*Pacific Journal of Mathematics*

# TWISTS AND GENERALIZED ZOLOTAREV POLYNOMIALS

Fumio Hazama

Volume 203 No. 2 April 2002

PACIFIC JOURNAL OF MATHEMATICS
Vol. 203, No. 2, 2002

# TWISTS AND GENERALIZED ZOLOTAREV POLYNOMIALS

Fumio Hazama

**A generalization of the so-called Zolotarev polynomial is investigated though the theory of twists and that of generalized Jacobian varieties. As an application, extremal properties, rationality, and a relation with multigrades are revealed.**

## 1. Introduction.

In the previous article [**3**], the author investigated Diophantine equations of the form

$$(*) \qquad X^2 - f(x)Y^2 = 1$$

and found that the set of the polynomial solutions of $(*)$ can be described in terms of the theory of twists and that of generalized Jacobian varieties. On the other hand, there are several articles ([**1**], [**7**]) which relate the solutions of $(*)$ with certain torsion points on the Jacobian variety of the hyperelliptic curve $y^2 = f(x)$. One of the purposes of the present paper is to show that our viewpoint reveals quite naturally the reason why the torsion points show up in this connection. Another purpose is to generalize the notion of the so-called *Zolotarev polynomials* and investigate the extremal property, which is studied in [**11**], and the arithmetic properties of the generalized ones. The original polynomials are investigated in [**4**] as the set of solutions of $(*)$ when $\deg f = 4$, in connection with the universal family the elliptic curves $y^2 = f(x)$ with a specified torsion point, hence with the arithmetic of the modular curve $X_1(N)$. Furthermore, it is pointed out in [**10**] that, when the base field is the field of complex numbers, $(*)$ is related with certain planar graphs through the notion of "*dessins d'enfants*". In the present paper, generalizing the method in [**3**], we will see the theory of twists provides us with natural and unified viewpoint to investigate these types of problems for polynomials $f(x)$ of any degree.

The plan of this paper is as follows. In Section 2 we recall the definition of twists and their fundamental properties. In Section 3, we will explain the reason why the polynomial solutions of $(*)$ are related with torsion divisors on the Jacobian variety of the hyperelliptic curve $y^2 = f(x)$, in terms of the theory of twists and that of the generalized Jacobian varieties. Section 4 is devoted to the investigation of extremal properties of the solutions. It

can be regarded as a generalization of some results in [**2**] where the authors considered $(*)$, or rather a differential equation closely related to it from an analytic viewpoint. In Section 5 the notion of *rational Zolotarev polynomials* is introduced and its relation with the so-called *multigrade* is related. In Section 6 several examples are given.

Thanks are due to the referee who pointed out several ambiguities in the original version and let the author know appropriate references related to the content of the present article.

## 2. Twist.

In this section we recall the main result of [**3**] which describes the set of polynomial solutions of a certain type of Diophantine equation in terms of the theory of twists.

Let $k$ be an arbitrary field of characteristic $\neq 2$. Let $C : y^2 = f(x)$ denote a hyperelliptic curve defined over $k$ with $f(x) \in k[x]$ a polynomial of even degree. Let $T'$ denote the curve over $k(x)$ defined by the following equation:

$$T' : f(x)Y^2 = X^2 - 1. \tag{2.1}$$

Note that this can be regarded as a quadratic twist of the conic $T : Y^2 = X^2 - 1$ by the quadratic extension $k(\sqrt{f(x)})/k(x)$. As for the set of all the polynomial solutions of (2.1), the following theorem is proved in [**3**]:

**Theorem 2.1** ([**3**, Theorem 3.1])**.** *Let $\infty_1, \infty_2$ denote the points above the infinity of $C$, and put $\mathbf{m} = \infty_1 + \infty_2$. Let $J = J(C)$ denote the Jacobian variety of $C$ and let $J_{\mathbf{m}}$ denote the generalized Jacobian variety of $C$ with modulus $\mathbf{m}$. Assume that there exists a $k$-rational branch point $P_0$ on $C$. Then there is a natural bijection between the set*

$$\mathrm{Sol}\,(T') = \{(X(x), Y(x)) \in T';\ X(x), Y(x) \in k[x]\}$$

*of polynomial solutions of $T'$ and the direct product*

$$G = \mathrm{Hom}_k(J_m, \mathbf{G}) \times \{\pm 1\}$$

*of the group $\mathrm{Hom}_k(J_{\mathbf{m}}, \mathbf{G}_m)$ of $k$-homomorphisms of $J_{\mathbf{m}}$ to the multiplicative group $\mathbf{G}_m$ and the 2-torsion subgroup $\{\pm 1\}$ of $\mathbf{G}_m$.*

**Remark.** It follows from [**9**, Chapter V, Corollary 1 to Theorem 2] that the map $\varphi_{\mathbf{m}}$ depends on the choice of the $k$-rational branch point $P_0$. If we take another branch point, then the polynomial solution $(X(x), Y(x))$ becomes the composition $(X(ax+b), Y(ax+b))$ of $(X(x), Y(x))$ and an affine transformation $x \mapsto ax + b$ which keeps the polynomial $f(x)$ (hence the branch points of $C$) invariant. (Note that the equation of $T'$ implies the equality $f(x) = (X(x)^2 - 1)/Y(x)^2$.)

