Алгебра и анализ
Том. 15 (2003), вып. 4

St. Petersburg Math. J.
Vol. 15 (2004), No. 4, Pages 587–602
S 1061-0022(04)00824-6
Article electronically published on July 7, 2004

PERIODS OF QUADRATIC IRRATIONALITIES, AND TORSION OF ELLIPTIC CURVES

V. A. MALYSHEV

Abstract. For rational A, B, C, D, the period length for the continued fraction of the square root

$$\sqrt{t^4+At^3+Bt^2+Ct+D}$$

can only take the values 1, 2, 3, 4, 5, 6, 8, 10, 14, 18, 22, and perhaps 9 and 11.

Introduction

By the Abel integrability criterion, for a polynomial

$$R=t^4+At^3+Bt^2+Ct+D$$

with distinct roots, a polynomial $\rho=at+b$ such that

$$\int\frac{\rho}{\sqrt{R}}\,dt=\ln\frac{P+\sqrt{R}Q}{P-\sqrt{R}Q}$$

with some polynomials P and Q exists if and only if the square root $\sqrt{R}$ has a periodic continued fraction expansion

$$\sqrt{R}=\varphi_0+\cfrac{1}{\varphi_1+\cfrac{1}{\varphi_2+\cfrac{1}{\varphi_3+\cdots}}}.$$

By the Abel periodicity criterion, the square root $\sqrt{R}$ has a periodic continued fraction expansion if and only if for the polynomial R the Abel equation

$$P^2-RQ^2=1$$

is solvable in the ring of polynomials. The polynomials P and Q in the integral

$$\int\frac{\rho}{\sqrt{R}}\,dt=\ln\frac{P+\sqrt{R}Q}{P-\sqrt{R}Q}$$

satisfy the Abel equation, and the polynomial ρ has the form

$$\rho=2\frac{P'}{Q}.$$

These statements were proved by Abel in [1].

Chebyshev observed a drawback of the Abel integrability criterion. The continued fraction expansion of the square root $\sqrt{R}$ may have an arbitrarily long period. Therefore, to use the integrability criterion we need to estimate the length of the period. In [2], Chebyshev obtained such an estimate for polynomials R with rational coefficients. In this connection Chebyshev supposed that for such polynomials the period of the continued

2000 *Mathematics Subject Classification.* Primary 14K20, 11A55.
Key words and phrases. Quadratic irrationalities, elliptic curves.

fraction expansion of the square root $\sqrt{R}$ may also be arbitrarily long. The explicit proof of Chebyshev's estimate was given by Zolotarev in [3].

Chebyshev reduced the problem to polynomials

$$R = t^4 + pt^2 + qt + r$$

with integral coefficients. The period of the continued fraction of the square root

$$\sqrt{t^4 + pt^2 + qt + r}$$

is estimated by the number n of solutions of the system of Diophantine equations

$$(x^2y^2 + 18xyz - 4x^3z - 4y^3 - 27z^2)z^2 = 16[(p^2 - 4r)^2 + 9pq^2]r - (4p^3 + 27q^2)q^2,$$
$$y^2 - 3xz = p^2 + 12r.$$

For this number Chebyshev obtained the estimate $n \le 12m$, where m is the number of quadratic divisors of the right-hand side of the first equation.

We shall prove that for the polynomials R with rational coefficients the length of the period of the square root $\sqrt{R}$ may take only finitely many values. Thus, Chebyshev's estimate solves the problem in principle, but is quite conservative.

By the *degree of the first solution of a polynomial* R, we mean the minimum integer n such that the Abel equation

$$P^2 - RQ^2 = 1$$

has a solution with a polynomial P of degree n. If for some R the Abel equation has no solution, then the degree of the first solution is not defined.

We shall prove that, for any polynomial R with rational coefficients, the degree of the first solution takes only 10 values:

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12.$$

The statement follows from a theorem of Mazur (see [4]). By that theorem, the order of a rational point on a rational elliptic curve takes precisely these 10 values. The length of the period can be expressed in terms of the degree of the first solution. As a result, for any polynomial R with rational coefficients the length of the period of the square root $\sqrt{R}$ may take only 14 values

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

Additional analysis shows that 7 is not realized by polynomials with rational coefficients. It is plausible that 9 and 11 are also not realized.

Now we list the integrals with rational coefficients that can be calculated by one logarithm. We split the set of integrals

$$\int \frac{\rho}{\sqrt{R}}\,dt = \ln\frac{P + \sqrt{R}Q}{P - \sqrt{R}Q}$$

into classes $J_2, J_3, \dots$, where the number of a class is the degree of the first solution of the polynomial R.

