CONTINUED FRACTIONS FOR RATIONAL TORSION

KATTHALEEYA DAOWSUD AND THOMAS A. SCHMIDT

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.

Contents

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.

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

Date: 27 July 2017.
2010 *Mathematics Subject Classification.* 11Y65, 11G30, 14H40, 14Q05.
Key words and phrases. continued fractions, genus 2 curves, torsion, Jacobians, rational point of order 11.

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

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

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 the paper 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.* [15], [14]. See also the recent work of Platonov [16].

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 find it more practical to solve for a quasi-period (or period) satisfying small sets of constraints.

2. Continued fractions and torsion at infinity

2.1. **Divisor at infinity.** If k is a field of characteristic zero (or sufficiently large), then each hyperelliptic curve $\mathcal{C}$ of even genus g over k is k-isomorphic to a curve of affine equation

$$\mathcal{C} : y^2 = u_0 x^{2g+2} + u_1 x^{2g+1} + \cdots + u_{2g+1} x + u_{2g+2} \tag{2}$$

with coefficients $u_i \in k$, and u_0 a square in k, see [13]. The affine curve $\mathcal{C}$ can be completed to a projective curve, for which one can take a smooth model (which we also denote by $\mathcal{C}$).

The *divisor group* of $\mathcal{C}$, $\mathrm{Div}(\mathcal{C})$, is the free abelian group generated by the $\bar{k}$-points of $\mathcal{C}$. The divisors of degree zero, $\mathrm{Div}^0(\mathcal{C})$ is the kernel of the homomorphism from the group $\mathrm{Div}(\mathcal{C})$ to the integers defined by sending a weighted sum of points to the sum of these weights. A *rational function* on $\mathcal{C}$ is a function to $\mathbb{P}^1(\bar{k})$ that can be locally expressed as the quotient of polynomials, the *divisor of a rational function* ϕ is the element of $\mathrm{Div}(\mathcal{C})$ given by the difference of the zeros and poles of ϕ, with multiplicity. It is a classical result that the divisors of the rational functions on $\mathcal{C}$ form a subgroup of $\mathrm{Div}^0(\mathcal{C})$, called the subgroup of *principal divisors*. The basic algebraic definition of the *Jacobian* of $\mathcal{C}$ is as the quotient group

$$\mathrm{Jac}(\mathcal{C}) = \mathrm{Div}(\mathcal{C})/\mathrm{Div}^0(\mathcal{C})\,.$$

The completion of the affine model of $\mathcal{C}$ leads to two points at infinity, say P, Q. Their formal difference then defines the *divisor at infinity*, $D_\infty = P - Q$, which we take to be the corresponding element of $\mathrm{Jac}(\mathcal{C})$. The hyperelliptic involution, defined by $(x, y) \mapsto (y, -x)$ interchanges P and Q, and thus D_∞ defines a point of $\mathrm{Jac}(\mathcal{C})$ defined over k. We say that D_∞ is *torsion of order* N if its class in $\mathrm{Jac}(\mathcal{C})$ has order N.

The goal of this work is to exhibit an elementary method to discover examples of hyperelliptic $\mathcal{C}$ of given genus g whose divisor at infinity is torsion of given order N.

2.2. **Continued fractions in function fields.** Given any field k, the order of vanishing of a polynomial $f \in k[x]$ at the origin $x = 0$ extends to define a valuation on the quotient field, the field of rational functions $k(x)$. The valuation is simply given by writing any non-zero rational function as an integral power of x times a rational function with neither zero nor pole at $x = 0$; the exponent of x is then the valuation of the initial rational function. One defines a metric on $k(x)$ in the usual manner; the completion of this field with respect to the metric of the ring of formal Laurent series, $k((x))$.

The point at infinity on the projective line over the field k can be viewed as corresponding to the vanishing of x^{-1}. A second valuation on $k(x)$, leads to a completion that is $k((x^{-1}))$. For $\alpha \in k((x^{-1}))$, say

$$\alpha = c_{-n}x^n + c_{-n+1}x^{n-1} + \cdots + c_{-1}x + c_0 + c_1x^{-1} + c_2x^{-2} + \cdots\,,$$

we define the *polynomial part* of α as

$$\lfloor\, \alpha \,\rfloor = c_{-n}x^n + c_{-n+1}x^{n-1} + \cdots + c_{-1}x + c_0\,.$$

We then define a continued fraction algorithm by way of the following sequences. Let $\alpha_0 = \alpha$; for $i \ge 0$ let $a_i = \lfloor\, \alpha_i \,\rfloor$ and while $\alpha_i - a_i \ne 0$, let $\alpha_{i+1} = (\alpha_i - a_i)^{-1}$. We then find an expansion of the form

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} =: [a_0; a_1, a_2, \ldots,]\,,$$

where we use the flat notation for typographic ease. The a_i are called the *partial quotients* of the expansion.

