split completely in Algorithm 3. It suffices to have $r\mathcal{O}_K = \mathfrak{r}\mathfrak{s}$, where \mathfrak{r} is prime and \mathfrak{s} may be prime or composite.

Remark 17. Note that if Algorithm 2 or 3 terminates, then K satisfies the conditions of Lemma 7, which are therefore not only sufficient, but also necessary for each of these algorithms to terminate.

Let A be a g -dimensional abelian variety over the finite field k of q elements. Its ρ -value with respect to a subgroup of $A(k)$ of order r is defined to be $\rho = g \log q / \log r$. As we have $\log \#A(k) \approx g \log q$, the ρ -value measures the ratio between the bit size of r and the bit size of the order of the full group of rational points on A . It is at least about 1 if q is large. If we have $A = J_C$, then a point on A can be represented by a g -tuple of points on C , hence ρ is also the ratio between the bit size of a group element of A and the bit size of r . For cryptography, one wants the ρ -value to be as small as possible to save bandwidth when transmitting points on J_C .

The prime p , computed as the norm of the element α in Step 4, is expected to satisfy $\log(p) \approx 4 \log(r)$. Since our p -rank-1 curve is defined over \mathbf{F}_{p^2} , its ρ -value is $\rho = 2 \log(p^2) / \log(r) \approx 16$. For a more detailed version of this heuristic analysis of the ρ -value, see Freeman, Stevenhagen, and Streng [5], who compute a ρ -value of about 8 for their ordinary abelian surfaces with prescribed embedding degree. For cryptographic applications, a ρ -value of 16 or even 8 is larger than desired, but it does show that pairing-based cryptography is possible for curves of genus 2 with p -rank 1.

When working with odd embedding degree κ , the *embedding field* $\mathbf{F}_p(\zeta_r)$ could be smaller than the field $\mathbf{F}_{p^2}(\zeta_r) = \mathbf{F}_{p^{2\kappa}}$ that is suggested by the embedding degree κ (see also Hitt [11]). This may influence the security of pairing-based cryptography, but can easily be avoided by restricting to even embedding degree κ , or by only accepting primes p such that r does not divide $p^\kappa - 1$.

5. CONSTRUCTING CURVES WITH GIVEN WEIL NUMBERS

We will now explain the explicit CM construction of a curve C/\mathbf{F}_{p^2} such that $J(\tilde{C})$ corresponds to our Weil p^2 -number π . A more detailed exposition can be found in [6].

Honda's CM construction of the abelian variety corresponding to a given Weil q -number π is based on the theory of *complex multiplication* of abelian varieties of Shimura and Taniyama [20, in particular §13, Thm. 1]. The analogous theory for elliptic curves is even more classical and dates back to the early 19th century. The first algorithmic application of the CM construction of elliptic curves is its application to primality proving by Atkin and Morain [1].

The construction starts by taking an abelian variety A over a number field F such that we have $\text{End}(A) \cong \mathcal{O}_K$, where K is a field containing π , and reduces this variety modulo an appropriate prime \mathfrak{P} of F . For our p -rank-1 Weil numbers π , one can take $K = \mathbf{Q}(\pi)$ and any prime \mathfrak{P} dividing p .

In the dimension-2 case, instead of writing down the abelian surface A itself, one only writes down the *absolute Igusa invariants* $j_1, j_2, j_3 \in F$ of the curve C of which A is the Jacobian. These invariants are the first three of a set of 10 invariants given on page 641 of [13]. One then reduces the invariants modulo \mathfrak{P} and, assuming $(j_1 \bmod \mathfrak{P})$ is a unit, constructs $\tilde{C} = (C \bmod \mathfrak{P})$ from the reduced invariants using

Mestre's algorithm [16]. Honda's construction shows that $J(\tilde{C})$ or its quadratic twist corresponds to our Weil p^2 -number π .