## 3. Character group of $J_{\mathbf{m}}$.

In this section we will determine the structure of the character group $\mathrm{Hom}_k(J_{\mathbf{m}}, G_m)$ explicitly.

For this purpose, we consider the following exact sequence:

$$0 \to L_{\mathbf{m}} \to J_{\mathbf{m}} \to J \to 0.$$

Here the kernel $L_{\mathbf{m}}$ is expressed as follows ([**9**, Chapter V, Section 3]). Let $U_P$ denote the group of units in the local ring $O_P$ at $P$, and let $U_P^{(n)}$denote the subgroup of $U_P$ whose elements consist of $g$ with $\nu_P(1-g) \geq n$. Then we have $L_{\mathbf{m}} \cong (U_{\infty_1}/U_{\infty_1}^{(1)} \times U_{\infty_2}/U_{\infty_2}^{(1)})/\Delta$, where $\Delta$ denotes the image of the diagonal mapping of $\mathbf{G}_m$. Hence we can identify $L_{\mathbf{m}}$ with $\mathbf{G}_m$ via the imbedding of the first factor. Therefore the exact sequence above yields the following long exact cohomology sequence:

$$0 \to \mathrm{Hom}_k(J_{\mathbf{m}}, \mathbf{G}_m) \to \mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m) \xrightarrow{d} \mathrm{Ext}_k(J, \mathbf{G}_m) \to \cdots .$$

(Note that $\mathrm{Hom}_k(J, \mathbf{G}_m) = \{0\}$.) The middle term $\mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m)$ is isomorphic to $\mathbf{Z}$, generated by $id$ the identity map, and the image of $id$ under the map $d$ is, by the definition of $d$, equal to the class of $J_{\mathbf{m}}$ as an extension of $J$ by $\mathbf{G}_m$. Moreover the group $\mathrm{Ext}_k(J, \mathbf{G}_m)$ is isomorphic to the group of the $k$-rational points on the Picard group of $J$, hence naturally isomorphic to the Mordel-Weil group $J(k)$. Under this correspondence, the class of $J_{\mathbf{m}}$ maps to $(\infty_1) - (\infty_2)$. (One can check this by a diagram chasing or consult [**12**] which deals with more general situations.) Summarizing we obtain the following:

**Proposition 3.1.**

$$\mathrm{Hom}_k(J_{\mathbf{m}}, \mathbf{G}_m) \cong \begin{cases} \mathbf{Z}, & \text{if } (\infty_1) - (\infty_2) \text{ is torsion in } J(k), \\ \{0\}, & \text{otherwise.} \end{cases}$$

In view of Theorem 2.1, this implies the following:

**Corollary 3.1.1.** *There exists a nontrivial polynomial solution for $T'$ if and only if the divisor $(\infty_1) - (\infty_2)$ is of finite order in the Jacobian variety $J$.*

The next problem which arises naturally is to explicate the set of polynomial solutions under the assumption that the divisor $(\infty_1) - (\infty_2)$ is of finite order. Let $n$ denote its order in the Jacobian variety. Then it follows from the above exact sequence and the existence of a natural isomorphism $\mathrm{Ext}_k(J, \mathbf{G}_m) \cong J(k)$ that $[n]_*(J_{\mathbf{m}})$ is trivial as an extension of $J$ by $\mathbf{G}_m$, where $[n]$ denotes the $n$-th power endomorphism of $\mathbf{G}_m$ and $[n]_*$ the push-forward morphism described in [**9**, Chapter VII, Section 1]. Therefore we have the following commutative diagram of short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{G}_m & \longrightarrow & J_{\mathbf{m}} & \longrightarrow & J & \longrightarrow & 0 \\ & & {\scriptstyle [n]_*}\downarrow & & {\scriptstyle \alpha}\downarrow & & {\scriptstyle id}\downarrow & & \\ 0 & \longrightarrow & \mathbf{G}_m & \xrightarrow{i} & [n]_* J_{\mathbf{m}} & \longrightarrow & J & \longrightarrow & 0 \end{array}$$

and a retraction homomorphism $r : [n]_*(J_{\mathbf{m}}) \to \mathbf{G}_m$ such that $r \circ i = id_{\mathbf{G}_m}$. Hence we see that the composite $r \circ \alpha$ is the homomorphism which generates $\mathrm{Ker}\,(d) \cong \mathrm{Hom}_k(J_{\mathbf{m}}, \mathbf{G}_m) \cong \mathbf{Z}$.

