ACTA ARITHMETICA
XCIX.3 (2001)

Genus one curves defined by separated variable polynomials and a polynomial Pell equation

by

Roberto M. Avanzi (Essen) and Umberto M. Zannier (Venezia)

1. Introduction and statement of the results. In this paper we discuss the following problem:

Problem 1.1. *Determine all pairs (G, H) of polynomials in one variable over a field K of characteristic zero such that the degrees m of G and n of H are coprime and the curve given by*

$$\mathcal{C}: \quad G(X) = H(Y)$$

has genus one.

We characterize all the solutions to the above problem. These are, apart from a finite number of cases, two infinite families whose elements correspond to the isomorphism classes of elliptic curves together with a torsion point. We exploit this to compute explicit presentations of all the solutions over the rationals.

The condition $(m, n) = 1$ alone implies the irreducibility of the curve (Ehrenfeucht's criterion, [E, Tv]), so it makes sense to speak of the genus.

Problem 1.1 finds its motivation in the more general problem of determining all the pairs (G, H) of polynomials with rational coefficients such that the value sets of G and H over the rationals have infinite intersection (i.e. that $\#\{G(\mathbb{Q}) \cap H(\mathbb{Q})\} = \infty$). By a theorem of Faltings [Fa] there must be an absolutely irreducible factor of the polynomial $G(X) - H(Y)$ of genus at most one. On the other hand, if we ask that the value sets over the integers have infinite intersection, then by a theorem of Siegel ([Sie], a proof is also given in [Sil, Ch. IX, §§3, 6]) the polynomial $G(X) - H(Y)$ must have a genus zero factor (with at most two infinite places).

2000 *Mathematics Subject Classification*: Primary 14H45; Secondary 11C08, 11D41, 12E05, 12E10, 12Y05, 14H25, 14H52.

Key words and phrases: separated variable polynomials, genus one curves, polynomial Pell equations, modular curves, Chebyshev and Dickson polynomials, computer-based calculations.

In the genus zero case with $(m,n)=1$, Ritt's Second Theorem gives a complete answer (see [Sch3, pp. 40–41]). Proved in 1922 by J. F. Ritt [Ri], it is equivalent to the following statement (see [Sch3, §5] and [Z]):

RITT'S SECOND THEOREM. *Let K be a field. Let G, $H \in K[t]$ have coprime degrees m, n resp. such that $G'H' \neq 0$ and that the curve $G(X) = H(Y)$ has genus zero. Then the pair (G,H) is equivalent over the algebraic closure of K (as in Definition 1.2 below) to*

$$(t^m, t^r P(t)^m) \tag{1}$$

for a suitable polynomial P and $r \in \mathbb{N}$, or to

$$(T_m(t), T_n(t)) \tag{2}$$

where the polynomials T_d are the normalized Chebyshev polynomials.

This results admits several proofs, including [Fr1], [Sch3, §5] and [Z]. The interesting work [Fr4] contains also a comprehensive set of references about recent developments. P. Müller [Mü] derives Ritt's theorems in a group-theoretical setting.

In the genus zero case Michael Fried [Fr1] went even further: he solved it when $(m,n) \leq 2$ and also for arbitrary $d=(m,n)$ provided the degrees m and n are larger than some number $N(d)$ and $\mathcal{C}$ is irreducible ([Fr1, Theorem 4]) ([1]).

Recently Yuri Bilu and Robert Tichy [BT] gave a very explicit finiteness criterion for *all* the polynomials of the form $G(X)-H(Y) \in \mathbb{Q}[X,Y]$ with infinitely many rational points with bounded denominators, going beyond [Fr1] in determining in which cases one actually gets infinitely many rational points with bounded denominators, removing Fried's *cyclic reduced pairs*.

The genus one case has not yet been investigated, as far as the authors are aware, apart from the very special case arising from the problem of finding arithmetic progressions with equal product of consecutive terms: the authors of [BST] find some polynomials which fall in our families as a special case. Later (Remark 1.12) we briefly go deeper into this problem.

Since the main motivations are diophantine, we have treated this problem only in characteristic zero.

We summarize a few facts about our solution, which is more complicated than in the genus zero case:

(i) the degree of one of the two polynomials is always bounded;

([1]) In passing we note he faced the older (see [DLS]) problem of the reducibility of arbitrary polynomials of the form $G(X)-H(Y)$. The case where one of G, H is indecomposable is essentially solved, assuming the Classification of the Finite Groups, in [Fr1], [Fr2, Theorem 1], [Fr3, Theorem 2.2] and [CC].

The general case when G and H are not indecomposable is still open.

(ii) we have some curves of the type $Y^m = G(X)$ which are the analogue of the solutions (1) of Ritt's Second Theorem (the *cyclic case*);

(iii) we get an *elliptic case* corresponding to the solutions of type (2);

(iv) there are, up to equivalence, 11 other curves not included in the cyclic and elliptic cases, which we call *sporadic*.

In the elliptic case we find polynomials defined over $\mathbb{C}$, which are essentially all solutions $G(X)$ to the polynomial Pell equation

$$G(X)^2 - f(X)R(X)^2 = 4 \tag{3}$$

for a suitable polynomial $R(X)$, where $f(X)$ is a degree 4 square-free monic polynomial (explicit formulae for the general solutions can be given, but we do not need them, as it suffices to prove that solutions exist and to compute those with rational coefficients). Some of these polynomials have been discovered by Akhiezer while studying polynomials which are extremal on two disjoint intervals ([2]) [A]. We generalize his terminology by calling them *elliptic polynomials*. The polynomials discovered by Akhiezer are sometimes called *Akhiezer polynomials*.

The solutions of the above equation (3) are parametrized by torsion points of elliptic curves as described in Theorem 2 below. This parametrization can be expressed in the language of modular curves.

We could say that torsion points on circles "parametrize" Chebyshev polynomials T_n in an analogous way.

The T_n's also satisfy a relation similar to (3), but with $f(X) = X^2 - 4$ of degree 2.

