The Splitting of Primes in Division Fields of Elliptic Curves

W. Duke and Á. Tóth

Dedicated to the memory of Petr Čižek

CONTENTS

We give a global description of the Frobenius for the division fields of an elliptic curve E that is strictly analogous to the cyclotomic case. This is then applied to determine the splitting of a prime p in a subfield of such a division field. These subfields include a large class of nonsolvable quintic extensions and our application provides an arithmetic counterpart to Klein's "solution" of quintic equations using elliptic functions. A central role is played by the discriminant of the ring of endomorphisms of the reduced curve modulo p.

1. INTRODUCTION

Given a Galois extension L/K of number fields with Galois group G, a fundamental problem is to describe the (unramified) primes $\mathfrak{p}$ of K whose Frobenius automorphisms lie in a given conjugacy class C of G. In particular, all such primes have the same splitting type in a subextension of L/K. In general, all that is known is that the primes have density $|C|/|G|$ in the set of all primes (the Chebotarev theorem).

For L/K, an abelian extension, Artin reciprocity describes such primes by means of their residues in generalized ideal classes of K. In the special case that L is obtained explicitly by adjoining to K the n-th division points of the unit circle, we have that $G \subset GL_1(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$ and the Frobenius of $\mathfrak{p}$ is determined by the norm $N(\mathfrak{p})$ modulo n. If $K = \mathbb{Q}$ (cyclotomic fields), we have that $G = GL_1(\mathbb{Z}/n\mathbb{Z})$ and any abelian extension of $\mathbb{Q}$ occurs as a subfield of such an L for a suitable n (Kronecker-Weber). Here the Chebotarev theorem reduces to the prime number theorem in arithmetic progressions.

In a similar manner, an elliptic curve E over K gives rise to its n-th division field L_n by adjoining to K all the coordinates of the n-torsion points. Now L_n is a (generally nonabelian) Galois extension of K with Galois group

2000 AMS Subject Classification: Primary 11G, 11R, 11G05, 11R32
Keywords: Elliptic curves, division fields, quintic expressions

1058-6458/2001 $0.50 per page
Experimental Mathematics **11**:4, page 555

G, a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$ (see [Serre 72]). In this paper, we will give a global description of the Frobenius for the division fields of an elliptic curve E that is strictly analogous to the cyclotomic case. This is then applied to determine the splitting of primes in fields contained in L_n or, as we shall say, uniformized by E. As observed by Klein (see [Klein 56]), such fields include a large class of nonsolvable quintic extensions. Our aim in this application is to provide an arithmetic counterpart to Klein's "solution" of quintic equations using elliptic functions.

By using CM curves, we may uniformize all abelian extensions of imaginary quadratic fields. A classical application here is the result of Gauss that

$$x^3 - 2$$

factors completely modulo a prime $p > 3$ if and only if

$$p = x^2 + 27y^2$$

for integers x and y (see [Cox 89]). One way to derive this is to determine the Frobenius class of p in the field obtained by adjoining to $\mathbb{Q}$ the x-coordinates of the 3-division points of the elliptic curve given by

$$y^2 = x^3 - 15x + 22,$$

which has CM by the quadratic order of discriminant -12.

Analogous results for nonsolvable quintics require non-CM curves. Consider the quintic

$$f(x) = x^5 + 90x^3 + 3645x - 6480,$$

which has discriminant $(2)^{12}(3)^{16}(5)^5(7)^6$. Its splitting field has Galois group S_5 over $\mathbb{Q}$. It follows from the results of this paper that $f(x)$ factors completely modulo $p > 7$ if and only if

$$p = x^2 - 25\Delta_p y^2$$

where Δ_p is the discriminant of the ring of endomorphisms of the elliptic curve

$$y^2 = x(x-1)(x-3)$$

reduced mod p. The first two such primes are 1259 and 1951 for which $\Delta_{1259} = -31$ and $\Delta_{1951} = -51$ and where

$$1259 = (22)^2 + 25 \cdot 31 \cdot 1^2$$

and

$$1951 = (26)^2 + 25 \cdot 51 \cdot 1^2.$$

As may be checked,

$$f(x) \equiv (x+734)(x+322)(x+26)(x+851)(x+585) \mod 1259$$

and

$$f(x) \equiv (x+1029)(x+1222)(x+839)(x+1771) \cdot (x+992) \mod 1951.$$

In the non-CM case, Δ_p is not determined by arithmetic progressions in p. A goal of this paper is to complement that of Shimura [Shimura 66] by pointing out the role of Δ_p in such questions.

2. OUTLINE OF RESULTS

Given an elliptic curve E defined over a number field K and a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ of good reduction for E, we shall define an integral matrix $\sigma_\mathfrak{p}$ of determinant $N(\mathfrak{p})$ whose reduction modulo n gives the action of the Frobenius for L_n, the n-th division field of E. Let $a_\mathfrak{p}$ be defined as usual by

$$\#E_\mathfrak{p}(k) = N(\mathfrak{p}) - a_\mathfrak{p} + 1 \tag{2–1}$$

where $E_\mathfrak{p}$ is the reduction of E at $\mathfrak{p}$ and is defined over k, the residue field of $\mathfrak{p}$ that satisfies $\#k = N(\mathfrak{p}) = p^r$.

Let R be the ring of those endomorphisms of E that are rational polynomial expressions in the Frobenius endomorphism $\phi_\mathfrak{p}$. If $\phi_\mathfrak{p}$ is multiplication by an integer, then $R = \mathbb{Z}$ and we define $\Delta_\mathfrak{p} = 1$ and $b_\mathfrak{p} = 0$. Otherwise the ring R is the centralizer of the Frobenius endomorphism in the endomorphism ring of $E_\mathfrak{p}$ over k and is an imaginary quadratic order whose discriminant we denote by $\Delta_\mathfrak{p}$. We shall see that p does not divide the conductor m of $\Delta_\mathfrak{p}$ and that there is a unique positive integer $b_\mathfrak{p}$ so that

$$4N(\mathfrak{p}) \;=\; a_\mathfrak{p}^2 \;-\; \Delta_\mathfrak{p}\, b_\mathfrak{p}^2. \tag{2–2}$$

We associate to $\mathfrak{p}$ the following integral matrix of determinant $N(\mathfrak{p})$:

$$\sigma_\mathfrak{p} = \begin{bmatrix} (a_\mathfrak{p} + b_\mathfrak{p}\delta_\mathfrak{p})/2 & b_\mathfrak{p} \\ b_\mathfrak{p}(\Delta_\mathfrak{p} - \delta_\mathfrak{p})/4 & (a_\mathfrak{p} - b_\mathfrak{p}\delta_\mathfrak{p})/2 \end{bmatrix} \tag{2–3}$$

where for a discriminant Δ we have $\delta = 0, 1$ according to whether $\Delta \equiv 0, 1 \bmod 4$. We shall show that $\sigma_\mathfrak{p}$ gives a global representation of the Frobenius class over $\mathfrak{p}$ for each n-th division field of E by reducing it modulo n, provided p is prime to n.