The local ring of regular functions at a non-singular point of a projective curve is a discrete valuation ring. In particular, its maximal ideal, defined by vanishing at the point, is principal. Any generator of this maximal ideal is called a local uniformizer. For the point at infinity of $\mathbb{P}^1$ we can take x^{-1} as a local uniformizer, thus leading to the valuation on $k(x)$ and the continued fractions as above.

Our insistence on affine equations of the form of Equation (2) is so that the degree two map from $\mathcal{C}$ to $\mathbb{P}^1$ defined by $(x, y) \mapsto x$ is such that the point at infinity of $\mathbb{P}^1$ has two pre-images. The local rings at these points are then isomorphic to the local ring uniformized by x^{-1}. From this, it follows that there is a square root of $y^2 = f(x)$ in $k((x^{-1}))$. Indeed, the completion of the "rational field" $k(x)$ with respect to the metric from our valuation is analogous to the completion of $\mathbb{Q}$ with respect to the usual metric. Our $y = \sqrt{f(x)}$ is of the type that Artin [2] called "real quadratic" — exactly because it is a value in the completed field.

Recall that the regular continued fraction expansion of $\sqrt{d}$ for non-square integers $d > 0$ is periodic and with a palindromic period. In general, it is not true that $y = \sqrt{f(x)}$ has a periodic expansion, but when it does the expansion shows similar symmetry. In fact, a new phenomenon arises: There may be further symmetry inside the period.

Definition 1. We call an even length sequence of $(a_1, \dots, a_{2\ell})$ *skew symmetric* of *skew value* γ if

$$a_{2(\ell-i)} = c_i \, a_{2i+1} \quad \forall \, 0 \le i < \ell \, ,$$

where

$$c_i = \begin{cases} \gamma & \text{if } \; 2|i\, ; \\ \gamma^{-1} & \text{otherwise} \, , \end{cases}$$

with nonzero $\gamma \in k$.

Proofs of the following are given in [10] when k is a finite field, and in [15] in general; see also [1], [17] and [14]. We use an overline to denote a repetition of a sequence of partial quotients.

Theorem 2. *Suppose that a non-square $f(x) \in k[x]$ is of even degree, with leading coefficient a square in k. If the continued fraction expansion of the Laurent series of $\sqrt{f(x)}$ is periodic, then it is of the form*

$$\sqrt{f(x)} = [\, a_0; \overline{a_1, \dots, a_{m-1}, 2\kappa a_0, a_{m-1}, \dots, a_1, 2a_0}\,] \, , \tag{3}$$

where $(a_1, \dots, a_{m-1})$ is skew symmetric of skew value κ.

Definition 2. In the setting of Theorem 2, we call (the minimal) m the *quasi-period* length.

Exactly when $\kappa = 1$, we have equality of the (minimal) period length with the quasi-period length. Furthermore, if these lengths are unequal, then the quasi-period length m must be odd; we then speak of a *strict* quasi-period length.

In what follows, we use m to denote the quasi-period length of an expansion, including the case where this is the period length.

Direct calculation gives the partial quotients for the members of the family $\mathcal{G}_u$.

Lemma 1. *For $y^2 = g_u(x)$ and $u \in \mathbb{Q} \setminus \{0\}$, the continued fraction expansion of y is quasi-periodic of quasi-period length $m = 7$ with skew-value $\kappa = u$. The initial partial quotients of this expansion are*

$$\begin{aligned} a_0(x) &= x^3 - 2x^2 + (4u+2)x - (8u+1) \\ a_1(x) &= [x^2 - x + (1+u)]/(8u) \\ a_2(x) &= -2x + 2 \\ a_3(x) &= -x/2 \end{aligned}$$

and thus we have

$$a_4(x) = -x/(2u), \; a_5(x) = (-2x+2)u, \; a_6(x) = [x^2 - x + (1+u)]/(8u^2),$$
$$a_7(x) = (2u)[x^3 - 2x^2 + (4u+2)x - (8u+1)]$$

and the rest of the period is determined by the palindromic property. (When $u = 1$, the period length is 7).

2.3. **Periodic continued fractions identify torsion divisors.** The following is given by Adams and Razar [1] in the genus $g = 1$ case. The general case is proven in [15], see also [14]. W. Schmidt [17] presents a large portion of this result in his Lemma 7.

Theorem 3. *Suppose that $\mathcal{C}$ is given by $y^2 = f(x)$, with $f(x)$ as in the right hand side of (2). If $\sqrt{f(x)}$ has periodic continued fraction expansion as in (3), then the divisor at infinity D_∞ is torsion of order*

$$N = g + 1 + \sum_{i=1}^{m-1} (\deg a_i)\,. \tag{4}$$

Furthermore, $1 \le \deg a_i \le g$ for each $1 \le i \le m-1$.

For ease of reference, we express the obvious corollary.

Corollary 1. *The torsion order N of the divisor at infinity satisfies*

$$g + m \le N \le mg + 1\,.$$

In light of Lemma 2, the following is a direct application of Theorem 3.