Composing Chebyshev polynomials with elliptic polynomials yields again elliptic polynomials: Theorem 2 gives a more precise statement.

Our results are collected in Theorems 1–3 and a Corollary.

Throughout this paper, $\Bbbk$ denotes a fixed algebraically closed field of characteristic zero.

DEFINITION 1.2. Two polynomials G and $\widetilde{G}$, with coefficients in $\Bbbk$, are said to be *equivalent* if there exists a linear function L such that $\widetilde{G} = G \circ L$, and write $\widetilde{G} \sim G$.

An ordered pair of polynomials (G, H) is said to be *equivalent* to the ordered pair $(\widetilde{G}, \widetilde{H})$ if there exist three linear functions M, L_1 and L_2 such that either

$$\widetilde{G} = M \circ G \circ L_1 \quad \text{and} \quad \widetilde{H} = M \circ H \circ L_2$$

or

$$\widetilde{G} = M \circ H \circ L_1 \quad \text{and} \quad \widetilde{H} = M \circ G \circ L_2,$$

and write $(G, H) \approx (\widetilde{G}, \widetilde{H})$.

([2]) This fact parallels the history of the first discovery of the Chebyshev polynomials, which are extremal on one interval.

THEOREM 1 (Main Theorem). *Let $G(X)$ and $H(Y)$ be two polynomials with coefficients in $\Bbbk$, and coprime degrees m and n. Then the irreducible curve $\mathcal{C} : G(X) = H(Y)$ has genus one if and only if the pair (G, H) is equivalent to some pair in one of the following families:*

(i) *the set $\mathcal{F}_1$ of pairs of type $(G(X), Y^n)$ such that the equation $Y^n = G(X)$ defines a genus one curve*;

(ii) *the sets $\mathcal{F}_2$ and $\mathcal{F}_3$ of elliptic cases, consisting of the pairs (G, H) where H is the normalized Chebyshev polynomial of degree 3 and 4 respectively, and G is a solution of the polynomial Pell equation (3) for a suitable monic square-free degree 4 polynomial $f(X)$: the $f(X)$'s such that the above equation is solvable are characterized by Theorem 2 below; moreover in $\mathcal{F}_3$ the sign of G is determined such that $G(X) + 2$ has exactly one root of odd multiplicity ([3]); and*

(iii) *the family $\mathcal{F}_s$ of the 11 sporadic pairs.*

A detailed definition of the sets $\mathcal{F}_1$, $\mathcal{F}_2$, $\mathcal{F}_3$ and $\mathcal{F}_s$ is given in Definitions 1.5–1.10.

Suppose now that K is an arbitrary field of characteristic zero.

Consider the polynomial Pell equation

$$G(X)^2 - f(X)R(X)^2 = \gamma \tag{4}$$

where $f(X)$ is a square-free degree 4 monic polynomial with coefficients in K. A solution of equation (4) over K is a triple $\tau = (G(X), R(X), \gamma)$ with $G(X)$ and $R(X) \in K[X]$ and $\gamma \in K^*$ which satisfy (4). The degree of τ is the degree of $G(X)$.

We endow the normalization Δ of the curve

$$Y^2 = f(X)$$

with an elliptic curve structure by choosing one of the two points at infinity (which, f being monic, are K-rational) as the identity element. Denote by π the other point at infinity.

The following theorem holds:

THEOREM 2. *The equation (4) is solvable with $G(X)$, $R(X)$ in $K[X]$ and $\gamma \in K^*$ if and only if π is a torsion point of Δ.*

Suppose now that π is a torsion point of order exactly N. Then (4) has a solution of degree dN for any positive integer d, and, for a fixed degree, the solution with G monic is unique (up to the sign of R).

Let (G_1, R_1, γ_1) be the solution with G_1 monic of minimal degree N. Then the solution (G_d, R_d, γ_d) with G_d monic of degree dN is given by

$$G_d(X) = D_d(G_1(X); \gamma_1/4), \qquad \gamma_d = 4^{1-d}\gamma_1^d$$

where D_d is the dth Dickson polynomial.

([3]) See Remark 1.6 below.

The polynomials $f(X)$ together with the solutions $G_1(X)$ of minimal degree correspond, up to linear change of the variable, to the isomorphism classes of elliptic curves together with a torsion point of given order.

There is a solution $(G_0, R_0, 4)$ with G_0 of degree N if and only if γ_1 is a square in K, and in this case, for any fixed d the polynomials $G(X)$ and $R(X)$ of degrees dN, resp. $dN-2$, which solve (3) are determined up to sign. Let G_0 be a solution to (3) of minimal degree N. Up to sign the solution $G_d(X)$ of degree dN is given by

$$G_d(X) = T_d(G_0(X)) \tag{5}$$

where T_d is the normalized Chebyshev polynomial of degree d.

If K is algebraically closed then we can clearly always suppose $\gamma = 4$ and N can be any natural number greater than 1.

Using Mazur's theorem ([Maz1, Maz2]) we get the following corollary to the above theorem:

COROLLARY 1.3. *If $K = \mathbb{Q}$ in Theorem 2 then N can only take the values $2 \le N \le 10$ and $N = 12$.*

It is possible to give explicit parametrizations of all the $f(X) \in \mathbb{Q}[X]$ such that the point π on the curve Δ has order exactly N. Moreover all solutions $(G_N(X;\mathbf{t}), R_N(X;\mathbf{t}), \gamma_N(\mathbf{t}))$ to (4) can be computed, with $G_N(X;\mathbf{t})$ monic of (minimal) degree N, where $\mathbf{t} = \{t_1, t_2, \ldots\}$ is a finite set of parameters which run through $\mathbb{Q}$ (except at most a finite number of values), $G_N(X;\mathbf{t})$ and $R(X;\mathbf{t}) \in \mathbb{Q}(\mathbf{t})[X]$ and $\gamma_N(\mathbf{t}) \in \mathbb{Q}(\mathbf{t})$.

