ORDERS OF THE TORSION OF POINTS OF CURVES OF GENUS 1

V. A. Dem'yanenko

UDC 511.51

Let K be an algebraic number field of degree n; let be the number of divisor classes of the field K; $\mathcal{C}: v^2=u^4+au^2+b$ is the Jacobian curve over K; $b(a^2-4b)=c^2\prod_{i=1}^{N}q_i$, where c is an integral divisor, $q_1,\ldots,q_N$ are distinct prime divisors. One proves that there exists an effectively computable constant $C=C(n,h(K),N)$, such that the order m of the torsion of any primitive K-point on $\mathcal{C}$ is bounded by it: $m\leqslant C$.

Let $\mathcal{K}$ be an algebraic number field of degree n; let $h(\mathcal{K})$ be the number of the divisor classes of the field $\mathcal{K}$; let $\mathcal{C}$ and $\mathcal{H}$ be the Jacobi curve

$$v^2=u^4+au^2+b$$

and the elliptic curve

$$y^2=x^3+rx+s,$$

respectively, defined over the ring of integers from $\mathcal{K}$.

In [2] one has proved the uniform boundedness of the torsion of the elliptic curves over an arbitrary $\mathcal{K}$; unfortunately, the proof given there is very cumbersome. In [3], Mazur has made a complete investigation of the torsion of the curve $\mathcal{H}$ in the case when $\mathcal{K}=\mathbb{Q}$, the field of rational numbers; one does not succeed to generalize those arguments to a field $\mathcal{K}$ of degree $n>1$.

The purpose of this paper is to give a simple proof of the following proposition.

THEOREM. Let

$$\mathcal{C}: v^2=u^4+au^2+b$$

be a Jacobi curve over the field $\mathcal{K}$;

$$b(a^2-4b)=c^2\prod_{i=1}^{N}q_i,$$

where c is an integer divisor, q_i $(i=1,2,\ldots,N)$ are distinct prime divisors. Then there exists an effectively computable constant $C=C(n,h(\mathcal{K}),N)$, depending only on n, $h(\mathcal{K})$, and N, such that the order m of any primitive $\mathcal{K}$-point on $\mathcal{C}$ is bounded by it: $m<C$.

In particular, this theorem yields a simple proof for the uniform boundedness of the torsions of the Jacobi curves in the formulation indicated by N. G. Chebotarev in his remarks to the Russian edition of Galois' works [1] (see, in particular, p. 240).

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova, AN SSSR, Vol. 82, pp. 5-28, 1979.

0090-4104/82/1806-0843$07.50

From this theorem, at the end of this paper, one derives a corollary regarding the torsion of elliptic curves.

Thus, let $\mathcal{G}$ be the curve $v^2=u^4+au^2+b$ and let $\mathcal{P}$ be a point on it taken in an arbitrary manner. First we note that if $t\mathcal{P}=\{u_t, v_t\}$, then on the basis of the formulas for the addition of points on $\mathcal{G}$,

$$u_{2t}=\frac{u_t^4-b}{2u_tv_t}, \qquad v_{2t}=\frac{v_t^4-(a^2-4b)u_t^4}{4u_t^2v_t^2},$$

$$u_{2t+1}u_1=\frac{u_t^2u_{t+1}^2-b}{u_t^2-u_{t+1}^2}, \qquad v_{2t+1}v_1=\frac{v_t^2v_{t+1}^2-(a^2-4b)u_t^2u_{t+1}^2}{(u_t^2-u_{t+1}^2)^2}.$$

Therefore, to the coordinates u_t, v_t one can associate U_t, V_t, W_t by the following recursion formulas

$$\left.\begin{aligned} &U_{2t}=U_t^4-bW_t^4, \quad V_{2t}=V_t^4-(a^2-4b)U_t^4W_t^4, \quad W_{2t}=2U_tV_tW_t,\\ &U_{2t+1}U_1=U_t^2U_{t+1}^2-bW_t^2W_{t+1}^2,\\ &V_{2t+1}V_1=V_t^2V_{t+1}^2-(a^2-4b)U_t^2U_{t+1}^2W_t^2W_{t+1}^2,\\ &W_{2t+1}W_1=U_t^2W_{t+1}^2-U_{t+1}^2W_t^2. \end{aligned}\right\} \tag{1}$$

LEMMA 1.

$$\left.\begin{aligned} U_t&=U_1^{\frac{1-(-1)^t}{2}}\sum_{\substack{i,j,s=0\\ i+j+s=[t^2/4]}}^{[t^2/4]\ [t^2/8]\ [t^2/4]} a_{i,j,s}\alpha^i\beta^j\gamma^s,\\ V_t&=V_1^{\frac{1-(-1)^t}{2}}\sum_{\substack{i,j,s=0\\ i+j+s=[t^2/2]}}^{[t^2/2]\ [t^2/4]\ [t^2/2]} b_{i,j,s}\alpha^i\beta^j\gamma^s,\\ W_t&=(U_1V_1)^{\frac{1+(-1)^t}{2}}W_1\sum_{\substack{i,j,s=0\\ i+j+s=[t^2/4]-\frac{1+(-1)^t}{2}}}^{[t^2/4]-\frac{1+(-1)^t}{2}\ [t^2/8]\ [t^2/4]-\frac{1+(-1)^t}{2}} c_{i,j,s}\alpha^i\beta^j\gamma^s, \end{aligned}\right\} \tag{2}$$

where $\alpha=U_1^4$, $\beta=4aU_1^2W_1^2$, $\gamma=bW_1^4$, and $a_{i,j,s}$, $2b_{i,j,s}$, $c_{i,j,s}$ are integral rational numbers satisfying the conditions

$$a_{[t^2/4],0,0}=b_{[t^2/2],0,0}=1, \quad a_{0,0,[t^2/4]}=(-1)^{[t/2]}t, \quad a_{i,j,s}=(-1)^{[t/2]}c_{s,j,i}$$

for $t\not\equiv 0 \pmod 2$,

$$a_{t^2/4,0,0}=b_{t^2/2,0,0}=1, \quad c_{t^2/4-1,0,0}=t, \quad a_{i,j,s}=(-1)^{t/2}a_{s,j,i}, \quad c_{i,j,s}=(-1)^{t/2-1}c_{s,j,i}$$

for $t\equiv 0 \pmod 2$, $a_{i,j,0}=0$ (for all $j>0$), $b_{i,j,s}=b_{s,j,i}$.

Proof. We use the method of mathematical induction. For $t=1$ the validity of the lemma is obvious. We assume now that the lemma holds for all $t<N$. We show that in this case it holds also for $t=N$. On the basis of the recursion formulas (1) we have

$$U_N = U_{N/2}^4 - 6W_{N/2}^4,\quad V_N = V_{N/2}^4 - (a^2-4b)U_{N/2}^4 W_{N/2}^4,\quad W_N = 2U_{N/2}V_{N/2}W_{N/2}$$

for $N \equiv 0 \pmod 2$ and

$$\left.\begin{aligned} U_N U_1 &= U_{\frac{N}{2}}^2 U_{\frac{N+1}{2}}^2 - 6W_{\frac{N}{2}}^2 W_{\frac{N+1}{2}}^2, \\ V_N V_1 &= V_{\frac{N}{2}}^2 V_{\frac{N+1}{2}}^2 - (a^2-4b)U_{\frac{N-1}{2}}^2 U_{\frac{N+1}{2}}^2 W_{\frac{N-1}{2}}^2 W_{\frac{N+1}{2}}^2, \\ W_N W_1 &= U_{\frac{N-1}{2}}^2 W_{\frac{N+1}{2}}^2 - U_{\frac{N+1}{2}}^2 W_{\frac{N-1}{2}}^2 \end{aligned}\right\} \qquad (3)$$

for $N \not\equiv 0 \pmod 2$. Let $t = (N \pm e)/2$, where e is the absolute smallest residue of the number N modulo 2. Since $t < N$, we have, by assumption,

$$\left.\begin{aligned} U_t &= U_1^{\frac{1-(-1)^t}{2}} \sum_{\substack{i+j+s=[t^2/4] \\ i=0}}^{[t^2/4]} \sum_{j=0}^{[t^2/8]} \sum_{s=0}^{[t^2/4]} a_{i,j,s}\alpha^i\beta^j\gamma^s, \\ V_t &= V_1^{\frac{1-(-1)^t}{2}} \sum_{\substack{i+j+s=[t^2/2] \\ i=0}}^{[t^2/2]} \sum_{j=0}^{[t^2/4]} \sum_{s=0}^{[t^2/2]} b_{i,j,s}\alpha^i\beta^j\gamma^s, \\ W_t &= (U_1V_1)^{\frac{1+(-1)^t}{2}} W_1 \sum_{\substack{i+j+s=[t^2/4]-\frac{1+(-1)^t}{2} \\ i=0}}^{[t^2/4]-\frac{1+(-1)^t}{2}} \sum_{j=0}^{[t^2/8]} \sum_{s=0}^{[t^2/4]-\frac{1+(-1)^t}{2}} c_{i,j,s}\alpha^i\beta^j\gamma^s, \end{aligned}\right\} \qquad (4)$$

where $a_{i,j,s}$, $2b_{i,j,s}$, $c_{i,j,s}$ are integral rational numbers and

$$a_{t^2/4,0,0} = b_{t^2/2,0,0} = 1,\quad c_{t^2/4-1,0,0} = t,\quad a_{i,j,s} = (-1)^{t/2}a_{s,j,i},\quad c_{i,j,s} = (-1)^{t/2-1}c_{s,j,i}$$