Theorem 2.1. *Let E be an elliptic curve defined over a number field K and $n > 1$ an integer. Let L_n be the n-th*

division field of E with Galois group G over K. Let $\mathfrak{p}$ be a prime of good reduction for E with $N(\mathfrak{p})$ prime to n. Then $\mathfrak{p}$ is unramified in L_n and the integral matrix $\sigma_\mathfrak{p}$ defined in (2–3), when reduced modulo n, represents the class of the Frobenius of $\mathfrak{p}$ in G.

The proof we give of this uses the theory of canonical lifts of endomorphisms due originally to Deuring.

In analogy to the cyclotomic case, we have associated to each curve a sequence of prime power matrices, defined in terms of arithmetic data from the reduced elliptic curve that give the Frobenius in all of the division fields. Let C be a conjugacy class of G and let $\pi_E(X; n, C)$ be the number of primes $\mathfrak{p}$ of good reduction with $N(\mathfrak{p}) \le X$ such that $\sigma_\mathfrak{p} \equiv C_0 \mod n$ for some $C_0 \in C$. By the Chebotarev theorem [Chebotarov 95], we derive the following strict analogue of the prime number theorem in progressions for the sequence $\sigma_\mathfrak{p}$:

$$\pi_E(X; n, C) \sim \frac{|C|}{|G|}\pi_K(X)$$

as $X \to \infty$, where $\pi_K(X)$ counts all primes of K with $N(\mathfrak{p}) \le X$.

Of more interest for us here is the fact that the splitting type of $\mathfrak{p}$ in any field between K and the n-th division field L_n is determined by $\sigma_\mathfrak{p} \bmod n$. For example, we get immediately a criterion for complete splitting in the full division field in terms of the invariants $a_\mathfrak{p}$ and $b_\mathfrak{p}$ modulo n, provided n is odd.

Corollary 2.2. *Let E be an elliptic curve defined over a number field K and $n > 1$ an odd integer. Then $\mathfrak{p}$, a prime of good reduction for E with $N(\mathfrak{p})$ prime to n, splits completely in L_n if and only if $a_\mathfrak{p} \equiv 2 \bmod n$ and $b_\mathfrak{p} \equiv 0 \bmod n$.*

For a discriminant Δ, let

$$Q_\Delta(x, y) = x^2 + \delta xy - ((\Delta - \delta)/4)y^2$$

be the principal form where $\delta = 0, 1$ according to whether $\Delta \equiv 0, 1 \bmod 4$. For $\mathfrak{p}$ a prime of good reduction for E we get a representation

$$N(\mathfrak{p}) = Q_{\Delta_\mathfrak{p}}(x, y) \tag{2–4}$$

with integral x, y upon using the change of variables

$$x = (a_\mathfrak{p} - b_\mathfrak{p}\delta_\mathfrak{p})/2 \qquad y = b_\mathfrak{p} \tag{2–5}$$

in (2-2). This representation is primitive if $\mathfrak{p}$ is ordinary. Let L_n^+ be the extension of K obtained by adjoining only the Weber functions of the n-th division points, that is the x-coordinates unless $j(E) = 0$ or $j(E) = 1728$, in which case we must first cube or square the coordinates, respectively. By Theorem 2.1, we may determine which sufficiently large ordinary primes split completely in L_n^+ from any such primitive representation.

Corollary 2.3. *Let E be an elliptic curve defined over a number field K as above and $n \ge 1$ an integer. Then there is a constant C_0 depending only on E and n so that for every ordinary prime $\mathfrak{p}$ of K with $N(\mathfrak{p}) > C_0$ we have that $\mathfrak{p}$ splits completely in L_n^+ if and only if $x \equiv \pm 1 \bmod n$ and $y \equiv 0 \bmod n$ in any primitive representation*

$$N(\mathfrak{p}) = Q_{\Delta_\mathfrak{p}}(x, y).$$

If E has CM by the ring of integers in an imaginary quadratic field of discriminant Δ, then the splitting completely condition in L_n^+ becomes simply

$$N(\mathfrak{p}) = Q_\Delta(x, y)$$

with integers $x \equiv \pm 1 \bmod n$ and $y \equiv 0 \bmod n$. Actually, suppose we take for E the elliptic curve with lattice given by the ring of integers of an imaginary quadratic field F of discriminant Δ and take $K = F(j(E))$, the Hilbert class field of F. It follows from Corollary 2.3 that a sufficiently large rational prime p splits in L_n^+ iff $p = Q_\Delta(x, y)$ with integers $x \equiv \pm 1 \bmod n$ and $y \equiv 0 \bmod n$. This is a well-known result of CM theory.

Another simple consequence in the CM case, this time of Corollary 2.2, is that the conditions

$$\#E_\mathfrak{p}(k) \equiv 0 \bmod n^2 \text{ and } N(\mathfrak{p}) \equiv 1 \bmod n,$$

which are clearly necessary for $\mathfrak{p}$ of good reduction to split completely in L_n, are also sufficient, at least when n is odd.

Our main application is to describe the primes that split completely in certain nonsolvable quintic extensions M/K. Suppose M is given by adjoining to K a solution of a principal quintic over K:

$$f(x) = x^5 + ax^2 + bx + c = 0$$

and that the discriminant of f is D. Suppose further that the Galois group of the normal closure L of M is S_5 and that $\sqrt{5D} \in K$.