If $N = 2$ or 3 then we can take $\#\mathbf{t} = 2$, and if $N > 3$ one parameter suffices.

In Section 5 we will discuss how to give explicit parametrizations for all the possible $f(X)$ and compute tables for $G(X)$, $R(X)$ and γ over $\mathbb{Q}$. The instructions we give are explicit enough to allow faithful reproduction of our computations, which required about 15 minutes with MAPLE [CGG$^+$] on an old IBM RS6000 workstation. More detailed information can be obtained from the authors.

The deep results of Merel, Oesterlé and Parent [Me, Oe, P] bound the torsion of elliptic curves over number fields. As a consequence, analogues of the preceding theorem hold for an arbitrary number field: in particular the degrees of the minimal solutions for any admissible $f(X)$ are bounded and explicit bounds can be given.

THEOREM 3. *Notation as in Corollary 1.3. Two polynomials $G(X)$ and $H(Y)$ with coefficients in $\mathbb{Q}$ and coprime degrees m and n, are such that the curve $\mathcal{C} : G(X) = H(Y)$ has genus one if and only if the pair (G, H) is equivalent over $\overline{\mathbb{Q}}$ to some pair in one of the following families*:

(i) $\mathcal{F}_1(\mathbb{Q})$, *that is, the elements of* $\mathcal{F}_1$ *with* $G(X) \in \mathbb{Q}[X]$.

(ii,a) *The set* $\mathcal{F}_2(\mathbb{Q})$ *of the polynomial pairs* (G, H) *defined by*

$$G(X) = D_d\Big(G_N(X;\mathbf{t}); \frac{\gamma_N(\mathbf{t})}{4}\Big),$$

$$H(Y) = \pm\Big(\frac{4}{\gamma_N(\mathbf{t})}\Big)^d D_3\Big(Y; \Big(\frac{\gamma_N(\mathbf{t})}{4}\Big)^d\Big)$$

for $N \in \{2, 4, 5, 7, 8, 10\}$, d *a positive integer coprime to* 3.

(ii,b) *The set* $\mathcal{F}_3(\mathbb{Q})$ *of the pairs* (G, H) *defined by*

$$G(X) = D_d\Big(G_N(X;\mathbf{t}); \frac{\gamma_N(\mathbf{t})}{4}\Big),$$

$$H(Y) = \varepsilon\Big(\frac{4}{\gamma_N(\mathbf{t})}\Big)^{3d/2} D_4\Big(Y; \Big(\frac{\gamma_N(\mathbf{t})}{4}\Big)^d\Big)$$

for $N \in \{3, 5, 7, 9\}$, d *an odd positive integer*, $\varepsilon \in \{\pm 1\}$. *For these values of* N, $\gamma_N(\mathbf{t})$ *is always a square in* $\mathbb{Q}(\mathbf{t})$, *and we can then fix a square root in* $\mathbb{Q}(\mathbf{t})$. *The sign of* $\sqrt{\gamma_N(\mathbf{t})}$ *can be chosen such that* $G(X)+2(\gamma_N(\mathbf{t})/4)^{d/2}$ *has exactly one root of odd multiplicity and* $\varepsilon = 1$, *that is,* $H(Y)+2(\gamma_N(\mathbf{t})/4)^{d/2}$ *is a square* (*cf. Proposition* 2.2).

(iii) *The family* $\mathcal{F}_s(\mathbb{Q})$ *of the* 7 *sporadic pairs with rational coefficients, which is a subset of* $\mathcal{F}_s$.

Remark 1.4. For a given number field K, Faltings's proof of the Mordell conjecture and the above results imply that the solution set over K is given, up to equivalence, by the solutions over the rationals plus a finite number of other pairs.

The rest of the paper contains the proofs of the above theorems and the necessary definitions. The largest part of the work is devoted to the proof of Theorem 1.

The main idea behind the proof of Theorem 1 is simple. We consider the following genus zero curves together with coverings

$$\mathcal{C}' : \quad Z = G(X) \quad \text{with} \quad \Phi_1 : \mathcal{C} \to \mathcal{C}',\ Y \mapsto Z = H(Y), \tag{6}$$

$$\mathcal{C}'' : \quad Z = H(Y) \quad \text{with} \quad \Phi_2 : \mathcal{C} \to \mathcal{C}'',\ X \mapsto Z = G(X), \tag{7}$$

then we apply Riemann–Hurwitz' genus formula to the coverings Φ_1 and Φ_2. To complete the classification using this idea is in principle straightforward but in practice tricky, as Section 4 shows.

We now give the definitions used in the statements of the theorems. The reader should be aware that, unfortunately, a few lengthy definitions need to be given.

Definition 1.5 (Standard pairs of cyclic type). Let $\mathcal{F}_1$ be the set of the following pairs of polynomials:

(i) $(Y^2, g_0 \prod_1^3 (X - x_i) G_0(X)^2)$;
(ii) $(Y^3, g_0[(X - x_1)(X - x_2)]^s G_0(X)^3)$ with $s = 1$ or 2;
(iii) $(Y^4, g_0(X - x_1)^s (X - x_2)^2 G_0(X)^4)$ with $s = 1$ or 3;
(iv) $(Y^6, g_0(X - x_1)^s (X - x_2)^3 G_0(X)^6)$ with $s = 2$ or 4;

where $G_0 \in \Bbbk[X]$ and $x_i \neq x_j$ for all i, j.

Note that in $\mathcal{F}_1(\mathbb{Q}) = \mathcal{F}_1 \cap \mathbb{Q}[X]$ the fact that $G(X) \in \mathbb{Q}[X]$ does not imply that the roots x_i's are rational, except in (iii) and (iv).

If we put $Z = Y/G_0(X)$ in the definition above, then we see that the above pairs define curves which are birational to the curves $Z^r = L(X) = \prod (X - x_i)^{s_i}$, where the covering $X \to L(X)$ has no more than 3 finite ramification points.