for $t \equiv 0 \pmod 2$;

$$a_{[t^2/4],0,0} = b_{[t^2/2],0,0} = 1,\quad a_{0,0,[t^2/4]} = (-1)^{[t/2]}t,\quad a_{i,j,s} = (-1)^{[t/2]}c_{s,j,i}$$

for $t \not\equiv 0 \pmod 2$ and $a_{i,j,0} = 0$ $(j>0)$, $b_{i,j,s} = b_{s,j,i}$. From (3) and (4) it follows that

$$U_N = U_1^{\frac{1-(-1)^N}{2}} \sum_{\substack{i+j+s=[N^2/4] \\ i=0}}^{[N^2/4]} \sum_{j=0}^{[N^2/8]} \sum_{s=0}^{[N^2/4]} a_{i,j,s}\alpha^i\beta^j\gamma^s,$$

$$V_N = V_1^{\frac{1-(-1)^N}{2}} \sum_{\substack{i+j+s=[N^2/2] \\ i=0}}^{[N^2/2]} \sum_{j=0}^{[N^2/4]} \sum_{s=0}^{[N^2/2]} b_{i,j,s}\alpha^i\beta^j\gamma^s,$$

$$W_N = (U_1V_1)^{\frac{1+(-1)^N}{2}} W_1 \sum_{\substack{i+j+s=[N^2/4]-\frac{1+(-1)^N}{2} \\ i=0}}^{[N^2/4]-\frac{1+(-1)^N}{2}} \sum_{j=0}^{[N^2/8]} \sum_{s=0}^{[N^2/4]-\frac{1+(-1)^N}{2}} c_{i,j,s}\alpha^i\beta^j\gamma^s,$$

where $a_{i,j,s}$, $2b_{i,j,s}$, $c_{i,j,s}$ are integral rational numbers, $a_{[N^2/4],0,0}=b_{[N^2/4],0,0}=1$, $c_{[N^2/4],0,0}=N$ for $N\not\equiv 0(\mathrm{mod}\,2)$, $a_{N^2/4,0,0}=b_{N^2/4,0,0}=1$, $c_{N^2/4-1,0,0}=N$ for $N\equiv 0(\mathrm{mod}\,2)$ and $a_{i,j,0}=0$ (for all $j>0$).

We perform the substitution $\{\alpha,\beta,\gamma\}\longrightarrow\{\gamma,\beta,\alpha\}$ in the expressions (3). By assumption, this substitution carries $\{U_{2t},V_{2t},W_{2t}/U_1V_1W_1\}$, $\{U_{2s+1}/U_1,V_{2s+1}/V_1,W_{2s+1}/W_1\}$ into $\{(-1)^tU_{2t},V_{2t},(-1)^{t-1}W_{2t}/U_1V_1W_1\}$, $\{(-1)^sW_{2s+1}/W_1,V_{2s+1}/V_1,(-1)^sU_{2s+1}/U_1\}$, respectively, only if $2t,\ 2s+1<N$. Because of this, from (3) it follows that

$$\{U_N,V_N,W_N/U_1V_1W_1\}\longrightarrow\{(-1)^{N/2}U_N,V_N,(-1)^{N/2-1}W_N/U_1V_1W_1\}$$

for $N\equiv 0(\mathrm{mod}\,2)$ and

$$\{U_N/U_1,V_N/V_1,W_N/W_1\}\longrightarrow\{(-1)^{[N/2]}W_N/W_1,V_N/V_1,(-1)^{[N/2]}U_N/U_1\}$$

for $N\not\equiv 0(\mathrm{mod}\,2)$. Thus,

$$a_{i,j,s}=(-1)^{N/2}a_{s,j,i},\quad b_{i,j,s}=b_{s,j,i},\quad c_{i,j,s}=(-1)^{N/2-1}c_{s,j,i}$$

in the case $N\equiv 0(\mathrm{mod}\,2)$ and

$$a_{i,j,s}=(-1)^{[N/2]}c_{s,j,i},\quad b_{i,j,s}=b_{s,j,i}$$

in the case $N\not\equiv 0(\mathrm{mod}\,2)$.

In the following three lemmas, we shall consider U_t, V_t, W_t over the ring $K[U_1,V_1,W_1]$

LEMMA 2. If $b(a^2-4b)\neq 0$, then the polynomials U_t,V_t,W_t are pairwise relatively prime.

Proof. Form $V^2=U^4+aU^2W^2+bW^4$ and Lemma 1 it follows that

$$(U^4,V^2,W^4)=(U^4,V^2)=(V^2,W^4)=(W^4,U^4). \tag{5}$$

Therefore, the polynomials U_1,V_1,W_1 are pairwise relatively prime. Then, by virtue of $b(a^2-4b)\neq 0$, formulas (1), and the same lemma, we have

$$\left.\begin{aligned}&(U_{t/2}^4,V_{t/2}^2,W_{t/2}^4)^4\equiv 0(\mathrm{mod}(U_t^4,V_t^2,W_t^4)),\ t\equiv 0(\mathrm{mod}\,2),\\&(U_{\frac{t-1}{2}}^4,V_{\frac{t-1}{2}}^2,W_{\frac{t-1}{2}}^4)^2(U_{\frac{t+1}{2}}^4,V_{\frac{t+1}{2}}^2,W_{\frac{t+1}{2}}^4)^2\equiv 0\\&\qquad(\mathrm{mod}(U_t^4,V_t^2,W_t^4)(U_1^4,V_1^2,W_1^4)),\ t\not\equiv 0(\mathrm{mod}\,2).\end{aligned}\right\} \tag{6}$$

Applying the method of mathematical induction to the congruences (6) and taking into account (5), we obtain the assertion of the lemma.

LEMMA 3. For arbitrary c and d we have

$$\left.\begin{aligned}&U_{c+d}U_{c-d}=U_c^2U_d^2-bW_c^2W_d^2,\quad W_{c+d}W_{c-d}=U_d^2W_c^2-U_c^2W_d^2,\\&V_{c+d}V_{c-d}=V_c^2V_d^2-(a^2-4b)U_c^2U_d^2W_c^2W_d^2.\end{aligned}\right\} \tag{7}$$

Proof. By assumption

$$u_\alpha = U_\alpha/W_\alpha,\quad v_\alpha = V_\alpha/W_\alpha^2 \quad (\alpha = c, d, c\pm d),$$

and therefore from the formulas of addition of points on the curve $\mathcal{G}$ we derive the following identities

$$\left.\begin{aligned} \frac{U_c^2U_d^2 - 6W_c^2W_d^2}{U_{c+d}U_{c-d}} &= \frac{U_d^2W_c^2 - U_c^2W_d^2}{W_{c+d}W_{c-d}} = \frac{f}{g}, \\ \frac{V_c^2V_d^2 - (a^2-4b)U_c^2U_d^2W_c^2W_d^2}{V_{c+d}V_{c-d}} &= \frac{f^2}{g^2}. \end{aligned}\right\} \tag{8}$$

Since $6(a^2-4b)\neq 0$ and the polynomials $U_\alpha, V_\alpha, W_\alpha$ are pairwise relatively prime, from (8) it follows that

$$\begin{aligned} &(U_{c-d}U_{c+d}, V_{c-d}V_{c+d}, W_{c-d}W_{c+d}) = 1, \\ &(U_c^2, V_c^2, W_c^4)(U_d^2, V_d^2, W_d^4) = 1 = O(\mathrm{mod}((U_d^2W_c^2 - U_c^2W_d^2)^2, \\ &V_c^2V_d^2 - (a^2-4b)U_c^2U_d^2W_c^2W_d^2, (U_c^2U_d^2 - 6W_c^2W_d^2)^2)); \end{aligned}$$

therefore

$$\left.\begin{aligned} \varepsilon U_{c+d}U_{c-d} &= U_c^2U_d^2 - 6W_c^2W_d^2,\ \varepsilon W_{c+d}W_{c-d} = U_d^2W_c^2 - U_c^2W_d^2, \\ \varepsilon^2 V_{c+d}V_{c-d} &= V_c^2V_d^2 - (a^2-4b)U_c^2U_d^2W_c^2W_d^2, \end{aligned}\right\} \tag{9}$$

where ε is the identity of the ring $\mathcal{K}[U_1, V_1, W_1]$. Due to the fact that the parameters U_1, W_1 are arbitrary and that under the substitution $\{U_1, V_1, W_1\} \longrightarrow \{tU_1, t^2V_1, tW_1\}$ ε is invariant, the equation satisfied by ε has only coefficients from the field $\mathcal{K}$. Thus, ε is the identity of the field $\mathcal{K}$, depending, possibly, on c and d, but independent of U_1, V_1, and W_1. Comparing the coefficients of the higher powers of U_1 in identities (9) and taking into account Lemma 1, we obtain $\varepsilon = 1$, which is what we had to prove.

LEMMA 4. For arbitrary c and d we have

$$U_{c\pm d}W_{c\mp d} = U_cW_cV_d \mp U_dW_dV_c, \tag{10}$$

where the upper or the lower signs are taken simultaneously.