Theorem 2.4. *Let M/K be a nonsolvable quintic extension as above. There exists an elliptic curve E defined*

over K so that a prime $\mathfrak{p}$ of K that has good reduction for E and is prime to 5 splits completely in M if and only if

$$b_{\mathfrak{p}} \equiv 0 \bmod 5$$

where $b_{\mathfrak{p}}$ is associated to the elliptic curve E.

In general, we have the following determination of the splitting type of $\mathfrak{p}$:

Splitting type of $\mathfrak{p}$ in M	$\left(\frac{a_{\mathfrak{p}}^2 - 4N(\mathfrak{p})}{5}\right)$	$\left(\frac{N(\mathfrak{p})}{5}\right)$	
$(1)(2)^2$	1	1	
$(1)(4)$	1	-1	
$(1)^2(3)$	-1	1	
$(1)^3(2)$	-1	-1	if $5 \mid a_{\mathfrak{p}}$
$(2)(3)$	-1	-1	if $5 \not\mid a_{\mathfrak{p}}$
(5)	0	if $5 \not\mid b_{\mathfrak{p}}$	
$(1)^5$	0	if $5 \mid b_{\mathfrak{p}}$	

Concerning the determination of E from f, it is enough to find the j-invariant of E. Explicit computations are provided below. We remark that it is also possible to formulate a similar result for A_5 extensions of K under otherwise identical assumptions. Furthermore, by allowing the elliptic curve to be defined over a quadratic or a biquadratic extension of K one may uniformize all nonsolvable quintic extensions.

It is also possible to explicitly uniformize certain degree 7 extensions whose normal closure have Galois group simple of order 168 by using the seventh division fields of elliptic curves (see [Radford 1898] and the references cited there.) By Theorem 2.1, one may similarly characterize the primes with a given splitting type in such extensions.

3. A GLOBAL REPRESENTATION OF THE FROBENIUS

In this section, we will prove Theorem 2.1 and its corollaries using an approach that compares the action of the Frobenius on the prime-to p division points with the action of the matrix (2–3) on $\mathbb{Z}^2$.

Proof of Theorem 2.1: Let E be an elliptic curve defined over a number field K. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathcal{K}}$ with residue field k $E_{\mathfrak{p}}$, the reduction of E mod $\mathfrak{p}$ (it is assumed that E has good reduction at $\mathfrak{p}$). That $\mathfrak{p}$ is unramified in the field L_n is well known, see e.g., [Silverman 86, VII.§4]. Also note that there is nothing to prove when $\phi_{\mathfrak{p}} \in \mathbb{Z}$, so we will assume throughout that this is not the case. The idea of the proof is that modulo $\mathfrak{p}$ the curve E can be replaced by a curve $\tilde{E}$ with complex multiplication so that the following diagram commutes:

$$\begin{array}{ccccc} E[n] & \xrightarrow{red} & E_{\mathfrak{p}}[n] & \xleftarrow{red} & \tilde{E}[n] \\ {\scriptstyle F_{\mathfrak{P}}}\downarrow & & {\scriptstyle \phi_{\mathfrak{p}}}\downarrow & & {\scriptstyle \tilde{\phi}_{\mathfrak{p}}}\downarrow \\ E[n] & \xrightarrow{red} & E_{\mathfrak{p}}[n] & \xleftarrow{red} & \tilde{E}[n] \end{array} \qquad (3\text{–}1)$$

where as usual $[n]$ stands for the n-division points on the curves in the algebraic closures of the appropriate fields.

We now explain this diagram in detail. To simplify matters, we fix a Weierstrass equation for E as in [**?**]Silverman. Let $\overline{K}, \overline{k}$ be the algebraic closures of K, k. To specify the horizontal maps *red*, we choose an embedding of $\overline{K}$ into the algebraic closure $\overline{K_{\mathfrak{p}}}$ of $K_{\mathfrak{p}}$, the completion of K at the valuation arising from $\mathfrak{p}$. We call the subgroup of torsion points whose orders are relatively prime to p the p'-torsion. Then the p'-torsion points on $E(\overline{K})$ are mapped into the p'-torsion of $E(\overline{K_{\mathfrak{p}}})$ and this being defined over an unramified extension, reduction modulo a prime $\mathfrak{P}$ above $\mathfrak{p}$ maps this latter group into the p'-torsion of $E(\overline{k})$. Both of these maps are isomorphisms on p' torsion. This is the map *red* for reduction, though as explained above it depends on many choices. Note, that after these choices are made, there is a unique element $F_{\mathfrak{p}} \in Gal(K_{\mathfrak{p}}^{unram}/K_{\mathfrak{p}})$ that satisfies $F_{\mathfrak{p}}(t) \equiv t^{\#k} \bmod \mathfrak{P}$, for all $t \in K_{\mathfrak{p}}^{unram}$.

We are interested in the action of the Frobenius automorphism $\phi_{\mathfrak{p}} \in Gal(\overline{k}/k)$ on the $\overline{k}$-valued points. In terms of the Weierstrass equation for E, this action on the coordinates is simply $(x, y) \mapsto (x^{\#k}, y^{\#k})$. By abuse of notation we also denote this action and the restriction of it to the n-division points by $\phi_{\mathfrak{p}}$.

Now the commutativity of the left half of the diagram is merely a restatement of the choices made above.

By Deuring's lifting theorem ([Deuring 41],[Lang 73, page 184]), there exists an elliptic curve $\tilde{E}$ defined over $K_{\mathfrak{p}}$ and an endomorphism $\tilde{\phi}_{\mathfrak{p}}$ of $\tilde{E}$ so that $\tilde{E}$ reduces to $E_{\mathfrak{p}}$ modulo $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ and that $\tilde{\phi}_{\mathfrak{p}} \in End(\tilde{E})$ reduces to $\phi_{\mathfrak{p}} \in End(E_{\mathfrak{p}})$. If E is super-singular, $\tilde{\phi}_{\mathfrak{p}}$ will be defined over a ramified extension. Reduction still makes sense since $\tilde{\phi}_{\mathfrak{p}}$ is an endomorphism and not a Galois automorphism.

This shows the commutativity of the right half of diagram (3–1).