The above pairs are the analogue to the cyclic case of Ritt's Second Theorem. The obvious example of elliptic curves in Weierstrass form is covered by (i).

Before giving the next definitions, we make the following

Remark 1.6. Note that if two polynomials $G(X)$, $f(X)$ of degrees n and 4 respectively and $f(X)$ square-free satisfy (4) for some $\gamma \in K^*$, then $(f(X), R(X))$ has degree d at most 1. If $d = 1$ then $R(X)$ is square-free whereas if $d = 0$ then $R(X)$ has at most one multiple root, of multiplicity exactly 2, all the other roots being simple (this can be proved using Mason's *abc*-Theorem (see [La]) or with the arguments used in the proof of Lemma 4.5).

The number of roots of odd multiplicity of $G(X) - 2$ plus the number of roots of odd multiplicity of $G(X) + 2$ is 4.

Definition 1.7 (Standard pairs of the first elliptic type). The set $\mathcal{F}_2$ is the set of pairs of polynomials $(T_3(Y), G(X))$ where $T_3(Y)$ is the normalized Chebyshev polynomial of degree 3, $G(X)$ is a solution to (3) and $3 \nmid n = \deg(G)$.

Definition 1.8 (Standard pairs of the second elliptic type). The set $\mathcal{F}_3$ is the set of pairs of polynomials $(T_4(Y), G(X))$ with $m = \deg(G)$ odd and such that $G(X)$ is a solution to (3), with the sign chosen in such a way that $G(X) - 2$ (resp. $G(X) + 2$) has exactly three roots of odd multiplicity (resp. one).

Definition 1.9 (Sporadic pairs). Let $\sqrt{-7}$ be a fixed square root of -7. We define the following polynomials:

$$B_1(X) = 3X^4 - 4X^3,$$
$$B_2(X) = (X^2 - 1)^3,$$
$$B_3(X) = X^4(4X - 5),$$

$$B_4(X) = \frac{1}{64}(X^2+3)^2(X+3)^2 - 1,$$
$$C_1(X) = -\frac{1}{108}X^3(X-5)^2,$$
$$C_2(X) = -1 - \frac{1}{108}(X^2+5)^2(2X-5).$$

We also define

$$C_{3,j}(X) = -\frac{\widetilde{C}_{3,j}(X)}{\widetilde{C}_{3,j}(\beta_j)},$$

for $j = 1$ or 2, where

$$\widetilde{C}_{3,j}(X) = (X^2+\alpha_j)^3(X+1),$$
$$\alpha_1 = \frac{1}{14}(-3-\sqrt{-7}), \quad \alpha_2 = \frac{1}{14}(-3+\sqrt{-7}),$$
$$\beta_j = -\frac{1}{7}(3+\sqrt{9-7\alpha_j});$$

and

$$C_4(X) = \frac{1}{1728}(X^3+9X+6)^3,$$
$$C_5(X) = -(X^2-1)^4,$$
$$C_6(X) = -\frac{1}{16}X^4(X-3)^2.$$

DEFINITION 1.10. The set $\mathcal{F}_s$ consists of the following 11 pairwise non-equivalent pairs of polynomials: (B_1, C_1), (B_1, C_2), $(B_1, C_{3,j})$ for $j = 1, 2$, (B_1, C_4), (B_2, C_1), $(B_2, C_{3,j})$ for $j = 1, 2$, (B_3, C_5), (B_3, C_6) and (B_4, C_2).

The set $\mathcal{F}_s(\mathbb{Q})$ consists of the 7 pairs: (B_1, C_1), (B_1, C_2), (B_1, C_4), (B_2, C_1), (B_3, C_5), (B_3, C_6) and (B_4, C_2).

REMARK 1.11. The last statement of Lemma 4.6 can be used to prove that a pair (G, H) of K-polynomials is equivalent to one of the 4 pairs $(B_l, C_{3,j})$ for $1 \le l, j \le 2$ if and only if -7 is a square in K.

Hence we can define $\mathcal{F}_s(K)$ to be $\mathcal{F}_s$ if -7 is a square in K or to be $\mathcal{F}_s(\mathbb{Q})$ otherwise.

REMARK 1.12. F. Beukers, T. N. Shorey and R. Tijdeman in [BST] are concerned with equations of the form

$$X(X+1)\dots(X+(m-1)) = Y(Y+\lambda)(Y+2\lambda)\dots(Y+(n-1)\lambda).$$

They do not assume $(m, n) = 1$. The pairs arising from the genus one cases 1 and 3 in their Theorem 2.2 are equivalent to objects in our $\mathcal{F}_1$. Their case 7 is equivalent to a pair belonging to $\mathcal{F}_2$ and to $\mathcal{F}_3$: this is due to the fact that

degree 3, 4 Chebyshev polynomials are equivalent to elliptic polynomials (just change the "defining" ramification points).

Acknowledgements. The authors wish to thank Yuri Bilu, Enrico Bombieri, Gerhard Frey, Michael Fried, Steven Galbraith, Peter Müller, Hans-Georg Rück, Dave Rusin and Helge Tverberg for interesting remarks, material and stimulating discussions. We want to thank also the referee for the valuable feedback and for showing us a simpler proof of formula (5).

The first author has been supported in part by a scholarship of the Graduiertenkolleg "Theoretische und experimentelle Methoden der reinen Mathematik". The first author also thanks Istituto Universitario di Architettura, Venezia, for partial support during his visits there.

2. Preliminary results. Following [Sch3] we define the *normalized Chebyshev polynomials* $T_d(X)$ by

$$T_0(X) = 2, \quad T_1(X) = X, \quad T_{d+1}(X) = XT_d(X) - T_{d-1}(X).$$

They are precisely the polynomials such that

$$T_d(z + z^{-1}) = z^d + z^{-d}. \tag{8}$$

They satisfy the relation

$$T_d \circ T_e = T_{de} = T_e \circ T_d$$

and are related to the classical Chebyshev polynomials

$$C_d(X) = \cos(d \arccos X)$$

by $T_d(2X) = 2C_d(X)$.

