MATHEMATICS OF COMPUTATION
Volume 83, Number 290, November 2014, Pages 3001–3004
S 0025-5718(2014)02831-7
Article electronically published on May 9, 2014

A RELATION BETWEEN EMBEDDING DEGREES AND CLASS NUMBERS OF BINARY QUADRATIC FORMS

SAN LING, ENVER OZDEMIR, AND CHAOPING XING

Abstract. In this paper, we describe a relation between the embedding degree of an elliptic curve over a prime field $\mathbb{F}_p$ and the inertial degree of the primes above p in a certain ring class field. From this relation, we conclude that the embedding degree divides the class number of a group of binary quadratic forms of a fixed discriminant.

1. Introduction

Determining the embedding degrees of elliptic curves over a finite field has attracted attention due to cryptographic applications ([2]). In this paper, we show that the n^{th} embedding degree of an ordinary elliptic curve E defined over a prime field $\mathbb{F}_p$ is equal to the inertial degree of the primes above p in the ring class field arising from an order of discriminant n^2D in an imaginary quadratic field, where D is the discriminant of the endomorphism ring of E. This implies that the n^{th} embedding degree divides the cardinality of the class group of the binary quadratic forms with discriminant n^2D.

The paper is organized as the follows. In Section 2, we introduce elliptic curves and embedding degrees. In Section 3, we prove our main result, Theorem 3.3, after the discussion of quadratic forms, endomorphism ring of elliptic curves and ring class fields.

2. Embedding degrees of elliptic curves

Let p be a prime integer and let $\mathbb{F}_p$ be the field with p elements. We denote by $\overline{\mathbb{F}}_p$ the algebraic closure of $\mathbb{F}_p$. The field $\mathbb{F}_{p^k}$ is a subfield of $\overline{\mathbb{F}}_p$ with p^k elements for an integer $k \geq 1$. An elliptic curve E over $\mathbb{F}_p$ is a smooth algebraic curve defined by an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with $a_i \in \mathbb{F}_p$. If $x, y \in \overline{\mathbb{F}}_p$ satisfy (2.1), we say that the point $(x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ is on the curve E. The set of all points on the curve with a point P_∞ (identity) at infinity forms an abelian group and the group is denoted by $E(\overline{\mathbb{F}}_p)$. The subgroup $E(\mathbb{F}_{p^k})$ of $E(\overline{\mathbb{F}}_p)$ consisting of points $(x, y) \in \mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ with P_∞ is of finite order for

Received by the editor December 11, 2012 and, in revised form, April 1, 2013.
2010 *Mathematics Subject Classification.* Primary 11R11, 11R29, 11G15, 11G05.
Key words and phrases. Imaginary quadratic fields, class number, elliptic curves, embedding degree.
This research was partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03 and the Singapore Ministry of Education under Research Grant T208B2206.

any positive integer k. The details for the group operation in $E(\overline{\mathbb{F}}_p)$ and computing the order of $E(\mathbb{F}_{p^k})$ can be found in [4, Chapter 4] or [8].

Throughout this paper, we make two assumptions: (i) n is a positive integer coprime to p; (ii) E is an ordinary elliptic curve over $\mathbb{F}_p$.

Definition 2.1. A point P in $E(\overline{\mathbb{F}}_p)$ is called an *n-torsion* point if $nP = P_\infty$.

The set $E[n]$ of all n-torsion points of E is a subgroup of $E(\overline{\mathbb{F}}_p)$ and it is isomorphic to $\mathbb{Z}_n \oplus \mathbb{Z}_n$ where $\mathbb{Z}_n$ is the quotient group $\mathbb{Z}/n\mathbb{Z}$ (see [8, Section 3.1]). An integer k such that $E[n]$ lies in $E(\mathbb{F}_{p^k})$ is called an n^{th} *embedding degree* of the curve E and the minimum of such an integer k is called the n^{th} embedding degree of E.

The following result provides a necessary condition for which k is an n^{th} embedding degree of the curve E.

Proposition 2.2. *Let p, E, n, k be the same as above. If we have $E[n] \subseteq E(\mathbb{F}_{p^k})$, then $p^k \equiv 1 \bmod n$.*

Proof. See the proof of Corollary 3.11 in [8]. □

We will see in a moment that under certain conditions the converse of the above statement is also correct.

3. Class numbers and embedding degrees

We first give a brief summary of binary quadratic forms, endomorphism rings of elliptic curves and ring class fields.