Now recall that an element $D$ of $J \cong \mathrm{Pic}^0(C_)$ corresponds to the 2-cocycle $f$ under the isomorphism $\mathrm{Ext}_k(J, \mathbf{G}_m) \cong \mathrm{Pic}^0(C)$ by the following rule:

$$(f) = s^{-1}(D) - p^{-1}(D) - p_2^{-1}(D),$$

where $s$ denotes the addition morphism of $J \times J$ and $p_i$ $(i = 1, 2)$ denotes the projection of $J \times J$ to its $i$-th factor (see [**9**, Chapter VII, Section 3]). Suppose $D$ is linearly equivalent to zero, therefore there exists a function $h$ on $C$ such that $D = (h)$. Then one can take $\delta h$, the coboundary of $h$, for $f$. In this case, one can check easily that the generator of $\mathrm{Hom}_k(J_{\mathbf{m}}, \mathbf{G}_m)$, which corresponds bijectively to the set

$$\{\alpha \in \mathrm{Rat}_k(C, \mathbf{G}_m);\ \alpha(P_0) = 1, \ \text{ and } \alpha \text{ has } \mathbf{m} \text{ for } a \text{ modulus}\}$$

by the universal property of the generalized Jacobian variety, is given by the rational map $h$ itself. Hence we obtain the following:

**Theorem 3.1.** *Notation being as above, suppose that the divisor* $(\infty_1) - (\infty_2)$ *on* $C$ *has order* $n$ *in the Jacobian variety* $J(C)$ *and let* $h$ *denote the rational function on* $C$ *such that* $n\{(\infty_1) - (\infty_2)\} = (h)$. *Then the group* $\mathrm{Hom}_k(J_{\mathbf{m}}, \mathbf{G}_m)$ *is generated by the element which corresponds to* $h$ *under the bijection above. Hence the set of all the polynomial solutions of* $T'$ *is generated by* $h$ *under the multiplication rule described in* [**3**].

## 4. Extremal property.

From now on we consider the Diophantine equation $f(x)Y^2 = X^2 - r^2$ with $r \in k$. Since this curve is isomorphic to $T'$ over $k(x)$ by the map $(X, Y) \mapsto (X/r, Y/r)$, the results in the previous sections remain valid. But when we analyze certain properties of each polynomial solution, this form will be more convenient.

**Definition 4.1.** Suppose we are given a monic separable polynomial $f(x) \in k[x]$ of degree $2g + 2$. Then a monic polynomial $X(x) \in k[x]$ of degree $n$ is said to be a generalized Zolotarev polynomial of degree $n$ associated to $f(x)$ if there exist a polynomial $Y(x) \in k[x]$ and an element $r \in k$ such that

$$f(x)Y(x)^2 = X(x)^2 - r^2 \tag{4.1.1}$$

holds.

From now on until the end of this section, we assume the base field $k$ is $\mathbf{R}$, the real number field. In order to justify the problem-setting in this section, we quote a part of [**2**, p. 453]:

"The curve $y$, $-1 \leq x \leq 1$, consists of $n-1$ monotonic arcs varying between $+1$ and $-1$, $y = 1$ for $x = 1$, and $y = (-1)^{n-1}$ for $x = -1$. Such a curve necessarily has $n-1$ roots in $-1 \leq x \leq 1$ and consequently one more outside this interval. If this additional root is $> 1$, then $y$ satisfies a differential equation of the form

$$n^2(1-y^2) = (1-x^2)y'^2\frac{(B-x)(C-x)}{(A-x)^2}$$

where $y' = 0$ for $x = A$, $y = 1$ for $x = B$, $y = -1$ for $x = C$, and $1 < A < B < C$."

Then they proceeded to consider some extremal properties which the solutions of this equation share. Note that their problem corresponds to the case $f(x) = (x^2-1)(x-B)(x-C)$ with $g = 1$ in our notation. Therefore, in order to generalize their result to the case of arbitrary genus, it is natural to assume the following conditions:

(i) $f(x)$ is an arbitrary separable monic polynomial of degree $2g+2$ with real coefficients such that it has only real zeros $a_1, \ldots, a_{2g+2}$.
(ii) The generalized Zolotarev polynomial $X(x)$ of degree $n$ associated with $f(x)$ has $n$ distinct real zeros.

Then we have the following:

**Theorem 4.2.** *Let $I$ denote the union of the closed intervals $[a_{2i-1}, a_{2i}]$ $(i = 1, \ldots, g+1)$. Let $X(x)$ denote a generalized Zolotarev polynomial of degree $n$ associated with $f(x)$ so that the equation $f(x)Y(x)^2 = X(x)^2 - r^2$ holds for some real polynomial $Y(x)$ and for some positive real number $r$. Then*

$$\min_{p \in P_n} \max\{|p(x)|;\ x \in I\} \geq r,$$

*where $P_n$ denotes the set of monic real polynomials of degree $n$. Moreover the equality holds if and only if $p(x) = X(x)$.*

*Proof.* Since $f(x) \leq 0$ for any $x \in I$, it follows from the defining equation $f(x)Y(x)^2 = X(x)^2 - r^2$ that $|X(x)| \leq r$ for any $x \in I$ and that $X(a_1) = \pm r$ for $i = 1, \ldots, 2g+2$. Hence the generalized Zolotarev polynomial of degree $n$ satisfies the equality $\max\{|X(x)|;\ x \in I\} = r$. To prove the converse we need the following:

**Lemma 4.2.1.** *The derivative $X'(x)$ has $n-1$ distinct real zeros $b_1, \ldots, b_{n-1}$ such that $b_1 \in (a_{2i}, a_{2i+1})$ $(1 \leq i \leq g)$ and that $b_i \in I$ $(g+1 \leq i \leq n-1)$.*

