Journal of Number Theory 181 (2017) 89–98

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Elliptic curves with isomorphic groups of points over finite field extensions

Clemens Heuberger [*,1], Michela Mazzoli [2]

Alpen-Adria-Universität Klagenfurt, Austria

ARTICLE INFO

Article history:
Received 11 May 2016
Accepted 15 May 2017
Available online 4 August 2017
Communicated by F. Breuer

Keywords:
Elliptic curve
Rational points
Finite field
Field extension
Isomorphism
Isogeny
Valuation

ABSTRACT

Consider a pair of ordinary elliptic curves E and E' defined over the same finite field $\mathbb{F}_q$. Suppose they have the same number of $\mathbb{F}_q$-rational points, i.e. $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. In this paper we characterise for which finite field extensions $\mathbb{F}_{q^k}$, $k \geq 1$ (if any) the corresponding groups of $\mathbb{F}_{q^k}$-rational points are isomorphic, i.e. $E(\mathbb{F}_{q^k}) \cong E'(\mathbb{F}_{q^k})$.

1. Introduction

Consider a pair of ordinary elliptic curves E and E' defined over the same finite field $\mathbb{F}_q$, where q is a prime power. Suppose E and E' have the same number of $\mathbb{F}_q$-rational points, i.e. $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. Equivalently, E and E' have the same characteristic polynomial, the same zeta function, hence the same number of $\mathbb{F}_{q^k}$-rational points for

* Corresponding author.
E-mail addresses: clemens.heuberger@aau.at (C. Heuberger), michela.mazzoli@aau.at (M. Mazzoli).

[1] Supported by the Austrian Science Fund (FWF): P 24644-N26.
[2] Supported by the Karl Popper Kolleg "Modeling Simulation Optimization" funded by the Alpen-Adria-Universität Klagenfurt and by the Carinthian Economic Promotion Fund (KWF).

http://dx.doi.org/10.1016/j.jnt.2017.05.028

every finite extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$, $k \geq 1$. This is equivalent to E and E' being $\mathbb{F}_q$-isogenous – cf. [3, Theorem 1]. In this paper we characterise for which field extensions $\mathbb{F}_{q^k}$, if any, the corresponding groups of $\mathbb{F}_{q^k}$-rational points are isomorphic, i.e. $E(\mathbb{F}_{q^k}) \cong E'(\mathbb{F}_{q^k})$.

The question was inspired by an article by C. Wittmann [5]; we have summarised his result for the ordinary case in Proposition 2.1. Wittmann's paper answers the question for $k = 1$. Our main results are illustrated in Theorem 2.4 and Theorem 2.7. The first theorem reduces the isomorphism problem to a divisibility question for individual k's. In the second theorem, the latter question is reduced to a simple verification of the multiplicative order of some elements, based only on information for $k = 1$. Combining Theorem 2.4 and Theorem 2.7, we are able to tell for which $k \geq 1$ we have $E(\mathbb{F}_{q^k}) \cong E'(\mathbb{F}_{q^k})$, given only the order of $E(\mathbb{F}_q)$ and the endomorphism rings of E and E'.

2. Isomorphic groups of $\mathbb{F}_{q^k}$-rational points

Let E be an *ordinary* elliptic curve defined over the finite field $\mathbb{F}_q$, where q is a prime power. Let τ be the Frobenius endomorphism of E relative to $\mathbb{F}_q$, namely $\tau(x, y) = (x^q, y^q)$. In the ordinary case, the endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_q}(E)$ of E is equal to $\mathbb{Q}(\tau)$ – cf. [3, Theorem 2].

Since $\mathbb{Q}(\tau)$ is an imaginary quadratic field, it can be written as $\mathbb{Q}(\sqrt{m})$ for some square-free integer $m < 0$. The ring of integers of $\mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\delta]$ where $\delta = \sqrt{m}$ if $m \equiv 2, 3 \pmod 4$, or $\delta = \frac{1+\sqrt{m}}{2}$ if $m \equiv 1 \pmod 4$.

Then we can write $\tau = a + b\delta$ for some $a, b \in \mathbb{Z}$. It is well-known that the endomorphism ring of E is an order in $\mathbb{Q}(\tau)$, that is $\mathrm{End}(E) \cong \mathcal{O}_g = \mathbb{Z} + g\mathbb{Z}[\delta] = \mathbb{Z} \oplus g\mathbb{Z}\delta$, where g is the *conductor* of the order $\mathcal{O}_g$. Since $\mathbb{Z}[\tau] = \mathcal{O}_b \subseteq \mathrm{End}(E)$, we have $g \mid b$.

Proposition 2.1 *([5, Lemma 3.1]). Let $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ be ordinary elliptic curves s.t. $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. Let $\mathrm{End}(E) = \mathcal{O}_g$ and $\mathrm{End}(E') = \mathcal{O}_{g'}$ be the orders in $\mathbb{Q}(\tau)$ of conductor g and g' respectively, let $\tau = a + b\delta$ as above. Then*

$$E(\mathbb{F}_q) \cong E'(\mathbb{F}_q) \quad \Leftrightarrow \quad \gcd(a-1, b/g) = \gcd(a-1, b/g').$$

We note that, since $|E(\mathbb{F}_q)| = q + 1 - \mathrm{Tr}(\tau)$, knowing the order of $E(\mathbb{F}_q)$ is equivalent to knowing the Frobenius endomorphism of E.

As $E/\mathbb{F}_q$ can always be seen as defined over any field extension $\mathbb{F}_{q^k}$, and the Frobenius endomorphism of E with respect to $\mathbb{F}_{q^k}$ is τ^k, we obtain the following

Corollary 2.2. *Let E and E' be as in Proposition 2.1. Fix an integer $k \geq 1$ and write $\tau^k = a_k + b_k\delta$ for suitable a_k, $b_k \in \mathbb{Z}$. Then*

$$E(\mathbb{F}_{q^k}) \cong E'(\mathbb{F}_{q^k}) \quad \Leftrightarrow \quad \gcd(a_k-1, b_k/g) = \gcd(a_k-1, b_k/g').$$