Kevser Aktaş; Hasan Şenay

On the arithmetic of the hyperelliptic curve $y^2 = x^n + a$

Czechoslovak Mathematical Journal, Vol. 66 (2016), No. 1, 35–40

Persistent URL: `http://dml.cz/dmlcz/144869`

Czechoslovak Mathematical Journal, 66 (141) (2016), 35–40

ON THE ARITHMETIC OF THE HYPERELLIPTIC CURVE $y^2 = x^n + a$

Kevser Aktaş, Hasan Şenay, Konya

(Received November 10, 2014)

Abstract. We study the arithmetic properties of hyperelliptic curves given by the affine equation $y^2 = x^n + a$ by exploiting the structure of the automorphism groups. We show that these curves satisfy Lang's conjecture about the covering radius (for some special covering maps).

Keywords: hyperelliptic curve; Lang's conjecture

MSC 2010: 11G30, 14H25

1. Introduction

The class of hyperelliptic curves has been the object of special treatment for both geometric and arithmetic problems related to curves. By the virtue of having a simple explicit form $y^2 = f(x)$, these curves are amenable to analysis by concrete and elementary techniques. In this paper, we specialize further to the hyperelliptic curves of the form

$$y^2 = x^n + a, \quad a \neq 0, \ n \geqslant 5$$

defined over number fields.

For each such curve X, we determine the group $\operatorname{Aut}(X)$ of automorphisms of X and exploit this information to prove that Lang's Conjecture on page 168 of [2] for the covering radius holds for X in the following special case: if $\Phi\colon D(r) \to X$ is the universal covering map where $D(r)$ is the disc of radius r centered at zero normalized such that $\Phi(0) \in X(\overline{\mathbb{Q}})$ *is a ramification point of a normal Belyi covering* $X \to \mathbb{P}^1$ and $\Phi'(0) \in \overline{\mathbb{Q}}$, then r is a transcendental number.

We would like to thank for the support of the Scientific and Technological Research Council of Turkey (TUBITAK).

Wolfart and Wüstholz [5] studied whether the radius is transcendental for such curve X. It is given how the radius is determined especially in Proposition 5 of their paper and finally Satz 5 states that the radius is transcendental for such curves. The transcendence of r is well defined in Wolfart [4] for special values of the Gamma function which also arise as periods as follows. Let the curve X be defined by the curves $y^2 = u^2 + v^2$ and $x^3 = uv^2$ in $\mathbb{P}^3(\mathbb{C})$ and assume that the universal covering map $\Phi\colon D(r) = \{z \in \mathbb{C};\ |z| < r\} \to X$ is normalized that $\Phi'(0)$ is algebraic with $\Phi(z) = (x, y, u, v)$.

(a) $\Phi(0) = (0, 1, \pm 1, 0)$ or $(0, 1, 0, \pm 1)$ or

(b) $\Phi(0) = (\mathrm{e}^{2\pi i n/12}, 0, \mathrm{e}^{2\pi i n/4}, 1)$ where $2 \nmid n \in \mathbb{Z}$.

Then the radius is,

$$r = \begin{cases} \pi^{-3}\Gamma(1/3)^6 & \text{for the case (a),} \\ \pi^{-2}\Gamma(1/4)^4 & \text{for the case (b).} \end{cases}$$

As a result we obtain the fact that, for such curve X, the radius r at the algebraic point $\Phi(0)$ is transcendental.

Throughout the paper,

- ▷ $\mathbb{Q}$, $\mathbb{C}$, K denote the rational numbers, complex numbers and a number field, respectively.
- ▷ $\overline{X}_{n,a}$ is the smooth complete curve defined over a number field by the affine equation $y^2 = x^n + a$, $a \neq 0$. $\overline{X}_n$ denotes the curve $\overline{X}_{n,-1}$.
- ▷ $g(\overline{X}_{n,a})$ is the genus of the curve $\overline{X}_{n,a}$.