To prove our theorem we need to determine the endomorphism ring S of $\tilde{E}$. Recall that the ring $R_{\mathfrak{p}}$ defined in the introduction is the centralizer of $\phi_{\mathfrak{p}}$ in the endomorphism ring of $E_{\mathfrak{p}}$ and is a quadratic order. We claim

that S is isomorphic to R. Since $R \subset S$, Deuring's reduction theorem implies equality if we can show that the conductor of R is prime to $N(\mathfrak{p})$, a fact that is trivial in the ordinary case and follows from [Waterhouse 69] in the super-singular case.

Let $\Delta_\mathfrak{p}$ be the discriminant of $R_\mathfrak{p}$. By choosing a complex square root of $\Delta_\mathfrak{p}$, we identify $R_\mathfrak{p}$ with a lattice in $\mathbb{C}$. After this identification $\phi_\mathfrak{p}$ corresponds to some complex number $\phi = (a_\mathfrak{p} + b_\mathfrak{p}\sqrt{\Delta_\mathfrak{p}})/2$. Clearly the lattice R is preserved by multiplication by ϕ and leads to the integral matrix (2-3), where we may choose $b_\mathfrak{p} \geq 0$. Instead of R one could, in fact, use any lattice whose endomorphism ring is R.

To finish the proof of Theorem 2.1, consider an embedding α of the algebraic closure of $K_\mathfrak{p}$ into $\mathbb{C}$. It allows us to view $\tilde{E}$ as an elliptic curve over the complex numbers, that we denote E_α. Since E_α has complex multiplication by R and $Gal(\mathbb{C}/\mathbb{Q})$ acts transitively on the set of elliptic curves with R as its endomorphism ring, we may and will assume the $j(E_\alpha) = j(R)$.

By choosing a nontrivial holomorphic differential ω on $\tilde{E}_\alpha$ appropriately the lattice of periods $\{\int_\gamma \omega : \gamma \in H_1(\tilde{E}_\alpha, \mathbb{Z}\} = R$. Then the period mapping $\Pi : \tilde{E}_\alpha \to \mathbb{C}/R$ is a biholomorphic isomorphism of complex analytic manifolds. The action of $\tilde{\phi}_\mathfrak{p}$ on $\tilde{E}$ defines an endomorphism of $\tilde{E}_\alpha$ and gives rise to a map ϕ_* on R. Since the Frobenius automorphism $\phi_\mathfrak{p}$ satisfies a quadratic equation

$$\phi_\mathfrak{p}^2 - a_\mathfrak{p}\ \phi_\mathfrak{p} + N(\mathfrak{p}) = 0. \tag{3–2}$$

ϕ_* can be identified with multiplication by one of the complex roots of this equation i.e., multiplication by $\phi : R \to R$ (viewed as complex numbers). Getting back to the n-division points we can again summarize the situation in the following diagram:

$$\begin{array}{ccccc} \tilde{E}_\mathfrak{p}[n] & \xrightarrow{\alpha} & \tilde{E}_\alpha[n] & \xrightarrow{n\times\Pi} & R/nR \\ \downarrow{\scriptstyle \tilde{\phi}_\mathfrak{p}} & & \downarrow{\scriptstyle \phi_\alpha} & & \downarrow{\scriptstyle \phi_*} \\ \tilde{E}_\mathfrak{p}[n] & \xrightarrow{\alpha} & \tilde{E}_\alpha[n] & \xrightarrow{n\times\Pi} & R/nR \end{array} \tag{3–3}$$

where $n \times \Pi$ is the period map followed by multiplication by n. This proves Theorem 2.1. □

Remark 3.1. If E is replaced by an Abelian variety V, then $\mathfrak{p}$ is still unramified [Shimura and Taniyama 61] and the left square of diagram (3–1) makes sense. If in addition V has ordinary reduction at $\mathfrak{p}$, then the right square in diagram (3–1) generalizes as shown by Deligne [Deligne 69] (and therefore the whole proof works). However the general case leads to substantial difficulties [Oort 85].

Corollary 2.2 is an immediate consequence of Theorem 2.1.

We now prove Corollary 2.3.

Proof of Corollary 2.3: Let E be an elliptic curve defined over a number field K as above and $n \geq 1$ an integer. Let $\mathfrak{p}$ be a prime of ordinary reduction for E. Given a primitive representation

$$p^r = Q_{\Delta_\mathfrak{p}}(x, y),$$

we know that x and y are uniquely determined up to (proper or improper) automorphs of $Q_{\Delta_\mathfrak{p}}$. If $-\Delta_\mathfrak{p} > 4$ and $x \equiv \pm 1 \bmod n$ and $y \equiv 0 \bmod n$, then it follows that

$$\sigma_\mathfrak{p} \equiv \begin{bmatrix} x + \delta y & y \\ y(\Delta_\mathfrak{p} - \delta_\mathfrak{p})/4 & x \end{bmatrix} \bmod n \tag{3–4}$$

and hence that $\mathfrak{p}$ splits completely in L_n^+. If $j = j(E)$ is not 0 or 1728, then for $\mathfrak{p}$ with $N(\mathfrak{p})$ sufficiently large, we have that $-\Delta_\mathfrak{p} > 4$. To see this, write $j = \alpha/\beta$ for $\alpha, \beta \in \mathcal{O}_\mathcal{K}$. We know that $j \equiv j(R_\mathfrak{p}) \bmod \mathfrak{p}$. If $j(R_\mathfrak{p}) = 0$ or 1728, then assuming that $j - j(R_\mathfrak{p}) \neq 0$, we have

$$N(\mathfrak{p}) \leq \max(|N(\alpha)|, |N(\alpha - 1728\beta)|).$$

In case $j = 0$ or $j = 1728$, the altered definition of L_n^+ leads again to the result. □

Finally, we prove the consequence of Corollary 2.2 mentioned below Corollary 2.3 that, in the CM case, a prime of good reduction $\mathfrak{p}$ splits completely in L_n if $a_\mathfrak{p} \equiv N(\mathfrak{p}) + 1 \bmod n^2$ and $N(\mathfrak{p}) \equiv 1 \bmod n$, provided n is odd.