*Proof.* By differentiating the defining Equation (4.1.1), we have

$$2XX' = f'Y^2 + 2fYY' = Y(f'Y + 2fY').$$

Since $X(x)$ and $Y(x)$ are relatively prime, this equality implies that $Y(x)$ must divide $X'(x)$, namely there exists a polynomial $S(x)$ of degree $g$ with $X'(x) = S(x)Y(x)$. (Recall that $\deg X = n$ $\deg Y = n - g - 1$.) Equation (4.1.1) implies that $X(a_i) = \pm r$ for $i = 1, \dots, 2g+2$ and that $|X(x)|$ cannot become smaller than $r$ for $x \notin I$. Hence the $g$ zeros of $S(x)$ belong necessarily to the compliment of $I$. Moreover no zero of $Y(x)$ is in $\mathbf{R} - I$. For otherwise the number of zeros of $X(x)$ would become smaller than $n$. This completes the proof of the lemma.

Now suppose that a monic polynomial $p(x)$ of degree $n$ satisfies the inequality $\max\{|p(x)|;\ x \in I\} < r$. Then $q(x) = X(x) - p(x)$ is a polynomial of degree less than $n$. Since $|p(x)| < r$ holds for any $x \in I$, we see that

$$\begin{aligned} &\operatorname{sign}(q(a_i)) = \operatorname{sign}(X(a_i)), \qquad 1 \le i \le 2g+2 \\ &\operatorname{sign}(q(b_i)) = \operatorname{sign}(X(b_i)), \qquad g+1 \le j \le n-1. \end{aligned}$$

Hence $q(x)$ has as many real zeros as $X(x)$, but this is impossible because $\deg q(x) \le n-1 < n = \deg X(x)$. This completes the proof of Theorem 4.2.

Next, we show that certain important polynomials do satisfy Conditions (i) and (ii). Let $u$ be a variable and put $x = u + 1/u$. Then, for any positive integer $n$, there exists a monic polynomial $t_n(x)$ of degree $n$ such that $t_n(x) = u^n + 1/u^n$. Note that these polynomials are related with the usual Chebyshev polynomials $T_n(x)$ by the relation $2T_n(x/2) = t_n(x)$ for each $n$. Moreover they have a multiplicative property:

$$t_m(t_n(x)) = t_{mn}(x), \quad m, n \ge 1.$$

Hence we have a polynomial map of the hyperelliptic curve $y^2 = t_{2g+2}(x)$ to the conic $y^2 = x^2 - 2$ $(= t_2(x))$ defined by the rule: $(x, y) \mapsto (t_{g+1}(x), y)$. It follows from Theorem 2.1 that this map corresponds to a polynomial solution of the Diophantine equation $t_{2g+2}(x)Y^2 = X^2 - 2$. Indeed it is easy to see that $(X, Y) = (t_{g+1}(x), 1)$ satisfies this equation. (Note also that, by [**3**], this solution is primitive, namely, all the solutions are obtained from this by the multiplication rule in [**3**].) Moreover, as it is well-known, all the zeros of $t_n(x)$ are real and belong to the closed interval $[-2, 2]$. Actually they are given by

$$2\cos\frac{(2j-1)\pi}{2n}, \qquad j = 1, \dots, n.$$

Hence we obtain the following:

**Proposition 4.1.** *For any $g > 0$, there exists a polynomial $f(x)$ of degree $2g+2$ and a generalized Zolotarev polynomial of degree $g+1$ associated with $f(x)$ for which both of Conditions* (i) *and* (ii) *are satisfied. More precisely,*

*the "modified" Chebyshev polynomial* $t_{g+1}(x)$ *is a generalized Zolotarev polynomial and have the extremal property stated in Theorem* 4.2 *with*

$$I = \bigcup_{1 \le i \le g+1} \left[ 2\cos\frac{(4i-1)\pi}{4g+4},\ 2\cos\frac{(4i-3)\pi}{4g+4} \right],$$
$$r = \sqrt{2}.$$

## 5. Rational Zolotarev polynomials and multigrades.

In this section we investigate the following arithmetic problem:

Does there exist a generalized Zolotarev polynomial $X(x)$ of given degree $n$ if we impose the condition that the constant $r$, the zeros $a_i$, $1 \le i \le 2g+2$ of $f(x)$, and the branch points $b_j$, $g+1 \le j \le n-1$ over $\pm r$ of $X(x)$ should belong to a fixed number field $k$?

Let us call the minimal one in the set of such fields *the definition field* of the generalized Zolotarev polynomial. Therefore the definition field of the polynomial given in Proposition 4.1 is $\mathbf{Q}(\sqrt{2}, \zeta_{4g+4} + \zeta_{4g+4})$, where $\zeta_n$ denotes a primitive $n$-th root of unity. The most interesting problem is, consequently, whether or not a generalized Zolotarev polynomial defined over $\mathbf{Q}$ exists for any degree $n$. Such a polynomial will be called a *rational Zolotarev polynomial*. We will see that this is related with a classical object known as *multigrade*. Let us recall the definition.

