Journal of Number Theory 133 (2013) 3755–3770

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Pairing-based algorithms for jacobians of genus 2 curves with maximal endomorphism ring

Sorina Ionica

Ecole Normale Supérieure [1]*, 45 Rue d'Ulm, Paris, 75005, France*

ARTICLE INFO

Article history:
Received 2 April 2012
Revised 26 March 2013
Accepted 2 April 2013
Available online 18 July 2013
Communicated by Fernando Rodriguez Villegas

Keywords:
Endomorphism ring
Jacobian
Tate pairing
Computation

ABSTRACT

Using Galois cohomology, Schmoyer characterizes cryptographic non-trivial self-pairings of the ℓ-Tate pairing in terms of the action of the Frobenius on the ℓ-torsion of the jacobian of a genus 2 curve. We apply similar techniques to study the non-degeneracy of the ℓ-Tate pairing restrained to subgroups of the ℓ-torsion which are maximal isotropic with respect to the Weil pairing. First, we deduce a criterion to verify whether the jacobian of a genus 2 curve has maximal endomorphism ring. Secondly, we derive a method to construct horizontal (ℓ, ℓ)-isogenies starting from a jacobian with maximal endomorphism ring.

1. Introduction

A central problem in elliptic and hyperelliptic curve cryptography is that of constructing an elliptic curve or an abelian surface having a given number of points on their jacobian. The solution to this problem relies on the computation of the Hilbert class polynomial for a quadratic imaginary field in the genus one case. The analogous genus 2 case needs the Igusa class polynomials for quartic CM fields. There are three different methods to compute these polynomials: an analytic algorithm [16], a p-adic algorithm [7] and a Chinese Remainder Theorem-based algorithm [5]. The last one relies heavily on an algorithm for determining endomorphism rings of the jacobians of genus 2 curves over prime fields. Eisenträger and Lauter [5] gave the first algorithm for computing endomorphism rings of jacobians of genus 2 curves over finite fields. The algorithm takes as input a jacobian J over a finite field and a primitive quartic CM field K, i.e. a purely imaginary quadratic extension field of a real quadratic field with no proper imaginary quadratic fields. The real quadratic subfield K_0 has

E-mail address: sorina.ionica@m4x.org.

[1] This work was carried during the author's stay at the Ecole Polytechnique, team TANC and at LORIA, Nancy, team CARAMEL.

0022-314X/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2013.04.023

class number 1. The main idea is to compute a set of generators of an order $\mathcal{O}$ in the CM field and then to test whether these generators are endomorphisms of J, in order to decide whether the order $\mathcal{O}$ is the endomorphism ring $\mathrm{End}(J)$ or not. In view of application to the CRT method for Igusa class polynomial computation, Freeman and Lauter bring a series of improvements to this algorithm, in the particular case where we need to decide whether $\mathrm{End}(J)$ is the maximal order or not. Note that the Eisenträger–Lauter CRT method for class polynomial computation searches for curves defined over some prime field $\mathbb{F}_p$ and belonging to a certain isogeny class. Once such a curve is found, the algorithm keeps the curve only if it has maximal endomorphism ring. This search is rather expensive and ends only when all curves having maximal endomorphism ring were found. Recent research in the area [1,15,4] has shown that we can significantly reduce the time of this search by using *horizontal isogenies*, i.e. isogenies between jacobians having the same endomorphism ring. Indeed, once a jacobian with maximal endomorphism ring is found, many others can be generated from it by computing horizontal isogenies. In this paper, we propose a new method for checking if the endomorphism ring is locally maximal at ℓ, for $\ell > 2$ prime, and a method to compute kernels of horizontal (ℓ,ℓ)-isogenies. Our methods rely on the computation of the Tate pairing.

Let H be a genus 2 smooth irreducible curve defined over a finite field $\mathbb{F}_q$, J its jacobian and suppose that $J[\ell^n] \subseteq J(\mathbb{F}_q)$ and that $J[\ell^{n+1}] \nsubseteq J(\mathbb{F}_q)$, with ℓ different from p and $n \geqslant 1$. We denote by $\mathcal{W}$ the set of rank 2 subgroups in $J[\ell^n]$, which are isotropic with respect to the ℓ^n-Weil pairing. We define k_ℓ to be

$$k_\ell = \max_{G \in \mathcal{W}} \bigl\{ k \bigm| \exists P, Q \in G \text{ and } T_{\ell^n}(P,Q) \in \mu_{\ell^k} \backslash \mu_{\ell^{k-1}} \bigr\}.$$

The jacobian J is ordinary, hence it has complex multiplication by an order in a quartic CM field K. We assume that $K = \mathbb{Q}(\eta)$, with $\eta = i\sqrt{a + b\sqrt{d}}$ if $d \equiv 2, 3 \bmod 4$ or $\eta = i\sqrt{a + b(\frac{-1+\sqrt{d}}{2})}$ if $d \equiv 1 \bmod 4$. We consider the decomposition of the Frobenius endomorphism π over a basis of the ring of integers of K: $\pi = a_1 + a_2\frac{-1+\sqrt{d}}{2} + (a_3 + a_4\frac{-1+\sqrt{d}}{2})\eta$, if $d \equiv 1 \bmod 4$ and $\pi = a_1 + a_2\sqrt{d} + (a_3 + a_4\sqrt{d})\eta$, if $d \equiv 2, 3 \bmod 4$. We assume that the coefficients verify the following condition

$$\max\left(v_\ell\left(\frac{a_3 - a_4}{\ell}\right), v_\ell\left(\frac{a_3 - \ell a_4}{\ell^2}\right)\right) < \min\bigl(v_\ell(a_3), v_\ell(a_4)\bigr). \tag{1}$$

We show that if condition (1) is satisfied, the computation of k_ℓ suffices to check whether the endomorphism ring is locally maximal at ℓ, in many cases. Moreover, our method to distinguish kernels of horizontal (ℓ,ℓ)-isogenies from other (ℓ,ℓ)-isogenies is also related to k_ℓ. Given G an element of $\mathcal{W}$, we say that the Tate pairing is k_ℓ-non-degenerate (or simply non-degenerate) on $G \times G$ if the restriction map

$$T_{\ell^n} : G \times G \to \mu_{\ell^{k_\ell}}$$

is surjective. Otherwise, we say that the Tate pairing is k_ℓ-degenerate (or simply degenerate) on $G \times G$. Our main result is the following theorem.

Theorem 1. *Let H be a genus 2 smooth irreducible curve defined over a finite field $\mathbb{F}_q$ and $\ell > 2$ a prime number. Let J be the jacobian of H, whose endomorphism ring is a locally maximal order at ℓ of a CM field K. Assume that the real quadratic subfield K_0 has class number 1. Suppose that the Frobenius endomorphism π is such that $\pi - 1$ is exactly divisible by ℓ^n, $n \in \mathbb{Z}$ and that $k_\ell > 0$. Let G be a subgroup of rank 2 in $J[\ell]$ which is isotropic with respect to the Weil pairing. Let $\bar{G}$ be a rank 2 subgroup in $J[\ell^n]$ isotropic with respect to the ℓ^n-Weil pairing and such that $\ell^{n-1}\bar{G} = G$. Then the following hold*

1. *If the isogeny of kernel G is horizontal, then the Tate pairing is k_ℓ-degenerate over $\bar{G} \times \bar{G}$.*
2. *If the condition (1) is satisfied and the Tate pairing is k_ℓ-degenerate over $\bar{G} \times \bar{G}$, then the isogeny is horizontal.*