Proof: Since these conditions immediately imply that $a_\mathfrak{p} \equiv 2 \bmod n$, by Corollary 2.2, we only must show that $n \mid b_\mathfrak{p}$. By our assumption

$$a_p^2 \equiv (N(\mathfrak{p}) - 1)^2 + 4N(\mathfrak{p}) \equiv 4N(\mathfrak{p}) \bmod n^2$$

we get, using

$$4N(\mathfrak{p}) \ = \ a_\mathfrak{p}^2 \ - \ \Delta_\mathfrak{p}\ b_\mathfrak{p}^2,$$

that

$$n^2 \mid \Delta_\mathfrak{p} b_\mathfrak{p}^2.$$

For a CM curve with fundamental Δ, the only possible prime dividing the square part of $\Delta_\mathfrak{p}$ is 2. In fact, $\Delta_\mathfrak{p} = \Delta$ for ordinary $\mathfrak{p}$ and for super-singular $\mathfrak{p}$, we have $\Delta_\mathfrak{p} = -p$ or $\Delta_\mathfrak{p} = -4p$, where $N(\mathfrak{p}) = p^r$. Since n is odd this implies that $n \mid b_\mathfrak{p}$. □

4. QUNITICS

In this section, we prove Theorem 2.4 and justify the general splitting criteria given after it as well as the example given in the introduction.

Proof of Theorem 2.4: Let M be given by adjoining to K a root of a principal quintic

$$f(x) = x^5 + ax^2 + bx + c = 0$$

defined over K. If the discriminant of f is 5 times a square then, by means of a Tschirnhausen transformation ([Dickson 26, page 218]), we may assume that M is determined by a Brioschi quintic

$$f_t(x) = x^5 - 10tx^3 + 45t^2x - t^2$$

for some $t \in K$ with $t \neq 0, \frac{1}{1728}$. It was shown by Kiepert [Kiepert 1878] already in 1879 (see [King 96] for an exposition) that M is contained in L_5^+ for any elliptic curve E over K with j-invariant $1728 - t^{-1}$. Recall that L_5^+ is, in this case, obtained by adjoining to K the x-coordinates of the 5 division points. One may take, for instance, the curve E_t given by

$$E_t : y^2 + xy = x^3 + 36tx + t. \tag{4–1}$$

If the splitting field of f over K is an S_5 extension then it must be the fixed field of the subgroup of scalars of G since $PGL_2(\mathbb{F}_5) \simeq S_5$. Theorem 2.4 now follows easily from Theorem 2.1. □

A calculation of conjugacy classes based on the identification of S_5 with $PGL_2(\mathbb{F}_5)$ leads to the determination of the splitting type of a prime $\mathfrak{p}$ of good reduction for E_t that is prime to 5. Recall that $A \in GL_2(\mathbb{F}_5)$ is called regular if it has different eigenvalues. Clearly A is regular if the discriminant of the characteristic equation $\mathrm{tr}(A)^2 - 4\det(A)$ is nonzero. Given such A, its conjugacy class is determined by its trace and determinant. It is clear that the values of the following Legendre symbols

$$\sigma = \left(\frac{\det(A)}{5}\right) \quad \text{and} \quad \rho = \left(\frac{\mathrm{tr}(A)^2 - 4\det(A)}{5}\right)$$

are determined by the conjugacy class of A in $PGL_2(\mathbb{F}_5)$. Now in case the characteristic polynomial of A splits, that is $\rho = 1$, the matrix A is conjugate to a diagonal matrix in $GL_2(\mathbb{F}_5)$ and so the value of σ already determines the cycle type of such matrices. When $\rho = -1$, one must take into account whether $\mathrm{tr}(A) \equiv 0$ or $\not\equiv 0 \bmod 5$. For A nonregular, $\mathrm{tr}(A)^2 - 4\det(A) = 0$ and one needs to know if A is semisimple or unipotent. This information cannot be extracted from the trace and determinant alone, but it is determined by the value of $b_{\mathfrak{p}}$. All that remains to be done is to identify each conjugacy classes with its cycle type.

The example in the introduction is obtained by taking $K = \mathbb{Q}$ and $t = \frac{-3^2}{2^8 5^2}$. Here we observe that since E has four 2-torsion points over $\mathbb{Q}$, both a_p and b_p will be even for p with good reduction. Thus the representation

$$4p \;=\; a_p^2 \;-\; \Delta_p \, b_p^2$$

yields

$$p \;=\; x^2 \;-\; \Delta_p \, y^2$$

and the condition for splitting completely is that $y \equiv 0 \bmod 5$, since x and y are determined uniquely up to sign.

5. SOME COMPUTATIONAL ISSUES

In this section, we discuss some of the computational issues that arise when considering examples.

First, given a principal quintic (slightly modified from above)

$$f(x) = x^5 + 5ax^2 + 5bx + c = 0 \tag{5–1}$$

defined over K with discriminant D such that $\sqrt{5D} \in K$, we must determine t so that the Brioschi quintic

$$f_t(x) = x^5 - 10tx^3 + 45t^2x - t^2 \tag{5–2}$$

determines the same extension. This is done using a Tschirnhausen transformation and is described in detail in [King 96, page 103], (see also [Dickson 26, page 128]) Here we will simply record the result in the case $a \neq 0$.

One determines t, λ and μ in the map

$$x \mapsto \frac{\lambda + \mu x}{(x^2/t) - 3} \tag{5–3}$$

in order to transform the general principal quintic (5–1) to the Brioschi quintic (5–2).