**Definition 5.1.** For an arbitrary positive integer $n$, the system of equations

$$\begin{cases} x_1 + \cdots + x_n = y_1 + \cdots + y_n, \\ x_1^2 + \cdots + x_n^2 = y_1^2 + \cdots + y_n^2, \\ \vdots \\ x_1^{n-1} + \cdots + x_n^{n-1} = y_1^{n-1} + \cdots + y_n^{n-1} \end{cases}$$

is said to be a multigrade of degree $n$.

In order to formulate our result we define the *multiplicity* of a solution $(x_1, \ldots, x_n, y_1, \ldots, y_n) = (c_1, \ldots, c_n, d_1, \ldots, d_n)$ of a multigrade as the maximum of the times in which each rational number occurs in $(c_1, \ldots, c_n, d_1, \ldots, d_n)$. Our result is stated as follows:

**Proposition 5.1.** *There is a bijective correspondence between the set of rational Zolotarev polynomials of degree* $n$ *and the set of the rational solutions of multigrades of degree* $n$ *with multiplicity at most two.*

*Proof.* Let $X(x)$ be a rational Zolotarev polynomial of degree $n$ associated with a polynomial $f(x)$ so that the following equation holds:

$$f(x)Y(x)^2 = X(x)^2 - r^2$$

for some $r \in \mathbf{Q}$ and a polynomial $Y(x)$. It follows from the definition and Lemma 4.2.1 that $f(x) = \prod_{1\le i\le 2g+2}(x-a_i)$ and $Y(x) = \prod_{g+1\le j\le n-1}(x-b_j)$ for some $a_i, b_i \in \mathbf{Q}$ in the notation of the previous section. Note that the two sets $\{a_1, \dots, a_{2g+2}\}$ and $\{b_{g+1}, \dots, b_{n-1}\}$ have no common element, as is seen in the proof of Theorem 4.1. Since the factors $X(x)-r$ and $X(x)+r$ are relatively prime, we may assume (after renumbering if necessary) there exists an integer $m$ with $m \le n-(g+1)$ such that

$$X(x) - r = \prod_{1\le i\le n-2m}(x-a_i)\cdot \prod_{g+1\le j\le g+m}(x-b_j)^2,$$
$$X(x) + r = \prod_{n-2m+1\le i\le 2g+2}(x-a_i)\cdot \prod_{g+m+1\le j\le n-1}(x-b_j)^2.$$

Therefore their difference

$$\prod_{n-2m+1\le i\le 2g+2}(x-a_i)\cdot \prod_{g+m+1\le j\le n-1}(x-b_j)^2 - \prod_{1\le i\le n-2m}(x-a_i)\cdot \prod_{g+1\le j\le g+m}(x-b_j)^2$$

is a rational constant. This implies that, for each $k$ with $1 \le k \le n-1$, the $k$-th elementary symmetric function of

$$a_1, \dots, a_{n-2m}, b_{g+1}, b_{g+1}, b_{g+2}, \dots, b_{g+m}, b_{g+m} \tag{5.1}$$

and that of

$$a_{n-2m+1}, \dots, a_{2g+2}, b_{g+m+1}, b_{g+m+1}, b_{g+m+2}, \dots, b_{n-1}, b_{n-1} \tag{5.2}$$

coincides. Hence, for every $k$ with $1 \le k \le n-1$, the sum of $k$-th power of $n$ elements in (5.1) and that of $n$ elements in (5.2) are equal. In other words, the $2n$ rational number in (5.1) and (5.2) give rise to the rational solution of the multigrade of degree $n$ with multiplicity at most two. To prove the converse, suppose that $x_i = c_i$ $(1 \le i \le n)$, $y_i = d_i$ $(1 \le i \le n)$ constitute a rational solution of the multigrade of degree $n$ with multiplicity at most two. Then by the reason explained above there exists a rational constant $r$ such that

$$\prod_{1\le i\le n}(x-c_i) - \prod_{1\le i\le n}(x-d_i) = 2r.$$

Let us put

$$X(x) = \prod_{1\le i\le n}(x-c_i) - r = \prod_{1\le i\le n}(x-d_i) + r.$$

Then we have

$$X(x)^2 - r^2 = (X(x)-r)(X(x)+r) = \prod_{1\le i\le n}(x-c_i)\prod_{1\le i\le n}(x-d_i).$$

Since the multiplicity of the solution $x_i = c_i$ $(1 \le i \le n)$, $y_i = d_i$ $(1 \le i \le n)$ is assumed to be at most two, the product on the rightmost side can be expressed as

$$\prod_{1 \le i \le 2g+2} (x - a_i) \left( \prod_{g+1 \le j \le n-1} (x - b_j) \right)^2$$

for some $a_i \in \mathbf{Q}$, $1 \le i \le 2g+2$ and $b_j \in \mathbf{Q}$, $g+1 \le j \le n-1$. Therefore, if we put $f(x) = \prod_{1 \le i \le 2g+2}(x - a_i)$ and $Y(x) = \prod_{g+1 \le j \le n-1}(x - b_j)$, we have

$$f(x)Y(x)^2 = X(x) - r^2,$$

hence $X(x)$ is a rational Zolotarev polynomial of degree $n$. This completes the proof of Proposition 5.1.