Lemma 2. *Let $\mathcal{G}_u$ be as in Theorem 1. Then the divisor at infinity of the Jacobian of $\mathcal{G}_u$ is torsion of order 11.*

3. Genus two

We show the usefulness of our continued fraction based approach mainly in the genus two setting. We use the Igusa invariants for distinguishing isomorphism classes in genus two.

3.1. **Igusa invariants.** The affine representation of $\mathcal{C}$ given in (2) is unique up to a fractional linear transformation of x, $x \mapsto (ax+b)/(cx+d)$ and the associated $y \mapsto ey/(cx+d)^{g+1}$, where $a, b, c, d \in k$, $ad - bc \neq 0$, $e \in k^*$. The invariants of Igusa [11], nearly those defined by Clebsch in 1872 (see [13]), uniquely identify isomorphism classes of curves of genus $g = 2$ by taking distinct values on the orbits of these fractional linear transformations.

Fix $f(x) = u_0x^6 + u_1x^5 + \cdots + u_5x + u_6$, of roots $\alpha_i \in \bar{k}$, and write (ij) for by $\alpha_i - \alpha_j$. Then, as in say [12], we write Igusa's invariants as

$$j_1(\mathcal{C}) = A^5/D, \quad j_2(\mathcal{C}) = A^3B/D, \quad j_3(\mathcal{C}) = A^4C/D\,,$$

where in Igusa's shorthand notation,

$$\begin{aligned}
A &= u_0^2 \sum_{15} (12)^2(34)^2(56)^2 \\
B &= u_0^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(46)^2 \\
C &= u_0^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(46)^2(14)^2(25)^2(36)^2 \\
D &= u_0^{10} \prod_{i<j} (ij)^2\,.
\end{aligned}$$

Thus, D is the discriminant of $f(x)$, hence for $\mathcal{C}$ to be non-singular, we must have $D \neq 0$; the summands given in the definition of the functions A, B, C have subscripts indicating the number of distinct summands to be taken. Since each of A, B, C, D is symmetric in the roots of f, each can be given in terms of the elementary symmetric polynomials of these six roots, and therefore in terms of the coefficients of $f(x)$. Thus, the invariants themselves are rational functions of these coefficients. Their expressions are sufficiently complicated that we follow tradition and do not give them here.

3.2. **Known examples of torsion order eleven.** Recall that Flynn [8, 9] gave a family of genus two curves defined over $\mathbb{Q}$ whose Jacobians each has a torsion point defined over $\mathbb{Q}$ of order 11. The family is given in terms of $t \in \mathbb{Q}$ by $\mathscr{F}_t : y^2 = f_t(x)$, where

$$f_t(x) = x^6 + 2x^5 + (2t+3)x^4 + 2x^3 + (t^2+1)x^2 + 2t(1-t)x + t^2\,, \tag{5}$$

for rational t. With obvious notation, one finds that

$$\begin{aligned}
A_t &= -8(3 - 16t + 56t^2 + 4t^3)\\
B_t &= 4(9 - 120t + 1045t^2 - 1120t^3 + 539t^4 + 448t^5 + 16t^6)\\
C_t &= -8(27 - 492t + 4328t^2 - 21984t^3 + 71544t^4 - 115456t^5 + 60168t^6 + 29984t^7 + 2688t^8 + 64t^9)\\
D_t &= -4096t^7(9 - 104t + 432t^2 + 16t^3)\,.
\end{aligned}$$

In particular, as [3] similarly deduced, since (in fact, each of) the invariants $j_1(\mathcal{C}_t), j_2(\mathcal{C}_t), j_3(\mathcal{C}_t)$ are non-constant, the Flynn family does indeed include infinitely many non-isomorphic curves.

As mentioned above, Bernard, Leprévost and Pohst [3] gave some 18 other curves over $\mathbb{Q}$ with divisor of infinity of torsion order 11.

3.3. **New family.** The family of genus 2 curves $\mathcal{G}_u$ shares no isomorphism class with any of the curves of Flynn's family, $\mathscr{F}_t$. This is verified by computation involving the Igusa invariants; the only values of (t, u) such that $(\,j_1(t), j_2(t), j_3(t)\,) = (\,j_1(u), j_2(u), j_3(u)\,)$ (where we mildly abuse notation for the sake of legibility) are trivial in the sense that the invariants are then zero or infinity. We now sketch this computation.

Denoting a numerator of a quotient by Numer, let $\text{res}_{12}(t)$ denote the polynomial in t given by taking the resultant with respect to the variable u of $\text{Numer}(\,j_1(t) - j_1(u)\,)$ with $\text{Numer}(\,j_2(t) - j_2(u)\,)$. Of course, the only values of (t, u) such that $(\,j_1(t), j_2(t))\,) = (\,j_1(u), j_2(u)\,)$ are with t a zero of this resultant polynomial. Similarly define $\text{res}_{13}(t)$. These two resultant polynomials both divisible by certain powers of t, $9 - 104t + 432t^2 + 16t^3$ and $3 - 16t + 56t^2 + 4t^3$. The first two of these divides D_t, the third A_t, see the display under (5), and therefore either of them vanishing corresponds to a degenerate case.