An analysis using invariant polynomials for the icosahedral group acting on the Riemann sphere leads eventually to the quadratic equation for λ given by

$$(a^4+abc-b^3)\lambda^2-(11a^3-ac^2+2b^2c)\lambda+64a^2b^2-27a^3c-bc^2 = 0.$$

The discriminant of this quadratic is

$$5^{-5}a^2D$$

and so $\lambda \in K$. Choose either solution and let

$$j = \frac{(a\lambda^2 - 3b\lambda - 3c)^3}{a^2(\lambda ac - \lambda b^2 - bc)}.$$

	t=1			t=2			t=3			t=4		
p	Δ_p	a_p	b_p	Δ_p	a_p	b_p	Δ_p	a_p	b_p	Δ_p	a_p	b_p
2	-7	-1	1	-	-	-	-7	-1	1	-	-	-
3	-8	-2	1	-11	1	1	-	-	-	-8	-2	1
5	-11	3	1	-	-	-	-16	2	1	-19	-1	1
7	-24	2	1	-12	-4	1	-19	-3	1	-24	-2	1
11	-	-	-	-43	1	1	-28	4	1	-40	-2	1
13	-12	2	2	-13	0	1	-27	5	1	-51	1	1
17	-8	-6	2	-59	-3	1	-52	4	1	-43	-5	1
19	-60	-4	1	-67	3	1	-15	4	2	-72	2	1
23	-76	-4	1	-56	-6	1	-56	6	1	-56	-6	1
29	-28	-2	2	-29	0	1	-100	-4	1	-35	-9	1
31	-24	10	1	-24	10	1	-31	0	1	-88	-6	1
37	-123	5	1	-84	-8	1	-139	3	1	-147	1	1
41	-8	-6	4	-139	-5	1	-128	6	1	-83	-9	1
43	-156	4	1	-39	4	2	-7	12	2	-72	-10	1
47	-172	-4	1	-152	6	1	-184	2	1	-152	6	1
53	-211	-1	1	-176	-6	1	-176	6	1	-52	-2	2
59	-232	2	1	-211	-5	1	-172	8	1	-40	14	1
61	-75	13	1	-61	0	1	-36	-10	2	-36	-10	2
67	-232	-6	1	-147	11	1	-187	9	1	-264	-2	1
71	-140	12	1	-248	-6	1	-	-	-	-248	6	1
73	-123	-13	1	-123	-13	1	-	-	-	-291	-1	1
79	-300	-4	1	-300	4	1	-291	-5	1	-252	8	1
83	-83	0	1	-331	1	1	-136	-14	1	-316	4	1
89	-187	-13	1	-355	-1	1	-89	0	1	-80	-6	2
97	-88	-6	2	-43	-1	3	-363	-5	1	-96	-2	2

TABLE 1. The invariants for the elliptic curves E_t for the first 25 primes (− indicates that the curve has bad reduction).

Then, provided $j \neq 0, 1728$ we may take

$$t = 1/(1728 - j)$$

in (5–2) and choose for the elliptic curve, any curve with this j invariant, say

$$E_t : y^2 + xy = x^3 + 36tx + t$$

as in (4–1). Also, one may determine μ in (5–3) to be given by

$$\mu = \frac{ja^2 - 8\lambda^3 a - 72\lambda^2 b - 72\lambda c}{\lambda^2 a + \lambda b + c}.$$

Note that the discriminant of f_t is

$$D_t = 5^5 t^8 (1728t - 1)^2$$

while that of E_t is

$$-t(1728t - 1)^2.$$

Another issue is to compute the invariants Δ_p and b_p in the rational case. An important study of Δ_p was made by Schoof in [Schoof 89]. The most straightforward way to determine b_p and to find the order R that appears in Deuring's theorem is to check all the possible singular invariants until we find one that is congruent to the given j-value modulo p. (Note that the discriminant of R must divide $a_p^2 - 4p$.) We assume that our input is an elliptic curve E, given in the Weierstrass equation, and p is a prime number that does not divide the discriminant of E. After computing a_p, we find Δ_p for an ordinary curve as follows; we first compute the square-free part D of $a_p^2 - 4p$ and then create a vector whose values are all possible discriminants

$$\Delta = b^2 D | (a_p^2 - 4p).$$

For a possible conductor Δ, we find the class group $\mathcal{C}(\Delta)$ of the proper ideal classes (using quadratic forms) and compute the integer

$$X_\Delta = \prod_{\Lambda \in \mathcal{C}(\Delta)} (j(E) - j(\Lambda)).$$

Note that the canonical lift $\tilde{E}$ is distinguished by the fact that its endomorphism ring is R and that $j(E) \equiv j(\tilde{E}) \bmod P$ for some prime P dividing p. Therefore, for any complex embedding $\alpha : \mathbb{Q}_p \to \mathbb{C}$,

$$\alpha(j(\tilde{E})) \in \{j(\mathbb{C}/\Lambda) : \Lambda \in \mathcal{C}_{\Delta_p}\},$$

	t=1			t=2			t=3			t=4		
p	Δ_p	a_p	b_p	Δ_p	a_p	b_p	Δ_p	a_p	b_p	Δ_p	a_p	b_p
541	-492	14	2	-1680	-22	1	-1539	25	1	-2115	7	1
547	-2088	-10	1	-1827	19	1	-351	-28	2	-1992	-14	1
557	-1939	-17	1	-2224	2	1	-464	42	1	-532	10	2
563	-563	0	1	-419	24	2	-2188	-8	1	-1676	24	1
569	-1051	35	1	-2107	13	1	-1792	-22	1	-1835	21	1
571	-2184	-10	1	-2275	-3	1	-375	-28	2	-168	46	1
577	-528	14	2	-576	2	2	-2139	13	1	-496	18	2
587	-2204	-12	1	-551	12	2	-1324	32	1	-584	42	1
593	-1283	33	1	-2203	13	1	-1076	36	1	-152	-42	2
599	-2392	-2	1	-2296	10	1	-2140	-16	1	-1240	-34	1
601	-2115	17	1	-2379	-5	1	-376	30	2	-227	19	3
607	-984	38	1	-2412	4	1	-607	0	1	-984	-38	1
613	-147	10	4	-1876	24	1	-1723	-27	1	-324	-34	2
617	-2107	19	1	-88	-46	2	-164	48	1	-88	46	2
619	-1032	-38	1	-955	39	1	-47	-28	6	-1800	-26	1
631	-924	40	1	-1228	-36	1	-2235	-17	1	-1368	34	1
641	-2483	-9	1	-632	-6	2	-2420	12	1	-560	-18	2
643	-1416	34	1	-2563	-3	1	-1611	-31	1	-2536	-6	1
647	-2264	18	1	-2444	-12	1	-284	-48	1	-2188	-20	1
653	-2603	-3	1	-2036	-24	1	-2608	-2	1	-652	-2	2
659	-2440	14	1	-623	12	2	-2312	-18	1	-1736	-30	1
661	-2619	5	1	-2640	2	1	-1419	-35	1	-1915	-27	1
673	-39	-14	8	-1851	-29	1	-2571	-11	1	-2643	-7	1
677	-2179	23	1	-1808	30	1	-2224	22	1	-2267	-21	1
683	-2056	-26	1	-2563	-13	1	-428	-48	1	-2156	24	1
691	-300	8	3	-	-	-	-495	-28	2	-2620	12	1

