Commun. Math. Res.
doi: 10.4208/cmr.2020-0071

Vol. **36**, No. 4, pp. 460-488
November 2020

On Two Problems About Isogenies of Elliptic Curves Over Finite Fields

Lixia Luo[1,2,*], Guanju Xiao[1,2] and Yingpu Deng[1,2]

[1] *Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, P.R. China.*
[2] *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, P.R. China.*

Received 11 August 2020; Accepted 4 September 2020

Abstract. Isogenies occur throughout the theory of elliptic curves. Recently, the cryptographic protocols based on isogenies are considered as candidates of quantum-resistant cryptographic protocols. Given two elliptic curves E_1,E_2 defined over a finite field k with the same trace, there is a nonconstant isogeny β from E_2 to E_1 defined over k. This study gives out the index of $\mathrm{Hom}_k(E_1,E_2)\beta$ as a nonzero left ideal in $\mathrm{End}_k(E_2)$ and figures out the correspondence between isogenies and kernel ideals. In addition, some results about the non-trivial minimal degree of isogenies between two elliptic curves are also provided.

AMS subject classifications: 11G05, 11G15, 11G20

Key words: Elliptic curve, isogeny, kernel ideal, minimal degree.

---

1 Introduction

Isogenies play an important part in the theory of elliptic curves. A recent research area is cryptographic protocols based on the difficulty of constructing isogenies between any two elliptic curves over finite fields [2, 5, 9]. These cryptographic

*Corresponding author. *Email addresses:* luolixia@amss.ac.cn (L. Luo), gjXiao@amss.ac.cn (G. Xiao), dengyp@amss.ac.cn (Y. Deng)

protocols are supposed to resist the quantum computations. To get more facts about isogenies, this paper concerns two problems related to isogenies.

Let F be a perfect field, and E_1,E_2 be elliptic curves defined over F, it has been proved that $\mathrm{Hom}(E_1,E_2)$ is a free $\mathbb{Z}$-module of rank at most 4 [15, Corollary III.7.5]. Furthermore, the possible ranks of $\mathrm{End}(E_1)$ (or $\mathrm{End}(E_2)$) are 1,2,4. The possible result that $\mathrm{rank}_{\mathbb{Z}}\,\mathrm{Hom}(E_1,E_2)=3$ is proved to be negative. If there is a nonconstant isogeny β from E_2 to E_1, $\mathrm{Hom}(E_1,E_2)\beta$ is a nonzero left ideal of $\mathrm{End}(E_2)$, then $\mathrm{rank}_{\mathbb{Z}}\,\mathrm{Hom}(E_1,E_2)=\mathrm{rank}_{\mathbb{Z}}\,\mathrm{End}(E_2)$. The index of $\mathrm{Hom}(E_1,E_2)\beta$ in $\mathrm{End}(E_2)$ is finite, but the exact result needs to be identified. Assume that the characteristic of F is not 0. In addition, for the case $\mathrm{char(F)}=0$, we will discuss it in Appendix A.

In Waterhouse's thesis [21], he introduced the concept of kernel ideals and proved that the left ideals of $\mathrm{End}(E)$ are all kernel ideals for any elliptic curve E over a finite field. Every such left ideal can induce an isogeny from E and ideal multiplication corresponds to isogeny composition. Kohel figured out the correspondence between the invertible ideals and the isogenies of ordinary elliptic curves with the same endomorphism type [10]. In this paper, we explore the index of $\mathrm{Hom}_k(E_1,E_2)\beta$ as a left ideal in $\mathrm{End}_k(E_2)$ for any nonconstant isogeny β from E_2 to E_1 defined over a finite field k as the first problem. For ordinary elliptic curves, not all isogenies can correspond to kernel ideals. We will also give out a way to judge whether the isogenies correspond to kernel ideals in this case. In addition, we consider the non-trivial minimal degree of isogenies between any two elliptic curves over finite fields as the second problem.

The paper is organized as follows. In Section 2, we provide the preliminaries on elliptic curves, isogenies, endomorphism rings and kernel ideals. The answer to the first problem will be given out by Theorems 3.1 and 3.2 in Section 3. In addition, the study of the second problem can be found in Section 4.

2 Preliminaries

2.1 Elliptic curves and isogenies

Let k be a finite field of characteristic p and let E be an elliptic curve defined over k. E can be written in a generalized Weierstrass equation

$$E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6.$$

For simplicity, if $p>3$, up to k-isomorphism, E can be written in the short Weierstrass form

$$E:y^2=x^3+Ax+B$$