The class

$$J_2: \quad \int \frac{4t}{\sqrt{(t^2+u)^2+v}}\,dt = \int \frac{2}{\sqrt{(t^2+u)^2+v}}\,dt^2$$

was known to Euler. In [1], Abel constructed four classes

$$J_3: \quad \int \frac{6t+2u}{\sqrt{(t^2+ut)^2+vt}}\,dt,$$
$$J_4: \quad \int \frac{8t+2u}{\sqrt{(t^2+ut+v)^2-4uvt}}\,dt,$$
$$J_5: \quad \int \frac{10t+4u-2v}{\sqrt{(t^2+(u-v)t+uv)^2+4uv^2t}}\,dt,$$
$$J_6: \quad \int \frac{12t+12u+4v}{\sqrt{(t^2+4ut+2(v^2-u^2))^2-8(3u-v)(v^2-u^2)t}}\,dt.$$

In the classes J_2, J_3, J_4, J_5, J_6 the integrals admit a rational parametrization of the coefficients. There are exactly 5 more classes J_7, J_8, J_9 J_{10}, J_{12} that consist of integrals with rational parametrizations. This makes it possible to construct integrals with rational coefficients in the classes J_2, J_3, J_4, J_5, J_6, J_7, J_8, J_9, J_{10}, J_{12}. There are no integrals with rational coefficients in the classes J_{11}, J_{13}, J_{14}, $J_{15}\ldots$.

§1. Chebyshev transformation

In Chebyshev's theory, the main role is played by the transformation of polynomials

$$\mathcal{T}: t^4+At^3+Bt^2+Ct+D \longmapsto t^4+Lt^3+Mt^2+Nt,$$

where

$$L=-\frac{3A^4-16A^2B+16AC+16B^2-64D}{2(A^3-4AB+8C)},$$
$$M=\frac{3A^2-8B}{4},$$
$$N=-\frac{A^3-4AB+8C}{8}.$$

This transformation was found by Chebyshev and is called after him. Zolotarev [3] observed that the Chebyshev transformation arises from the Jacobi substitution

$$(at^2+2bt+c)z^2+2(a't^2+2b't+c')z+(a''t^2+2b''t+c'')=0$$

for an appropriate choice of the parameters a, b, c, a', b', c', a'', b'', c''.

The Chebyshev transformation is well defined only if $A^3-4AB+8C\neq 0$. To explain this, we write the identity

$$t^4+At^3+Bt^2+Ct+D$$
$$=\tau^4-\frac{3A^2-8B}{8}\tau^2+\frac{A^3-4AB+8C}{8}\tau-\frac{3A^4-16A^2B+64AC-256D}{256},$$

where

$$t=\tau-\frac{A}{4}.$$

This means that the Chebyshev transformation applies only to the polynomials that cannot be reduced to t^4+pt^2+q by translation.

Given a polynomial $f(t)$, we denote by $f_x(t)$ the polynomial $f_x(t)=f(t+x)$. Let $\rho(f,g)$ be the resultant of f and g. Observe that $\rho(f,g)=\rho(f_x,g_x)$ for all x.

Theorem 1. *The Chebyshev transformation is translation invariant.*

Proof. We must prove that $\mathcal{T}R = \mathcal{T}(R_x)$ for all x. Write

$$R_x = t^4 + A_x t^3 + B_x t^2 + C_x t + D_x,$$

where

$$\begin{aligned} A_x &= 4x + A, \\ B_x &= 6x^2 + 3Ax + B, \\ C_x &= 4x^3 + 3Ax^2 + 2Bx + C, \\ D_x &= x^4 + Ax^3 + Bx^2 + Cx + D. \end{aligned}$$

The relations

$$3A^2 - 8B = -\frac{\rho(R'', R'')}{144}$$

and

$$A^3 - 4AB + 8C = -\frac{\rho(R', R''')}{1728}$$

prove the identities

$$3A^2 - 8B = 3A_x^2 - 8B_x$$

and

$$A^3 - 4AB + 8C = A_x^3 - 4A_x B_x + 8C_x.$$

The identity

$$B^2 - 3AC + 12D = B_x^2 - 3A_x C_x + 12D_x$$

(which is easy to check) and the identity

$$3A^4 - 16A^2B + 16AC + 16B^2 - 64D = -\frac{\rho(R, R''')}{1296} + 16(B^2 - 3AC + 12D)$$

complete the proof. □

Theorem 2. *The Chebyshev transformation admits the invariants*

$$\begin{aligned} I_1(R) &= \rho(R, R'), \\ I_2(R) &= B^2 - 3AC + 12D, \\ I_3(R) &= 9ABC - 2B^3 - 27C^2 - 27A^2D + 72BD. \end{aligned}$$

Proof. We must prove that

$$\begin{aligned} I_1(R) &= I_1(\mathcal{T}R), \\ I_2(R) &= I_2(\mathcal{T}R), \\ I_3(R) &= I_3(\mathcal{T}R). \end{aligned}$$

Direct inspection shows that

$$I_1(R) = \frac{4I_2(R)^3 - I_3(R)^2}{27}.$$

Thus, only two identities need a proof. Since the Chebyshev transformation is translation invariant, the problem is reduced to the polynomials of the form

$$R = t^4 + Bt^2 + Ct + D.$$

In this case, the coefficients of the polynomial

$$\mathcal{T}R = t^4 + Lt^3 + Mt^2 + Nt$$

are of the form

$$L = -\frac{B^2 - 4D}{C}, \quad M = -2B, \quad N = -C,$$

and the identities

$$I_2(R) = I_2(\mathcal{T}R),$$
$$I_3(R) = I_3(\mathcal{T}R)$$

are trivial. □

Corollary. *If a polynomial R admits the Chebyshev transformation, then the polynomial R has mutually distinct roots if and only if $\mathcal{T}R$ has the same property.*

It is useful to note that

$$I_1(R) = I_1(R_x),$$
$$I_2(R) = I_2(R_x),$$
$$I_3(R) = I_3(R_x)$$

for all x. For a polynomial

$$R = t^4 + At^3 + Bt^2 + Ct,$$

the invariants of the Chebyshev transformation have the form

$$I_1(R) = (A^2B^2 + 18ABC - 4A^3C - 4B^3 - 27C^2)C^2,$$
$$I_2(R) = B^2 - 3AC,$$
$$I_3(R) = 9ABC - 2B^3 - 27C^2.$$

In the Introduction we already encountered the first and the second invariant; they are involved in Chebyshev's system of Diophantine equations. In Zolotarev's paper [3], these invariants were obtained by a bulky calculation.