In all practical implementations, the invariants $j_n \in F$ are represented by polynomials H_1, H_2, H_3 or $H_1, \hat{H}_2, \hat{H}_3$ called *Igusa class polynomials*. We explain the polynomials \hat{H}_n later, but the polynomials H_n are given by

$$H_n = \prod_C (X - j_n(C)),$$

where the product ranges over isomorphism classes of curves C such that we have $\text{End}(J(C)) \cong \mathcal{O}_K$. For every triple (j_1, j_2, j_3) of zeroes $j_n \in \overline{\mathbf{F}}_p$ of H_n with $j_1 \neq 0$, one thus obtains a unique $\overline{\mathbf{F}}_p$ -isomorphism class of curves. Assuming $j_1(C) \notin \mathfrak{P}$ for some C , a twist of at least one of the curves we obtain has Weil number π . Let \tilde{C} be such a curve. As we know the group order $N(\pi - 1)$ of $J(\tilde{C})(\mathbf{F}_{p^2})$, we can quickly check whether we have the correct curve by taking random points on its Jacobian and multiplying them by $N(\pi - 1)$.

As the field K is fixed, so are its class polynomials. They can therefore be pre-computed using any of the three known algorithms: the complex analytic method of Spallek [21] and van Wamelen [25], for which Streng [23] recently gave the first runtime analysis and proof of correctness, the 2-adic method of Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng [7], and the Chinese remainder method of Eisenträger and Lauter [3]. Alternatively, class polynomials can be found in the ECHIDNA database [14].

The alternative class polynomials \hat{H}_n are given by

$$\hat{H}_n = \sum_C j_n(C) \prod_{C' \neq C} (X - j_1(C')), \quad (n = 2, 3)$$

where both the product and the sum range over isomorphism classes of curves C for which $\text{End}(J(C)) \cong \mathcal{O}_K$ holds. For any such C , we have $j_n(C)H'_1(j_1(C)) = \hat{H}_n(j_1(C))$. This implies that if every coefficient of H_1 has a denominator that is not divisible by p , and $(H_1 \bmod p)$ has a non-zero root of multiplicity 1, then we can compute the Igusa invariants of a curve \tilde{C} , which is automatically either the curve we want or a quadratic twist. The idea of using \hat{H}_n and not the more standard Lagrange interpolation is due to Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng, who show in [7] that \hat{H}_n heuristically has a much smaller height.

6. A SUFFICIENT AND NECESSARY CONDITION FOR ALGORITHM 1

As said before, the condition of Lemma 7 are sufficient for all three algorithms to work and necessary for Algorithms 2 and 3. They are also easy to check and true for 'most' non-Galois quartic CM-fields. The current section gives a weaker condition that is both sufficient and necessary for Algorithm 1 to work. We also give examples to show that this condition is non-trivial and strictly weaker than that of Lemma 7.

Let K be a non-Galois CM-field of degree 4. Let C/\overline{K} be a curve of genus 2 over the algebraic closure \overline{K} of K such that $\text{End}(J_C) \cong \mathcal{O}_K$ holds. Such C are known to exist. The field $\mathbf{Q}(j) \subset \overline{K}$ generated over \mathbf{Q} by all 10 absolute Igusa invariants $j_1(C), \dots, j_{10}(C)$ of [13, page 641] is called the *field of moduli* of C . For any subfield $X \subset \overline{K}$, let $X(j)$ be the compositum $X \cdot \mathbf{Q}(j)$. Write $K = K_0(\sqrt{r})$ for some $r \in K_0$ and let $K_0^r = \mathbf{Q}(\sqrt{N_{K_0/\mathbf{Q}}(r)})$ (as before).

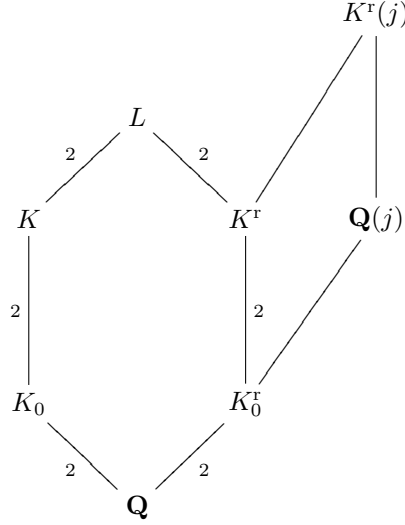


FIGURE 1. Inclusions between the fields

Lemma 18. *Let $K, K_0^r, K(j)$ be as above and let G be the Galois group of the normal closure of $K(j)$ over \mathbf{Q} . Let S be the set of primes p that factor in K as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$ and such that there exists a Weil p^2 -number π such that we have $\pi\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$.*