In this paper when we write Chebyshev polynomials we always mean the normalized ones.

For $a \in \Bbbk$, the nth *Dickson polynomial* $D_n(X; a)$ is defined by the relation

$$D_d(z + a/z; a) = z^d + (a/z)^d,$$

which, once a square root of a is fixed, gives

$$a^{d/2} T_d(a^{-1/2} X) = D_d(X; a). \tag{9}$$

Further information about Dickson polynomials can be found in [LMT, Chapter 2]. If $a \in \mathbb{Q}$ then $D_n(X; a) \in \mathbb{Q}[X]$.

Definition 2.1. We say that λ is an *extremum* of $F(X)$ if $F(X) - \lambda$ has a multiple root. The extrema of $F(X)$ are precisely the values taken by $F(X)$ at the zeros of $F'(X)$.

For any polynomial $F(X)$ we define its *root type*, denoted by $\mathcal{M}(F)$, as the unordered list of the multiplicities of the distinct roots of $F(X)$. For example, if $F(X) = 5(X^2 - 1)^3(X - 3)^2(X + 2)$ then $\mathcal{M}(F) = [3, 3, 2, 1]$.

n roots of multiplicity m are denoted by m^n, so that the above example can be written as $\mathcal{M}(F) = [3^2, 2, 1]$.

The *type* of an extremum λ of $F(X)$ is the root type of $F(X) - \lambda$.

The following result, which can be deduced by the corresponding properties of the Chebyshev polynomials and (9), is also proved in [B].

PROPOSITION 2.2. *If $a \neq 0$ and $d \geq 3$ then $D_n(x; a)$ has exactly two extrema, namely $\pm 2a^{d/2}$. If d is odd then both have type $[2^{(d-1)/2}, 1]$. If d is even then $2a^{n/2}$ has type $[2^{(d-2)/2}, 1^2]$ and $-2a^{n/2}$ has type $[2^{d/2}]$.*

More precisely, for odd d we have

$$D_d(X; a) \pm 2a^{d/2} = (X \pm 2\sqrt{a})\Delta_d(X, \pm\sqrt{a})^2,$$

and for even d we have

$$D_d(X; a) - 2a^{d/2} = (X^2 - 4a)\Delta_d(X, \sqrt{a})^2,$$
$$D_d(X; a) + 2a^{d/2} = D_2(D_{d/2}(X; a); a^{d/2}) + 2a^{d/2} = D_{d/2}(X; a)^2$$

where the Δ_d are suitable polynomials.

REMARK 2.3. Let K be a characteristic zero field, $F(X) \in K[X]$ and α be algebraic over K. Then any element of the Galois group over K sends $F(X) - \alpha$ to a polynomial of the same root type. Therefore if the types of the extrema of $F(X)$ are pairwise distinct, then all extrema belong to K. In particular if α and β are conjugate over K then they have the same type.

The letters X, Y, Z denote indeterminates, and x, y, z are their images in the rational function fields.

Let $F = \Bbbk(x, y)$ be the function field of the curve $\mathcal{C}$. If $z = G(x) = H(y)$, then $\Bbbk(x) = \Bbbk(x, z)$ is the function field of the curve $\mathcal{C}'$. Let π run over all places of $F/\Bbbk(x)$.

We use the Riemann–Hurwitz formula applied to the function field extension $F/\Bbbk(x)$ (equivalently, to the covering Φ_1):

$$0 = 2g - 2 = \sum_{\pi} (e_\pi - 1) - 2n, \tag{10}$$

where g is the genus of $\mathcal{C}$, the sum is over the places π of $F/\Bbbk(x)$ and e_π is the ramification index of π over $\Bbbk(x)$.

DEFINITION 2.4. For any $x_0 \in \Bbbk$ define $r(x_0)$ to be the order of the root x_0 as root of $G(X) - G(x_0)$, i.e. $(X - x_0)^{r(x_0)} \parallel (G(X) - G(x_0))$.

For any $y_0 \in \Bbbk$ define $s(y_0)$ by $(Y - y_0)^{s(y_0)} \parallel (H(Y) - H(y_0))$.

It is clear that

$$n - 1 = \deg(H'(Y)) = \sum_{y_0 \in \Bbbk} (s(y_0) - 1). \tag{11}$$

The following statement is given without proof. Proofs of more general results can be found in [Z].

PROPOSITION 2.5. *If the point* $(x_0, y_0) \in \mathcal{C}/\Bbbk$, *i.e. if* $G(x_0) = H(y_0) = z_0$, *then there are exactly* $(r(x_0), s(y_0))$ *places* π *of* F *such that* $x(\pi) = x_0$ *and* $y(\pi) = y_0$ *and for all such* π *we have*

$$e_\pi = \frac{s(y_0)}{(r(x_0), s(y_0))}.$$

Moreover the (*only*) *place at infinity of* $\Bbbk(x)$ *is totally ramified in* F. *If* π_∞ *is the place at infinity of* F *then* $e_{\pi_\infty} = n = \deg(H)$.

For all finite points (x_0, y_0) of the curve $\mathcal{C}$ define

$$c(x_0, y_0) = \sum_{\pi : x(\pi) = x_0,\, y(\pi) = y_0} (e_\pi - 1).$$

As an immediate consequence of the above result, we get

$$c(x_0, y_0) = s(y_0) - (r(x_0), s(y_0)). \tag{12}$$

Fix y_0 and define

$$\sigma(y_0) = \sum_{x_0 : (x_0, y_0) \in \mathcal{C}} c(x_0, y_0) = \sum_{\substack{x_0 : (x_0, y_0) \in \mathcal{C} \\ s(y_0) \nmid r(x_0)}} \{s(y_0) - (r(x_0), s(y_0))\}. \tag{13}$$

All summands in the above formula are non-negative by definition: omitting some of them gives a lower bound for $\sigma(y_0)$ (see for example equations (30) and (31)).