Let

$$R = t^4 + At^3 + Bt^2 + Ct + D$$

be a polynomial with mutually distinct roots. With R we associate the elliptic curve

$$E^R: \quad 27Y^2 = X^3 - 3I_2(R)X - I_3(R).$$

The curve E^R is obtained by eliminating L from the system

$$\begin{cases} M^2 - 3LN = I_2(R), \\ 9LMN - 2M^3 - 27N^2 = I_3(R). \end{cases}$$

Therefore, the point (M, N) lies on the curve E^R.

Direct inspection shows that

$$\rho(H, H') = -729\rho(R, R'),$$

where

$$H = X^3 - 3I_2(R)X - I_3(R).$$

Consequently, the curve E^R is nonsingular. The group of the elliptic curve E will be denoted by $G(E)$. As usual, the zero element $\mathcal{O}$ is located at infinity.

Later we shall describe the relationship between the elliptic curve E^R and the quadratic irrationality $\sqrt{R}$. Here we only explain how the elliptic curve E^R is related to the Chebyshev transformation.

Theorem 3. *Let*

$$R = t^4 + At^3 + Bt^2 + Ct,$$
$$\mathcal{T}R = t^4 + Lt^3 + Mt^2 + Nt.$$

Then

$$(M, N) = 2(B, C)$$

on the elliptic curve E^R.

Proof. Obviously, the points (B, C) and (M, N) belong to E^R. It is easy to check that the tangent line to E^R at the point (B, C) has the form

$$X = B + 6\lambda,$$
$$Y = C + A\lambda.$$

Substituting X and Y in the equation of E^R, we obtain the parameter

$$\lambda_0 = \frac{A^2 - 4B}{8}.$$

Therefore, the tangent line intersects the curve at the third point

$$X_0 = \frac{3A^2 - 8B}{4},$$
$$Y_0 = \frac{A^3 - 4AB + 8C}{8}.$$

By the definition of the group law, we have

$$2(B, C) = (X_0, -Y_0) = (M, N).$$

This proves the theorem. □

§2. Zolotarev representation

In this section we give a generalization of Zolotarev's classical theorem about the representation of solutions of the Abel equation. The original theorem of Zolotarev looks like this.

For the polynomial

$$R = t(t - 1)(t - \alpha)(t - \beta),$$

where $1 < \alpha < \beta < \infty$, *the Abel equation*

$$P^2 - RQ^2 = 1$$

is solvable if and only if

$$\alpha = \mathrm{dn}^{-2}[rK(\kappa), \kappa],$$
$$\beta = \mathrm{cn}^{-2}[rK(\kappa), \kappa]$$

with rational $0 < r < 1$ *and real* $0 < \kappa < 1$.

In Zolotarev's theorem, it is essential that $t = 0$ is a root of R. The restrictions on the other three roots can be relaxed.

Suppose a polynomial

$$R = t^4 + At^3 + Bt^2 + Ct$$

has distinct roots. With R, we associate the elliptic curve

$$E_R : \quad Y^2 = 4X^3 - g_2X - g_3$$

with the invariants

$$g_2 = \frac{4}{3}\frac{I_2(R)}{C^2}, \qquad g_3 = \frac{4}{27}\frac{I_3(R)}{C^3}.$$

Simultaneously, with R we associate the Weierstrass function $\wp_R$ having the same invariants g_2 and g_3. We explain how the polynomials $t^3 + At^2 + Bt + C$ and $4X^3 - g_2X - g_3$ are related to each other. Put $t = \frac{1}{\tau}$. After division by C, the polynomial

$$t^3 + At^2 + Bt + C$$

becomes

$$\tau^3 + \frac{B}{C}\tau^2 + \frac{A}{C}\tau + \frac{1}{C}.$$

We put

$$\tau = X - \frac{1}{3}\frac{B}{C}.$$

After multiplying by 4, the polynomial

$$\tau^3 + \frac{B}{C}\tau^2 + \frac{A}{C}\tau + \frac{1}{C}$$

becomes

$$4X^3 - g_2X - g_3.$$

In particular, under a proper enumeration, the roots of the polynomials

$$t^3 + At^2 + Bt + C = (t - t_1)(t - t_2)(t - t_3)$$

and

$$4X^3 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3)$$

satisfy the relations

$$\frac{1}{t_k} = e_k - \frac{1}{3}\frac{B}{C},$$

where $k = 1, 2, 3$. Here

$$e_1 = \wp_R\left(\frac{\omega_1}{2}\right), \quad e_2 = \wp_R\left(\frac{\omega_1 + \omega_2}{2}\right), \quad e_3 = \wp_R\left(\frac{\omega_2}{2}\right),$$

where ω_1 and ω_2 are the periods of the Weierstrass function $\wp_R$.