The Dirichlet density of S is

$$\frac{\#\{\sigma \in G \mid \text{ord } \sigma = 2, \sigma|_{K_0^r} \neq \text{id}_{K_0^r}\}}{\#G}.$$

If S is non-empty, then it has positive density.

Corollary 19. *If Algorithm 1 terminates on input K , then σ as in Lemma 18 exists for K . Conversely, if K is fixed and σ exists for K , then Algorithm 1 heuristically has a polynomial runtime.*

Proof of Corollary 19. If Algorithm 1 terminates, then S is non-empty, hence σ exists by Lemma 18. If σ exists, then the proof of Theorem 9 is valid, so Algorithm 1 heuristically has a polynomial runtime. \square

To prove Lemma 18, we need some more theory. Let L be the normal closure of K . A *CM-type* of K is a set Φ of two embeddings $\varphi : K \rightarrow L$ that satisfies $\Phi \cap \overline{\Phi} = \emptyset$. Let C be a curve as above, and let $\Phi = \{\varphi_1, \varphi_2\}$ be its CM-type as defined in [20, §5.2]. The exact definition of this CM-type will not be important to us.

The *reflex field*

$$K^r = \mathbf{Q}(\sum_i \varphi_i(x) : x \in K) \subset L$$

of K with respect to Φ is one of the two non-Galois CM subfields of L of degree 4 that are not conjugates of K . Its real quadratic subfield K_0^r does not depend on Φ and is exactly the field K_0^r that we have seen above Lemma 7. By [19, Prop. 20.3(i)], we have $K_0^r \subset \mathbf{Q}(j)$, so that we have the inclusions of fields shown in Figure 1.

The main theorem of complex multiplication gives $K^\tau(j)$ as an unramified abelian extension of K^τ . To state it, we need to define the *type norm* of the *reflex type* of Φ . Let Φ_L be the set of extensions of elements of Φ to L , so Φ_L is a CM-type of L and so is the set Φ_L^{-1} of inverses of elements of L . The set of restrictions of Φ_L^{-1} to K^τ is a CM-type $\Phi^\tau = \{\psi_1, \psi_2\}$ of K^τ called the *reflex* of Φ [20, §8.3]. By [20, §8.3 Prop. 29], for any fractional \mathcal{O}_{K^τ} -ideal \mathfrak{a} , there is a unique fractional \mathcal{O}_K -ideal $N_{\Phi^\tau}(\mathfrak{a})$ such that we have

$$N_{\Phi^\tau}(\mathfrak{a})\mathcal{O}_L = \prod_{i=1}^2 \psi_i(\mathfrak{a})\mathcal{O}_L.$$

The map N_{Φ^τ} from ideals of K^τ to ideals of K is called the *type norm* with respect to Φ^τ .

Theorem 20 (Main Theorem 1 in §15.3 of [20]). *The extension $K^\tau(j)/K^\tau$ is abelian and unramified. Its Galois group corresponds via the Artin map to Cl_{K^τ}/H_0 , where H_0 is the group of ideal classes $[\mathfrak{a}]$ such that $N_{\Phi^\tau}(\mathfrak{a})$ is principal and generated by an element $\mu \in K$ with $\mu\bar{\mu} \in \mathbf{Q}^*$. \square*

The following lemma computes $N_{\Phi^\tau}(\mathfrak{q})$ for certain primes \mathfrak{q} .