We consider here binary quadratic forms in two variables $f = ax^2 + bxy + cy^2 = (a, b, c)$ of discriminant $D = b^2 - 4ac$. We assume $D < 0 < a$ and $\gcd(a, b, c) = 1$. A form of this kind is called a *positive definite form*. From now on, we assume all forms are positive definite. Let

$$g(x', y') = a'x'^2 + b'x'y' + c'y'^2 \text{ and } f(x, y) = ax^2 + bxy + cy^2$$

be two forms of the same discriminant. They are called *equivalent* if there exist integers

$$\alpha, \beta, \gamma, \delta \text{ with } \alpha\delta - \beta\gamma = 1$$

such that

$$x_1 = \alpha x' + \beta y' \ , \ y_1 = \gamma x' + \delta y' \text{ and } f(x_1, y_1) = g(x', y').$$

This equivalence relation makes the set of binary quadratic forms of the same discriminant an abelian group which we will denote by $C(D)$. The group $C(D)$ is isomorphic to the ideal class group of an order $\mathcal{O}_D$ of discriminant D in an imaginary quadratic field. Let p be a prime integer such that D is a square mod p. Then we have a form $f_p = (p, b, c)$ for some $b, c \in \mathbb{Z}$ which is called a *prime form*, and prime forms generate the group $C(D)$ [7]. See [3] for justification of the above statements.

Let E be an ordinary elliptic curve over a finite field $\mathbb{F}_p$. The endomorphism ring of the elliptic curve E is isomorphic to an order $\mathcal{O}_D$ with a discriminant D in an imaginary quadratic field K. The ideal class group $C(\mathcal{O}_D)$ of $\mathcal{O}_D$ is isomorphic to the group $C(D)$ of the binary quadratic forms of discriminant D. Hence any ideal class I of $C(\mathcal{O}_D)$ is represented by a triple $[A, B, C]$ such that $B^2 - 4AC = D$ and the number $\tau = \frac{-B+\sqrt{D}}{2A}$ is in the standard fundamental domain. The corresponding

j value for the ideal I is $j\left(\frac{-B+\sqrt{D}}{2A}\right)$, where $j(\tau)$ is Klein's j-function, and each j value is the j-invariant of an elliptic curve over $\mathbb{C}$ with the endomorphism ring $\mathcal{O}_D$. This implies that there are h_D isomorphism classes of elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_D$, where h_D is the class number of $C(D)$. The extension field K_D of K generated by these j values is called *the ring class field* for $\mathcal{O}_D$. The extension is finite abelian and has degree h_D. The common minimal polynomial $P_D(x)$ for the j values is called the Hilbert class polynomial for $\mathcal{O}_D$.

Let p be a prime integer such that p splits completely in K and let $\wp$ be a prime ideal above p in K. The inertial degree of the primes above $\wp$ in K_D is the degree of the irreducible factors of $P_D(x) \bmod p$ as $[\mathcal{O}_K/\wp : \mathbb{Z}/(p)] = 1$ where $\mathcal{O}_K$ is the ring of integers of K. By Deuring's lifting theorem [5], the inertial degree of the primes above $\wp$ in K_D is the smallest k such that $\mathbb{F}_{p^k}$ is the definition field of elliptic curves over $\overline{\mathbb{F}}_p$ with the endomorphism ring $\mathcal{O}_D$ as the j-invariants of such elliptic curves E are the roots of $P_D(x)$.

Let $\mathcal{F}_{p^t}$ be the $(p^t)^{th}$-power Frobenious endomorphism of E, i.e., $\mathcal{F}_{p^t}(x,y) = (x^{p^t}, y^{p^t})$ for $(x,y) \in E(\overline{\mathbb{F}}_p)$. Since the endomorphism ring of E is isomorphic to the order $\mathcal{O}_D$, each endomorphism of E corresponds to a number in $\mathcal{O}_D$. The following propositions give relations between an n^{th} embedding degree k and n.

Proposition 3.1. *Let E, $E[n]$, k, p be as above such that $\#E(\mathbb{F}_p)$ is divisible by n and $n \nmid p(p-1)$. $E[n] \subseteq E(\mathbb{F}_{p^k})$ if and only if $p^k \equiv 1 \bmod n$.*

Proof. See the proof of Proposition 5.9 in [8] or [1]. □

Proposition 3.2. *Let the notations be the same as above. If $E[n] \subseteq E(\mathbb{F}_{p^k})$, then $\mathcal{F}_{p^k} \equiv 1 \bmod n\mathcal{O}_D$, where $\mathcal{O}_D$ is the the endomorphism ring of E.*

Proof. $\mathcal{F}_{p^k} \equiv 1 \bmod n\mathcal{O}(D)$ means the $p^{k^{th}}$ power Frobenious $\mathcal{F}_{p^k}$ acts as the identity on the subgroup of n-torsions, that is, $\mathcal{F}_{p^k}(x,y) = (x^{p^k}, y^{p^k}) = (x,y)$ for $(x,y) \in E[n]$. For more details see [6, Proposition 3.7] or [8, Section 10.4]. □

The following theorem shows that the embedding degree divides the class number $C(n^2D)$, where D is the discriminant of the endomorphism ring of the elliptic curve.