In the paper [5] we proved the following statement.

For a polynomial

$$R = t^4 + At^3 + Bt^2 + Ct,$$

the Abel equation

$$P^2 - RQ^2 = 1$$

is solvable if and only if

$$\wp_R\left(\frac{k_1\omega_1 + k_2\omega_2}{2n}\right) = \frac{1}{3}\frac{B}{C}$$

with some integers k_1 and k_2.

As an easy consequence, we obtain the following statement.

For a polynomial

$$R = t^4 + At^3 + Bt^2 + Ct,$$

the degree of the first solution is equal to n if and only if

$$\wp_R\left(\frac{k_1\omega_1 + k_2\omega_2}{2n}\right) = \frac{1}{3}\frac{B}{C}$$

for some integers k_1 and k_2 such that $\gcd(n, k_1, k_2) = 1$.

It is useful to note that two elliptic curves are associated with the polynomial

$$R = t^4 + At^3 + Bt^2 + Ct.$$

Namely, these are the curves

$$2E^R: \qquad 27Y^2 = X^3 - 3I_2(R)X - I_3(R),$$

$$E_R: \qquad Y^2 = 4X^3 - \frac{4}{3}\frac{I_2(R)}{C^2}X - \frac{4}{27}\frac{I_3(R)}{C^3}.$$

The linear mapping

$$(X, Y) \longmapsto \left(3CX, \frac{1}{2}C^{3/2}Y\right)$$

is an isomorphism of the group $G(E_R)$ onto $G(E^R)$. Therefore, the elliptic curves E_R and E^R are practically identical. Nevertheless, these curves arise differently. The first arises from the Chebyshev transformation. The second arises from the Zolotarev representation.

§3. Quadratic irrationalities

Let

$$R = t^4 + At^3 + Bt^2 + Ct + D$$

be a polynomial with distinct roots. We expand the square root $\sqrt{R}$ in a continued fraction:

$$\sqrt{R} = \varphi_0 + \cfrac{1}{\varphi_1 + \cfrac{1}{\varphi_2 + \cfrac{1}{\varphi_3 + \cdots}}}.$$

Consider the numerators and denominators of the convergents

$$P_{-2} = 0, \qquad P_{-1} = 1, \qquad P_k = \varphi_k P_{k-1} + P_{k-2},$$
$$Q_{-2} = 1, \qquad Q_{-1} = 0, \qquad Q_k = \varphi_k Q_{k-1} + Q_{k-2}.$$

Suppose that $\sqrt{R}$ has a periodic continued fraction. Then among the polynomials $\varphi_1, \varphi_2, \dots$ there is a polynomial of degree two. The number m of the first polynomial of degree two in the sequence $\varphi_1, \varphi_2, \dots$ will be called the *number of the first solution*. We use this term because the polynomials P_{m-1} and Q_{m-1} satisfy the Abel equation

$$P_{m-1}^2 - RQ_{m-1}^2 = \text{const}$$

with some nonzero constant. Since $\deg \varphi_0 = 2$, the integer

$$n = m + 1 = \deg P_{m-1}$$

is the degree of the first solution of the polynomial R. In accordance with the parity of m and the value of const, we have three cases:

- if m is even, then the period has the form $\varphi_1, \dots, \varphi_m$;
- if m is odd and const $\neq -1$, then the period has the form $\varphi_1, \dots, \varphi_{2m}$;
- if m is odd and const $= -1$, then the period has the form $\varphi_1, \dots, \varphi_m$.

This was proved in [5]. The following statement is our aim in the present paper.

Theorem 4. *For a polynomial*

$$R = t^4 + At^3 + Bt^2 + Ct + D$$

with distinct roots, let n be the degree of the first solution. Then the point (M, N) with the coordinates

$$M = \frac{3A^2 - 8B}{4}, \quad N = -\frac{A^3 - 4AB + 8C}{8}$$

has order n on the elliptic curve

$$27Y^2 = X^3 - 3I_2(R)X - I_3(R).$$

Proof. Obviously, for any x the degree of the first solution of the polynomial R_x is equal to n. Formulas for the coefficients of the polynomial

$$R_x = t^4 + A_x t^3 + B_x t^2 + C_x t + D_x$$

were given in the proof of Theorem 1.

1^0. Suppose the polynomial R does not admit the Chebyshev transformation. Then $N = 0$. We claim that the degree of the first solution is $n = 2$. Indeed, let $x = -\frac{A}{4}$. Then $A_x = 0$ and $C_x = 0$. Consequently,

$$R_x = t^4 + B_x t^2 + D_x.$$

We write

$$R_x = (t^2 + p)^2 + q.$$

Since $q \neq 0$, the relation

$$(t^2 + p)^2 - R_x = -q$$

implies that $n = 2$. Since $N = 0$, we have

$$C = -\frac{A^3 - 4AB}{8}.$$

It is easy to verify that

$$M^3 - 3I_2(R)M - I_3(R) = 0.$$

Therefore, the point $(M, 0)$ lies on the curve E^R. The order of such a point $(M, 0)$ is $n = 2$. This proves the claim.