Lemma 21. *Let K be a quartic CM-field and p a prime that factors in K as $p\mathcal{O}_K = \mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2^e$.*

- (1) *The prime p factors in K_0^τ as \mathfrak{s}^e for a prime \mathfrak{s} , which splits in K^τ as $\mathfrak{s}\mathcal{O}_{K^\tau} = \mathfrak{q}\bar{\mathfrak{q}}$; and*
- (2) *we have $N_{\Phi^\tau}(\mathfrak{q}) = \mathfrak{p}_1^{2/e}\mathfrak{p}_2$ (up to complex conjugation).*

Proof. Let $\mathfrak{P} \subset \mathcal{O}_L$ be the unique prime over \mathfrak{p}_1 . Part (1) follows from the fact that the decomposition group of \mathfrak{P} is $\text{Gal}(L/K)$ and that the inertia group has order e .

For part (2), let s be the generator of $\text{Gal}(L/K)$, let s' be the generator of $\text{Gal}(L/K^\tau)$ and set $r = ss'$. Then $\Phi_L \subset \text{Gal}(L/\mathbf{Q})$ has 4 elements and satisfies $\Phi_L \langle s \rangle = \Phi_L$ and $\Phi_L^{-1} \langle s' \rangle = \Phi_L^{-1}$, hence Φ_L^{-1} is $\{1, s, s', ss'\}$ or its complex conjugate, and we have $\Phi^\tau = \{1, s|_{K^\tau}\}$ up to complex conjugation. Take $\psi_1 = 1, \psi_2 = s$. We compute

$$\begin{aligned} N_{\Phi^\tau}(\mathfrak{q})\mathcal{O}_L &= (\mathfrak{q}\mathcal{O}_L)^{(s\mathfrak{q}\mathcal{O}_L)} = \left(\mathfrak{P}^{(s'\mathfrak{P})}\right) \left(\mathfrak{P}^{(s\mathfrak{P})}\right)^{(ss'\mathfrak{P})} \\ &= \mathfrak{P}^2 \left(\mathfrak{P}^{(s'\mathfrak{P})}\right)^{(ss'\mathfrak{P})} = (\mathfrak{p}_1^{2/e}\mathcal{O}_L)(\mathfrak{p}_2\mathcal{O}_L), \end{aligned}$$

up to complex conjugation, which proves (2). \square

Proof of Lemma 18. Let p be a prime number that is unramified in K . We prove that p is in S if and only if its decomposition group in the normal closure of $K(j)$ is of order 2 and acts non-trivially on K_0^τ . Chebotarev's density theorem [17, Theorem 13.4] then proves the formula for the density. Moreover, if S is non-empty, then σ exists, hence the density is positive.

Let p be a prime number and let $\sigma \in G$ be its p -th power Frobenius. Suppose p is in S and write $p\mathcal{O}_K = \mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2$. The image of σ in $\text{Gal}(L/\mathbf{Q})$ generates $\text{Gal}(L/K)$ or its conjugate, hence has order 2. It follows that p is inert in K_0^τ/\mathbf{Q} and splits into two factors \mathfrak{q} and $\bar{\mathfrak{q}}$ in K^τ . Lemma 21 shows that the type norm of \mathfrak{q} is $N_{\Phi^\tau}(\mathfrak{q}) = \mathfrak{p}_1^2\mathfrak{p}_2 = \pi\mathcal{O}_K$ or its complex conjugate, and we have $\pi\bar{\pi} \in \mathbf{Q}^*$, so we find $[\mathfrak{q}] \in H_0$, hence σ^2 is trivial on $K^\tau(j)$ and in particular on $\mathbf{Q}(j)$.

Recall that $\mathbf{Q}(j)$ is the field generated over \mathbf{Q} by the absolute Igusa invariants of C and that C is any curve with CM by \mathcal{O}_K . In particular, we can replace C by ${}^\tau C$ for any automorphism τ of \overline{K}/\mathbf{Q} . This shows that σ^2 is also trivial on ${}^\tau \mathbf{Q}(j)$ for any τ , and hence σ^2 is trivial on the normal closure of $\mathbf{Q}(j)$. As it is also trivial on the normal closure L of K , we find that it is trivial on the normal closure of $K(j)$ and hence σ is in the set of Lemma 18.