Proof. Since, by virtue of the addition formulas, we have

$$\frac{U_{c+d}W_{c-d}}{U_{c-d}W_{c+d}} = \frac{U_cW_cV_d - U_dW_dV_c}{U_cW_cV_d + U_dW_dV_c},$$

while on the basis of Lemma 3,

$$\begin{aligned} U_{c+d}U_{c-d}W_{c+d}W_{c-d} &= (U_{c+d}W_{c-d})(U_{c-d}W_{c+d}) = \\ &= (U_d^2W_c^2 - U_c^2W_d^2)(U_c^2U_d^2 - 6W_c^2W_d^2) = U_c^2W_c^2V_d^2 - U_d^2W_d^2V_c^2, \end{aligned}$$

it follows that

$$\varepsilon U_{c\pm d} W_{c\mp d} = U_c W_c V_d \mp U_d W_d V_c, \tag{11}$$

where ε does not depend on U_1, V_1, W_1 and $\varepsilon^2=1$. Comparing, as in the previous lemma, the coefficients of the highest powers of U_1, we obtain from (11): $\varepsilon(c\mp d)=c\mp d$, $\varepsilon=1$. The lemma is proved.

We note that since for $b=0$ we have

$$U_t=U_1^{t^2},\quad V_t=U_1^{2t^2-2t}\,\frac{(V_1+\sqrt{a}\,U_1W_1)^t+(V_1-\sqrt{a}\,U_1W_1)^t}{2},$$

$$W_t=U_1^{t^2-2t}\,\frac{(V_1+\sqrt{a}\,U_1W_1)^t-(V_1-\sqrt{a}\,U_1W_1)^t}{2\sqrt{a}},$$

while for $a^2-4b=0$ we have

$$V_t=V_1^{t^2},\quad U_{2t}=V_1^{2t^2-2t}\,\frac{(U_2+\sqrt{-a/2}\,W_2)^t+(U_2-\sqrt{-a/2}\,W_2)^t}{2},$$

$$W_{2t}=V_1^{2t^2-2t}\,\frac{(U_2+\sqrt{-a/2}\,W_2)^t-(U_2-\sqrt{-a/2}\,W_2)^t}{\sqrt{-2a}},$$

it follows that relation (7) and (10) are valid for arbitrary values of a and b.

LEMMA 5. If $O_m=\{U/W, V/W^2\}$ is a primitive point of order m on φ, then for any h, relatively prime with m, we have

$$(W_h/(U_h, W_h))=(W_1/(U_1, W_1)). \tag{12}$$

Proof. First we note that for any natural t we have.

$$W_t/(U_t, W_t)\equiv 0 \pmod{W_1/(U_1, W_1)}.$$

Indeed, for $t=1$ the validity of this statement is obvious, therefore, if it holds for all $t<N$, then from the formulas

$$U_{N+1}=U_{\frac{N+1}{2}}^2-bW_{\frac{N+1}{2}}^2,\quad W_{N+1}=2U_{\frac{N+1}{2}}V_{\frac{N+1}{2}}W_{\frac{N+1}{2}}\quad (N\not\equiv 0(\mathrm{mod}\,2)),$$

$$\left.\begin{aligned} U_{N+1}U_1&=U_{N/2}^2U_{N/2+1}^2-bW_{N/2}^2W_{N/2+1}^2,\\ W_{N+1}W_1&=U_{N/2}^2W_{N/2+1}^2-U_{N/2+1}^2W_{N/2}^2 \end{aligned}\right\}(N\equiv 0(\mathrm{mod}\,2))$$

it follows that

$$\frac{W_{N+1}}{(U_{N+1}, W_{N+1})}\equiv 0\left(\mathrm{mod}\,\frac{W_{(N+1)/2}}{(U_{\frac{N+1}{2}}, W_{\frac{N+1}{2}})}\right),\quad N\not\equiv 0(\mathrm{mod}\,2),$$

$$\frac{W_{N+1}W_1}{(U_{N+1},W_{N+1})(U_1,W_1)} \equiv 0 \left(\mathrm{mod}\ \frac{W_{N/2}W_{N/2+1}}{(U_{N/2},W_{N/2})(U_{N/2+1},W_{N/2+1})}\right).$$
$$N \equiv 0 \pmod 2,$$

which, by virtue of the assumption

$$W_t/(U_t,W_t) \equiv 0 \pmod{W_1/(U_1,W_1)} \qquad (t<N)$$

gives

$$W_{N+1}/(U_{N+1},W_{N+1}) \equiv 0 \pmod{W_1/(U_1,W_1)}.$$

Thus,

$$\left.\begin{aligned} W_h/(U_h,W_h) &\equiv 0 \pmod{W_1/(U_1,W_1)}, \\ W_{h^q}/(U_{h^q},W_{h^q}) &\equiv 0 \pmod{W_h/(U_h,W_h)}. \end{aligned}\right\} \tag{13}$$

Then, since $(h,m)=1$, the congruence $h^q \equiv 1 \pmod m$ is always solvable. Therefore, selecting for q one of the solutions of the mentioned congruence, from (13) we obtain

$$W_h/(U_h,W_h) \equiv 0 \pmod{W_1/(U_1,W_1)},$$
$$W_1/(U_1,W_1) \equiv 0 \pmod{W_h/(U_h,W_h)},$$

whence

$$(W_h/(U_h,W_h)) = (W_1/(U_1,W_1)).$$

LEMMA 6. If σ_m is a primitive $\mathcal{K}$-point of order m on φ, then for $\varphi(m)>n$ we have

$$U_1 \equiv 0 \pmod{W_1}, \qquad V_1 \equiv 0 \pmod{W_1^2}. \tag{14}$$

Proof. Let $m = 2^{t_0}\prod_{i=1}^{s} p_i^{t_i}$ be the canonical expansion of the number m into prime factors. If $t_0>0$, then necessarily $U_{m/2}V_{m/2}=0$, which by virtue of Lemma 1 gives (14). Therefore, it is sufficient to consider only the case $m = \prod_{i=1}^{s} p_i^{t_i}$, $(p_i,2)=1$.

a) $q \geq 2$. We rewrite the equality $m\sigma_m = \sigma$ in the form $p_i(m\sigma_m/p_i) = \sigma$ $(i=1,2)$. Then

$$W_m = W_{m/p_i} \sum_{i=0}^{[m^2/4p_i^2]} \sum_{j=0}^{[m^2/8p_i^2]} \sum_{s=0}^{[m^2/4p_i^2]} c_{i,j,s}\alpha^i\beta^j\gamma^s = 0 \quad .$$
$$i+j+s=[m^2/4p_i^2]$$

We have $W_{m/p_i} \neq 0$ since in the opposite case the point σ_m would have order $<m$. Consequently,

$$\sum_{i,j,s} c_{i,j,s}\alpha^i\beta^j\gamma^s = 0, \quad \alpha = U_{m/p_i}^4, \ \beta = 4aU_{m/p_i}^2/W_{m/p_i}^2, \ \gamma = 6W_{m/p_i}^4,$$

from where, by virtue of Lemma 1, we have

$$p_i \equiv 0 (\mathrm{mod}\, W_{m/p_i}/(U_{m/p_i}, W_{m/p_i})) \quad (i=1,2).$$

But $(p_1, p_2)=1$, and, on the basis of Lemma 5,

$$W_{m/p_i}/(U_{m/p_i}, W_{m/p_i}) \equiv 0 (\mathrm{mod}\, W_1/(U_1, W_1)),$$

therefore $U_1 \equiv 0 (\mathrm{mod}\, W_1)$, $V_1 \equiv 0 (\mathrm{mod}\, W_1^2)$.

b) $m=p^q$. We divide the group of all points $\alpha O_p + \beta O_p'$ $(\alpha, \beta = 0, 1, \ldots, p-1)$ of order p on φ into $p+1$ disjoint classes T_t $(t=1,2,\ldots,p+1)$ in such a manner that to the same class there should belong the points $h\alpha O_p + h\beta O_p'$, where $h=1,2,\ldots,p-1$, while α and β are fixed numbers for the same class.

Since

$$W_m = W_{m/p} \sum_{i=0}^{[p^2/4]} \sum_{j=0}^{[p^2/8]} \sum_{s=0}^{[p^2/4]} c_{i,j,s} \alpha^i \beta^j \gamma^s$$

and $W_{m/p} \neq 0$, we have

$$\sum_{\substack{i+j+s=[p^2/4] \\ i=0}}^{[p^2/4]} \sum_{j=0}^{[p^2/8]} \sum_{s=0}^{[p^2/4]} c_{i,j,s} \alpha^i \beta^j \gamma^s, \tag{15}$$

where $\alpha = U_{m/p}^4$, $\beta = 4a U_{m/p}^2 W_{m/p}^2$, $\gamma = b W_{m/p}^4$. Assume that for the same class T_t we have $W_{\alpha,\beta}/(U_{\alpha,\beta}, W_{\alpha,\beta}) = q_t$. On the basis of Lemma 1, we have $c_{[p^2/4],0,0} = p$ and $c_{0,0,[p^2/4]} = (-1)^{[p/2]}$ and therefore, by virtue of Lemma 5,

$$p \equiv 0 (\mathrm{mod} (\prod_{t=1}^{p+1} q_t)^{p-1}). \tag{16}$$

From (15) it follows that

$$\sum_{j,s} c_{i,j,s} (4a)^j b^s = p \sum_{\alpha_i, \beta_i} u_{\alpha_1,\beta_1} u_{\alpha_2,\beta_2} \ldots u_{\alpha_t,\beta_t}, \quad 2j+4s=t,$$

from where, taking into account (16), the arbitrariness of a, b, and the rationality of $c_{i,j,s}$, we obtain

$$c_{i,j,s} \equiv 0 (\mathrm{mod}\, p), \quad 2j+4s < p-1. \tag{17}$$

We write the following system of equalities

$$\left.\begin{aligned} U_{m/p^t} &= U_{m/p^{t+1}} \sum_{i=0}^{[p^2/4]} \sum_{j=0}^{[p^2/8]} \sum_{s=0}^{[p^2/4]} a_{i,j,s} \alpha^i \beta^j \gamma^s, \\ W_{m/p^t} &= W_{m/p^{t+1}} \sum_{i=0}^{[p^2/4]} \sum_{j=0}^{[p^2/8]} \sum_{s=0}^{[p^2/4]} c_{i,j,s} \alpha^i \beta^j \gamma^s. \end{aligned}\right\} \tag{18}$$