The polynomial GCD of $\text{res}_{12}(t)$ and $\text{res}_{13}(t)$, after dividing by the aforementioned powers of the innocuous factors, is a nonzero constant (indeed, on the order of 10^{250}). Therefore, the resultants have no common nontrivial zero and there is indeed no non-trivial occurrence of $(\,j_1(t),\, j_2(t),\, j_3(t)\,) = (\,j_1(u),\, j_2(u),\, j_3(u)\,)$.

Involved in the above is the fact that the Igusa invariants for the family $\mathcal{G}_u$ are non-constant, and thus $\mathcal{G}_u$ is indeed an infinite family of non-isomorphic genus two curves.

4. Bounding torsion order and partial quotient degree

The naive upper bound on the order of the divisor at infinity is almost never achieved.

Theorem 4. *The torsion order N of the divisor at infinity of $\mathcal{C}$ satisfies*

$$N < 1 + mg$$

whenever $g > 1$ and $m > 2$.

In fact, from Theorem 5 below, it follows that $N < (\frac{5m}{6} + 1)g + m/2$. Furthermore, our results give clear restrictions on the "search space" when we set out to determine the curves of a fixed genus with divisors at infinity of fixed order.

4.1. **Restrictions on partial quotients: statements.** Further restrictions then simply an upper bound of degree g are imposed on the degrees of the partial quotients when one fixes genus g, that is when $\deg(a_0) = g+1$. In this subsection we list several results, with proofs delayed until the following subsection.

Theorem 5. *Let m be the quasi-period length of the continued fraction of y for the hyperelliptic curve $\mathcal{C}$ over a field k. Then for any $1 \le j \le m$,*

$$\deg(a_{j-1}) + \deg(a_j) \le g + 1 + \deg(a_1)\,. \tag{6}$$

Equality in (6) holds when $j = m$, and never holds for any three consecutive values of j with $j \le m/2$. Furthermore, whenever equality fails, then

$$\deg(a_{j-1}) + \deg(a_j) \le g + 1\,. \tag{7}$$

In fact, we expect that equality in (6) never holds for two consecutive values of j with $j \le m/2$. However, this entails a long and tedious calculation, whereas we are able to prove the above statement in a fairly straightforward manner. Furthermore, this already provides a helpful improvement in the upper bound of the order of the divisor at infinity. The proof is given in terms of a certain sequence of rational functions, h_j, see below. (That the h_j are in fact polynomials is show in Daowsud's Ph.D. thesis [7].) Focusing on leading coefficients of the a_i, we were lead to the h_j. The first, h_1, comes from the following straightforward variant of Friesen's result.

The proof of the following lemma is purely algebraic; the result thus holds for example in the case of regular continued fraction expansions of square roots. We use the notation $lc(p)$ to denote the leading coefficient of a polynomial $p(x)$.

Lemma 3. *Suppose that $\sqrt{f(x)}$ has a continued fraction expansion as in (3), with quasi-period length m, value κ, and period length n. Let p_j/q_j denote the approximants to the purely periodic $1/(\sqrt{f(x)} - a_0)$. Then*

$$f(x) - a_0^2 = q_{n-1}/p_{n-2} = q_{m-1}/(\kappa\, p_{m-2})\,.$$

In particular, $f(x) - a_0^2 \in k[x]$ is of degree $g + 1 - \deg(a_1)$ and has leading coefficient $2/lc(a_1)$.

We remark that setting $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$ gives

$$\begin{aligned} p_0 &= a_1, & q_0 &= 1,\\ p_1 &= a_2 a_1 + 1, & q_1 &= a_2;\\ \text{and for } j \ge 2: p_j &= a_{j+1}p_{j-1} + p_{j-2}, & q_j &= a_{j+1}q_{j-1} + q_{j-2}. \end{aligned}$$

Recall that c_j is related to the skew value by $c_j = \kappa^{\pm 1}$, depending upon the parity of j.

Definition 3. For $j \le m$, define the following rational functions:

$$\begin{aligned} h_1 &= \frac{c_1\, q_{m-1}}{p_{m-2}}\,,\\ h_2 &= \frac{c_2 p_{m-4} h_1 - q_{m-3}}{p_{m-3}}\,, \text{ and}\\ h_j &= \frac{c_j(p_{j-3}h_{j-1} + q_{j-3})p_{m-(j+2)} - p_{j-4}q_{m-(j+1)}}{p_{m-(j+1)}p_{j-4}}\,, \end{aligned} \tag{8}$$

for $3 \le j \le m$.

The h_j enjoy a palindromic symmetry, which in particular accounts for the hypothesis that $j \leq m/2$ in our statements about consecutive vanishing values. Since we do not use this aspect here, we merely state that : For $m-1 \geq j \geq 2$, $h_{m+1-j} = h_j$.

Note that the h_j are certainly rational functions, and thus each has a degree defined as usual as the difference between the degrees of numerator and denominator.