By Proposition 2.5 we can rewrite (10) as

$$0 = \sum_{(x_0, y_0) \in \mathcal{C}} c(x_0, y_0) + (e_{\pi_\infty} - 1) - 2n$$

so that by (12) and (13),

$$\begin{aligned} n + 1 &= \sum_{(x_0, y_0) \in \mathcal{C}} c(x_0, y_0) \\ &= \sum_{(x_0, y_0) \in \mathcal{C}} \{s(y_0) - (r(x_0), s(y_0))\} = \sum_{y_0 \in \Bbbk} \sigma(y_0). \end{aligned} \tag{14}$$

Subtracting (11) from (14) we obtain

$$2 = \sum_{y_0 \in \Bbbk} \{\sigma(s_0) - (s(y_0) - 1)\} = \sum_{y_0 : H'(y_0) = 0} \{\sigma(s_0) - (s(y_0) - 1)\}. \tag{15}$$

For all $x_0 \in \Bbbk$ define

$$\varrho(x_0) = \sum_{\substack{y_0 \,:\, (x_0, y_0) \in \mathcal{C} \\ r(x_0) \nmid s(y_0)}} \{r(x_0) - (r(x_0), s(y_0))\}$$

and by symmetry

$$2 = \sum_{x_0 \in \Bbbk} \{\varrho(x_0) - (r(x_0) - 1)\} = \sum_{x_0 : G'(x_0) = 0} \{\varrho(x_0) - (r(x_0) - 1)\}. \tag{16}$$

REMARK 2.6. Formulae (16) and (15) are indeed "genus formulae". If we do not assume that the genus of our curve is 1, then the left hand side of both formulae reads $2g$ (in place of 2).

If we do not assume m and n to be coprime, then the number of places above w_∞ is (m, n) and the left hand sides read $2g + (m, n) - 1$.

Similar formulae were used by Fried ([Fr1]).

3. The polynomial Pell equation. In this section we prove Theorem 2.

This kind of problem has been already considered by Schinzel ([Sch1, Sch2]), Abel (see references in [Sch2]) and Hellegouarch and Lozach ([HL]) among others. Our solution paves the way for the computations described in Section 5.

Consider the normalization Δ of the curve

$$Y^2 = f(X).$$

There are two K-rational points at infinity. Let ∞_0 be the point chosen as zero element and $\pi = \infty_1$ be the other one.

The Jacobian variety $\mathcal{J}(\Delta)$ of Δ is the curve itself and for any point $\alpha \in \Delta$ we denote by $[\alpha]$ its image in the Jacobian.

We use the symbols $\oplus, \ominus$ to indicate sum and difference on the curve.

In the function field of the curve $Y^2 = f(X)$ the left hand side of (4) factorizes as follows:

$$G(x)^2 - (yR(x))^2 = (G(x) + yR(x))(G(x) - yR(x)),$$

which allows us to obtain the following relation between divisors:

$$\operatorname{div}(G(x) + yR(x)) + \operatorname{div}(G(x) - yR(x)) = 0.$$

In view of this relation, the rational functions $G(x) \pm yR(x)$, whose poles occur only at ∞, cannot vanish for finite x. Hence we can write

$$\operatorname{div}(G(x) - yR(x)) = m \cdot (-\infty_0 + \infty_1) \tag{17}$$

for a suitable choice of the sign of y and a suitable integer m.

Applying the map $[\cdot]$ to (17) we get by the Abel–Jacobi Theorem

$$m \cdot [\infty_1] = m \cdot (\ominus[\infty_0] \oplus [\infty_1]) = [m \cdot (-\infty_0 + \infty_1)] = 0. \tag{18}$$

Conversely, if (18) is satisfied then there exists a function ϕ on Δ such that $\operatorname{div}(\phi) = -m\infty_0 + m\infty_1$: since this ϕ has no finite poles, we can write $\phi = G(x) + yR(x)$ for suitable polynomials $G(X)$, $R(X) \in K[X]$ of degrees

m and $m-2$ respectively. Therefore we have reduced the problem of the existence of the polynomial G to the existence of curves Δ as above such that ∞_1 is a torsion point of order N dividing m.

It is clear that over an algebraically closed field of characteristic zero this is possible for every m.

It is also clear that if the order of ∞_1 is N then there are solutions with $G(X)$ of minimal degree, which is exactly N.

The divisor determines the function ϕ, and thus also $G(X)$ and $R(X)$, up to multiplication by a non-zero constant, hence monic solutions are uniquely determined by $f(X)$ and their degree.

Let $\sqrt{\gamma}$ be a square root of γ, possibly in a suitable extension L of K. Then there exist polynomials $\widetilde{G}(X) = \frac{2}{\sqrt{\gamma}}G(X)$ and $\widetilde{R}(X) = \frac{2}{\sqrt{\gamma}}R(X)$ in $L[X]$ such that

$$\widetilde{G}(X)^2 - f(X)\widetilde{R}(X)^2 = 4.$$

As solutions of the above equation, $\widetilde{G}(X)$ and $\widetilde{R}(X)$ are determined up to sign. Let $m = \deg(G)$ and write the above expression as

$$\left(\frac{\widetilde{G}(X)}{2}\right)^2 - f(X)\left(\frac{\widetilde{R}(X)}{2}\right)^2 = 1$$

and note that

$$\left(\frac{\widetilde{G}(X)}{2} \pm \sqrt{f(X)}\,\frac{\widetilde{R}(X)}{2}\right)^d = \frac{\widetilde{G}_d(X)}{2} \pm \sqrt{f(X)}\,\frac{\widetilde{R}_d(X)}{2} \tag{19}$$

for any $d > 1$, so that ([4])

$$\widetilde{G}_d(X)^2 - f(X)\widetilde{R}_d(X)^2 = 4$$

where $\widetilde{G}_d$ is up to sign the unique solution of degree dm for the given $f(X)$.