## 6. Examples.

It follows from Theorem 3.1 that the construction of a generalized Zolotarev polynomial is equivalent to that of a hyperelliptic curve with a point which becomes a torsion point on its Jacobian variety. For the latter task, there are several article where the authors are interested in the existence of rational torsion points on the Jacobian variety of order as high as possible (see [**6**]). In view of the results in Sections 4 and 5, however, it might be of some interest to construct *rational* Zolotarev polynomials. Unfortunately, the hyperelliptic curves constructed in [**6**] do not provide us with rational Zolotarev polynomials. The purpose of this section is to give some examples of them.

In view of the results of the previous sections, the simpliest nontrivial examples of rational Zolotarev polynomials should come from the elliptic curve

$$y^2 + (1-c)xy - by = x^3 - bx^2, \quad b = c + c^2,\ c = (10 - 2\alpha)/(\alpha^2 - 9),$$

which has torsion structure $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and on which $(0, 0)$ is a torsion point of order six (see [**5**, Table 3]). (Note that a generalized Zolotarev polynomial of degree $g+1$ associated with a polynomial of degree $2g+2$ falls in the class of "nondegenerate" ones investigated in [**3**], and such a polynomial is easy to construct, even if we demand it to be a rational one.) By the coordinate change

$$\begin{cases} X = 4x, \\ Y = 8\left(y + \frac{(1-c)x - b}{2}\right), \end{cases}$$

it becomes an elliptic curve

$$E : Y^2 = X^3 + (-3c^2 - 6c + 1)X^2 - 8c(1 - c^2)X + 16c^2(1 + c)^2$$

with a torsion point $P = (0, -4b)$ of order six. To find the Zolotarev polynomial, we need a rational function $h$ on $E$ such that $3(P) - 3(-P) = (h)$. This can be readily found by the chord-tangent method as follows.

$$\begin{aligned}
&(P) + (P) - (2P) - (\infty) = (\ell_1/\ell_2),\\
&\qquad \text{with}\ \ \ell_1 = (1-c)X - Y - 4(c+c^2), \quad \ell_2 = X - 4(c+c^2),\\
&(2P) + (P) - (3P) - (\infty) = (\ell_3/\ell_4),\\
&\qquad \text{with}\ \ \ell_3 = (1+c)X - Y - 4(c+c^2), \quad \ell_4 = X - 4c,\\
&(3P) + (3P) - 2(\infty) = (X - 4c).
\end{aligned}$$

On the other hand, we have

$$3(P) + 3(-P) - 6(\infty) = (X^3).$$

Combining these, we obtain

$$3(P) - 3(-P) = (h),$$

where

$$h = \frac{\{(1-c)X - Y - 4(c+c^2)\}^2\{(1+c)X - Y - 4(c+c^2)\}^2}{\{X - 4(c+c^2)\}^2(X-4c)X^3}.$$

Furthermore, in order to map the two points $P, -P$ to the points above infinity $\infty_1, \infty_2$ of an elliptic quadratic curve, we change the coordinates by the formula

$$\begin{cases} x = \frac{1}{X}, \\ y = \frac{Y}{4c(c+1)X^2}. \end{cases}$$

Then we have

$$E' : y^2 = x^4 + \frac{c-1}{2c(c+1)}x^3 - \frac{3c^2+6c-1}{16c^2(c+1)^2}x^2 + \frac{1}{16c^2(c+1)^2}x$$

with

$$3(\infty_1) - 3(\infty_2) = (\tilde{h}),$$

where

$$\tilde{h} = \frac{\{4(c+c^2)x^2 - (1-c)x + 4(c+c^2)y\}^2\{4(c+c^2)x^2 - (1+c)x + 4(c+c^2)y\}^2}{\{4(c+c^2)x - 1\}^2(-4cx+1)x^2}.$$

Using the defining equation, this simplifies to

$$\tilde{h} = \frac{a^2 + 64c^2(c+1)^2y^2 + 64c^2(c+1)^2ay}{-4cx+1},$$

with $a = (4cx-1)(2(c+1)x+1)$. Composing this with the isomorphism $\mathbf{G}_m \to T$ defined by $t \mapsto ((1+t^2)/2t,\ (1-t^2)/2t)$, we obtain the polynomial

solution $(X(x), Y(x))$ of $T'$ corresponding to the torsion point $(\infty_1) - (\infty_2)$ of order three, where

$$\begin{aligned} X(x) &= -32c(c+1)^2x^3 + 8(-3c^2 - 2c + 1)x^2 + 8x + 1, \\ Y(x) &= -16c(c+1)(2(c+1)x + 1). \end{aligned}$$