Proposition 1. *For $1 \leq j \leq m$, h_j has non-negative degree. If h_j is non-zero, then:*

$$\begin{aligned} \deg h_1 &= g + 1 - \deg(a_1)\,; \\ \deg h_j &= g + 1 - \deg(a_{j-1}) - \deg(a_j) \quad \textit{when } j > 1\,. \end{aligned}$$

Furthermore, for $j > 1$ we have that $h_j = 0$ if and only if $g+1+\deg(a_1) = \deg(a_{j-1}) + \deg(a_j)$; in particular, $h_m = 0$. Finally, $h_2 = 0$ if and only if $m \leq 2$.

As an easy application, consider the "greedy" situation (of partitioning $N - g - 1$, see Step (2) of the Method of Section 5) where we set $\delta_j = g$. We note that since $\delta_0 + \delta_1 = 2g+1$ is never equal to $2g$ and $\delta_0 \geq 2g$ can only be satisfied when $g = 1$, it follows that if $g > 1$ and $m > 2$ then the equality $\delta_1 = g$ implies that any $\delta_{j-1} + \delta_j \leq g + 1$ and in particular we cannot have consecutive partial quotients of degree g. This implies that the naive upper bound of Corollary 1 is almost never achieved, that is Theorem 4 holds.

4.2. **Restrictions on partial quotients: proofs.** Theorem 4 directly follows from Theorem 5. The proof of Theorem 5 follows directly from considering equation (4) with Proposition 1 and Lemma 6 (below). The following three lemmas yield the result of Proposition 1.

Definition 4. For ease of expression, let us define for each $0 \leq j \leq m$,

$$\delta_j = \deg(a_j)\,.$$

Thus $\delta_0 = g+1$, $\delta_{m-j} = \delta_j$. Also, we have $\deg(p_j) - \deg(q_j) = \delta_1$ and $\deg(p_j) - \deg(p_{j-1}) = \delta_{j+1}$ (and similarly for consecutively indexed q_j).

Lemma 4. *For $2 \leq j \leq m$, if h_j is non-zero, then:*

$$\deg h_j = \delta_0 - \delta_{j-1} - \delta_j\,.$$

Furthermore, $h_j = 0$ if and only if $\delta_0 + \delta_1 = \delta_{j-1} + \delta_j$; in particular, $h_m = 0$.

Proof. We argue by induction; for brevity's sake, we do not write out the straightforward proofs for the base cases.

Consider first the case of $h_j \neq 0$. Since $\deg(p_{j-4}q_{m-(j+1)}) - \deg(p_{m-(j+1)}p_{j-4})$ is clearly negative, the degree of the numerator in h_j as given in equation (8) is determined by its first summand. Since $\deg(p_{j-3}) > \deg(q_{j-3})$, when $h_{j-1} \neq 0$ we have

$$\begin{aligned} \deg(h_j) &= \deg(h_{j-1}) + \deg(p_{j-3}) + \deg(p_{m-(j+2)}) - \deg(p_{j-4}) - \deg(p_{m-(j+1)}) \\ &= \deg(h_{j-1}) + \big(\deg(p_{j-3}) - \deg(p_{j-4})\big) + \big(\deg(p_{m-(j+2)}) - \deg(p_{m-(j+1)})\big) \\ &= \deg(h_{j-1}) + \delta_{j-2} - \delta_{m-j} = \deg(h_{j-1}) + \delta_{j-2} - \delta_j \\ &= \delta_0 - \delta_{j-1} - \delta_j\,. \end{aligned}$$

If $h_{j-1} = 0$, then

$$\begin{aligned}\deg(h_j) &= \deg(q_{j-3}) + \deg(p_{m-(j+2)}) - \deg(p_{j-4}) - \deg(p_{m-(j+1)})\\ &= \big(\deg(q_{j-3}) - \deg(p_{j-4})\big) + \big(\deg(p_{m-(j+2)}) - \deg(p_{m-(j+1)})\big)\\ &= \big(\delta_{j-2} - \delta_1\big) - \delta_{m-j} = \delta_{j-2} - \delta_1 - \delta_j\\ &= \delta_0 - \delta_{j-1} - \delta_j\,.\end{aligned}$$

This last equality is by the induction argument whose hypothesis is: $h_{j-1} = 0$ implies $\delta_{j-2} = \delta_0 + \delta_1 - \delta_{j-1}$.