Since $a_{[p^2/4],0,0}=1$ and on the basis of Lemma 5, we have

$$W_{m/p^t}/(U_{m/p^t},W_{m/p^t})=0(\mathrm{mod}\, W_{m/p^{t+1}}/(U_{m/p^{t+1}},W_{m/p^{t+1}})), \tag{19}$$

from (16)-(19) one obtains immediately

$$\left.\begin{aligned} W_p/(U_p,W_p)&=0(\mathrm{mod}\,[W_1/(U_1,W_1)]^p)\ ,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ W_{pq-1}/(U_{pq-1},W_{pq-1})&=0(\mathrm{mod}\,[W_{pq-2}/(U_{pq-2},W_{pq-2})]^p)\ ,\\ p&=0(\mathrm{mod}\,[W_{pq-1}/(U_{pq-1},W_{pq-1})]^{p-1})\ ,\\ p&=0(\mathrm{mod}\,[W_1/(U_1,W_1)]^{\varphi(m)}). \end{aligned}\right\} \tag{20}$$

By assumption, the degree of the field K does not exceed n, therefore for $(U_1,W_1)\not\equiv 0(\mathrm{mod}\, W_1)$ from (20) we have $p^n\equiv 0(\mathrm{mod}\, p^{\varphi(m)})$, and hence there follows $n\geqslant\varphi(m)$, which contradicts the condition $\varphi(m)>n$. The lemma is proved

Let K' be the minimal field in which the divisors from K are principal.

LEMMA 7. If O_m is a primitive K-point of order $\varphi(m)>4n$ on φ, then

$$u_1=qu_1',\quad v_1=q^2v_1',\quad a=q^2A,\quad b=q^4B,\quad (A,B)=1, \tag{21}$$

where q, u_1', v_1', A, B are integers from K'.

Proof. Since, by assumption, a, b are integers and $\varphi(m)>n$, on the basis of Lemma 6 it follows that u_1 and v_1 are integers from the field K. Then, if q is an integer from K' and $\nu_q(au_1^2)>\nu_q(u_1^4)$ or $\nu_q(b)$, where $\nu_q(c)$ is the q-exponent of the number c, then $\nu_q(u_1^4)=\nu_q(b)$. Indeed, in the case $m\not\equiv 0(\mathrm{mod}\,2)$ $\nu_q(u_1^4)>\nu_q(b)$ is not possible since

$$W_m/W_1^{m^2}=0=\sum_{i,j,s}c_{i,j,s}u_1^{4i+2j}(4a)^jb^s,\quad c_{0,0,[m^2/4]}=(-1)^{[m/2]}$$

and $a, b, u_1, c_{i,j,s}$ are integers, while $\nu_q(b)>\nu_q(u_1^4)$, similarly to Lemma 6, contradicts the condition $\varphi(m)>4n$. However, in the case $m\equiv 0(\mathrm{mod}\,2)$, but $m\not\equiv 0(\mathrm{mod}\,4)$, for

$$V_{m/2}/W_1^{m^2/2}=v_1\sum_{i,j,s}b_{i,j,s}u_1^{4i+2j}(4a)^jb^s=0$$

by virtue of $v_1=0$, $b_{[m^2/8],0,0}=b_{0,0,[m^2/8]}=1$ $\nu_q(b)=\nu_q(u_1^4)$, for

$$U_{m/2}/W_1^{m^2/4}=u_1\sum_{i,j,s}a_{i,j,s}u_1^{4i+2j}(4a)^jb^s=0,\quad u_1\neq 0$$

$\nu_q(u_1^4)<\nu_q(b)$ is not possible by virtue of $a_{[m^2/16],0,0}=1$, while $\nu_q(6)<\nu_q(u_1^4)$, similarly to Lemma 6, is not feasible for $\varphi(m)>4n$, provided one notes that for $u_1\to\sqrt{b}/u_1$ $U_{m/2}$ becomes $u_1^{-m^2/4}b^{(m^2+4)/16}W_{m/2}$. If, however, $m\equiv 0(\mathrm{mod}\,4)$, then $\nu_q(b)=\nu_q(u_1^4)$ follows from the conditions: $U_{m/2}V_{m/2}=0$,

$$U_{m/2}=W_1^{m^2/4}\sum_{i,j,s}a_{i,j,s}u_1^{4i+2j}(4a)^jb^s,\quad a_{m^2/16,0,0}=(-1)^{m/4}a_{0,0,m^2/16}=1,$$

$$V_{m/2}=W_1^{m^2/4}\sum_{i,j,s}b_{i,j,s}u_1^{4i+2j}(4a)^jb^s,\quad b_{m^2/8,0,0}=b_{0,0,m^2/8}=1.$$

Further, if $v_q(au_1^2) \leqslant v_q(u_1^4)$, $v_q(b)$, then for $v_q(au_1^2) < v_q(b)$, $v_q(au_1^2) < v_q(u_1^4)$ from $v_1^2 = u_1^4 + au_1^2 + b$ we have $a = q^2\mathcal{A}$, $b = q^4\mathcal{B}$, $u_1 = qu_1'$, $v_1 = q^2v_1'$, $v_q(\mathcal{A}, \mathcal{B}) = 0$, while for $v_q(au_1^2) = v_q(b)$, $v_q(au_1^2) < v_q(u_1^4)$ in the case $m \not\equiv 0 \pmod 2$, taking into account the conditions $c_{0,j,5} = 0$ (for all $j > 0$) and $c_{0,0,[m^2/4]} = (-1)^{[m/2]}$, proved in Lemma 1, we obtain $v_q(u_1^4) = v_q(au_1^2) = v_q(b)$, that is, $a = q^2\mathcal{A}$, $b = q^4\mathcal{B}$, $u_1 = qu_1'$, $v_1 = q^2v_1'$, $v_q(\mathcal{A}, \mathcal{B}) = 0$, while in the case $m \equiv 0 \pmod 2$, $U_{m/2}V_{m/2} = 0$ we have: a) $v_{m/2}^2 = b$, $b = q^{2\beta}\mathcal{B}$, $v_q(au_1^2) = v_q(b)$, $a = q^{2\alpha}\mathcal{A}$, $u_1 = q^\alpha u_1'$, $v_1 = q^{2\alpha}v_1'$, $b = q^{4\alpha}\mathcal{B}'$, $v_q(\mathcal{A}, \mathcal{B}') = 0$; b) $(2u_{m/2}^2 + a)^2 = a^2 - 4b$, $v_q(b) = q^{2\beta}\mathcal{B}$, $v_q(au_1^2) = v_q(b)$, $a = q^{2\alpha}\mathcal{A}$, $u_1 = q^\alpha u_1'$, $v_1 = q^{2\alpha}v_1'$, $b = q^{4\alpha}\mathcal{B}'$, $v_q(\mathcal{A}, \mathcal{B}') = 0$, which is what we intended to prove.

LEMMA 8. For any integer p from $\mathcal{K}'$ and point O_m for which $uv \neq 0$, we have

$$v_p(b) \geqslant 2v_p(u), \quad v_p(a^2 - 4b) \geqslant 2v_p(v). \tag{22}$$

Proof. According to Lemma 1, we have

$$\left.\begin{aligned}
&\text{a) } W_t/W_1^{t^2} = \sum_{i,j,s} c_{i,j,s} u_1^{4i+2j} (4a)^j b^s, \quad c_{0,0,[t^2/4]} = (-1)^{[t/2]}, \quad t \not\equiv 0 \pmod 2,\\
&\quad U_t/U_1 \to (-1)^{[t/2]} (b^{1/4}/u_1)^{t^2-1} W_t/W_1 \text{ for } u_1 \to b^{1/2}/u_1, \quad t \not\equiv 0 \pmod 2,\\
&\text{b) } V_t/W_1^{2t^2} = \sum_{i,j,s} b_{i,j,s} u_1^{4i+2j} (4a)^j b^s, \quad b_{0,0,[t^2/2]} = 1, \quad U_t V_t = 0,\\
&\quad U_{2t}/W_1^{4t^2} = \sum_{i,j,s} a_{i,j,s} u_1^{4i+2j} (4a)^j b^s, \quad a_{0,0,t^2} = (-1)^t,\\
&\text{c) } V_{4t}/W_1^{8t^2} = \sum_{i,j,s} b_{i,j,s} u_1^{4i+2j} (4a)^j b^s, \quad b_{0,0,2t^2} = 1, \quad U_{2t} V_{2t} = 0.
\end{aligned}\right\} \tag{23}$$

Therefore, taking into account that $a_{i,j,s}$, $2b_{i,j,s}$, $c_{i,j,s}$ are rational integers, from (23) we obtain: a) $v_p(b) \geqslant 2v_p(u_1)$ $(m = t, m \not\equiv 0 \pmod 2)$, b) $v_p(b) \geqslant 2v_p(u_1)$ $(m = 2t, t \not\equiv 0 \pmod 2)$, c) $v_p(b) \geqslant 2v_p(u_1)$ $(m = 4t)$.

The inequality $v_p(a^2 - 4b) \geqslant 2v_p(v_1)$ follows a completely similar manner from the relations of Lemma 1 if one takes into account the isogeny of the curves $v^2 = u^4 + au^2 + b$ and $v^2 = u^4 - 2au^2 + a^2 - 4b$.