Hence we obtain the primitive solution

$$\begin{cases} X_0(x) = x^3 + \dfrac{(3c-1)}{4c(c+1)}x^2 - \dfrac{1}{4c(c+1)^2}x - \dfrac{1}{32c(c+1)^2} \\ \qquad = x^3 + \dfrac{(\alpha+3)(\alpha-3)(\alpha^2+6\alpha-39)}{8(\alpha-5)(\alpha-1)^2}x^2 + \dfrac{(\alpha+3)^2(\alpha-3)^2}{8(\alpha-5)(\alpha-1)^2}x \\ \qquad\quad + \dfrac{(\alpha+3)(\alpha-3)^2}{64(\alpha-5)(\alpha-1)^2}. \\ Y_0(x) = x + \dfrac{1}{2(c+1)} \\ \qquad = x + \dfrac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2} \end{cases}$$

of the Diophantine equation $f(x)Y^2 = X^2 - r^2$, where

$$\begin{aligned} f(x) &= x^4 + \frac{c-1}{2c(c+1)}x^3 - \frac{3c^2+6c-1}{16c^2(c+1)^2}x^2 + \frac{1}{16c^2(c+1)^2}x \\ &= x\left(x + \frac{(\alpha+3)(\alpha-3)}{8(\alpha-5)}\right)\left(x + \frac{(\alpha+3)(\alpha-3)^2}{(\alpha-1)^2(\alpha-5)}\right) \\ &\quad \cdot \left(x + \frac{(\alpha+3)^2(\alpha-3)}{8(\alpha-1)^2}\right), \\ r &= \frac{1}{32c(c+1)^2} \\ &= \frac{(\alpha+3)^3(\alpha-3)^3}{64(\alpha-1)^4(5-\alpha)}. \end{aligned}$$

The rational solution of multligrade of degree 3 which corresponds to this Zolotarev polynomial is found as follows. Since

$$\begin{aligned} X_0(x) - r &= x\left(x + \frac{(\alpha+3)(\alpha-3)^2}{(\alpha-1)^2(\alpha-5)}\right)\left(x + \frac{(\alpha+3)^2(\alpha-3)}{8(\alpha-1)^2}\right), \\ X_0(x) + r &= x\left(x + \frac{(\alpha+3)(\alpha-3)}{8(\alpha-5)}\right)\left(x + \frac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2}\right)^2, \end{aligned}$$

we have

$$\left(\frac{(\alpha+3)(\alpha-3)}{8(\alpha-5)}\right)\left(x+\frac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2}\right)^2 - x\left(x+\frac{(\alpha+3)(\alpha-3)^2}{(\alpha-1)^2(\alpha-5)}\right)\left(x+\frac{(\alpha+3)^2(\alpha-3)}{8(\alpha-1)^2}\right) = \frac{(\alpha+3)^3(\alpha-3)^3}{32(\alpha-1)^4(5-\alpha)}.$$

This implies the equalities

$$\frac{(\alpha+3)(\alpha-3)}{8(\alpha-5)}+\frac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2}+\frac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2} = 0+\frac{(\alpha+3)(\alpha-3)^2}{(\alpha-1)^2(\alpha-5)}+\frac{(\alpha+3)^2(\alpha-3)}{8(\alpha-1)^2},$$

$$\left(\frac{(\alpha+3)(\alpha-3)}{8(\alpha-5)}\right)^2+\left(\frac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2}\right)^2+\left(\frac{(\alpha+3)(\alpha-3)}{2(\alpha-1)^2}\right)^2 = 0^2+\left(\frac{(\alpha+3)(\alpha-3)^2}{(\alpha-1)^2(\alpha-5)}\right)^2+\left(\frac{(\alpha+3)^2(\alpha-3)}{8(\alpha-1)^2}\right).$$

**Remark.** If one uses the one-parameter family of elliptic curves with torsion structure $\mathbf{Z}/8\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ listed in [**4**, Table 3], then one obtains a primitive rational Zolotarev polynomial of degree four in a similar way.

In [**6**], several examples of rational solutions of multigrades of degree up to ten. (As far as the author knows, "ten" is the largest degree among the known examples of the rational solutions.) We pick up some of these examples and compute the corresponding rational Zolotarev polynomials and hyperelliptic curves with torsion points.

(6.1) ([**6**, (4.4)]):

$$x^2(x-5)^2-(x+1)(x-2)(x-3)(x-6)=36.$$

Multigrade:

$$\begin{cases}0+0+5+5=(-1)+2+3+6,\\ 0^2+0^2+5^2+5^2=(-1)^2+2^2+3^2+6^2,\\ 0^3+0^3+5^3+5^3=(-1)^3+2^3+3^3+6^3.\end{cases}$$

Rational Zolotarev polynomial:

$$X(x)=x^4-10x^3+25x^2-18(-x^2(x-5)^2-18).$$

Hyperelliptic curve (elliptic curve in this case):

$$y^2=(x+1)(x-2)(x-3)(x-6),\qquad g=1,$$

the divisor $(\infty_1)-(\infty_2)$ has order four.