2^0. Suppose the polynomial R admits the Chebyshev transformation. Let x be any root of R. Then the polynomial R_x has the form

$$R_x = t^4 + A_x t^3 + B_x t^2 + C_x t.$$

Consider the polynomial

$$H = \mathcal{T} R_x = t^4 + Lt^3 + Mt^2 + Nt.$$

With R_x, we associate the Weierstrass function $\wp_{R_x}$ with invariants

$$g_2 = \frac{4}{3}\frac{I_2(R)}{C_x^2}, \qquad g_3 = \frac{4}{27}\frac{I_3(R)}{C_x^3}$$

and periods ω_1 and ω_2. Similarly, with H we associate the Weierstrass function $\wp_H$ with invariants

$$G_2 = \frac{4}{3}\frac{I_2(R)}{N^2}, \qquad G_3 = \frac{4}{27}\frac{I_3(R)}{N^3}$$

and periods Ω_1 and Ω_2. From the relations

$$G_2 = \lambda^2 g_2, \quad G_3 = \lambda^3 g_3,$$

where

$$\lambda = \frac{C_x}{N},$$

we obtain

$$\Omega_1 = \frac{\omega_1}{\sqrt{\lambda}}, \quad \Omega_2 = \frac{\omega_2}{\sqrt{\lambda}}.$$

Hence,

$$\wp_H\left(\frac{u}{\sqrt{\lambda}}\right) = \lambda \wp_{R_x}(u).$$

By assumption, the degree of the first solution of the polynomial R_x is equal to n. Consequently,

$$\wp_{R_x}(u_0) = \frac{1}{3}\frac{B_x}{C_x},$$

where

$$u_0 = \frac{k_1\omega_1 + k_2\omega_2}{2n}$$

with integers k_1 and k_2 such that $\gcd(k_1, k_2, n) = 1$. Using the duplication formula

$$\wp_{R_x}(2u) = \frac{1}{16}\frac{16\wp_{R_x}^4(u) + 8g_2\wp_{R_x}^2(u) + 32g_3\wp_{R_x}(u) + g_2^2}{4\wp_{R_x}^3(u) - g_2\wp_{R_x}(u) - g_3},$$

we obtain

$$\wp_{R_x}(2u_0) = \frac{1}{3}\frac{M}{C_x} = \frac{1}{3\lambda}\frac{M}{N}.$$

Thus,

$$\frac{1}{3}\frac{M}{N} = \lambda\wp_{R_x}(2u_0) = \wp_H\left(\frac{2u_0}{\sqrt{\lambda}}\right),$$

whence

$$\wp_H\left(\frac{k_1\Omega_1 + k_2\Omega_2}{n}\right) = \frac{1}{3}\frac{M}{N}.$$

Let $\mathbb{T}^2$ be the group $\mathbb{C}^2$ modulo the lattice generated by the periods Ω_1 and Ω_2. Obviously, the point

$$\frac{k_1\Omega_1 + k_2\Omega_2}{n}$$

is of order n in the group $\mathbb{T}^2$. The mapping

$$u \longmapsto (\wp_H(u), \wp_H'(u))$$

is an isomorphism of $\mathbb{T}^2$ onto the group $G(E_H)$ of the elliptic curve

$$E_H: \quad Y^2 = 4X^3 - G_2X - G_3.$$

In particular,

$$\frac{k_1\Omega_1 + k_2\Omega_2}{n} \longmapsto (X_0, Y_0),$$

where

$$X_0 = \frac{1}{3}\frac{M}{N},$$
$$Y_0 = \frac{2}{3}\frac{(M^3 - 3I_2(R)M - I_3(R))^{1/2}}{3^{1/2}N^{3/2}}.$$

Therefore, the point (X_0, Y_0) has order n in the group $G(E_H)$. The mapping

$$(X, Y) \longmapsto (U, V),$$

where

$$U = 3NX, \qquad V = \frac{1}{2}N^{3/2}Y,$$

is an isomorphism of the group $G(E_H)$ onto the group $G(E^H)$ of the elliptic curve

$$E^H: \quad 27V^2 = U^3 - 3I_2(R)U - I_3(R).$$

Let

$$(X_0, Y_0) \longmapsto (U_0, V_0).$$

Then the point $(M, N) = (U_0, V_0)$ is of order n in the group $G(E^H) = G(E^R)$. □

Corollary 1. *For a polynomial R with rational coefficients, the degree of the first solution n may be equal only to*

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 12.$$

Indeed, the rational point (M, N) lies on the rational elliptic curve E^R. By the Mazur theorem, the order of the point (M, N) on the elliptic curve E^R may only take one of these values.

Corollary 2. *For a polynomial R with rational coefficients, the period of the continued fraction of the square root $\sqrt{R}$ may be only of length*

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

Put $m = n - 1$. If the degree of the first solution takes the odd values $n = 3,\ 5,\ 7,\ 9$, then the period takes the even values $m = 2,\ 4,\ 6,\ 8$. If the degree of the first solution takes the even values $n = 2,\ 4,\ 6,\ 8,\ 10,\ 12$, then the period takes the even values $2m = 2,\ 6,\ 10,\ 14,\ 18,\ 22$ or the odd values $m = 1,\ 3,\ 5,\ 7,\ 9,\ 11$.