LEMMA 9. If p is an odd number such that $v_p(b) > 0$, then for any natural $t < \varphi(m)/4n$ for $(a, b) = 1$ we have

$$v_p(u_t)/v_p(b) = \{t\, v_p(u_1)/v_p(b)\}, \tag{24}$$

where $\{c\}$ is the distance from c to the nearest integer.

Proof. We carry out the proof by the method of mathematical induction. Since on the basis of (22) we have $v_p(u_1)/v_p(b) \leqslant 1/2$, it follows that $v_p(u_1)/v_p(b) = \{v_p(u_1)/v_p(b)\}$. Thus, for $t = 1$ the lemma holds. We assume now that the lemma has been proved for $t < N$ and we show that in this case it holds also for $t = N$. We consider separately the following two cases: 1) $N \equiv 0 \pmod 2$, 2) $N \not\equiv 0 \pmod 2$.

1) $N\equiv 0(\mathrm{mod}\,2)$. By the formulas (1) we have

$$U_N = U_{N/2}^4 - 6W_{N/2}^4, \quad W_N = 2U_{N/2}V_{N/2}W_{N/2}.$$

If $\nu_p(u_{N/2}) = \nu_p(6)/4$, then, taking into account that $\nu_p(u_{N/2}) = \nu_p(v_{N/2})$, by virtue of $(a,6)=1$ we have $\nu_p(u_N) \geqslant \nu_p(6)/2$. On the other hand, by Lemma 8 we have $\nu_p(u_N) < \nu_p(6)/2$ and, consequently, $\nu_p(u_N) = \nu_p(6)/2$. By assumption, $\nu_p(u_{N/2}) = \nu_p(6)/4 = \{N\nu_p(u_1)/2\nu_p(6)\}\nu_p(6)$, that is, $\pm 1/4 + \tau = N\nu_p(u_1)/2\nu_p(6)$, r being an integer, which yields $N\nu_p(u_1)/\nu_p(6) = \pm 1/2 + 2\tau$, $\{N\nu_p(u_1)/\nu_p(6)\}\nu_p(6) = \nu_p(6)/2 = \nu_p(u_N)$.

If, however, $\nu_p(u_{N/2}) \neq \nu_p(6)/4$, then by virtue of the fact that p is odd we have $\nu_p(u_N) = \min\{4\nu_p(u_{N/2}), \nu_p(6) - 2\nu_p(u_{N/2})\}$. From here one can easily conclude that in the case $4\nu_p(u_{N/2}) < \nu_p(6)$ one has

$$\nu_p(u_N) = 2\nu_p(u_{N/2}) = 2\{N\nu_p(u_1)/2\nu_p(6)\}\nu_p(6) = \{N\nu_p(u_1)/\nu_p(6)\}\nu_p(6),$$

while in the case $4\nu_p(u_{N/2}) > \nu_p(6)$ one has

$$\nu_p(u_N) = \nu_p(6) - 2\nu_p(u_{N/2}) = \nu_p(6) - 2\{N\nu_p(u_1)/2\nu_p(6)\}\nu_p(6) = \{N\nu_p(u_1)/\nu_p(6)\}\nu_p(6),$$

that is, again $\nu_p(u_N) = \{N\nu_p(u_N)/\nu_p(6)\}\nu_p(6)$.

2) $N \not\equiv 0(\mathrm{mod}\,2)$. By the formulas (1) we have

$$U_N U_1 = U_{\frac{N-1}{2}}^2 U_{\frac{N+1}{2}}^2 - 6W_{\frac{N-1}{2}}^2 W_{\frac{N+1}{2}}^2,$$

$$W_N W_1 = U_{\frac{N-1}{2}}^2 W_{\frac{N+1}{2}}^2 - U_{\frac{N+1}{2}}^2 W_{\frac{N-1}{2}}^2.$$

a) $\nu_p(u_{\frac{N-1}{2}}) = \nu_p(u_{\frac{N+1}{2}})$. By assumption,

$$\nu_p(u_{\frac{N-1}{2}})/\nu_p(6) = \{(N-1)\nu_p(u_1)/2\nu_p(6)\},$$

$$\nu_p(u_{\frac{N+1}{2}})/\nu_p(6) = \{(N+1)\nu_p(u_1)/2\nu_p(6)\}.$$

Let $(N+1)\nu_p(u_1)/2\nu_p(6) = \alpha + \tau$, $(N-1)\nu_p(u_1)/2\nu_p(6) = \pm\alpha + s$, where τ, s are integers and $|\alpha| \leqslant 1/2$. Since $\nu_p(u_1)/\nu_p(6) < 1/2$, we have $(N-1)\nu_p(u_1)/2\nu_p(6) = -\alpha + s$, $2\nu_p(u_{\frac{N-1}{2}}) + 2\nu_p(u_{\frac{N+1}{2}}) \neq \nu_p(6)$; indeed, if $2\nu_p(u_{\frac{N+1}{2}}) + 2\nu_p(u_{\frac{N-1}{2}}) = \nu_p(6)$, then $(\tau+s)/N - 1/2$ has to be an integer which, by virtue of the fact that N is odd, is not possible. Consequently, $\nu_p(u_1)/\nu_p(6) = \{2\alpha\}$, $\nu_p(W_1W_N)/\nu_p(6) \geqslant 2|\alpha| + 2\nu_p(W_{\frac{N-1}{2}}, W_{\frac{N+1}{2}})/\nu_p(6)$, whence

$$0 \leqslant \nu_p(u_N)/\nu_p(6) < \min\{1, 4|\alpha|\} - 2|\alpha| - \{2\alpha\} < 0, \quad \nu_p(u_N) = 0.$$

But $N\nu_p(u_1)/\nu_p(6) = \tau + s$, therefore $0 = \nu_p(u_N)/\nu_p(6) = \{N\nu_p(u_1)/\nu_p(6)\}$.

b) $2\nu_p(u_{\frac{N-1}{2}}) + 2\nu_p(u_{\frac{N+1}{2}}) = \nu_p(6)$. As in the previous case, we set $(N+1)\nu_p(u_1)/2\nu_p(6) = \alpha + \tau$, $(N-1)\nu_p(u_1)/2\nu_p(6) = \beta + s$, where $|\alpha|, |\beta| \leqslant 1/2$, while τ, s are integers. On the basis of what we had before, $|\alpha| \neq |\beta|$, therefore $\nu_p(u_N)/\nu_p(6) \geqslant 1 - 2\min\{|\alpha|, |\beta|\} > 1/2$, which is not possible.

c) $\nu_p(u_{\frac{N-1}{2}}) \neq \nu_p(u_{\frac{N+1}{2}})$, $2\nu_p(u_{\frac{N-1}{2}}) + 2\nu_p(u_{\frac{N+1}{2}}) \neq \nu_p(6)$. We have

$$\nu_p(u_N)+\nu_p(u_1)=\min\{2\nu_p(u_{\frac{N-1}{2}})+2\nu_p(u_{\frac{N+1}{2}}),\ \nu_p(6)\}-2\min\{\nu_p(u_{\frac{N-1}{2}}),\nu_p(u_{\frac{N+1}{2}})\}.$$

We denote $\nu_p(u_{\frac{N+1}{2}})/\nu_p(6)$, $\nu_p(u_{\frac{N-1}{2}})/\nu_p(6)$ by α and β. If $2\{\alpha\}+2\{\beta\}<1$, then $\alpha<\beta$, therefore $\nu_p(u_N)+\nu_p(u_1)=2\max\{\alpha,\beta\}\nu_p(6)=2\alpha\nu_p(6)$, whence $\nu_p(u_N)/\nu_p(6)=\{N\nu_p(u_1)/\nu_p(6)\}$.

If, however, $2\{\alpha\}+2\{\beta\}>1$, then

$$\nu_p(u_N)+\nu_p(u_1)=\nu_p(6)-2\min\{\alpha,\beta\}\nu_p(6),$$

from where we obtain

$$(N+1)\nu_p(u_1)/2\nu_p(6)=\pm\alpha+\tau,\quad (N-1)\nu_p(u_1)/2\nu_p(6)=\pm\beta+\sigma,$$

$$N\nu_p(u_1)/\nu_p(6)=\pm\alpha\pm\beta+\tau+\sigma,\quad \nu_p(u_1)/\nu_p(6)=\pm\alpha\mp\beta+\tau-\sigma,$$

$$\nu_p(u_N)/\nu_p(6)=1-2\min\{\alpha,\beta\}-\nu_p(u_1)/\nu_p(6)=1-2\min\{\alpha,\beta\}-\{\alpha-\beta\}=\{\alpha+\beta\}=\{N\nu_p(u_1)/\nu_p(6)\}.$$

The lemma is proved.

LEMMA 10. We have congruence

$$m\nu_p(u_1)\equiv 0(\mathrm{mod}\,\nu_p(6)). \tag{25}$$

Proof. By the definition of points of finite order, for any number t we have $\nu_p(u_t)=\nu_p(u_{m-t})$; therefore, for $(p,2)=1$ and $t<\varphi(m)/4n$ we have

$$\{t\nu_p(u_1)/\nu_p(6)\}=\{(m-t)\nu_p(u_1)/\nu_p(6)\},$$

from where, by virtue of the arbitrariness of t, we obtain (25).