We note that

$$\begin{aligned}\widetilde{G}_d(X) &= \left(\frac{\widetilde{G}(X)}{2} + \sqrt{f(X)}\,\frac{\widetilde{R}_d(X)}{2}\right)^d + \left(\frac{\widetilde{G}(X)}{2} + \sqrt{f(X)}\,\frac{\widetilde{R}_d(X)}{2}\right)^{-d} \\ &= T_d\left(\frac{\widetilde{G}(X)}{2} + \sqrt{f(X)}\,\frac{\widetilde{R}_d(X)}{2} + \left(\frac{\widetilde{G}(X)}{2} + \sqrt{f(X)}\,\frac{\widetilde{R}_d(X)}{2}\right)^{-1}\right) \\ &= T_d(\widetilde{G}(X)).\end{aligned}$$

This proves formula (5).

If d is even then $\widetilde{G}_d(X)$, $\widetilde{R}_d(X) \in K[X]$, otherwise it is enough to multiply them by $\sqrt{\gamma}$. If we multiply them by $(\gamma/4)^{d/2}$ we get monic solutions—which by the above arguments are necessarily the unique monic solutions in

([4]) The argument is the same used to get all the solutions of a classical Pell equation from the minimal one.

$K[X]$—and (9) shows that the monic solution $G_d(X)$ of degree dN is given by $D_d(G(X);\gamma/4)$.

The other assertions now follow. ∎

4. Proof of the Main Theorem. In this section assumptions are as in the statement of the Main Theorem, the exception being Lemma 4.6 which does not require them.

The proof is divided into several smaller cases; first we consider the case when one of the two polynomials has only one extremum (Proposition 4.3), then the case when both have at least two extrema. We subdivide the latter case further according to the degree of H in three subcases: $\deg(H) = 3$, 4 and larger than 4, which are considered in Propositions 4.7, 4.8 and 4.12 respectively.

We recall that $\Bbbk$ is algebraically closed.

NOTATION 4.1 (for the whole section). Let $\lambda_1, \dots, \lambda_T$ be the T distinct extrema of $H(Y)$ in $\Bbbk$. Choose $y_1, \dots, y_T$ among the roots of $H'(Y)$ in such a way that $H(y_i) = \lambda_i$ and $s_i = s(y_i) > 1$ is maximal in the sense that if $H(y^*) = \lambda_i$ then $s(y^*) \le s_i$.

Clearly, $H(Y) - \lambda$ is a square-free polynomial for all $\lambda \notin \{\lambda_1, \dots, \lambda_T\}$.

By M_i we denote the number of distinct roots of $G(X) - \lambda_i$ whose multiplicity is not divisible by s_i. For each i, $1 \le i \le T$, we write

$$G(X) - \lambda_i = g_0\Big(\prod_{j=1}^{M_i} (X - x_{ij})^{r(x_{ij})}\Big) G_i(X)^{s_i} \tag{20}$$

with $s_i \nmid r(x_{ij})$ for all i,j, and $x_{ij} \ne x_{kl}$ if $i \ne k$ or $j \ne l$.

By S we denote the number of distinct values taken by $G(X)$ at the zeros of $G'(X)$.

Hence, T and S are the numbers of finite ramification points of the coverings Φ_1, respectively Φ_2 defined in (6) and (7).

LEMMA 4.2. *Let $y_0 \in \Bbbk$ be such that $s(y_0) > 1$ and let M be the number of the distinct points $x_{0i} \in \Bbbk$ such that $(x_{0i}, y_0) \in \mathcal{C}$ and $s(y_0) \nmid r(x_{0i})$ (i.e. the x_{0i} are the distinct roots of $G(X) - H(y_0)$ whose multiplicity is not a multiple of $s(y_0)$). Suppose that $G(X) - H(y_0)$ is not the t-th power of a polynomial of strictly smaller degree, with $t > 1$ and $t \mid s(y_0)$. In particular $M \ge 1$. Then*

$$\sigma(y_0) \ge s(y_0) - 1$$

and (up to a permutation of the indices) the following assertions hold:

(i) $\sigma(y_0) = s(y_0) - 1$ *if and only if* $M = 1$;
(ii) $\sigma(y_0) = s(y_0)$ *if and only if* $M = 2$, $s(y_0) = 2$;

(iii) $\sigma(y_0) = s(y_0) + 1$ *if and only if one of the following conditions is satisfied:*

(a) $s(y_0) = 2$, $M = 3$;
(b) $s(y_0) = 3$, $M = 2$;
(c) $s(y_0) = 4$, $M = 2$ *and* $(r(x_{01}), 4) = 1$, $(r(x_{02}), 4) = 2$;
(d) $s(y_0) = 6$, $M = 2$ *and* $(r(x_{01}), 6) = 2$, $(r(x_{02}), 6) = 3$;

(iv) $\sigma(y_0) > s(y_0) + 1$ *otherwise.*

Proof. Put $s = s(y_0)$. First, s cannot divide $r(x_0)$ for all x_0 such that $(x_0, y_0) \in \mathcal{C}$, otherwise $G(X) - H(y_0)$ would be an sth power of a polynomial of strictly smaller degree.

If $M = 1$ we put $d = (s, r(x_{01}))$, then $d \,|\, r(x_0)$ for all x_0 such that $(x_0, y_0) \in \mathcal{C}$ and $G(X) - H(y_0)$ is a dth power, whence $d = 1$ and, obviously, $\sigma(y_0) = s - 1$.

