Finite Fields and Their Applications 58 (2019) 174–176

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Loops of isogeny graphs of supersingular elliptic curves at $j = 0$

Yi Ouyang, Zheng Xu *

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China

ARTICLE INFO

Article history:
Received 23 December 2018
Received in revised form 2 April 2019
Accepted 11 April 2019
Available online xxxx
Communicated by Neal Koblitz

MSC:
11G20
11G15
14G15
14H52
94A60

Keywords:
Supersingular elliptic curves over finite fields
Isogeny graphs

ABSTRACT

We improve Adj et al.'s bound in [1, Theorem 12] from $p > 4\ell$ to $p > 3\ell$ for the loops of $E_0 : y^2 = x^3 + 1$ in the ℓ-isogeny graph $G_\ell(\mathbb{F}_{p^2}, -2p)$ of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with trace $-2p$.

Let ℓ and p be distinct prime numbers. The ℓ-isogeny graph $G_\ell(\mathbb{F}_{p^2})$ over $\mathbb{F}_{p^2}$ is the graph whose vertices are $\mathbb{F}_{p^2}$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ and edges are equivalent classes of ℓ-isogenies defined over $\mathbb{F}_{p^2}$. If replacing the field of definition $\mathbb{F}_{p^2}$ of the curves and isogenies by the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, we get

* Corresponding author.
E-mail addresses: yiouyang@ustc.edu.cn (Y. Ouyang), xuzheng1@mail.ustc.edu.cn (Z. Xu).

https://doi.org/10.1016/j.ffa.2019.04.002

the definition of $G_\ell(\overline{\mathbb{F}}_p)$. By Tate's result ([4]), two elliptic curves over a finite field $\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if the traces of the Frobenius ($x \mapsto x^q$) on their Tate modules are the same. For a fixed $t \in \mathbb{Z}$, let $G_\ell(\mathbb{F}_{p^2}, t)$ be the subgraph of $G_\ell(\mathbb{F}_{p^2})$ consisting of vertices whose underlying curves are of Frobenius trace t and edges connecting the vertices. In this graph, two isogenies from E_1 to E_2 are equivalent if they have the same kernel. Then the graph $G_\ell(\mathbb{F}_{p^2})$ is the disjoint union of $G_\ell(\mathbb{F}_{p^2}, 0)$, $G_\ell(\mathbb{F}_{p^2}, \pm p)$ and $G_\ell(\mathbb{F}_{p^2}, \pm 2p)$, as the trace of Frobenius ($x \mapsto x^{p^2}$) of a supersingular elliptic curve over $\mathbb{F}_{p^2}$ must belong to the set $\{0, \pm p, \pm 2p\}$. Adj et al. determined the subgraphs $G_\ell(\mathbb{F}_{p^2}, 0)$ and $G_\ell(\mathbb{F}_{p^2}, \pm p)$ in [1, Theorems 3-5]. The subgraphs $G_\ell(\mathbb{F}_{p^2}, 2p)$ and $G_\ell(\mathbb{F}_{p^2}, -2p)$ are isomorphic, hence to study $G_\ell(\mathbb{F}_{p^2})$, it suffices to study $G_\ell(\mathbb{F}_{p^2}, -2p)$. One problem of interest is to determine the number of loops in $G_\ell(\mathbb{F}_{p^2}, -2p)$.

Let E_0 be the curve $y^2 = x^3 + 1$ if $p \equiv 2 \bmod 3$ and E_{1728} be the curve $y^2 = x^3 + x$ if $p \equiv 3 \bmod 4$. Then E_0 and E_{1728} are supersingular elliptic curves over $\mathbb{F}_{p^2}$ of Frobenius trace $-2p$ and j-invariants 0 and 1728 respectively. Adj et al. [1, Theorems 10 and 12] determined the number of loops of E_0 and E_{1728} in the subgraph $G_\ell(\mathbb{F}_{p^2}, -2p)$ if $p > 4\ell$. In this note, we improve the bound $p > 4\ell$ in [1, Theorem 12] to $p > 3\ell$ for E_0 and prove the following theorem:

Theorem. *Suppose p and ℓ are distinct prime numbers, $p \equiv 2 \bmod 3$ and $p > 3\ell$. If $\ell \equiv 1 \bmod 3$, E_0 has exactly two loops in $G_\ell(\mathbb{F}_{p^2}, -2p)$. If $\ell \equiv 2 \bmod 3$, E_0 has no loop in $G_\ell(\mathbb{F}_{p^2}, -2p)$. If $\ell = 3$, E_0 has one loop in $G_\ell(\mathbb{F}_{p^2}, -2p)$.*

Remark. (1) From Table 1 in [1], if $\ell = 5, 7$ and 17, the largest prime p satisfying $p \equiv 2 \bmod 3$ and $p < 3\ell$ is 11, 17 and 47, the number of loops at E_0 in $G_\ell(\mathbb{F}_{p^2}, -2p)$ is at least 1, 3 and 1 respectively, larger than the prediction in our theorem. In this sense, the bound $p > 3\ell$ is sharp (hence $p > 3\ell + 1$ since $p \equiv 2 \bmod 3$). On the other hand, there are many examples that $\ell \equiv 1 \bmod 3$ (resp. $\ell \equiv 2 \bmod 3$), p is the largest prime satisfying $p < 3\ell$ and $p \equiv 2 \bmod 3$, and E_0 has exactly two loops (resp. no loop) in $G_\ell(\mathbb{F}_{p^2}, -2p)$.