We turn now to the case of $h_j = 0$. We must have

$$\begin{aligned}0 &= \deg(\,(p_{j-3}h_{j-1} + q_{j-3})p_{m-(j+2)}) - \deg(p_{j-4}q_{m-(j+1)})\\ &= \deg(\,(p_{j-3}h_{j-1} + q_{j-3}) - \deg(p_{j-4}) + \deg(p_{m-(j+2)}) - \deg(q_{m-(j+1)})\\ &= \deg(\,p_{j-3}h_{j-1} + q_{j-3}) - \deg(p_{j-4}) - \delta_{m-j} + \delta_1\,.\end{aligned}$$

If also $h_{j-1} = 0$, then we find that $\delta_{j-2} = \delta_j$; again by induction, the result follows. Otherwise, we have

$$0 = \deg(\,p_{j-3}h_{j-1}) - \deg(p_{j-4}) - \delta_{m-j} + \delta_1\,,$$

with $\deg(\,h_{j-1}\,) = \delta_0 - \delta_{j-2} - \delta_{j-1}$. The result thus also easily follows. □

Lemma 5. *We have $h_2 = 0$ if and only if $m \leq 2$.*

Proof. From the previous result, we need only show that $h_2 = 0$ implies $m \leq 2$. The vanishing of h_2 gives that $g + 1 + \delta_1 = \delta_1 + \delta_2$. That is, $\deg a_2 = g + 1$, which by Theorem 3 signals the end of the (quasi-)period. □

There is an alternate expression for h_j. This follows directly from Daowsud's thesis [7], see sections 3.1, 3.2 and especially (3.15).

Proposition 2. *(Daowsud) If $j \geq 5$, then*

$$h_j = \frac{p_{j-3}(p_{j-4}h_{j-2} + q_{j-4} - a_{j-1}p_{j-5}h_{j-1}) - p_{j-5}q_{j-2}}{p_{j-5}p_{j-4}}\,.$$

Lemma 6. *If $m > 2$, then for each $3 \leq j \leq m/2$, not all three h_j, h_{j-1}, h_{j-2} are zero.*

Proof. We again skip the straightforward proofs in the cases of small j. Suppose that $j \geq 6$ and $h_j = h_{j-1} = 0$. From Proposition 2, we find

$$h_{j+1} = \frac{p_{j-2}q_{j-3} - p_{j-4}q_{j-1}}{p_{j-3}p_{j-4}}$$

and

$$h_{j-2} = \frac{p_{j-5}q_{j-2} - p_{j-3}q_{j-4}}{p_{j-3}p_{j-4}}.$$

We thus consider

$$\begin{aligned}
p_{j-2}q_{j-3} - p_{j-4}q_{j-1} - [p_{j-5}q_{j-2} - p_{j-3}q_{j-4}] &= p_{j-2}q_{j-3} + p_{j-3}q_{j-4} - [p_{j-4}q_{j-1} + p_{j-5}q_{j-2}]\\
&= p_{j-2}q_{j-3} + p_{j-3}q_{j-4} - [p_{j-4}q_{j-1} + p_{j-5}q_{j-2}]\\
&= (a_{j-1}p_{j-3} + p_{j-4})q_{j-3} + p_{j-3}q_{j-4}\\
&\quad - [p_{j-4}(a_jq_{j-2} + q_{j-3}) + p_{j-5}q_{j-2}]\\
&= p_{j-3}(a_{j-1}q_{j-3} + q_{j-4}) - (a_jp_{j-4} + p_{j-5})q_{j-2}\\
&= p_{j-3}q_{j-2} - (a_jp_{j-4} + p_{j-5})q_{j-2}\,.
\end{aligned}$$

We find that the above equals zero if and only if $a_j = a_{j-2}$. Thus, $h_j = h_{j-1} = 0$ implies the equivalence of $h_{j-2} = h_{j+1}$ with $a_j = a_{j-2}$.

We now find that

$$\begin{aligned}
h_{j+1}p_{j-3}p_{j-4} &= p_{j-2}q_{j-3} - p_{j-4}q_{j-1}\\
&= (a_{j-1}p_{j-3} + p_{j-4})q_{j-3} - p_{j-4}(a_jq_{j-2} + q_{j-3})\\
&= a_{j-1}p_{j-3}q_{j-3} - a_jq_{j-2}p_{j-4}\\
&= a_{j-1}(a_{j-2}p_{j-4} + p_{j-5})q_{j-3} - a_j(a_{j-1}q_{j-3} + q_{j-4})p_{j-4}\\
&= a_{j-1}(a_{j-2} - a_j)p_{j-4}q_{j-3} + a_{j-1}p_{j-5}q_{j-3} - a_jq_{j-4}p_{j-4}\,.
\end{aligned}$$

But, $h_j = h_{j-1} = 0$ implies that $\deg a_j = \deg a_{j-2}$ and in particular $\deg(a_{j-1}a_{j-2}) > \deg a_j$. From this, if $a_{j-2} \neq a_j$ then $a_{j-1}(a_{j-2} - a_j)p_{j-4}q_{j-3}$ is the unique highest degree summand in the final line of this last display. Thus, if $h_{j+1} = 0$ then this term must vanish, therefore $a_{j-2} = a_j$ and thus also $h_{j-2} = h_{j+1}$ must vanish. From this, we can continue with ever decreasing indices k with $h_k = 0$, until we reach a contradiction.

□

As we mentioned above, in her thesis [7], Daowsud also proves the following.

Theorem 6. *Each h_j is a polynomial.*

5. Solving for $f(x)$, a naive method

We deduce a naive method for finding curves over a field with low order torsion points on their Jacobians. We assume that $g > 1$ and $m > 2$.