Example. For the polynomial

$$(t^2 + 3t + 30)^2 + 360t,$$

the degree of the first solution equals 12, and the square root

$$\sqrt{(t^2 + 3t + 30)^2 + 360t}$$

has a continued fraction with period length 22. In particular, the point

$$(M, N) = (-111, -360)$$

is of order 12 on the elliptic curve

$$27Y^2 = X^3 - 17523X + 2921778.$$

§4. Rational parametrizations

Two questions arise: which degrees of the first solutions

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12$$

and which period lengths

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

can be realized by polynomials R with rational coefficients?

Answers: the degrees 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 and the lengths 1, 2, 3, 4, 5, 6, 8, 10, 14, 18, 22 admit such a realization. The length 7 has no realization. The question about the lengths 9 and 11 is open.

Given a polynomial

$$R = t^4 + At^3 + Bt^2 + Ct + D,$$

we write the identity

$$t^4 + At^3 + Bt^2 + Ct + D = \left(t^2 + \frac{A}{2}t + \frac{4B - A^2}{8}\right)^2 + \frac{A^3 - 4AB + 8C}{8}t - \frac{A^4 - 8A^2B + 16B^2 - 64D}{64}.$$

If

$$A^3 - 4AB + 8C = 0,$$

then an appropriate translation transforms R to

$$(t^2 + x)^2 + y.$$

The degree of the first solution of this polynomial is 2.

If $A^3 - 4AB + 8C \neq 0$, then a translation transforms R to

$$(t^2 + xt + y)^2 + zt.$$

We consider this case in more detail. With the polynomial $R = (t^2 + xt + y)^2 + zt$, we associate the polynomial

$$R_* = (1 + x\tau + y\tau^2)^2 + z\tau^3.$$

Using the expansion

$$\sqrt{R_*} = 1 + \lambda_{-1}\tau + \lambda_0\tau^2 + \lambda_1\tau^3 + \lambda_2\tau^4 + \lambda_3\tau^5 + \lambda_4\tau^6 + \lambda_5\tau^7 + \cdots,$$

we introduce the Hankel determinants

$$\Delta_m = \begin{vmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_m \\ \lambda_2 & \lambda_3 & \cdots & \lambda_{m+1} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_m & \lambda_{m+1} & \cdots & \lambda_{2m-1} \end{vmatrix}.$$

The first five determinants look like this:

$$\begin{aligned} \Delta_1 &= 2^{-1}z, \\ \Delta_2 &= -2^{-2}z^2y, \\ \Delta_3 &= -2^{-7}z^4(z + 4xy), \\ \Delta_4 &= -2^{-12}z^6(z^2 + 4xyz - 16y^3), \\ \Delta_5 &= 2^{-16}yz^9(z^2 + 6xyz + 8y^2x^2 - 8y^3). \end{aligned}$$

In [5] it was proved that, for the polynomial $R = (t^2 + xt + y)^2 + zt$, the degree of the first solution is equal to $n \geq 3$ if and only if

$$\Delta_1 \neq 0, \ \ldots, \ \Delta_{n-2} \neq 0 \ \text{ and } \ \Delta_{n-1} = 0.$$

Putting $n = 3, 4, 5, 6, 7, 8, 9, 10, 12$ we calculate the factors of the determinants Δ_{n-1} that are not involved in the determinants with smaller indices. These factors are as follows:

$$\begin{aligned} F_3 &= y, \\ F_4 &= z + 4xy, \\ F_5 &= z^2 + 4xyz - 16y^3, \\ F_6 &= z^2 + 6xyz - 8y^3 + 8x^2y^2, \\ F_7 &= z^4 + 12xyz^3 + 48x^2y^2z^2 + 16y^3z^2 + 64xy^4z - 256y^6 + 64x^3y^3z, \\ F_8 &= z^4 + 8xyz^3 - 64y^3z^2 + 16x^2y^2z^2 - 320xy^4z + 512y^6 - 256x^2y^5, \\ F_9 &= 3z^6 + 48xyz^5 + 304x^2y^2z^4 - 64y^3z^4 + 960x^3y^3z^3 - 576xy^4z^3 + 1536x^4y^4z^2 \\ &\quad - 1536x^2y^5z^2 + 768y^6z^2 + 3072xy^7z + 1024x^5y^5z - 1024x^3y^6z - 4096y^9, \\ F_{10} &= z^6 + 20xyz^5 + 160x^2y^2z^4 + 80y^3z^4 + 640x^3y^3z^3 + 960xy^4z^3 + 4096x^2y^5z^2 \\ &\quad - 1280y^6z^2 + 1280x^4y^4z^2 + 1024x^5y^5z + 7168x^3y^6z \\ &\quad - 8192xy^7z + 4096y^7x^4 + 4096y^9 - 12288x^2y^8, \\ F_{12} &= z^8 + 20xyz^7 + 168x^2y^2z^6 - 32y^3z^6 + 768x^3y^3z^5 - 352xy^4z^5 + 1280y^6z^4 \\ &\quad + 2048x^4y^4z^4 - 1152x^2y^5z^4 + 3072x^5y^5z^3 + 10240xy^7z^3 - 512x^3y^6z^3 \\ &\quad + 2048x^4y^7z^2 + 20480x^2y^8z^2 + 2048x^6y^6z^2 - 20480y^9z^2 - 90112xy^{10}z \\ &\quad - 32768x^2y^{11} + 98304y^{12}. \end{aligned}$$