We first recall the well-known construction of the projective curve $\overline{X}$. Given

$$y^2 = f(x) = x^n + a = \prod_{i=1}^{n} (x - x_i)$$

where $x_i = |a|^{1/n}\xi_n^i$, ξ_n is a primitive n-th root of unity, we obtain $\overline{X}_{n,a}$ by introducing a second chart

$$y'^2 = \prod_{i=1}^{n} (1 - x_i x') \quad \text{if } n = 2m,$$
$$y'^2 = x' \prod_{i=1}^{n} (1 - x_i x') \quad \text{if } n = 2m - 1$$

and by glueing the two charts via the identification $x' = 1/x,\ y' = y/x^m$. The points at ∞ for the chart (x, y) are:

$$\begin{aligned} \infty_1, \infty_2 \quad & \text{given by } x' = 0,\ y' = \pm 1 \text{ if } n \text{ is even,} \\ \infty \quad & \text{given by } x' = 0 = y' \text{ if } n \text{ is odd.} \end{aligned}$$

Applying the Riemann-Hurwitz formula to the hyperelliptic map

$$\varphi\colon\ \overline{X}_{n,a} \to \mathbb{P}^1 \quad \text{given } (x,y) \mapsto x$$

one finds

$$g(\overline{X}_{n,a}) = \begin{cases} \dfrac{n-1}{2} & \text{if } n \text{ is odd,} \\[2ex] \dfrac{n-2}{2} & \text{if } n \text{ is even.} \end{cases}$$

Lemma 1.1. *For $a, b \in K^*$, $\overline{X}_{n,a}$ and $\overline{X}_{n,b}$ are isomorphic over $K((b/a)^{1/n})$ if n is even, and over $K((b/a)^{1/n}, (b/a)^{1/2})$ if n is odd.*

P r o o f. We have an explicit isomorphism

$$\Psi\colon\ \overline{X}_{n,a} \to \overline{X}_{n,b} \quad \text{given } (x,y) \mapsto ((b/a)^{1/n}x, (b/a)^{1/2}y)$$

which proves the lemma. □

Without explicitly referring to this lemma, the properties which are independent of the precise field of definition of $\overline{X}_{n,a}$ will be proved for the special case of $\overline{X}_n$. Necessary modifications for arithmetic results which require the essential use of the field of definition, will be included as remarks.

2. Automorphism group of $\overline{X}_n$

The double cover

$$\varphi\colon\ \overline{X}_n \to \mathbb{P}^1 \quad \text{given } (x,y) \mapsto x$$

is unique and corresponds to an involution $\tau_h \in \mathrm{Aut}(\overline{X}_n)$ which commutes with all $\sigma \in \mathrm{Aut}(\overline{X}_n)$. φ ramifies precisely at Weierstrass points

$$(\omega_k, 0), \quad k = 1, \dots, n \text{ if } n \text{ is even,}$$
$$(\omega_k, 0), \quad k = 1, \dots, n \text{ and at } \infty \text{ if } n \text{ is odd}$$

where $\omega_k = \zeta_n^k$.

We define the reduced automorphism group as the quotient group

$$\overline{G} = \mathrm{Aut}(\overline{X}_n)/\langle \tau_h \rangle.$$

Lemma 2.1. *Notice that*

$$\overline{G} \backsimeq \begin{cases} D_n & \text{if } n \text{ is even,} \\ \mathbb{Z}_n & \text{if } n \text{ is odd,} \end{cases}$$

where D_n is the dihedral group of order $2n$.

P r o o f. Case n is even: Let $\sigma \in \overline{G}$. Then σ permutes the Weierstrass points. On the other hand since σ commutes with τ_h, σ induces $T_\sigma \in \mathrm{Aut}(\mathbb{P}^1)$ via its action on the first coordinate x. The linear fractional transformation T_σ maps $|x| = 1$ onto itself; hence we may assume that T_σ maps the unit disc onto itself. Now it is easy to check that the permutation induced on the vertices ω_k of the corresponding regular n-gon is a rotation. That is

$$\sigma \in \mathrm{Aut}(n\text{-gon}) = D_n = \langle a, b;\ a^2 = b^n = (ab)^2 \rangle$$

where $a(z) = 1/z$ and $b(z) = \xi_n z$. Hence $\overline{G} \leqslant D_n$.