Conversely, suppose that σ^2 is trivial and σ is non-trivial on K_0^τ . As $\sigma|_L$ generates $\text{Gal}(L/K)$ or a conjugate, we find that p factors as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$. Again, the prime p is inert in K_0^τ/\mathbf{Q} and splits into two factors \mathfrak{q} and $\overline{\mathfrak{q}}$ in K^τ with type norms $\mathfrak{p}_1^2\mathfrak{p}_2$ and its complex conjugate. As we have $\sigma^2 = 1$, we find by Theorem 20 that $\mathfrak{p}_1^2\mathfrak{p}_2 = \pi\mathcal{O}_K$ holds for some $\pi \in \mathcal{O}_K$ that satisfies $\pi\overline{\pi} \in \mathbf{Q}^*$. Since also $\pi\overline{\pi}$ is positive and has absolute value p^2 , it is a Weil p^2 -number and p is in S . \square

Example 22. For the field $K = \mathbf{Q}[X]/(X^4 + 12X^2 + 2)$ of Example 8, we can find $\mathbf{Q}(j)$ in the ECHIDNA database [14] and compute that $\mathbf{Q}(j)$ contains the field $F = \mathbf{Q}(\sqrt{2 + \sqrt{2}})$, which is cyclic Galois over \mathbf{Q} and contains $K_0^\tau = \mathbf{Q}(\sqrt{2})$. Any automorphism of F of order 2 is trivial on K_0^τ , so the density of S in Lemma 18 is 0 and none of our algorithms works for this field.

Example 23. For the field $K = \mathbf{Q}[X]/(X^4 + 20X^2 + 5)$, we have $13 \in S$, so that S has positive density and Algorithm 1 works for K . However, the discriminant $d^\tau = 5$ of $K_0^\tau = \mathbf{Q}(\sqrt{5})$ is a prime discriminant and occurs in the prime discriminant factorization $d = (-4) \cdot (5) \cdot (-19)$ of K_0 . This shows that K does not satisfy the conditions of Lemma 7, which are therefore too strong for Algorithm 1.

7. FACTORIZATION OF CLASS POLYNOMIALS MODULO p

While experimenting with the explicit CM construction for curves of p -rank 1, we found that in the (ramified) case $e = 2$ of Lemma 1, the polynomial $H_1 \bmod p$ has no roots of multiplicity 1 in $\overline{\mathbf{F}_p}$, which made working with \widehat{H}_n impossible. The current section explains this phenomenon, and shows how to adapt $H_1, \widehat{H}_2, \widehat{H}_3$ to deal with this situation. We also explain the analogue of this for the situation $e = 1$, for which there is no problem.

Let K, C , and j be as in Section 6. If $j_1(C) \neq 0$ is a simple root of H_1 , which is ‘usually’ the case, then we have $\mathbf{Q}(j) = \mathbf{Q}(j_1(C))$ since we can compute $j_n(C)$ from $j_1(C)$ using the polynomials \widehat{H}_2 and \widehat{H}_3 as we have seen in Section 5. The Kummer-Dedekind theorem thus relates the factorization of $(H_1 \bmod p) \in \mathbf{F}_p[X]$ to the factorization of p in (an order in) $\mathbf{Q}(j)$.

Lemma 24. *Let p be a prime that factors in K as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2$, and let n be the smallest positive integer such that en is even and $(\mathfrak{p}_1\mathfrak{p}_2^{e/2})^n$ is generated by a Weil p^n -number π . Then any prime \mathfrak{q} of K^τ lying over p decomposes in $K^\tau(j)/K^\tau$ into distinct primes of residue degree $en/2$.*

Proof. Recall from Theorem 20 that $K^\tau(j)$ is the unramified abelian extension of K^τ such that the Artin map induces an isomorphism $\text{Cl}_K/H_0 \rightarrow \text{Gal}(K^\tau(j)/K^\tau)$, where $H_0 \subset \text{Cl}_K$ is the subgroup of ideal classes $[\mathfrak{a}]$ such that $N_{\mathbb{F}^\tau}(\mathfrak{a})$ is principal and generated by an element $\mu \in K$ with $\mu\overline{\mu} \in \mathbf{Q}^*$.