To solve the problem about the degrees, we must find rational points (x, y, z) on the varieties

$$F_n(x, y, z) = 0.$$

The first four varieties

$$F_3(x,y,z)=0,$$
$$F_4(x,y,z)=0,$$
$$F_5(x,y,z)=0,$$
$$F_6(x,y,z)=0$$

were constructed by Abel [1]. These varieties have rational parametrizations:

$$\begin{cases} x=u,\\ y=0,\\ z=v, \end{cases} \qquad \begin{cases} x=u,\\ y=v,\\ z=-4uv, \end{cases} \qquad \begin{cases} x=u-v,\\ y=uv,\\ z=4uv^2, \end{cases} \qquad \begin{cases} x=4u,\\ y=2(v^2-u^2),\\ z=8(v-3u)(v^2-u^2). \end{cases}$$

This gives all polynomials

$$R=(t^2+xt+y)^2+zt$$

for which the degree of the first solution is $n=3,4,5,6$.

Obviously,

$$F_7(\lambda x,\lambda^2 y,\lambda^3 z)=\lambda^{12}F_7(x,y,z),$$
$$F_8(\lambda x,\lambda^2 y,\lambda^3 z)=\lambda^{12}F_8(x,y,z),$$
$$F_9(\lambda x,\lambda^2 y,\lambda^3 z)=\lambda^{18}F_9(x,y,z),$$
$$F_{10}(\lambda x,\lambda^2 y,\lambda^3 z)=\lambda^{18}F_{10}(x,y,z),$$
$$F_{12}(\lambda x,\lambda^2 y,\lambda^3 z)=\lambda^{24}F_{12}(x,y,z).$$

It is easy to show that there are no nontrivial rational points on the algebraic curves

$$F_7(0,y,z)=0,$$
$$F_8(0,y,z)=0,$$
$$F_9(0,y,z)=0,$$
$$F_{10}(0,y,z)=0,$$
$$F_{12}(0,y,z)=0.$$

Therefore, in order to find polynomials R with the degree of the first solution $n=7,8,9,10,12$, we must find rational points on the algebraic curves

$$F_7(1,y,z)=0,$$
$$F_8(1,y,z)=0,$$
$$F_9(1,y,z)=0,$$
$$F_{10}(1,y,z)=0,$$
$$F_{12}(1,y,z)=0.$$

N. Tzanakis and D. Poulakis have drawn the author's attention to the fact that the the first two curves have genus 0. It can be checked that all five curves have genus 0. Any curve of genus 0 has a rational parametrization. This gives all polynomials

$$R=(t^2+xt+y)^2+zt$$

with the degree of the first solution $n=7,8,9,10,12$.

For example, the curve

$$F_7(1,y,z)=z^4+12yz^3+48y^2z^2+16y^3z^2+64y^4z-256y^6+64y^3z=0$$

admits the parametrization

$$y=-4\frac{v^2(9v+1)(7v+1)}{(31v^2+12v+1)^2},\qquad z=16\frac{v^2(9v+1)(7v+1)^3}{(31v^2+12v+1)^3},$$

and the curve

$$F_8(1,y,z)=z^4+8yz^3-64y^3z^2+16y^2z^2-320y^4z+512y^6-256y^5=0$$

admits the parametrization

$$y=\frac{1}{2}\frac{v(4v+1)(2v+1)^2}{(2v^2+4v+1)^2},\qquad z=-2\frac{v(3v+1)(4v+1)(2v+1)^3}{(2v^2+4v+1)^3}.$$

Therefore, the variety

$$F_7(x,y,z)=z^4+12xyz^3+48x^2y^2z^2+16y^3z^2+64xy^4z-256y^6+64x^3y^3z=0$$

admits the parametrization

$$x=u,\qquad y=-4u^2\frac{v^2(9v+1)(7v+1)}{(31v^2+12v+1)^2},\qquad z=16u^3\frac{v^2(9v+1)(7v+1)^3}{(31v^2+12v+1)^3},$$

and the variety

$$F_8(x,y,z)=z^4+8xyz^3-64y^3z^2+16x^2y^2z^2-320xy^4z+512y^6-256x^2y^5=0$$

admits the parametrization

$$x=u,\qquad y=\frac{1}{2}u^2\frac{v(4v+1)(2v+1)^2}{(2v^2+4v+1)^2},\qquad z=-2u^3\frac{v(3v+1)(4v+1)(2v+1)^3}{(2v^2+4v+1)^3}.$$

