ARTICLE IN PRESS YJNTH:5942

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Continued fractions for rational torsion

Katthaleeya Daowsud [a], Thomas A. Schmidt [b,*]

[a] Department of Mathematics, Faculty of Science, Kasetsart University, 50 Ngam Wong Wan Rd, Ladyaow, Chatuchak, Bangkok, 10900, Thailand
[b] Oregon State University, Corvallis, OR 97331, United States

ARTICLE INFO

Article history:
Received 28 August 2017
Accepted 13 November 2017
Available online xxxx
Communicated by A. Pal

MSC:
11Y65
11G30
14H40
14Q05

Keywords:
Continued fractions
Genus 2 curves
Torsion
Jacobians
Rational point of order 11

ABSTRACT

We exhibit a method to use continued fractions in function fields to find new families of hyperelliptic curves over the rationals with given torsion order in their Jacobians. To show the utility of the method, we exhibit a new infinite family of curves over $\mathbb{Q}$ with genus two whose Jacobians have torsion order eleven.

1. Introduction

As Cassels and Flynn express in the introduction to their text [6], there is still a need for interesting examples of curves of low genus over number fields. Here, we show that the decidely “low brow” method of continued fractions over function fields continues to have much to offer.

* Corresponding author.
E-mail addresses: fsciky@ku.ac.th (K. Daowsud), toms@math.orst.edu (T.A. Schmidt).

https://doi.org/10.1016/j.jnt.2017.11.014

We show that with a fixed base field, (low) genus and desired (small) torsion order, one can search fairly easily for hyperelliptic curves of the given genus over the field whose divisor at infinity is of the given order. As we recall with more details below, the divisor at infinity has finite order in the Jacobian of the hyperelliptic curve if and only if a corresponding continued fraction expansion, in polynomials, is periodic; the order itself is the sum of the degrees of initial partial quotients. Given genus g and torsion order N, there are then finitely many possible partitions for the degrees of these initial partial quotients; by making appropriate choices relating the coefficients of these partial quotients, it is often possible to determine a curve with the desired genus and order.

It has been known since 1940 [5] that 11 is the smallest prime for which there is no elliptic curve defined over the rationals with rational point of order the prime. Thus, our continued fraction approach must certainly fail with $k = \mathbb{Q}$, and $N = 11$, $g = 1$. It is natural to ask about $N = 11$ and higher genus. Indeed, using a different method, Flynn [8], [9] gave a one-dimensional family $\mathcal{F}_t$, see (5), of hyperelliptic curves with $g = 2$ and $N = 11$. Much more recently, Bernard et al. [3] found some 18 additional individual curves with $(g, N) = (2, 11)$. (They state that they have found 19, but their table of results lists one curve twice.) They explicitly state that they sought infinite families of such curves.

We exhibit a new infinite family of this type. Let

$$g_u(x) := x^6 - 4x^5 + 8(1+u)x^4 - (10+32u)x^3 + 8(1+6u+2u^2)x^2 - 4(1+6u+16u^2)x + 64u^2 + 1. \quad (1)$$

Theorem 1. *For each $u \in \mathbb{Q} \setminus \{0\}$, let $\mathcal{G}_u$ be the smooth projective curve of affine equation $y^2 = g_u(x)$. Then the divisor at infinity of the Jacobian of $\mathcal{G}_u$ has order 11. There are infinitely many non-isomorphic $\mathcal{G}_u$, none of which is isomorphic to any of Flynn's curves $\mathcal{F}_t$.*

The proof that the torsion orders are 11 is given in Lemma 2. In Subsection 3.3 we sketch the computation that this is a new infinite family. Our naive method which led us to this new family of curves (and other similar curves) is discussed in Sections 4 through 6.

That finite torsion order is related to periodicity of continued fraction expansions is a notion that can be traced back to Abel and Chebychev. We first learned of this history, and the relationship itself, from work of Adams and Razar [1]. Other authors who have discussed these notions include Berry [4] and van der Poorten with various coauthors, see e.g. [17], [14]. See also the recent work of Platonov [15].

The study of the arithmetic of function fields over finite fields goes back at least to E. Artin's Ph.D. dissertation, [2]. Much more recently, Friesen in particular has studied the structure of class groups using continued fractions, see say [10]. Our method can be viewed as a variant of that used by Friesen; whereas he solves for the initial partial quotient in terms of the remaining terms of a given (quasi)-period, for small genus we