The Artin isomorphism sends $[\mathfrak{q}]$ to a generator of the decomposition group of \mathfrak{q} , so it suffices to prove that $[\mathfrak{q}]$ has order $en/2$ in the quotient group Cl_{K^τ}/H_0 .

Lemma 21 computes that $N_{\mathbb{F}^r}(\mathfrak{q}^m)$ is either $(\mathfrak{p}_1^{2/e}\mathfrak{p}_2)^m$ or its complex conjugate, so the smallest integer m with $[\mathfrak{q}^m] \in H_0$ is exactly $m = en/2$. \square

Corollary 25. *Let p, n be as in Lemma 24. Then p splits into prime factors of residue degree n in $\mathbf{Q}(j)/\mathbf{Q}$. Each factor occurs exactly e times.*

Proof. Each prime factor \mathfrak{p} has residue degree $en/2$ in $K^r(j)/K^r$ by Lemma 24 and $2/e$ in K^r/\mathbf{Q} by Lemma 21, hence n in $K^r(j)/\mathbf{Q}$. As all ramification of \mathfrak{p} takes place in K_0^r/\mathbf{Q} , we find that the ramification index of \mathfrak{p} in $K^r(j)/\mathbf{Q}$ is e .

We have seen in Figure 1 on page 12 that $\mathbf{Q}(j)$ contains K_0^r . As the residue degree and ramification index of \mathfrak{p} in K^r/K_0^r are 1, we find that the residue degree and ramification index of \mathfrak{p} are also n and e in $\mathbf{Q}(j)/\mathbf{Q}$. \square

Corollary 26. *If p factors in K as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^2$, then $(H_1 \bmod p) \in \mathbf{F}_p[X]$ has no roots of multiplicity 1 in $\overline{\mathbf{F}_p}$.*

Proof. The polynomial $H_1 \in \mathbf{Q}[X]$ is monic and the denominators of the coefficients are not divisible by p because they are Igusa invariants of a curve that has potential good reduction modulo p . Let $c \in \mathbf{Z}$ not divisible by p be such that $H_1(cX)$ is in $\mathbf{Z}[X]$ and let $f \in \mathbf{Z}[X]$ be an arbitrary irreducible factor of $H_1(cX) \in \mathbf{Z}[X]$. We find an order $\mathcal{O} = \mathbf{Z}[X]/f$ in $\mathbf{Q}(j)$. Each irreducible factor $g \in \mathbf{F}_p[X]$ of $(H_1 \bmod p)$ corresponds to the prime ideal $\mathfrak{p} = (p, g(X))$ of \mathcal{O} . As every prime over p ramifies in $\mathbf{Q}(j)/\mathbf{Q}$ by Corollary 25, we find that \mathfrak{p} is either ramified or singular. By the Kummer-Dedekind theorem (Theorem 8.2 of [22]), both cases imply that the roots of g have multiplicity at least 2 as roots of H_1 . \square

This shows that $H_1, \widehat{H}_1, \widehat{H}_2$ cannot be used for the case $e = 2$. To get around this, we replace H_1 by an irreducible factor $f \in K_0^r[X]$ and \widehat{H}_n by the unique polynomial S_n of degree at most $\deg(f) - 1$ that is congruent modulo f to $\widehat{H}_n(H_1/f)^{-1}$. If we write $p\mathcal{O}_{K^r} = \mathfrak{s}^2$, then $(f \bmod \mathfrak{s}), (S_2 \bmod \mathfrak{s}), (S_3 \bmod \mathfrak{s}) \in \mathbf{F}_p[X]$ can be used in exactly the same way as $(H_1 \bmod p), (\widehat{H}_2 \bmod p), (\widehat{H}_3 \bmod p)$ and do not suffer from Corollary 26.