Naive Method

`Given:` field k, genus g, torsion order N (with $N > g + 1$).
`Searches for:` $f(x) \in k[x]$ such that $y^2 = f(x)$ has divisor at infinity of order N.

(1) Fix $m \in [N - g, (N - 1)/g]$
(2) Choose a symmetric partition $(\delta_1, \dots, \delta_{m-1})$ of $N - g - 1$, with each $g \geq \delta_i \geq 1$ and $g + 1 + \delta_1 = \delta_{j-1} + \delta_j$ satisfied at most twice in a row for indices less than $m/2$, and $g + 1 \geq \delta_{j-1} + \delta_j$ for all other such j. Furthermore, if $m > 2$, then $g + 1 \geq \delta_1 + \delta_2$ must hold.
(3) Introduce variables $c_{i,j}$ for $1 \leq i \leq \lfloor m/2 \rfloor$ and $0 \leq j \leq \delta_i$
(4) Set $a_i = a_i(x) = \sum_{j=0}^{\delta_i} c_{i,j}\, x^j$, $1 \leq i \leq \lfloor m/2 \rfloor$
(5) If m is even then set $\kappa = 1$, else assign a variable κ taking values in $k \setminus \{0, 1\}$.
(6) For $1 \leq i \leq \lfloor m/2 \rfloor$ set $a_{m-i}(x) = \kappa^{\pm} a_i(x)$ with alternating powers of κ
(7) Introduce variables $r_0, \dots, r_g$ and set $a_0 = a_0(x) = x^{g+1} + \sum_{j=0}^{g} r_jx^j$.
(8) Expand the various p_j and q_j in terms of the a_i.
(9) Introduce variables $b_0, \dots, b_{\delta_0 - \delta_1 - 1}$

(10) Set $h_1(x) = (2/c_{1,\delta_1})\, x^{\delta_0-\delta_1} + \sum_{i=0}^{\delta_0-\delta_1-1} b_i x^i$.
(11) Solve the equation $h_1 = \dfrac{q_{m-1}}{\kappa p_{m-2}}$ in the form

$$\kappa p_{m-2} h_1 - q_{m-3} - 2\kappa a_0 q_{m-2} = 0$$

for the various $b_j, r_j, c_{i,j}$ (and κ as appropriate) under the restriction that no c_{i,δ_i} vanishes.

By induction, one shows that collecting powers of x in (11) leads to $N - \delta_1$ equations. The number of variables is $M := (\delta_0 - \delta_1) + (\lfloor m/2 \rfloor + \sum_{i=1}^{\lfloor m/2 \rfloor} \delta_i) + (m \pmod 2)) + (g+1)$. For an upper bound on M, we use $N \geq \lfloor m/2 \rfloor + \sum_{i=1}^{\lfloor m/2 \rfloor} \delta_i$ and $g \geq \delta_0 - \delta_1$. Similarly, for a (rough) lower bound, we use $\delta_0 - \delta_1 \geq 1$, $\sum_{i=1}^{\lfloor m/2 \rfloor} \delta_i \geq \frac{N-g-1}{2} \geq \frac{N-g-1}{2g}$, and $\lfloor m/2 \rfloor \geq \frac{N-1}{2g} \geq \frac{N-g-1}{2g}$. Therefore, the number M of variables is such that

$$g + 1 + N \geq M \geq g + 1 + (N-1)/g\,.$$

6. Applications of the method

6.1. **An impossible partition.** To illustrate this method, we sketch how when $g = 2, N = 11, m = 6$ (this even m is thus the period length), the partition of $N - g - 1 = 2+1+2+1+2 = \delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5$ gives no admissible solution (over any coefficient field).

For increased legibility, we set some variable names other than those given in the recipe. Let

$$\begin{aligned} a_0 &:= x^3 + r_2 x^2 + r_1 x + r_0 \\ a_1 &:= l_1 x^2 + c_1 x + k_1 \\ a_2 &:= l_2 x + k_2 \\ a_3 &:= l_3 x^2 + c_3 x + k_3 \\ h_1 &:= (2/l_1) x^2 + b_1 x + b_0, \text{and} \\ J &:= (p_4 h_1 - q_3) - 2 a_0 q_4\,, \end{aligned} \tag{9}$$

where $l_i \neq 0$ for each i, and we must solve so that the polynomial $J(x)$, which a priori is of degree 8, in fact vanishes. Eliminating coefficients of decreasing powers of x, leads to (in this order, from top to bottom) the admissible values

$$\begin{aligned} b_0 &= \frac{-2(c_1 - r_2 l_1)}{l_1^2} \\ k_1 &= \frac{2(r_1 l_1^2 - r_2 c_1 l_1 + c_1^2)}{l_1} \\ r_0 &= \frac{-2c_1^2 l_1 r_2 - c_1 l_2 l_1^2 r_1 + c_1 l_2 l_1^2 r_2^2 - l_2 l_1^3 r_2 r_1 - l_1^2 + l_2 c_1^3}{l_1^3 l_2} \\ r_2 &= \frac{(l_2 c_1 + l_1 k_2)}{l_1 l_2} \end{aligned} \tag{10}$$

However, one finds that $J(x)$ then has its coefficient of x^4 being $-l_2 l_3^2$, which cannot vanish! Thus, there is no genus two curve corresponding to this partition of $N - g - 1$.