In particular, this allows us to construct the classes J_7 and J_8 of integrals

$$\int\frac{at+b}{\sqrt{(t^2+xt+y)^2+zt}}\,dt.$$

In the classes J_7 and J_8, the coefficients have the form

$$\begin{cases}a=14,\\ b=4u\dfrac{29v^2+12v+1}{31v^2+12v+1},\\ x=u\\ y=-4u^2\dfrac{v^2(9v+1)(7v+1)}{(31v^2+12v+1)^2},\\ z=16u^3\dfrac{v^2(9v+1)(7v+1)^3}{(31v^2+12v+1)^3},\end{cases}\qquad\begin{cases}a=16,\\ b=4u\dfrac{v^2+4v+1}{2v^2+4v+1},\\ x=u,\\ y=\dfrac{1}{2}u^2\dfrac{v(4v+1)(2v+1)^2}{(2v^2+4v+1)^2},\\ z=-2u^3\dfrac{v(3v+1)(4v+1)(2v+1)^3}{(2v^2+4v+1)^3}.\end{cases}$$

Remark. The algebraic curves

$$F_n(1,y,z)=0$$

can be defined for all degrees $n\geq 3$. The curves with $n=3,4,5,6,7,8,9,10,12$ have genus 0. The other curves have genus ≥ 1. The curve with $n=11$ has genus 1, the curve with $n=13$ has genus 2, and so on.

For $n=2$ the square root

$$\sqrt{(t^2+x)^2+y}$$

has a period of length 2 if $y\neq 1$, and it has a period of length 1 if $y=1$.

For $n\geq 3$ we consider the cases of odd n and even n separately. Let $n=3,5,7,9$, and let (x,y,z) be a point on the variety

$$F_n(x,y,z)=0.$$

Then the square root

$$\sqrt{(t^2+xt+y)^2+zt}$$

has a period of length $m=n-1$.

The curve

$$P_{m-1}^2 - RQ_{m-1}^2 = -1$$

on the variety

$$F_{m+1}(x,y,z)=0$$

will be called the *special curve*. Here P_{m-1}/Q_{m-1} is a convergent of the square root $\sqrt{R}$.

Let $n=4,6,8,10,12$, and let (x,y,z) be a point on the variety

$$F_n(x,y,z)=0.$$

If (x,y,z) does not lie on the special curve, then the square root

$$\sqrt{(t^2+xt+y)^2+zt}$$

has a period of length $2m=2(n-1)$. If (x,y,z) lies on the special curve, then the square root

$$\sqrt{(t^2+xt+y)^2+zt}$$

has a period of length $m=n-1$.

For $m=3$ and $m=5$, the special curves admit the following rational parametrizations:

$$\begin{cases} x=u, \\ y=1/(4u^2), \\ z=-1/u, \end{cases} \qquad \begin{cases} x=2u^3-1/(2u), \\ y=u^2(4u^4+1), \\ z=2u(4u^4+1). \end{cases}$$

This allows us to construct all square roots

$$\sqrt{(t^2+xt+y)^2+zt}$$

with periods of length 3 and 5.

We show that for $m=7$ the special curve has no rational points. Indeed, if we substitute the rational parametrization of the variety

$$F_8(x,y,z)=0$$

in

$$P_6^2 - RQ_6^2 = -1,$$

we obtain the equation

$$16(2v+1)(4v+1)(3v+1)^4v^2u^4+(2v^2+4v+1)^4=0.$$

Suppose this equation has rational solutions v and u. Then

$$vu(3v+1)(2v^2+4v+1)\neq 0.$$

Consequently, the equation

$$(2v+1)(4v+1)v^2+w^4=0$$

has rational solutions $v\neq 0$ and $w\neq 0$. Since $v\neq -1/3$, we have $v\neq w$. Putting $v=p/q$ and $w=r/q$, we see that the equation

$$(2p+q)(4p+q)p^2+r^4=0$$

has integral solutions $p\neq 0, r\neq 0, q\neq 0$ such that $p\neq r$. From the identity

$$q=-3p\pm\sqrt{\frac{p^4-r^4}{p^2}}$$

it follows that the equation

$$r^4 + p^2 s^2 = p^4$$

has integral solutions $p \neq 0, r \neq 0, s \neq 0$. Putting $X = r/p$ and $Y = s/p$, we conclude that the equation

$$X^4 + Y^2 = 1$$

has rational solutions $X \neq 0$ and $Y \neq 0$. This is a contradiction: the above equation does not admit such solutions.

References

[1] N. H. Abel, *Ueber die Integration der Differentialformel* $\frac{\rho dx}{\sqrt{R}}$, *wenn* R *und* ρ *ganze Functionen sind*, J. Reine Angew. Math. **1** (1826), 185–221.

[2] P. L. Chebyshev, *On integration of irrational differentials*, Selected Works, Akad. Nauk SSSR, Moscow, 1955, pp. 227–255. (Russian) MR 0067792 (16:781k)

[3] E. I. Zolotarev, *Sur la méthode d'intégration de M. Tchébycheff*, Complete Works. Issue 1, Akad. Nauk SSSR, Leningrad, 1931, pp. 161–360.

[4] B. Mazur, *Rational points on modular curves*, Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., vol. 601, Springer, Berlin, 1977, pp. 107–148. MR 0450283 (56:8579)

[5] V. A. Malyshev, *The Abel equation*, Algebra i Analiz **13** (2001), no. 6, 1–55; English transl., St. Petersburg Math. J. **13** (2002), no. 6, 893–938. MR 1883839 (2003a:14064)

Rybinsk State Aviation Technology Academy, Rybinsk, Russia
E-mail address: wmal@ryb.adm.yar.ru

Received 10/MAR/2003

Translated by THE AUTHOR