To prove that in fact $\overline{G} \backsimeq D_n$ we check that $h \in D_n$ defines $\sigma_h \in \mathrm{Aut}(\overline{X}_n)$

$$\sigma_h \colon \overline{X}_n \to \overline{X}_n \quad \text{given } (x, y) \mapsto (hx, y).$$

Thus, we have

$$D_n \hookrightarrow \overline{G} \quad \text{given } h \mapsto \sigma_h$$

and it follows that $\overline{G} \backsimeq D_n$.

Case n is odd: In this case, since $a(\infty) = 0$ is not a Weierstrass point, $a \in D_n$ does not define an element in $\overline{G}$. Hence $\overline{G} = \langle b \rangle \backsimeq \mathbb{Z}_n$. $\square$

3. $\overline{X}_{n,a}$ and Lang's conjecture

In this section we prove Lang's conjecture in the following special case: if $\Phi\colon D(r) \to \overline{X}_{n,a}$ is the universal covering map normalized that $\Phi(0) \in \overline{X}_{n,a}(\overline{\mathbb{Q}})$ *is a ramification point of a normal Belyi covering* $\overline{X}_{n,a} \to \mathbb{P}^1$ and $\Phi'(0) \in \overline{\mathbb{Q}}$, then r is a transcendental number.

Definition 3.1 ([3])**.** Let X be a compact Riemann surface. A nonconstant meromorphic function f on X is said to be a Belyi function if f ramifies over at most three points. Then X is a Belyi surface if X admits a Belyi function.

Lemma 3.2. *$\overline{X}_{n,a}$ is a Belyi surface.*

P r o o f. It suffices to prove this result for $\overline{X}_n$ (Lemma 1.1).

n is odd: We showed that the map

$$b\colon \overline{X}_n \to \overline{X}_n \quad \text{given } (x, y) \mapsto (\xi_n x, y)$$

is an element of $\mathrm{Aut}(\overline{X}_n)$. Then $\langle b\rangle = H$ is a subgroup of order n of $\mathrm{Aut}(\overline{X}_n)$ and we obtain a holomorphic map

$$f\colon \overline{X}_n \to \overline{X}_n/H \quad \text{given } (x,y) \mapsto [x,y].$$

This map ramifies over a point if the length of the corresponding orbit $[x,y]$ of (x,y) under the action of H is less than n. Thus f ramifies totally at each of the three points $[0,\mathrm{i}]$, $[0,-\mathrm{i}]$, ∞. This map is a normal covering since it is induced by action of a subgroup of $\mathrm{Aut}(\overline{X}_n)$.

From the Riemann-Hurwitz formula it follows that $g(\overline{X}_n/H) = 0$. Thus f is a Belyi function on $\overline{X}_n$.

n is even: We use the elements of $\mathrm{Aut}(\overline{X}_n)$ given by

$$b\colon \overline{X}_n \to \overline{X}_n \quad \text{given } (x,y) \mapsto (\xi_n x, y)$$

and

$$\tau_h\colon \overline{X}_n \to \overline{X}_n \quad \text{given } (x,y) \mapsto (x,-y).$$

Then $\langle b, \tau_h\rangle = H$ is a subgroup of order $2n$ of $\mathrm{Aut}(\overline{X}_n)$, since $\tau_h b = b\tau_h$ and $\tau_h^2 = b^n = 1$ and we obtain a normal covering

$$f\colon \overline{X}_n \to \overline{X}_n/H \quad \text{given } (x,y) \mapsto [x,y]$$

which ramifies at the three points $[0,\mathrm{i}]$, $[\infty,\infty]$ and $[\xi_n, 0]$.

