Journal of Number Theory 136 (2014) 165–194

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Explicit points on the Legendre curve ☆

Douglas Ulmer

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, United States

ARTICLE INFO

Article history:
Received 6 May 2013
Received in revised form 19 September 2013
Accepted 20 September 2013
Available online 20 November 2013
Communicated by David Goss

MSC:
11G05
11G40

Keywords:
Elliptic curves
Ranks
Conjecture of Birch and Swinnerton-Dyer

ABSTRACT

We study the elliptic curve E given by $y^2 = x(x+1)(x+t)$ over the rational function field $k(t)$ and its extensions $K_d = k(\mu_d, t^{1/d})$. When k is finite of characteristic p and $d = p^f + 1$, we write down explicit points on E and show by elementary arguments that they generate a subgroup V_d of rank $d-2$ and of finite index in $E(K_d)$. Using more sophisticated methods, we then show that the Birch and Swinnerton-Dyer conjecture holds for E over K_d, and we relate the index of V_d in $E(K_d)$ to the order of the Tate–Shafarevich group $Ш(E/K_d)$. When k has characteristic 0, we show that E has rank 0 over K_d for all d.

1. Introduction

Throughout the paper, $p > 2$ is a prime number, $\mathbb{F}_p$ is the field of p elements, $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_p$ of cardinality q, and $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. We write $\mathbb{F}_p(t)$, $\mathbb{F}_q(t)$, and $\overline{\mathbb{F}}_p(t)$ for the rational function fields over $\mathbb{F}_p$, $\mathbb{F}_q$, and $\overline{\mathbb{F}}_p$ respectively.

There are now several constructions of elliptic curves (and higher-dimensional Jacobians) of large rank over $\mathbb{F}_p(t)$ or $\overline{\mathbb{F}}_p(t)$. The first results in this direction are due to Shafarevich and Tate [TS67], and their arguments as well as more recent results

☆ This paper is based upon work partially supported by the National Science Foundation under Grant No. DMS 0701053.

E-mail address: ulmer@math.gatech.edu.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.09.010

on large ranks are discussed in [Ulm11]. Most of these constructions rely on relatively sophisticated mathematics, such as the theory of algebraic surfaces, cohomology, and L-functions.

Our first aim in this note is to give an explicit, elementary construction of points on a certain non-isotrivial elliptic curve over $\mathbb{F}_p(t)$, the Legendre curve. We then show that the rank of the group these points generate can be arbitrarily large. The arguments are elementary and could have been given fifty years ago.[1] It is remarkable that such a classical and well-studied object as the Legendre curve still has a few surprises.

Further pleasant surprises appear when we look deeper into the arithmetic of the Legendre curve. Specifically, we find that the index of the points we have constructed in the full Mordell–Weil group is a power of p, and the square of this index is the order of a Tate–Shafarevich group. This "class number formula" is reminiscent of formulas appearing in the contexts of cyclotomic units and of Heegner points. See Theorem 12.1 for a precise statement of our main results.

Here is an outline of the paper: In Sections 2 and 3, we write down the relevant curve and a collection of points on it, and in Section 4 we prove that the rank of the group they generate is large. The arguments require only elementary aspects of the theory of elliptic curves and Galois theory. Using slightly more advanced ideas, (namely Galois cohomology), in Section 5 we then calculate the exact rank of the Mordell–Weil group and see that our points generate a subgroup of finite index. The tools used up to this point will be familiar to anyone who has studied Silverman's book [Sil09]. In Section 6 we compute the torsion subgroup, and in Sections 7 through 10, we use more sophisticated techniques (heights, L-functions, and the Birch and Swinnerton-Dyer formula) to bound the index and relate it to the Tate–Shafarevich group of E. Finally, in Section 11 we make a connection with our paper [Ulm13] and Berger's construction, which yields strong results on the Birch and Swinnerton-Dyer conjecture for E.

There are several avenues for further exploration of the arithmetic of the Legendre curve, including a more general rank formula, more explicit points, and a full calculation of the Tate–Shafarevich group. These are stated more precisely at the end of Section 12 and will be taken up in subsequent publications.

This note came about as a result of conversations with Dick Gross at the 2009 IAS/Park City Mathematics Institute. It is a pleasure to thank the organizers of the meeting for the opportunity to give a course, the audience for their attention and comments, and Gross for his interest and incisive questions. Thanks are also due to Chris Hall for thought-provoking data on L-functions and stimulating conversations on questions related to the topics of this paper, and to Lisa Berger and Alice Silverberg for several useful comments.

The exposition of the final version of the paper was influenced by the possibility of generalizations to higher genus. These were worked out with an energetic group of

[1] We note that in [Ca09], Conceição gives an equally simple construction of polynomial points on certain *isotrivial* elliptic curves over $\mathbb{F}_p(t)$ and uses them to show that the rank is large.