On the basis of the isogeny of the curves $v^2=u^4+au^2+6$ and $v^2=u^4-2au^2+a^2-4b$, we obtain by analogy:

LEMMA 11. If p is odd number such that $\nu_p(a^2-4b)>0$, then for any natural number $t<\varphi(m)/4n$ we have

$$\nu_p(v_t)=\{t\nu_p(v_1)/\nu_p(a^2-4b)\}\nu_p(a^2-4b). \tag{26}$$

LEMMA 12.

$$m\nu_p(v_1)\equiv 0(\mathrm{mod}\,\nu_p(a^2-4b)). \tag{27}$$

LEMMA 13. Assume that $\delta_p(u)=\nu_p(u)-\nu_p(2)$, $\delta_p(6)=\nu_p(6)-4\nu_p(2)$. For any natural number $t<\varphi(m)/4n$ we have

$$\delta_p(u_t)=\delta_p(6)/4 \tag{28}$$

in the case $\delta_p(6)\leqslant 0$ and

$$\delta_p(u_t)=\{t\delta_p(u_1)/\delta_p(6)\}\delta_p(6)$$

in the case $\delta_p(6)>0$

Since for an odd p the formulas (24), (28) coincide, it is sufficient to consider only the case $2\equiv 0(\mathrm{mod}\, p)$.

If $\nu_p(b)\leqslant 4\nu_p(2)$, then by virtue of Lemmas 1 and 7 we have $\nu_p(u^4)=\nu_p(4u^2)=\nu_p(b)$ for $\nu_p(b)=4\nu_p(2)$ and $\nu_p(u^4)=\nu_p(b)$ for $\nu_p(b)<4\nu_p(2)$. If, however, $\nu_p(b)>4\nu_p(2)$, then on the basis of the same lemmas we have $\nu_p(u)>\nu_p(2)$, as a consequence of which, setting $\delta_p(u)=\nu_p(u)-\nu_p(2)$, $\delta_p(b)=\nu_p(b)-4\nu_p(2)$ and applying the reasoning of Lemma 9, we obtain as a result the relation (28).

On the same basis we have

LEMMA 14. Let $\delta_p(v)=\nu_p(v)-2\nu_p(2)$, $\delta_p(a^2-4b)=\nu_p(a^2-4b)-8\nu_p(2)$. For any natural number $t<\varphi(m)/4n$ we have

$$\left.\begin{aligned}\delta_p(v_t)&=\delta_p(a^2-4b)/4\\ \delta_p(v_t)&=\{t\delta_p(v_1)/\delta_p(b)\}\delta_p(b)\end{aligned}\right\} \tag{29}$$

in the case $\delta_p(a^2-4b)\leqslant 0$ and in the case of $\delta_p(a^2-4b)>0$.

We separate the divisors of u_1 and v_1 into classes in such a manner that to the same class there will belong those a_i and b_i for which $\delta_{a_i}(u_1)/\delta_{a_i}(b)=i$, $\delta_{b_i}(v_1)/\delta_{b_i}(a^2-4b)=i$. Then, on the basis of the above-proved lemma we can easily derive the

COROLLARY. Let $\mathcal{K}'$ be the minimal field in which all the divisors from $\mathcal{K}$ are principal. For any natural number $t<m/2$ we have

$$\left.\begin{aligned}u_t&=\varepsilon_t\mathcal{P}_0\sigma_0 T_{(m,t)}^{(-1)^{m/(m,t)}}\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}A_{d_i,j}^{\{t_j/d_i\}d_i},\\ v_t/u_t&=\varepsilon_t'\mathcal{P}_0\sigma_0' T_{(m,t)}^{-1}\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}B_{d_i,j}^{\{t_j/d_i\}d_i},\end{aligned}\right. \tag{30}$$

$$(d_i,j)=1$$

$$b=\sigma_0^4\mathcal{P}_0^4\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}A_{d_i,j}^{d_i}\cdot c,$$

$$a^2-4b=\sigma_0'^4\mathcal{P}_0^4\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}B_{d_i,j}^{d_i}\cdot d,$$

where $\varepsilon_t,\varepsilon_t',\ldots$, c, d are integers from $\mathcal{K}'$, $1\equiv 0(\mathrm{mod}\,\varepsilon)$, $4\equiv 0(\mathrm{mod}\,\sigma_0^3,\sigma_0')$; A,B,c,d are pairwise relatively prime, $m\equiv 0\ (\mathrm{mod}\, T_{(m,t)})$. $T_{(m,t)}=1$ in the case $m/(m,t)\neq p^q, 2p^q$ (p is prime) or $\varphi(m)/4n>t$.

Proof of the Theorem. Let $\mathcal{H}$ be the curve

$$au^4-b=cv^2 \tag{31}$$

By the geometric method of tracing secants to the curve (31), it is easy to establish that if $\mathcal{P}_1=\{u_1,v_1\}$, $\mathcal{P}_2=\{u_2,v_2\}$ are points on $\mathcal{H}$, then $\mathcal{P}_1\pm\mathcal{P}_2=\{u_\pm,v_\pm\}$, where

$$u_\pm=\frac{u_1v_2\mp u_2v_1}{u_2^2-u_1^2},\quad v_\pm=\frac{cv_1v_2(u_1^2+u_2^2)\mp 2u_1u_2(au_1^2u_2^2-b)}{(u_2^2-u_1^2)^2} \tag{32}$$

and $\{u_\pm,v_\pm\}$ are points of the curve $c^2u^4-ab=v^2$. First of all we note that if $(a,b,c)=1$, $\nu_q(u,bc)=\nu_q(v,ab)=0$ and $\nu_{q_1}(u_1)\nu_{q_1}(u_2)\gtrless 0$, $\nu_{q_2}(v_1/u_1)\nu_{q_2}(v_2/u_2)\gtrless 0$, where q_1 is arbitrary and q_2 is odd, then $\nu_{q_1}(u_\pm)\lessgtr 0$, $\nu_{q_2}(v_\pm/u_\pm)\lessgtr 0$, respectively. Indeed, we set $u_i=\alpha_i/\beta_i$, $v_i=\gamma_i/\beta_i^2$, where $(\alpha_i,\beta_i)=1$ $(i=1,2)$. Then, by multiplying the formulas (32) one can obtain

$$cu_+u_-=\frac{a\alpha_1^2\alpha_2^2+b\beta_1^2\beta_2^2}{\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2},\quad v_+v_-=\frac{c^2\gamma_1^2\gamma_2^2-4ab\alpha_1^2\alpha_2^2\beta_1^2\beta_2^2}{(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2)^2}. \tag{33}$$

a) $\nu_{q_1}(u_1)\nu_{q_1}(u_2)<0$. Obviously, for this case $\nu_{q_1}(u_1),-\nu_{q_1}(u_2)>0,\ \nu_{q_1}(\alpha_2\beta_1)=0$ or $\nu_{q_1}(u_1)$, $\nu_{q_1}(u_2)>0,\ \nu_{q_1}(\alpha_1\beta_2)=0$. Therefore, $\nu_{q_1}(\alpha_1\beta_1\gamma_2\mp\alpha_2\beta_2\gamma_1)>0,\ \nu_{q_1}(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2)=0$, i.e., $\nu_{q_1}(u_\pm)>0$.

b) $\nu_{q_2}(v_1/u_1)\nu_{q_2}(v_2/u_2)<0$. Since $\nu_{q_2}(\alpha_1\beta_1),\ \nu_{q_2}(\gamma_2)>0$ or $\nu_{q_2}(\alpha_2\beta_2),\ \nu_{q_2}(\gamma_1)>0$ and $\nu_{q_2}(\alpha_i,\beta_i)=0$ $(i=1,2)$, we have $\nu_{q_2}(\alpha_2^2\beta_1-\alpha_1^2\beta_2^2)=0$, $\nu_{q_2}\{c\gamma_1\gamma_2(\alpha_1^2\beta_2^2+\alpha_2^2\beta_1^2)\mp 2\alpha_1\alpha_2\beta_1\beta_2(a\alpha_1^2\alpha_2^2-b\beta_1^2\beta_2^2)\}>0$, whence $\nu_{q_2}(v_\pm/u_\pm)>0$.

c) $\nu_{q_1}(u_1)\nu_{q_1}(u_2)>0$. According to (33) and the conditions $\nu_{q_1}(\alpha_1\alpha_2)=0$, $\nu_{q_1}(\beta_1),\nu_{q_1}(\beta_2)>0$ or $\nu_{q_1}(\beta_1\beta_2)=0,\nu_{q_1}(\alpha_1),\nu_{q_1}(\alpha_2)>0$, we have

$$\nu_{q_1}(u_+u_-)=-\nu_{q_1}(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2), \tag{34}$$

but

$$\nu_{q_1}(u_\pm)=\nu_{q_1}(\alpha_1\beta_1\gamma_2\mp\alpha_2\beta_2\gamma_1)-\nu_{q_1}(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2)>-\nu_{q_1}(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2),$$

as a consequence of which, on the basis of (34), each of the numbers $\nu_{q_1}(u_\pm)$ must be negative.