Corollary 27. *For all but finitely many of the primes p that decompose as $p\mathcal{O}_K = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2^e$, the reduction $(H_1 \bmod p) \in \mathbf{F}_p[X]$ is a product of distinct irreducible polynomials in $\mathbf{F}_p[X]$ of degree n for n given in Lemma 24 (and depending on p).*

Proof. We exclude the primes dividing the denominator of any coefficient of H_1 , as well as those dividing the discriminant. Then all roots of $(H_1 \bmod p)$ in $\overline{\mathbf{F}_p}$ are simple roots. Let f, \mathcal{O} be as in the proof of Corollary 26. Then p does not divide the index of \mathcal{O} in its maximal order. The fact that every prime of $\mathbf{Q}(j)$ has residue degree n implies that every irreducible factor of $f \bmod p$ has degree n . \square

8. EXAMPLES

Algorithm 1. We provide examples of p -rank-1 curves C/\mathbf{F}_{p^2} such that the Jacobian J_C is simple and has prime order. The CM-field for all examples is $K = \mathbf{Q}(\alpha)$, where α is a root of the polynomial $X^4 + 34X^2 + 217 \in \mathbf{Q}[X]$, which satisfies the conditions of Lemma 7. We give the prime p , the coefficients a_1 and a_2 of the minimal polynomial

$$f = X^4 - a_1X^3 + (a_2 + 2p^2)X^2 - a_1p^2X + p^4$$

of the Frobenius endomorphism and the coefficients $c_i \in \mathbf{F}_{p^2}$ of the curve equation

$$C : y^2 = c_6x^6 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

The group order of the Jacobian is $\#J_C(\mathbf{F}_{p^2}) = N(\pi - 1) = f(1)$. The field \mathbf{F}_{p^2} is given as $\mathbf{F}_p(\sigma)$, where $\sigma^2 = -3$. Section headings describe the number of bits of the group order $\#J_C(\mathbf{F}_{p^2})$.

Each example was generated in a few seconds on a standard PC after pre-computation of the Igusa class polynomials of K .

160-bit group size.

$$\begin{aligned} p &= 924575392409, & a_1 &= 3396725192754 \\ a_2 &= 2876182159630959921399337, & c_6 &= \sigma \\ c_4 &= 349419850452 \cdot \sigma + 621473390194 \\ c_3 &= 638315825844 \cdot \sigma + 895470286740 \\ c_2 &= 247903071476 \cdot \sigma + 504258872407 \\ c_1 &= 494346973570 \cdot \sigma + 326558224146 \\ c_0 &= 721392332677 \cdot \sigma + 210623692149 \end{aligned}$$

192-bit group size.

$$\begin{aligned} p &= 236691298903769, & a_1 &= -9692493559086 \\ a_2 &= -58992172275797931791883572663, & c_6 &= \sigma \\ c_4 &= 144046547562595\sigma + 31854049506043 \\ c_3 &= 134634542821316\sigma + 20155601614364 \\ c_2 &= 159093189820788\sigma + 52669766944798 \\ c_1 &= 223684436822489\sigma + 66232364455191 \\ c_0 &= 206430094481010\sigma + 170879851904277 \end{aligned}$$

256-bit group size.

$$\begin{aligned} p &= 15511800964685067143, & a_1 &= 2183138494024250742 \\ a_2 &= -871403391229975003782565554464700664457, & c_6 &= 1 \\ c_4 &= 7019198877313644539 \cdot \sigma + 8886572032497699458 \\ c_3 &= 8069566800142565548 \cdot \sigma + 11092851174307405252 \\ c_2 &= 8339873208295381793 \cdot \sigma + 13688811293938352344 \\ c_1 &= 10474983032301001361 \cdot \sigma + 14509908493781086362 \\ c_0 &= 4803877905347330504 \cdot \sigma + 12900291622358663970 \end{aligned}$$

Algorithm 3.