TABLE 2. The invariants for the elliptic curves E_t for the primes from $p_{100} = 541$ to $p_{125} = 691$.

	t=1			t=2			t=3			t=4		
p	Δ_p	a_p	b_p	Δ_p	a_p	b_p	Δ_p	a_p	b_p	Δ_p	a_p	b_p
7927	-236	172	3	-14284	-132	1	-5991	88	2	-31608	-10	1
7933	-28011	61	1	-16848	-122	1	-12411	-139	1	-116	166	6
7937	-7888	14	2	-18979	113	1	-28148	60	1	-31387	19	1
7949	-22771	95	1	-17872	-118	1	-6196	-160	1	-31627	-13	1
7951	-23340	92	1	-14380	132	1	-26179	75	1	-29868	44	1
7963	-31276	-24	1	-3063	-140	2	-31491	-19	1	-16476	-124	1
7993	-3539	-11	3	-1888	42	4	-876	134	4	-23323	-93	1
8009	-5408	-102	2	-27811	-65	1	-19040	114	1	-28315	61	1
8011	-21228	-104	1	-17403	-121	1	-8019	155	1	-21640	102	1
8017	-16443	-125	1	-6648	-74	2	-24843	-85	1	-31779	-17	1
8039	-7192	158	1	-28556	60	1	-31672	22	1	-22940	-96	1
8053	-6964	-66	2	-32176	6	1	-25651	81	1	-22011	101	1
8059	-30636	-40	1	-24315	89	1	-7995	16	2	-31080	-34	1
8069	-32267	-3	1	-32020	16	1	-9776	150	1	-1807	58	4
8081	-22123	-101	1	-30115	47	1	-32128	14	1	-1520	162	2
8087	-31772	24	1	-32344	2	1	-21112	106	1	-31324	-32	1
8089	-29331	55	1	-8947	-153	1	-7360	54	2	-896	-10	6
8093	-31147	35	1	-32228	12	1	-20708	-108	1	-32363	3	1
8101	-275	-173	3	-11668	-144	1	-30003	49	1	-3612	134	2
8111	-30680	42	1	-1240	-38	5	-11708	-144	1	-31148	36	1
8117	-10859	147	1	-31684	-28	1	-27284	72	1	-7948	-26	2
8123	-26716	-76	1	-10291	-149	1	-32488	2	1	-32236	16	1
8147	-32104	-22	1	-26659	-77	1	-30824	42	1	-24844	-88	1
8161	-32	-62	30	-9235	-153	1	-29163	-59	1	-984	130	4
8167	-2236	-112	3	-20124	-112	1	-30267	49	1	-32632	-6	1

TABLE 3. The invariants for the elliptic curves E_t for the primes from $p_{1001} = 7927$ to $p_{1025} = 8167$.

t	1	2	3	4	5	6	7	8	9	10	11
Δ_{23}	-76	-56	-56	-56	-83	-56	-91	-	-28	-23	-19
a_{23}	-4	-6	6	-6	3	-6	-1	-	-8	0	4
b_{23}	1	1	1	1	1	1	1	-	1	1	2

t	12	13	14	15	16	17	18	19	20	21	22
Δ_{23}	-88	-76	-83	-7	-76	-11	-88	-43	-67	-83	-91
a_{23}	2	4	3	-8	4	-9	2	-7	5	-3	1
b_{23}	1	1	1	2	1	1	1	1	1	1	1

TABLE 4. For the prime 23, the invariants of the curve E_t, (at $t = 8$, E_t is singular).

t	$b_p = 1$	2	3	4	5	6	7	8	9	10	11	12
1	77	10	6	3	0	1	0	2	0	0	0	1
2	74	15	5	1	1	0	1	2	0	0	0	0
3	80	15	1	2	0	1	1	0	0	0	0	0
4	78	14	2	4	0	1	0	0	0	0	0	1
5	82	11	5	1	1	0	0	0	0	0	0	0
6	78	14	5	2	0	1	0	0	0	0	0	0
7	81	12	4	2	1	0	0	0	0	0	0	0
8	76	13	4	5	0	0	0	1	0	0	0	0
9	79	16	2	2	1	0	0	0	0	0	0	0
10	88	6	2	2	0	0	1	0	0	0	0	1
11	75	15	3	5	1	0	0	1	0	0	0	0
12	75	16	6	1	1	0	0	1	0	0	0	0
13	73	15	6	1	2	1	0	1	0	0	0	0
14	79	11	7	2	1	0	0	0	0	0	0	0
15	80	12	3	0	3	1	0	0	0	0	0	0
16	79	12	1	4	0	3	0	0	0	0	0	0
17	84	9	1	2	2	1	0	1	0	0	0	0
18	83	12	3	0	2	0	0	0	0	0	0	0
19	77	16	3	3	1	0	0	0	0	0	0	0
20	81	15	2	1	0	0	0	0	1	0	0	0
21	81	17	2	0	0	0	0	0	0	0	0	0
22	77	17	6	0	0	0	0	0	0	0	0	0
23	73	18	4	3	0	0	0	1	0	0	0	0
24	84	8	3	2	3	0	0	0	0	0	0	0
25	76	10	4	6	1	0	1	2	0	0	0	0

TABLE 5. For a given t, the table shows the number of primes in the range $p_{101} = 547 \leq p \leq p_{200} = 1223$, for which the invariant b_p of E_t is $1, 2...,$.

where Δ_p is the actual discriminant of R. Also note that if $\Lambda' \in \mathcal{C}_{\Delta'}$ for $\Delta' \neq \Delta_p$, then the corresponding elliptic curve reduces to a curve whose endomorphism ring has discriminant Δ' for any place above p.

