Journal of Number Theory 191 (2018) 194–212

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Elliptic curves in isogeny classes

Igor E. Shparlinski *, Liangyi Zhao

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history:
Received 27 March 2018
Received in revised form 9 April 2018
Accepted 10 April 2018
Available online 29 May 2018
Communicated by S.J. Miller

MSC:
11G07
11L40
11N35

Keywords:
Elliptic curves
Isogeny classes
Class number

ABSTRACT

We show that the distribution of elliptic curves in isogeny classes of curves with a given value of the Frobenius trace t becomes close to uniform even when t is averaged over very short intervals inside the Hasse–Weil interval. This result is based on a new form of the large sieve inequality for sparse sequences.

1. Introduction

1.1. Motivation

Various properties of quadratic fields $\mathbb{Q}\left(\sqrt{f(t)}\right)$, for a polynomial f with integer coefficients, have been studied in a number of papers, mostly with the emphasis on

* Corresponding author.
E-mail addresses: igor.shparlinski@unsw.edu.au (I.E. Shparlinski), l.zhao@unsw.edu.au (L. Zhao).

https://doi.org/10.1016/j.jnt.2018.04.017
0022-314X/

their discriminants, see [4,9] and references therein. Here we address an apparently new question of obtaining nontrivial estimates for the average values of the class numbers of such fields. Moreover, we are interested in the estimates which hold in a very broad range of uniformity with respect to the size of coefficients of f. We note that in the case of linear polynomials, an asymptotic formula for the average value of the class number $h(-D)$ of $\mathbb{Q}\left(\sqrt{-D}\right)$ over $1 \le D \le T$ is due to the classical result of Jutila [7]. Furthermore, Nagoshi [11] gives an asymptotic formula in the case when t ranges over primes $t \le D$. However no results seem to be known for more rapidly growing sequences, such as values of polynomials.

Here we have chosen to demonstrate how one can approach this problem in the special example of the polynomial $t^2 - 4p$ (with a prime p), which has direct applications to the classical question about the distribution of elliptic curves in isogeny classes over the finite field $\mathbb{F}_p$ of p elements, we refer to [12, Section III.4] for a precise definition.

Indeed, it is well-known that the size of isogeny classes of elliptic curves over finite fields is directly related to the class numbers. Namely, for a prime p, the size $I(t)$ of the isogeny class of curves with the trace Frobenius equal to t (see Section 1.2 for precise definitions) is given by

$$I(t) = H(t^2 - 4p),$$

where the *Kronecker class number* $H(D)$ is defined via the ordinary class number $h(D)$ of $\mathbb{Q}(\sqrt{D})$ as

$$H(D) = \sum_{\substack{d:d^2 \mid D \\ D/d^2 \equiv 0,1 \pmod 4}} h(D/d^2),$$

see [8, Section (1.5)]. In turn, it is also related to certain L-functions, see Section 3.1.

We note that in principle, our method can be extended to higher degree polynomials, however exactly as in the case of discriminants (see [4,9]) one expects quantitatively weaker results in this case.

The second part of our motivation comes from the intention to investigate the limits of the large sieve techniques when it is applied to sparse sequences of moduli. In our case it is of the shape $4p - t^2$ with t ranging over a short interval, or length less than any positive power of p. In particular, it is important for us to obtain uniform results with respect to the parameter ν in an application of Hölder's inequality in the proof of Lemma 2.4, which underlies our results. We believe that these ideas can be of use in other applications of the large sieve techniques in number theory and harmonic analysis.

1.2. Set-up

Let $p > 3$ be prime and let E be an elliptic curve over the field $\mathbb{F}_p$ of p elements given by an affine *Weierstrass equation* of the form