192-bit group size, embedding degree 12. Let K be the field $K = \mathbf{Q}[X]/(X^4 + 13X^2 + 41)$ and let $\kappa = 12$. It took a few seconds to find the smallest prime $r > 2^{192}$ that splits completely in K and $\mathbf{Q}(\zeta_{12})$, which is $r = 2^{192} + 18513$. We ran Algorithm 3 with input K, κ, r . The algorithm terminated after about 11 minutes and found a prime p and a Weil p^2 number with p -rank 1 and embedding degree 12 with respect to a subgroup of order r . Using p and precomputed Igusa class polynomials, we were able to find an equation for the corresponding hyperelliptic curve C in less

than a second. We only give p , because π and the coefficients of C would take up too much space.

$$\begin{aligned}
 p = & 1420038565958074827476353870489770880715201360323415690146120568 \\
 & 6404970976014364663695672498066437749119607973051961772352102985 \\
 & 5649462172148699393958968638652107696147277436345811056227385195 \\
 & 781997362304851932650270514293705125991379
 \end{aligned}$$

Acknowledgements. We thank Peter Bruin, David Kohel, Tanja Lange, Hendrik Lenstra, Joe Silverman, and Peter Stevenhagen for helpful advice.

REFERENCES

- [1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61:29–68, 1993. <http://www.inria.fr/rrrt/rr-1256.html>.
- [2] H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.
- [3] K. Eisentraeger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2004. To appear in *Arithmetic, Geometry and Coding Theory - AGCT-10 (Marseille)*, 2005. arXiv:math/0405305v2.
- [4] D. Freeman. Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 152–176. Springer-Verlag, Berlin, 2007.
- [5] D. Freeman, P. Stevenhagen, and M. Streng. Abelian varieties with prescribed embedding degree. In A. J. van der Poorten and A. Stein, editors, *ANTS*, volume 5011 of *Lecture Notes in Computer Science*, pages 60–73. Springer-Verlag, 2008. arXiv:0802.1886v1.
- [6] G. Frey and T. Lange. Complex multiplication. In H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors, *Handbook of elliptic and hyperelliptic curve cryptography*, pages 455–473. Chapman & Hall/CRC, 2006.
- [7] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in Cryptology - ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129. Springer-Verlag, Berlin, 2006. arXiv:math/0503148.
- [8] J. González. On the p -rank of an abelian variety and its endomorphism algebra. *Pub. Math.*, 42(1):119–130, 1998.
- [9] E. Z. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta Math.*, 94(1):33–43, 1997.
- [10] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1938.
- [11] L. Hitt. On the minimal embedding field. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer-Verlag, 2007.
- [12] T. Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.
- [13] J.-I. Igusa. Arithmetic variety of moduli for genus 2. *The Annals of Mathematics*, 72(3):612–649, 1960.
- [14] D. Kohel. ECHIDNA databases for elliptic curves and higher dimensional analogues. <http://echidna.maths.usyd.edu.au/echidna/dbs/index.html>.
- [15] D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.
- [16] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglione, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.
- [17] J. Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.
- [18] K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, volume 2442 of *Lecture Notes In Computer Science*, pages 336 – 353, 2002.

- [19] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998. Sections 1–16 essentially appeared before in G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, Mathematical Society of Japan, 1961.
- [20] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.
- [21] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
- [22] P. Stevenhagen. The arithmetic of number rings. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory*. Cambridge University Press, 2008.
- [23] M. Streng. Computing Igusa class polynomials. arXiv:0903.4766v1, 2008.
- [24] J. Tate. Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda). *Sémin. Bourbaki 1968/69, No.352*, pages 95–110, 1971.
- [25] P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.
- [26] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 2001. <http://www.iem.uni-due.de/zahlentheorie/preprints/wengthesis.pdf>.
- [27] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72(241):435–458, 2003.

LAURA HITT O’CONNOR AND GARY MCGUIRE, SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY COLLEGE DUBLIN, IRELAND
E-mail address: hitt36@gmail.com, gary.mcguire@ucd.ie

MICHAEL NAEHRIG, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EINDHOVEN UNIVERSITY OF TECHNOLOGY, DEN DOLECH 2, 5600 MB EINDHOVEN, THE NETHERLANDS, AND MICROSOFT RESEARCH, ONE MIROSOFT WAY, REDMOND, WA 98052, USA
E-mail address: michael@cryptojedi.org
URL: <http://www.cryptojedi.org/users/michael/>

MARCO STRENG, MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN, POSTBUS 9512, 2300 RA LEIDEN, THE NETHERLANDS
E-mail address: streng@math.leidenuniv.nl
URL: <http://www.math.leidenuniv.nl/~streng/>