Theorem 3.3. *Let E, $E[n]$, k, p be as above such that $n \nmid p(p-1)$, n is squarefree and $\#E(\mathbb{F}_p) = in$ for some integer $i < n$. Then the n^{th} embedding degree of $E(\mathbb{F}_p)$ is equal to the inertial degree of the primes above p in the ring class field K_{n^2D} of K. Consequently, the n^{th} embedding degree k of E divides the order of $C(n^2D)$.*

Proof. Let b be $p^k + 1 - \#E(\mathbb{F}_{p^k})$. We first show that the equations

$$4p^k = b^2 - v^2(n^2D) \quad \text{for some integer } v \tag{3.1}$$

and

$$p^k \equiv 1 \mod n, \tag{3.2}$$

are equivalent.

Assume that (3.1) holds. Then we have

$$4p^k \equiv (-\#E(\mathbb{F}_{p^k}) + p^k + 1)^2 \equiv (p^k+1)^2 \mod n.$$

This is equivalent to (3.2) as n is squarefree. Now assume that equation (3.2) holds. By Proposition 3.1, k is an n^{th} embedding degree of E. By Proposition 3.2, the element $(\mathcal{F}_{p^k} - 1)/n$ belongs to $\mathcal{O}_D$. Thus, $\mathbb{Z}[(\mathcal{F}_{p^k} - 1)/n]$ is a subring of $\mathcal{O}_D$. This

implies that the discriminant of $\mathbb{Z}[(\mathcal{F}_{p^k}-1)/n]$ is equal to v^2D for some integer v. A simple computation shows that the the discriminant of $\mathbb{Z}[(\mathcal{F}_{p^k}-1)/n]$ is $(b^2-4p^k)/n^2$, where b is equal to $\#E(\mathbb{F}_{p^k})-(p^k+1)$. Thus, equation (3.1) holds.

By Proposition 3.1, the smallest positive integer k satisfying equation (3.1) is the n^{th} embedding degree of E. Similarly, we know that the smallest k satisfying equation (3.1) gives the definition field $\mathbb{F}_{p^k}$ of an elliptic curve with the endomorphism ring $\mathcal{O}_{n^2D}$. Hence, the inertial degree of the primes above p in the ring class field K_{n^2D} is the smallest k satisfying equation (3.1). This implies that the n^{th} embedding degree of $E(\mathbb{F}_p)$ is equal to the inertial degree of the primes above p in the ring class field K_{n^2D}.

Since the inertial degree divides the extension degree $h_{n^2D}=[K_{n^2D}:K]$, the second result follows. □

References

[1] R. Balasubramanian and Neal Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), no. 2, 141–145, DOI 10.1007/s001459900040. MR1620936 (2000f:94024)

[2] Dan Boneh and Matt Franklin, *Identity-based encryption from the Weil pairing*, Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 2139, Springer, Berlin, 2001, pp. 213–229, DOI 10.1007/3-540-44647-8_13. MR1931424 (2003h:94054)

[3] Duncan A. Buell, *Binary quadratic forms*, Classical theory and modern computations, Springer-Verlag, New York, 1989. MR1012948 (92b:11021)

[4] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen and Frederik Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. MR2162716 (2007f:14020)

[5] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR0005125 (3,104f)

[6] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211, DOI 10.1016/0097-3165(87)90003-3. MR914657 (88k:14013)

[7] R. J. Schoof, *Quadratic fields and factorization: Computational methods in number theory, Part II*, Math. Centre Tracts, vol. 155, Math. Centrum, Amsterdam, 1982, pp. 235–286. MR702519 (85g:11118b)

[8] Lawrence C. Washington, *Elliptic curves,* Number theory and cryptography, 2nd ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008. MR2404461 (2009b:11101)

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

E-mail address: lingsan@ntu.edu.sg

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

Current address: Informatics Institute, Istanbul Technical University, 34469 Istanbul, Turkey

E-mail address: ozdemiren@itu.edu.tr

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

E-mail address: xingcp@ntu.edu.sg