d) $\nu_{q_2}(v_1/u_1)\,\nu_{q_2}(v_2/u_2)>0$. If $\nu_{q_2}(\gamma_1/\alpha_1\beta_1)$, $\nu_{q_2}(\gamma_2/\alpha_2\beta_2)<0$, then $\nu_{q_2}(v_\pm/u_\pm)<0$ on the basis of what has been proved before and, therefore, it is sufficient to consider only the case $\nu_{q_2}(\gamma_1),\ \nu_{q_2}(\gamma_2)>0$. For $\nu_{q_2}(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2)=0,\ \nu_{q_2}(\alpha_1\beta_1\gamma_2\mp\alpha_2\beta_2\gamma_1)>0,\ \nu_{q_2}(u_\pm)>0$ and $\nu_{q_2}(v_\pm/u_\pm)<0$; in the case $\nu_{q_2}(\alpha_2^2\beta_1^2-\alpha_1^2\beta_2^2)>0$ We rewrite Eq. (31) in the form $a-bu_1^4=cv_1^2$, where $u_1=1/u$, $v_1=v/u^2$. Then, since q_2 is odd, $(a\alpha_1^2\alpha_2^2-b\beta_1^2\beta_2^2)^2-ab(\alpha_1^2\beta_2^2-\alpha_2^2\beta_1^2)^2=c^2\gamma_1^2\gamma_2^2$ and $\nu_{q_2}(\gamma_1),\ \nu_{q_2}(\gamma_2),\ \nu_{q_2}(\alpha_1^2\beta_2^2-\alpha_2^2\beta_1^2)>0$, we have $\nu_{q_2}(a\alpha_1^2\alpha_2^2+b\beta_1^2\beta_2^2)=0$ and $1/u_\pm=(\alpha_1\beta_1\gamma_2\pm\alpha_2\beta_2\gamma_1)/(a\alpha_1^2\alpha_2^2+b\beta_1^2\beta_2^2)$, therefore $\nu_{q_2}(v_\pm')=0$. Consequently $\nu_{q_2}(v_\pm'/u_\pm')<0$, but $v_\pm'/u_\pm'=(v_\pm/u_\pm^2)/(1/u_\pm)=v_\pm/u_\pm$, whence $\nu_{q_2}(v_\pm/u_\pm)<0$.

Assume now that $\mathcal{O}_m=\{u_1,v_1\}$ is a $\mathcal{K}$-point of order m on φ and $\varphi(m)>4n$. Then for every t from the interval $1,2,\ldots,[m/2]$, satisfying the condition $m/(m,t)>4n$, on the basis of the corollary we have

$$
\left.
\begin{aligned}
&u_t^4+au_t^2+b=v_t^2\ ,\\
&u_{2t}=\varepsilon_{2t}\sigma_0\mathcal{P}_0\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}\mathcal{A}_{d_i,j}^{\{2t_j/d_i\}d_i}=\\
&=E_t\sigma_0\mathcal{P}_0\mathcal{A}_t^2\prod_{\substack{d_i\|m\\(d_i,2)=1}}\prod_{j=1}^{[d_i/2]}\mathcal{A}_{d_i,j}^{\{2t_j/d_i\}d_i}\\
&v_{2t}/u_{2t}=\varepsilon'_{2t}\sigma'_0\mathcal{P}_0\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}\mathcal{B}_{d_i,j}^{\{2t_j/d_i\}d_i}=\\
&=E'_t\sigma'_0\mathcal{P}_0\mathcal{B}_t^2\prod_{\substack{d_i\|m\\(d_i,2)=1}}\prod_{j=1}^{[d_i/2]}\mathcal{B}_{d_i,j}^{\{2t_j/d_i\}d_i}
\end{aligned}
\right\}
\tag{35}
$$

(E_t , E'_t are some products of the first powers of basis units of the field $\mathcal{K}'$),

$$
b(a^2-4b)=cd\,C^2\prod_{(d_i,2)=1}\prod_{j=1}^{[d_i/2]}(\mathcal{A}_{d_i,j}\mathcal{B}_{d_i,j})^{d_i}=q_\nu^2\prod_{s=1}^{N}q_s\,.
$$

Since $c,d,\mathcal{A},\mathcal{B}$ are pairwise relatively prime, it follows that $\mathcal{A}=\prod_{i=1}^{N_1}q_{\nu_i}A^2$, $\mathcal{B}=\prod_{j=1}^{N_2}q_{\nu_j}B^2$ ($N_1,N_2\leqslant N$) for all $d_i\not\equiv 0\pmod 2$, where A,B are elements of the field $\mathcal{K}'$. According formulas (10) we have

$$
\left.
\begin{aligned}
&u_{\alpha+\beta}+u_{\alpha-\beta}=2\,\frac{u_\alpha u_\beta}{u_\alpha^2-u_\beta^2}\,\frac{v_\alpha}{u_\alpha}\,,\\
&u_{\alpha+\beta}-u_{\alpha-\beta}=2\,\frac{u_\alpha u_\beta}{u_\alpha^2-u_\beta^2}\,\frac{v_\beta}{u_\beta}\,.
\end{aligned}
\right\}
\tag{36}
$$

From (35) and (36) we obtain

$$
a^2u^4-b^2=cv^2,\qquad \prod_{s=1}^{N}q_s\equiv 0\pmod{abc}.
\tag{37}
$$

$$
\left.
\begin{aligned}
&au^2/b=\varepsilon_{2\alpha+2\beta}\varepsilon^{-1}_{2\alpha-2\beta}\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}\mathcal{A}_{d_i,j}^{[\{2(\alpha+\beta)j/d_i\}-\{2(\alpha-\beta)j/d_i\}]d_i}\,,\\
&cv^2=\varepsilon_{2\alpha}\varepsilon^{-1}_{2\beta}\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}\mathcal{B}_{d_i,j}^{[\{2\alpha j/d_i\}-\{2\beta j/d_i\}]d_i}\times\\
&\times\left[\varepsilon_{2\alpha+2\beta}\varepsilon^{-1}_{2\alpha-2\beta}\prod_{d_i\|m}\prod_{j=1}^{[d_i/2]}\mathcal{A}_{d_i,j}^{[\{2(\alpha+\beta)j/d_i\}-\{2(\alpha-\beta)j/d_i\}]d_i}-1\right]^2,\\
&1\equiv 0(\mathrm{mod}\,\varepsilon),\quad u,v\in\mathcal{K}'.
\end{aligned}
\right\}
\tag{38}
$$

Thus, if $a^2u^4-b^2=cv^2$ is a group of curves, related by the condition $abc=C,\ \sum_s\nu_{q_s}(abc)<N$ then, at least on one of them there exist at least $m/c(n,h(\mathcal{K}),N)$ points, whose coordinates are determined by the formulas (38).

Obviously, the rank r of the curve (37) does not exceed the constant $c(n, h(\mathcal{K}), N)$, which depends only on n, N and on the number of classes of the divisors $h(\mathcal{K})$ of the given field $\mathcal{K}$.

Any $r+1$ points $Q_j = \{U_j/W_j, V_j/W_j^2\}$ (from $j=1,2,\ldots,r+1$) from (38) are linearly dependent, i.e., for some integral rationals a_j (not simultaneously equal to 0) one has

$$\sum_{j=1}^{r+1} a_j Q_j = O, \tag{39}$$

where O is the zero point on the curve $E: v^2 = u^4 - a^2b^2c^2$.

First of all we note that due to $2\alpha, 2\beta, 2\alpha \pm 2\beta \not\equiv 0 \pmod m$, we have

$$\{2(\alpha+\beta)j/m\} \neq \{2(\alpha-\beta)j/m\}, \quad \{2\alpha j/m\} \neq \{2\beta j/m\}. \tag{40}$$

Applying now Lemma 1 to the curve (37), we have: if $\mathcal{P} = \{U_1/W_1, V_1/W_1^2\}$ is an arbitrary point on (37) and $2^t\mathcal{P} = \{U_{2^t}/W_{2^t}, V_{2^t}/W_{2^t}^2\}$, then

$$\left.\begin{aligned} U_{2^t} &= \sum_{i=0}^{2^{2t-2}} \sum_{j=0}^{2^{2t-2}} a_{i,j} (a^2U_1^4)^i (-b^2W_1^4)^j, \quad a_{i,j} = (-1)^{2^{t-1}} a_{j,i}, \\ V_{2^t} &= \sum_{i=0}^{2^{2t-1}} \sum_{j=0}^{2^{2t-1}} b_{i,j} (a^2U_1^4)^i (-b^2W_1^4)^j, \quad b_{i,j} = b_{j,i}, \\ W_{2^t} &= U_1V_1W_1 \sum_{i=0}^{2^{2t-2}-1} \sum_{j=0}^{2^{2t-2}-1} c_{i,j} (a^2U_1^4)^i (-b^2W_1^4)^j, \quad c_{i,j} = (-1)^{2^{t-1}-1} c_{j,i}, \end{aligned}\right\} \tag{41}$$

where $a_{2^{2t-2},0} = b_{2^{2t-1},0} = 1$. From formulas (41) one can see that for the points $O_{2^t} = \{u_{2^t}, v_{2^t}\}$, $t>0$, of order 2^t of the curve E v_{2^t} consists of powers of the divisor 2, while u_{2^t} is a unit. Therefore, if in (39) $\nu_2(a_j) > 0$, then, setting $a_j = 2b_j$ and taking into account that, on the basis of (40) and on the basis of the assertion proved at the beginning of the theorem, we have

$$Q_+ = \sum_{j=1}^{r+1} b_j Q_j = O_2 = \{U_+/W_+, V_+/W_+^2\},$$
$$(U_+, V_+, W_+) = 1, \quad U_+V_+W_+ \equiv 0 \pmod{\prod \mathcal{A}_{d_{i,j}} \mathcal{B}_{d_{i,j}}},$$

we obtain that $\mathcal{A}_{d_{i,j}}, \mathcal{B}_{d_{i,j}}$ consists of powers of the divisors of the pair. We assume now that in (39) $(a_1, a_2, \ldots, a_{r+1}, 2) = 1$. The points $\{U/W, V/W^2\}$, $(U, V, W) = 1$ and $\{U'/W', V'/W'^2\}$, $(U', V', W') = 1$ will be considered equivalent if their coordinates satisfy the congruences

$$UW' \equiv U'W, \quad VW'^2 \equiv V'W^2 \pmod{\prod_{d_{i,j}} \mathcal{A}_{d_{i,j}} \mathcal{B}_{d_{i,j}}}.$$