(2) The method in our proof can be applied to give a new proof of [1, Theorem 10]. One just needs to work on the order $\mathrm{End}(E_{1728})$ and solve the Diophantine equation $(2a + c)^2 + (2b + d)^2 + p(c^2 + d^2) = 4\ell$ if $p > 4\ell$.

Proof. First note that by [1, Theorem 6], $G_\ell(\mathbb{F}_{p^2}, -2p) \cong G_\ell(\overline{\mathbb{F}}_p)$, hence we can and will work on the graph $G_\ell(\overline{\mathbb{F}}_p)$ instead.

For $p \equiv 2 \bmod 3$, we can represent the definite quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and ∞ as $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ with $i^2 = -3$, $j^2 = -p$, $ij = -ji = k$. From [3],

$$\mathcal{O} = \mathrm{End}(E_0) = \mathbb{Z} + \mathbb{Z}\frac{-1 + i}{2} + \mathbb{Z}j + \mathbb{Z}\frac{3 + i + 3j + k}{6}$$

is a maximal order of $B_{p,\infty}$.

By Deuring's Correspondence Theorem (see [2,3,5]), the ℓ-isogeny classes from E_0 to itself defined over $\overline{\mathbb{F}}_p$ correspond to the left principal $\mathcal{O}$-ideals with reduced norm ℓ. To find the number of loops at E_0 in the graph $G_\ell(\overline{\mathbb{F}}_p)$, it suffices to find the number of left principal $\mathcal{O}$-ideals with reduced norm ℓ.

For the left principal $\mathcal{O}$-ideal $I = (a + b\frac{-1+i}{2} + cj + d\frac{3+i+3j+k}{6})$, its reduced norm

$$\mathrm{Nrd}(I) = \left(a - \frac{b}{2} + \frac{d}{2}\right)^2 + 3\left(\frac{b}{2} + \frac{d}{6}\right)^2 + p\left(c + \frac{d}{2}\right)^2 + p \cdot \frac{d^2}{12}.$$

We are reduced to solve the Diophantine equation

$$\frac{(2a - b + d)^2}{4} + \frac{(3b + d)^2}{12} + \frac{p(3c^2 + 3cd + d^2)}{3} = \ell.$$

We solve this equation when $p > 3\ell$.

If $(0, 0) \neq (c, d) \in \mathbb{Z}^2$, then $3c^2 + 3cd + d^2 \geq 1$ and $\frac{p(3c^2+3cd+d^2)}{3} > \ell$, not possible. This means $c = d = 0$. We are reduced to solve $a^2 - ab + b^2 = \ell$.

Since the class number of $\mathbb{Q}(\sqrt{-3})$ is one, its ring of integers $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a PID. Every ideal of $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is of the form $(-a + b\frac{1+\sqrt{-3}}{2})$, whose norm is $a^2 - ab + b^2$. We need to study the decomposition of the ideal (ℓ).

For $\ell \neq 2$ and $\ell \equiv 2 \bmod 3$, $\left(\frac{-3}{\ell}\right) = -1$ and ℓ is inert in $\mathbb{Q}(\sqrt{-3})$, so there is no $(a, b) \in \mathbb{Z}^2$ such that $a^2 - ab + ab = \ell$. This means there is no ℓ-isogeny from E_0 to itself defined over $\overline{\mathbb{F}}_p$, and hence E_0 has no loop in $G_\ell(\overline{\mathbb{F}}_p) \cong G_\ell(\mathbb{F}_{p^2}, -2p)$. For $\ell \equiv 1 \bmod 3$, $\left(\frac{-3}{\ell}\right) = 1$ and ℓ is split in $\mathbb{Q}(\sqrt{-3})$. Up to units, there are two pairs of $(a, b) \in \mathbb{Z}^2$ such that $a^2 - ab + ab = \ell$ and hence two left principal $\mathcal{O}$-ideals of reduced norm ℓ. This means there are two ℓ-isogeny classes from E_0 to itself defined over $\overline{\mathbb{F}}_p$, and E_0 has exactly two loops in $G_\ell(\mathbb{F}_{p^2}, -2p)$. For $\ell = 2$, there is no $(a, b) \in \mathbb{Z}^2$ such that $a^2 - ab + b^2 = 2$, hence E_0 has no loop in $G_2(\mathbb{F}_{p^2}, -2p)$. For $\ell = 3$, ℓ is ramified in $\mathbb{Q}(\sqrt{-3})$. Then $(a, b) = \pm(1, 2), \pm(2, 1)$ or $\pm(1, -1)$, all corresponding to the same left principal $\mathcal{O}$-ideal. This means E_0 has one loop in $G_3(\mathbb{F}_{p^2}, -2p)$. $\square$

Acknowledgments

Research is partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200) and NSFC (Grant No. 11571328).

References

[1] G. Adj, O. Ahmadi, A. Menezes, On isogeny graphs of supersingular elliptic curves over finite fields, Finite Fields Appl. 55 (2019) 268–283.
[2] K. Lauter, K. McMurdy, Explicit generators for endomorphism rings of supersingular elliptic curves, preprint available.
[3] K. McMurdy, Explicit representation of the endomorphism rings of supersingular elliptic curves, https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf, 2014.
[4] J. Tate, Endomorphisms of abelian varieties over finite fields 2 (1966) 134–144.
[5] J. Voight, Quaternion algebras. Version v0.9.7, September 3, 2017.