By computing the ramification indices and applying the Riemann-Hurwitz formula we obtain

$$2\frac{n-2}{2} - 2 = 2n(2g-2) + 2(n-1) + 2(n-1) + n.$$

Hence $g(\overline{X}_n/H) = 0$ and thus f is Belyi function on $\overline{X}_n$. $\square$

Definition 3.3 ([3]). A compact Riemann surface X of genus $g > 1$ is said to have many automorphisms if the corresponding point $c = p(X)$ in the moduli space M_g of compact Riemann surfaces of genus g has (in the complex topology) a neighbourhood $U \subset M_g$ with the following property: For any $q \in U$, $q \neq p$, the order of the automorphism group of the corresponding Riemann surface $Y(q)$ is strictly less than the order of $\mathrm{Aut}(X)$.

Example. The curve $\overline{X}_6$ has many automorphisms. In fact, in the notation of Definition 3.3 we can take $U = M_2 - \{p_1, p_2\}$ where p_1 or p_2 is the point corresponding to the curve $y^2 = x(x^4-1)$ or $y^2 = x(x^5-1)$, respectively, because $\mathrm{Aut}(\overline{X}_6)$ is strictly bigger than the automorphism groups of all genus 2 curves except the curves given by $y^2 = x(x^4-1)$ and $y^2 = x(x^5-1)$ (page 340 in [1]).

Theorem 3.4 (Theorem 6 in [3]). *A compact Riemann surface X of genus $g > 1$ has many automorphisms if and only if there exists a Belyi function β defining a normal covering $\beta\colon X \to \mathbb{P}^1$.*

Lemma 3.5. *$\overline{X}_{n,a}$ has many automorphisms.*

P r o o f. Follows from Lemma 3.2. □

Corollary 3.6. *Lang's conjecture is valid for $\overline{X}_{n,a}$ for covering maps*

$$\Phi\colon D(r) \to \overline{X}_{n,a}$$

normalized such that $\Phi(0)$ is a ramification point of the Belyi map f.

P r o o f. We apply (Satz 5 in [5]) to $\overline{X}_{n,a}$. □

Acknowledgement. We would like to thank Professor Hurşit Önsiper for giving us a lot of advice and would like to thank the referee for his helpful remarks.

References

[1] *C. Birkenhake, H. Lange*: Complex Abelian Varieties. Grundlehren der Mathematischen Wissenschaften 302, Springer, Berlin, 2004.

[2] *S. Lang*: Hyperbolic and Diophantine analysis. Bull. Am. Math. Soc., New Ser. *14* (1986), 159–205.

[3] *J. Wolfart*: The 'Obvious' part of Belyi's theorem and Riemann surfaces with many automorphisms. Geometric Galois Actions. 1. Around Grothendieck's "Esquisse d'un Programme" (L. Schneps et al., eds.). Proc. Conf. on geometry and arithmetic of moduli spaces, Luminy, France, 1995. Lond. Math. Soc. Lect. Note Ser. 242, Cambridge University Press, Cambridge, 1997, pp. 97–112.

[4] *J. Wolfart*: Taylorentwicklungen automorpher Formen und ein Transzendenzproblem aus der Uniformisierungstheorie. Abh. Math. Semin. Univ. Hamb. *54* (1984), 25–33. (In German.)

[5] *J. Wolfart, G. Wüstholz*: Der Überlagerungsradius gewisser algebraischer Kurven und die Werte der Betafunktion an rationalen Stellen. Math. Ann. *273* (1985), 1–15. (In German.)

Authors' addresses: K e v s e r A k t a ş, Department of Mathematics, Faculty of Science, Selçuk University, Campus, 42003, Selçuklu, Konya, Turkey, e-mail: kevseraktas@gazi.edu.tr; H a s a n Ş e n a y, Department of Mathematics Education, Mevlana University, Yeni Istanbul Cad 235, 42003 Selçuklu, Konya, Turkey, e-mail: hsenay@mevlana.edu.tr.