Extremal property:

$$\max_{p\in P_4}\{|p(x)|;\ x\in[-1,2]\cup[3,6]\}\geq 18,\quad \text{and}$$
$$\max_{x\in[-1,2]\cup[3,6]}\{|X(x)|\}=18.$$

(6.2) ([**8**, (4.5)]):

$$x^2(x+7)^2(x-7)^2-(x+8)(x+5)(x+3)(x-3)(x-5)(x-8)$$
$$=5!\cdot 2^3\cdot 3\cdot 5.$$

Multigrade:

$$\begin{cases}0+0+(-7)+(-7)+7+7=(-8)+(-5)+(-3)+3+5+8,\\ 0^2+0^2+(-7)^2+(-7)^2+7^2+7^2=(-8)^2+(-5)^2+(-3)^2+3^2+5^2+8^2,\\ 0^3+0^3+(-7)^3+(-7)^3+7^3+7^3=(-8)^3+(-5)^3+(-3)^3+3^3+5^3+8^3,\\ 0^4+0^4+(-7)^4+(-7)^4+7^4+7^4=(-8)^4+(-5)^4+(-3)^4+3^4+5^4+8^4,\\ 0^5+0^5+(-7)^5+(-7)^5+7^5+7^5=(-8)^5+(-5)^5+(-3)^5+3^5+5^5+8^5.\end{cases}$$

Rational Zolotarev polynomial:

$$X(x)=x^3(x+7)^2(x-7)^2-5!\cdot 2^2\cdot 3\cdot 5.$$

Hyperelliptic curve:

$$y^2=(x+8)(x+5)(x+3)(x-3)(x-5)(x-8),\quad g=2,$$
the divisor $(\infty_1)-(\infty_2)$ has order six.

Extremal property:

$$\max_{p\in P_6}\{|p(x)|;\ x\in[-8,-5]\cup[-3,3]\cup[5,8]\}\geq 5!\cdot 2^2\cdot 3\cdot 5,\quad \text{and}$$
$$\max_{x\in[-8,-5]\cup[-3,3]\cup[5,8]}\{|X(x)|\}=5!\cdot 2^2\cdot 3\cdot 5.$$

(6.3) ([**8**, (4.7)]):

$$(x^2-5^2)(x^2-14^2)(x^2-23^2)(x^2-24^2)$$
$$-(x^2-2^2)(x^2-16^2)(x^2-21^2)(x^2-25^2)$$
$$=7!\cdot 2^4\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13.$$

Rational Zolotarev polynomial:

$$X(x)=(x^2-5^2)(x^2-14^2)(x^2-23^2)(x^2-24^2)-7!\cdot 2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13.$$

Hyperelliptic curve:

$$y^2 = (x^2-5^2)(x^2-14^2)(x^2-23^2)(x^2-24^2)$$
$$\cdot (x^2-2^2)(x^2-16^2)(x^2-21^2)(x^2-25^2), \quad g = 7,$$

the divisor $(\infty_1) - (\infty_2)$ has order eight.

Extremal property:

$$\max_{p \in P_8}\{|p(x)|;\ x \in [-25,-24] \cup [-23,-21] \cup [-16,-14] \cup [-5,-2]$$
$$\cup [2,5] \cup [14,16] \cup [21,23] \cup [24,25]\} \geq 7! \cdot 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,$$

the maximal of $X(x)$ on this union is equal to

$$7! \cdot 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13.$$

## References


[1] T.G. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math., **55** (1990), 259-266, MR 91h:11049, Zbl 728.14027.

[2] P. Erdös and G. Szegö, *On a problem of I. Schur*, Ann. of Math., **43** (1942), 451-470, Zbl 060.05503.

[3] F. Hazama, *Pell equations for polynomials*, Indag. Math., **8** (1997), 387-397, MR 99d:11068, Zbl 894.11008.

[4] F. Hirzebruch, T. Berger and R. Jung, *Manifolds and Modular Forms*, Vieweg, Braunschweig/Wiesbaden, 1994, MR 94d:57001, Zbl 767.57014.

[5] D.S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc., **33** (1976), 193-237, MR 55 #7910, Zbl 331.14010.

[6] F. Leprévost, *Sur une conjecture sur les points de torsion rationnels des Jacobiennes de courbes*, J. Reine Angew. Math., **473** (1996), 59-68, MR 97b:11085, Zbl 924.14015.

[7] F. Pakovitch, *Combinatoire des arbres planaires et arithmetique des courbes hyperelliptiques*, Ann. Inst. Fourier, **48** (1998), 323-351, MR 99h:11055, Zbl 911.14013.

[8] E. Rees and C. Smith, *On the constant in the Tarry-Escott problem*, in 'Cinquante Ans de Polynômes', Lecture Notes in Math., **1415**, Springer-Verlag, New York, 1990, MR 90j:00018, Zbl 683.00011.

[9] F.-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Math., **117**, Springer-Verlag, New York, 1988, MR 88i:14041, Zbl 703.14001.

[10] G. Shabat and A. Zvonkin, *Plane trees and algebraic numbers*, in 'Contemporary Math.', **178** (1994), 233-275, MR 96d:14028, Zbl 816.05024.

[11] S. Yuditskii, *Functions deviating least from zero on closed subset of the real exies*, S.-Peterbourg Math. J., **4** (1993), 201-249.

[12] B. Zhang, *Sur les Jacobiennes des courbes à singularitiés*, Manuscripta Math., **92** (1997), 1-12, MR 98b:14028, Zbl 893.14005.


Received July 20, 1999 and revised October 12, 1999.

Tokyo Denki University
Hatoyama, Saitama
350-0394, Japan