Journal of Symbolic Computation 76 (2016) 200–218

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Periodic continued fractions and elliptic curves over quadratic fields

Mohammad Sadek

Department of Mathematics and Actuarial Science, American University in Cairo, Egypt

ARTICLE INFO

Article history:
Received 1 April 2015
Accepted 22 December 2015
Available online 19 January 2016

MSC:
11A55
11J70

Keywords:
Elliptic curves
Continued fractions
Quadratic fields

ABSTRACT

Let $f(x)$ be a square free quartic polynomial defined over a quadratic field K such that its leading coefficient is a square. If the continued fraction expansion of $\sqrt{f(x)}$ is periodic, then its period n lies in the set

$$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,17,18,22,$$
$$26,30,34\}.$$

We write explicitly all such polynomials for which the period n occurs over K but not over $\mathbb{Q}$ and $n \notin \{13,15,17\}$. Moreover we give necessary and sufficient conditions for the existence of such continued fraction expansions with period 13, 15 or 17 over K.

1. Introduction

Let E be an elliptic curve defined over a field K whose characteristic is different from 2, 3. One can describe E using an affine equation of the form $y^2 = f(x) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ where $f(x)$ is a square free polynomial whose leading coefficient is a square in K. The affine curve described by the latter equation has a double point at infinity. One considers the projective desingularization which is obtained by gluing the affine curves $y^2 = f(x)$ and $w^2 = z^4 f(1/z) = a_4z^4 + a_3z^3 + a_2z^2 + a_1z + a_0$ via $x = 1/z$ and $y = w/z^2$. The singularity at infinity on the affine curve $y^2 = f(x)$ now corresponds to the points ∞^+ and ∞^- given by $(z, w) = (1, \sqrt{a_0})$ and $(1, -\sqrt{a_0})$, respectively, on the affine curve $w^2 = z^4 f(1/z)$. One remarks that since a_0 is a square in K, the points ∞^+ and ∞^- are K-rational points on E.

E-mail address: mmsadek@aucegypt.edu.

http://dx.doi.org/10.1016/j.jsc.2016.01.003

In Adams and Razar (1980), the authors were able to prove that the continued fraction expansion of $\sqrt{f(x)}$ is periodic if and only if the point $\infty^+ - \infty^-$ is of finite order in $E(K)$. Furthermore it was shown that the period of the continued fraction expansion can be determined once the order of the point $\infty^+ - \infty^-$ is known. More precisely, if the order of $\infty^+ - \infty^-$ is n then the period of the continued fraction is either $n-1$ or $2(n-1)$ where the second case occurs only if n is even.

The above argument leads one to study elliptic curves with torsion points in order to investigate quartic polynomials $f(x)$ where the continued fraction expansion of $\sqrt{f(x)}$ is periodic. An elliptic curve E with a K-rational torsion point of order n can be written in Tate's normal form; namely, there exist $b, c \in K$ such that E is isomorphic to the following elliptic curve

$$E_{b,c} : y^2 + (1-c)xy - by = x^3 - bx^2.$$

The interested reader may consult (Kubert, 1976) to see how elliptic curves with a nontrivial K-torsion point may be parametrized. In fact the parameters b and c are obtained by considering a transformation that takes the torsion point of order n to $(0,0)$ and moves its tangent to $y=0$. Consequently if $f(x)$ has a square leading coefficient such that the continued fraction expansion of $\sqrt{f(x)}$ is periodic then there exist $b, c \in K$ such that the curve $C : y^2 = f(x)$ is isomorphic to $E_{b,c}$.

In Van der Poorten (2004), the author wrote explicitly all square free quartic polynomials $f(x)$ over $\mathbb{Q}$ with a square leading coefficient such that $\sqrt{f(x)}$ is periodic. Following Mazur's classification of torsion points of elliptic curves over $\mathbb{Q}$ the possible periods are

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 18, 22\}.$$

In fact it was shown that all of these periods occur over $\mathbb{Q}$ except for 9 and 11 as there is no polynomial over $\mathbb{Q}$ such that the continued fraction expansion of $\sqrt{f(x)}$ is of period 9 or 11.

In this article we write down all square free quartic polynomials $f(x)$ with a square leading coefficient such that the continued fraction expansion of $\sqrt{f(x)}$ is periodic over some quadratic field K. According to the classification of torsion points of elliptic curves over quadratic fields the possible periods are the ones over $\mathbb{Q}$ together with

$$\{9, 11, 12, 13, 15, 17, 26, 30, 34\}.$$

We prove that the periods $9, 11$ occur over some quadratic fields. Moreover we display all quartic polynomials that give rise to the periods $12, 26, 30, 34$. In addition we present the quadratic fields with the smallest absolute value of their discriminants over which these periods occur. Finally we give necessary and sufficient conditions for the odd periods $13, 15, 17$ to occur over a quadratic field K. More precisely we introduce a polynomial $\alpha_n(T,S) \in \mathbb{Z}[T,S]$, $n = 13, 15, 17$, such that the period n occurs if and only if there exists a $z \in K$ such that $z^2 = \alpha_n(t,s)$ for some K-rational point (t,s) lying on the modular curve $X_1(n+1)$.

One remarks that the modular curve $X_1(14)$ is an elliptic curve whereas the curves $X_1(16)$ and $X_1(18)$ are of genus 2. The reason why it is computationally difficult to test whether the period n, $n = 13, 15, 17$, is realized over a certain quadratic field K is that one has to produce the set of K-rational points of $X_1(n+1)$, then check whether the polynomial $\alpha_n(T,S)$ is a K-square when evaluated at one of these K-rational points. The set $X_1(14)(K)$ is a finitely generated abelian group while $X_1(16)(K)$ and $X_1(18)(K)$ are finite sets. Yet there is no known algorithm guaranteed to produce K-rational points on algebraic curves of genus $g \ge 1$ over any quadratic field K.

The organization of this paper is as follows. In section 2 we present the basic background needed to describe periodic continued fraction expansions of square roots of quartic polynomials whose leading coefficient is a square. In section 3 we discuss some of the known results on torsion points of an elliptic curve defined either over the rational field $\mathbb{Q}$ or a quadratic field extension of $\mathbb{Q}$. In section 4 we parametrize quartic polynomials with square leading coefficients whose square root has a periodic continued fraction expansion. In section 5 we write explicitly quartic polynomials with square leading coefficients such that the square root has a periodic continued fraction expansion over a quadratic extension of $\mathbb{Q}$.