Obviously,

$$\sum_{j=1}^{r+1} a_j Q_j \sim \sum_{j=1}^{r+1} e_j Q_j, \tag{42}$$

where e_j is the absolute smallest residue of the number a_j relative to mod 2. For sufficiently large values of d_i in comparison with r, one may select points Q_{d_j} $(j=1,2,\dots r+1)$ such that on the basis of (42) one should have the congruences

$$U_+ \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,j_1}}), \quad W_+ \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,j_2}}),$$

where

$$(U_+/W_+, V_+/W_+^2) = \sum_{j=1}^{r+1} a_j Q_j, \quad (U_+, V_+, W_+) = 1.$$

Indeed, by virtue of (42), for the proof of our assertion it is sufficient to consider only equivalent points and, therefore, without loss of generality, one can set $a_t \not\equiv 0 (\mathrm{mod}\, 2)$ $(j<t,\ t<r+1)$. Assume that in (36) we have $\alpha+\beta = \alpha_i+1$, $\alpha-\beta = \alpha_i-1$ $(i=1,2,\dots,t)$, where $\alpha_i \neq 1, >0$ and are sufficiently small in comparison with d_i, and also $\alpha_i > \alpha_{i-1}+2$. In this case $\nu_{\mathfrak{A}_{d_{i,1}}}(u_{\alpha_i+1})$ and $\nu_{\mathfrak{A}_{d_{i,1}}}(u_{\alpha_i-1})$ are equal to α_i+1 and α_i-1, respectively. Now we select s so that we should have the inequalities

$$\{(\alpha_i+1)s/d_j\} > \{(\alpha_i-1)s/d_j\} \qquad (i=1,2,\dots,t-1)$$

and

$$\{(\alpha_t+1)s/d_j\} < \{(\alpha_t-1)s/d_j\}.$$

For this it is sufficient to take

$$(\alpha_t-1)s = (d_j-c)/2,$$

where $0<c<2(\alpha_t-1)$. Indeed,

$$\{(\alpha_t+1)s/d_j\}d_j = \{(d_j-c)/2d_j + (d_j-c)/d_j(\alpha_t-1)\}d_j = \{(d_j+c)2d_j - (d_j-c)/d_j(\alpha_t-1)\}d_j < \{(d_j-c)/2d_j\}d_j$$

and

$$\{(\alpha_i+1)s/d_j\}d_j = (\alpha_i+1)s, \quad \{(\alpha_i-1)s/d_j\}d_j = (\alpha_i-1)s \quad (i=1,2,\dots,t-1)$$

by virtue of $\alpha_t > \alpha_i+2$ and $s=(d_j-c)/2(\alpha_t-1)$. For such values of α_i, on the basis of (42) we have

$$\left.\begin{aligned} &U_+ \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,1}}); \quad W_+ \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,s}}) \\ &\text{in the case } t \not\equiv 0 (\mathrm{mod}\, 2) \text{ and} \\ &U_+ \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,s}}), \quad W_+ \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,1}}) \end{aligned}\right\} \tag{43}$$

in the case $t \equiv 0 (\mathrm{mod}\, 2)$. Since $\sum_{j=1}^{r+1} a_j Q_j = O$, from (43) it follows that

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,1}}) \qquad (t \not\equiv 0 (\mathrm{mod}\, 2)),$$

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_{i,s}}) \qquad (t \equiv 0 (\mathrm{mod}\, 2)).$$

Selecting for the basis point $O_m = \{u_1, v_1\}$ of order m on φ the point $\{u_l, v_l\}$, where l is arbitrary, relatively prime with m, for $t \not\equiv 0 (\mathrm{mod}\, 2)$ we shall have

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_i,(1/c)}),$$

i.e., all $\mathfrak{A}_{d_i,j}$ for $d_i > c(n, h(\mathcal{K}), N)$ are units of the field $\mathcal{K}'$.

In the case $t \equiv 0 (\mathrm{mod}\, 2)$ we denote by $\mathcal{R}$ the sum of the ranks τ of all group curves (37), related by the condition $abc = C$, $\prod_{s=1}^{N} q_s \equiv 0 (\mathrm{mod}\, C)$, and we consider the system

$$T_i = \{u_i, v_i\} = \sum_{j=1}^{\mathcal{R}} a_{j,i} Q_j,$$

where $Q_j \in$ (37) and all the possible coordinates u_i, v_i are determined by formulas (38). From the collection of points T_i we select $\mathcal{R}$ points for which

$$T_i = \sum_{j=1}^{\mathcal{R}} a_{j,i} Q_j \quad (i = 1, 2, \ldots, \mathcal{R}) \text{ and } \nu_2(\|a_{j,i}\|) = \min.$$

Then for any of the remaining points T_s one has the equality

$$\sum_{i=1}^{\mathcal{R}} b_i T_i + b_s T_s = O, \tag{44}$$

where b_i, b_s are integers and $b_s \not\equiv 0 (\mathrm{mod}\, 2)$. From (44) one can see that for at least $d_i / c(n, h(\mathcal{K}), N)$ points one has the relation

$$T_{s_1} \sim T_{s_2} \quad (s_1 \neq s_2). \tag{45}$$

Inserting in (36) $\{\alpha, \beta\} = \{2 + \beta_i, \beta_i\}, \{2 - \beta_j, \beta_j\}$, $\beta_i, \beta_j \in \{1, 2, \ldots, [d_i/2]\}$, from (44) we derive

$$u_{2+2\beta_1} / u_2 \sim u_2 / u_{2-2\beta_2}, \quad u_2^2 \sim u_{2+2\beta_1} u_{2-2\beta_2}. \tag{46}$$

Obviously, for any β_1 and β_2 we have

$$\nu_{\mathfrak{A}_{d_i,[d_i/2]}}(u_2^2) < \nu_{\mathfrak{A}_{d_i,[d_i/2]}}(u_{2+2\beta_1} u_{2-2\beta_2}),$$

and therefore from (46) it follows that

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_i,[d_i/2]}). \tag{47}$$

As in the previous case, together with (47) one has the congruences

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_i,([d_i/2]/t)}), \quad (t, m) = 1,$$

whence

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{A}_{d_i,j}), \quad j = 1, 2, \ldots, [d_i/2], \quad (j, d_i) = 1.$$

Finally, making use of the isogeny of the curves $u^4 + au^2 + b = v^2$ and $u^4 - 2au^2 + a^2 - 4b = v^2$, we obtain similarly

$$1 \equiv 0 (\mathrm{mod}\, \mathfrak{B}_{d_i,j}), \quad j = 1, 2, \ldots, [d_i/2], \quad (j, d_i) = 1.$$

Thus, for sufficiently large d_i in comparison with $c(n, h(\mathcal{K}), N)$, we have

$$1 \equiv 0 \pmod{\prod_{d_{i,j}} \mathfrak{B}_{d_{i,j}} \mathfrak{A}_{d_{i,j}}}.$$

Taking in (36) $\alpha, \beta \equiv 0 \pmod{\text{g.c.d.}(d_i)}$ $(d_i < c(n, h(\mathcal{K}), N))$, we have

$$\left.\begin{aligned} &\varepsilon_x + 1 = \varepsilon_y(\varepsilon_x - 1), \quad 1 \equiv 0 \pmod{\varepsilon_x}, \\ &\varepsilon_x = u_{(2d+1)\text{g.c.d.}(d_i)} / u_{\text{g.c.d.}(d_i)} \end{aligned}\right\} \tag{48}$$

But Eq. (48) over the field $\mathcal{K}'$ has only a finite number of solutions.

Therefore, taking into account that $u_{(2d_1+1)\text{g.c.d}(d_i)} \neq u_{(2d_2+1)\text{g.c.d.}(d_i)}$ for $2d_1 \not\equiv 2d_2 \pmod{m/\text{g.c.d.}(d_i)}$, from this we deduce that

$$m < c(n, h(\mathcal{K}), N).$$

The theorem is proved.

COROLLARY. The torsion of the elliptic curves, birationally isomorphic over some extensions of the field $\mathcal{K}$ with the curve

$$T: \quad y^2 = x(x-1)(x-t^2),$$

is uniformly bounded by the constant $c(n, h(\mathcal{K}))$, depending only on the power n and on the number of classes of divisors $h(\mathcal{K})$ of this field.

Indeed, it is sufficient to rewrite the equation of the curve T in the form

$$v^2 = (u^2 - (t-1)^2)(u^2 - (t+1)^2),$$

$$u = y/x, \qquad v = 2x - 1 - t^2 - y^2/x^2$$

and to take into account that from the birational isomorphism of the elliptic curves there follows the birational isomorphism of the corresponding Jacobi curves.

Thus, we have proved the uniform boundedness of the torsion of the Jacobi and elliptic curves in that formulation of the problem which was indicated in [1, p. 240].

LITERATURE CITED

1. E. Galois, Works [Russian translation], Moscow–Leningrad (1936).
2. V. A. Dem'yanenko, "The torsion of analytic curves," Izv. Akad. Nauk SSSR, Ser. Mat., 35, 280-307 (1971).
3. B. Mazur, "Rational points on modular curves," in: Lect. Notes Math., 601, 107-148. Springer-Verlag, Berlin (1977).