Therefore, Δ_p is uniquely characterized by the fact that

$$X_{\Delta_p} \equiv 0 \bmod p.$$

Occasionally the computation of X_Δ involves complex numbers of rather large size. To make the algorithm efficient, one needs to determine the needed precision in advance.

Assume that the lattices are given in the form $\mathbb{Z}+\mathbb{Z}\tau_i$, with τ_i in the upper half plane. Then the number of significant digits one must use is approximately

$$\sum_{\tau_i} \frac{\log(j(E)) + 2\pi Im(\tau_i)}{\log(10)}.$$

It follows from Lemma 2.2 of [Schoof 89] that the required precision is approximately of size $\sqrt{p}$.

p	$b_p = 1$	2	3	4	5	6	7	8	9	10	11	12
233	187	34	0	8	0	0	1	1	0	0	0	0
239	201	31	0	0	3	0	1	0	0	1	0	0
241	175	33	16	6	3	3	0	3	0	0	0	0
251	206	38	0	0	4	0	0	0	0	0	1	0
257	206	39	0	8	0	0	0	2	0	0	0	0
263	223	37	0	0	0	0	1	0	0	0	0	0
269	209	43	0	11	4	0	0	0	0	0	0	0
271	208	35	18	0	4	4	0	0	0	0	0	0
277	207	35	19	10	0	2	1	0	0	0	0	1
281	219	43	0	9	3	0	2	2	0	1	0	0
283	216	42	19	0	0	3	0	0	1	0	0	0
293	235	44	0	12	0	0	0	0	0	0	0	0
307	235	45	20	0	0	4	0	0	1	0	0	0
311	263	41	0	0	4	0	0	0	0	1	0	0
313	235	40	20	9	0	3	0	2	1	0	0	1
317	257	43	0	13	0	0	2	0	0	0	0	0
331	247	49	22	0	5	4	1	0	1	0	0	0
337	253	42	22	10	0	4	1	2	0	0	0	1
347	288	54	0	0	0	0	1	0	0	0	0	0
349	255	45	23	14	4	4	0	0	1	1	0	0
353	285	51	0	12	0	0	0	2	0	0	1	0
359	300	49	0	0	6	0	1	0	0	0	0	0
367	283	51	25	0	0	5	0	0	0	0	1	0
373	278	48	25	14	0	3	1	0	1	0	0	1
379	284	53	25	0	4	5	1	0	1	2	1	0

TABLE 6. Given p, the table shows the number of t in the range $1 \leq t \leq p-1$ for which the invariant b_p of E_t takes the value $1, 2, \ldots$.

Tables 1–5 give information about the invariants of the family of elliptic curves

$$E_t : y^2 + xy = x^3 + 36tx + t$$

associated as above to the quintic

$$f_t(x) = x^5 - 10tx^3 + 45t^2x - t^2.$$

We made use of pari-gp in these computations.

ACKNOWLEDGMENTS

We would like to thank N. Katz for his helpful comments. W. Duke was supported by NSF grant DMS-98-01642, the Clay MAthematics Institute, and the American Institute of Mathematics. Á. Tóth was supported by a Rackham grant.

REFERENCES

[Chebotarov 95] N. Chebotarov. "Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören." *Math. Ann.* 95 (1926), 191–228.

[Cox 89] D. A. Cox. *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication.* New York: John Wiley & Sons, Inc., 1989.

[Deligne 69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini." *Invent. Math.* 8 (1969), 238-243.

[Deuring 41] M. Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkorper." *Abh. Math. Sem. Hamburg* 14 (1941), 197–272.

[Dickson 26] L. E. Dickson. *Modern Algebraic Theories.* Chicago: Benj. H. Sanborn & Co., 1926.

[Kiepert 1878] L. Kiepert. "Auflösung der Gleichungen fünften Grades." *J. für Math.* 87 (1878), 114–133

[King 96] R.B. King. *Beyond the Quartic Equation.* Boston, MA: Birkhäuser Boston, Inc., 1996.

[Klein 56] F. Klein. *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree.* New york: Dover Publications, Inc., 1956

[Lang 73] S. Lang. *Elliptic Functions.* Reading, MA: Addison-Wesley, 1973.

[Oort 85] F. Oort. "Lifting Algebraic Curves, Abelian Varieties, and their Endomorphisms to Characteristic Zero." In *Algebraic Geometry Bowdoin 1985 (Proc. Sympos. Pure Math., 46, Part 2)* pp. 165–195. Providence: Amer. Math. Soc., 1987.

[Radford 1898] E. M. Radford. "On the Solution of Certain Equations of the Seventh Degree." *Quarterly J. Math.* 30 (1898), 263–306.

[Schoof 89] R. Schoof. "The Exponents of the Groups of Points on the Reductions of an Elliptic Curve." in *Arithmetic Algebraic Geometry (Texel, 1989),* Progr. Math. 89. pp. 325–335. Boston, MA: Birkhäuser Boston, 1991.

[Serre 72] J-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Inventiones Math.* 15 (1972), 259–331.

[Silverman 86] J. Silverman. *The Arithmetic of Elliptic Curves.* New York: Springer-Verlag, 1986.

[Shimura 66] G. Shimura. "A Reciprocity Law in Non-Solvable Extensions." *J. Crelle* 221 (1966), 209–220.

[Shimura and Taniyama 61] G. Shimura and Y. Taniyama. *Complex Multiplication of Abelian Varieties and its Applications to Number Theory.* Tokyo: The Mathematical Society of Japan, 1961.

[Stark 94] H. M. Stark. "Counting Points on CM Elliptic Curves." *Rocky Mountain J. Math.* 26:3 (1996), 1115–1138.

[Waterhouse 69] W. C. Waterhouse. "Abelian Varieties Over Finite Fields." *Ann. Sci. Ècole Norm. Sup.* 4:2 (1969), 521–560.

William Duke, Department of Mathematics, UCLA, Mathematics Department, Box 951555, Los Angeles, CA 90095-1555 (duke@math.ucla.edu)

Á. Tóth, Princeton University, 316 Fine Hall, Department of Mathematics, Washington Road, Princeton, NJ 08544 (atoth@math.princeton.edu)

Received June 6, 2002; accepted October 8, 2002.