6.2. **New family in genus two.** Of course, the naive method must in some cases lead to the existence of curves. Indeed, for $g = 2, N = 11, m = 7$ (as a strict quasi-period) and the partition of $N-g-1 = 2+1+1+1+1+2$, we set a_0, a_2 as above, but now set $a_1 := l_1x+k_1, a_3 := l_3x+k_3$ and $J := (\kappa p_5 h_1 - q_4) - 2\kappa a_0 q_5$.

Eliminating coefficients as above, results in exactly the same formulas for b_0, k_1, r_0 and r_2. However, there is no contradiction this time; we can continue to eliminate coefficients. After values for l_3, k_2, r_1 and c_1 are so determined, there is one remaining equation: $l_1^2 l_2^{11}\kappa^2 = -32$. For ease, we set $l_2 = -2, l_1 = -1/(8\kappa)$. There then results a family in the variables κ, k_3. The one dimensional family $\mathcal{G}_u$ is determined by setting $k_3 = 0$ and replacing κ by u.

6.3. **Examples in genus greater than two.** In her thesis [7] Daowsud gave examples for all possible genera g of curves defined over $\mathbb{Q}$ with Jacobian of divisor at infinity having torsion order 11. For brevity's sake, we simply report the basic form of the expansions that she found when $g > 2$.

g	m	$(\delta_0, \delta_1, \cdots, \delta_{m-1})$
3	6	(4,2,1,1,1,2)
4	4	(5,1,2,2,1)
5	4	(6,1,3,1)
6	3	(7,2,2)
7	4	(8,1,1,1)
8	2	(9,2)
9	2	(10,1)
10	1	(11)

Table 1. Genera, period length and partition of $N = 1$ for examples in [7] for higher genus.

References

[1] W. Adams and M. Razar, *Multiples of points on elliptic curves and continued fractions*, Proc. London Math. Soc. (3) 41 (1980), no. 3, 481–498.

[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*, Math. Zeitschr.19 (1924), pp. 153–246. In: The collected papers of Emil Artin, 1–94 Addison–Wesley, Reading, WA, 1965.

[3] N. Bernard, F. Leprévost, and M. Pohst, *Jacobians of genus-2 curves with a rational point of order 11*, Experiment. Math. 18 (2009), no. 1, 65–70.

[4] T. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math. (Basel) 55 (1990), no. 3, 259–266.

[5] G. Billing and K. Mahler, *On exceptional points on cubic curves*, J. London Math. Soc. 15, (1940), 32–43.

[6] J. W. S. Cassels and E. V. Flynn, Prolegomena to a middlebrow arithmetic of curves of genus 2. London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996.

[7] K. Daowsud, *Continued fractions and the divisor at infinity on a hyperelliptic curve: Examples and order bounds*, Ph.D. dissertation, Oregon State University, 2013.

[8] E. V. Flynn, *Large rational torsion on abelian varieties*, J. Number Theory 36 (1990), no. 3, 257–265.

[9] ———, *Sequences of rational torsions on abelian varieties*, Invent. Math. 106 (1991), no. 2, 433–442.

[10] C. Friesen, *Continued fraction characterization and generic ideals in real quadratic function fields*, In: The arithmetic of function fields (Columbus, OH, 1991), 465–474, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.

[11] J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) 72 (1960), 612–649.

[12] K. Lauter and T. Yang, *Computing genus 2 curves from invariants on the Hilbert moduli space*, J. Number Theory 131 (2011), no. 5, 936–958.

[13] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules.* In Effective methods in algebraic geometry (Castiglioncello, 1990), 313–334, Progr. Math., 94, Birkhäuser, Boston, Boston, MA, 1991.

[14] F. Pappalardi and A. van der Poorten, *Pseudo-elliptic integrals, units, and torsion*, J. Aust. Math. Soc. 79 (2005), no. 3, 335–347.

[15] A. van der Poorten and X. Tran, *Quasi-elliptic integrals and periodic continued fraction*, Monatsh. Math. 131 (2000), no. 2, 155–169.

[16] V. P. Platonov, *Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field* (Russian. Russian summary), Uspekhi Mat. Nauk 69 (2014), no. 1(415), 3–38; translation in Russian Math. Surveys 69 (2014), no. 1, 1–34.

[17] W. Schmidt, *On continued fractions and Diophantine approximation in power series fields*, Acta Arith. 95 (2000), no. 2, 139–166.

Department of Mathematics, Faculty of Science, Kasetsart University, 50 Ngam Wong Wan Rd, Ladyaow, Chatuchak, Bangkok, 10900, Thailand
E-mail address: fsciky@ku.ac.th

Oregon State University, Corvallis, OR 97331
E-mail address: toms@math.orst.edu