We now consider the case $M > 1$. We have $\{s - (s, r_{0i})\} \geq s/2$ for $i = 1, 2$ and $\sigma(y_0) \geq s$. Equality holds only if $M = 2$ and $\{s - (s, r_{0i})\} = s/2$ (in which case s must be equal to 2), as $\sigma(y_0) > s$ in all other cases. To complete the proof note that if $s = 5$ or $s \geq 7$ then $\sigma(y_0) \geq s + 3$ and the remaining cases can be handled one by one. ∎

Proposition 4.3. *Let $T = 1$. Then (G, H) is equivalent to some pair in $\mathcal{F}_1$.*

Proof. It is easy to see that $T = 1$ if and only if $H(Y) \sim h_0 Y^n$. Assume then that $H(Y) = h_0 Y^n$. By (15), we must have $\sigma(0) = s(0) + 1$ and the result follows from Lemma 4.2. ∎

From now on we can assume that G' and H' each have at least two distinct roots (equivalently, that G and H are not equivalent to monomials) so that S and T are > 1 and the degrees of G and H are greater than 2.

Remark 4.4. Differentiate both sides of (20) and, for all i, define the polynomial

$$V_i(X) = \Big(\prod_{j=1}^{M_i} (X - x_{ij})^{r(x_{ij})-1} \Big) G_i(X)^{s_i - 1}, \tag{21}$$

which is clearly a factor of $G'(X)$. Since $V_i(X) \,|\, (G(X) - \lambda_i)$ and the λ_i are pairwise distinct, the polynomials $V_i(X)$ are pairwise coprime, which also means that the sum of their degrees is bounded by $m - 1$.

We clearly have

$$\deg(G_i) \leq \frac{1}{s_i}(m - M_i) \tag{22}$$

and, since $\deg(G_i) + \deg(V_i) + M_i = m$, we see immediately that

$$\deg(V_i) \geq (m - M_i)\left(1 - \frac{1}{s_i}\right). \tag{23}$$

LEMMA 4.5. *Suppose $T > 1$. Put $M = M_1 + M_2$. Then*

$$m - (M - 1) \leq \deg(G_1) + \deg(G_2).$$

In general, if $\mathcal{T} \subseteq \{1, \dots, T\}$ where $\#\mathcal{T} \geq 2$, then

$$(\#\mathcal{T} - 1)m \leq \Big\{ \sum_{i \in \mathcal{T}} \deg(G_i) + M_i \Big\} - 1.$$

Proof. The first inequality is a particular case of the second one, so we just prove the latter. By Remark 4.4 we have

$$m - 1 \geq \sum_{i \in \mathcal{T}} \deg(V_i) = \sum_{i \in \mathcal{T}} (m - \deg(G_i) - M_i)$$

and the result follows. ∎

The following is a characterization of the polynomials defined in 1.9, which appear in the "sporadic" solutions to our problem.

LEMMA 4.6. *Let $F \in \Bbbk[X]$ be a polynomial. The following assertions hold:*

(i) *if $\mathcal{M}(F) = [3, 1]$ and $\mathcal{M}(F + 1) = [2, 1^2]$ then $F \sim B_1$;*
(ii) *if $\mathcal{M}(F) = [3^2]$ and $\mathcal{M}(F + 1) = [2, 1^4]$ then $F \sim B_2$;*
(iii) *if $\mathcal{M}(F) = [4, 1]$ and $\mathcal{M}(F + 1) = [2, 1^3]$ then $F \sim B_3$;*
(iv) *if $\mathcal{M}(F) = [3, 1^3]$ and $\mathcal{M}(F + 1) = [2^3]$ then $F \sim B_4$;*
(v) *if $\mathcal{M}(F) = [3, 2]$ and $\mathcal{M}(F + 1) = [2, 1^3]$ then $F \sim C_1$;*
(vi) *if $\mathcal{M}(F) = [3, 1^2]$ and $\mathcal{M}(F + 1) = [2^2, 1]$ then $F \sim C_2$;*
(vii) *if $\mathcal{M}(F) = [3^2, 1]$ and $\mathcal{M}(F + 1) = [2^2, 1^3]$ then $F \sim C_{3,j}$ for $j = 1$ or 2;*
(viii) *if $\mathcal{M}(F) = [3^3]$ and $\mathcal{M}(F + 1) = [2^2, 1^5]$ then $F \sim C_4$;*
(ix) *if $\mathcal{M}(F) = [4^2]$ and $\mathcal{M}(F + 1) = [2, 1^6]$ then $F \sim C_5$;*
(x) *if $\mathcal{M}(F) = [4, 2]$ and $\mathcal{M}(F + 1) = [2, 1^4]$ then $F \sim C_6$.*

Over a field K of characteristic zero there are polynomials satisfying the hypothesis of (vii) *if and only if -7 is a square in K. In particular, this does not happen if $K = \mathbb{Q}$.*

Proof. We note that if F or $F + 1$ satisfy any of the hypotheses (i)–(x), then also F' is completely determined—that is, the roots of F' are among the roots of F and of $F + 1$ (in other words such an F has precisely two extrema). Moreover we can always without loss of generality make a linear change of variables such that two roots of F or $F + 1$ are given.

• In case (i) we have $F(X) = cX^3(X-\alpha)$. Then $F'(X) = cX^2(4X-3a)$. Without loss of generality we can pick $\alpha = 4/3$, so that the two roots of $F'(X)$ are 0 and 1. Then $F(1) = -c/3$ and we pick $c = 3$.

• Cases (ii), (iii), (v), (ix) and (x) are handled along the same lines.

• In case (iv) we start with $\widetilde{F}(X) = (X^2+3)^2(X+\alpha)^2$ for α not yet determined and such that $\alpha^2+3 \neq 0$. Then $\widetilde{F}'(X) = 6(X^2+3)(X+\alpha)P(X)$ with $P(X) = X^2 + \frac{2}{3}\alpha X + 1$. In order for $\widetilde{F}(X) - \lambda$ to have a root of multiplicity 3 for some $\lambda \neq 0$, $P(X)$ must be a square and $\lambda = \widetilde{F}(\varrho)$ where ϱ is the double root of $P(X)$. This is achieved if and only if $\alpha = 3$ or -3: since the two values lead to equivalent polynomials (obtained through the substitution $X \mapsto -X$) we just fix $\alpha = 3$. Now $\varrho = -1$ and $\widetilde{F}(-1) = 64$, hence $F(X) = \widetilde{F}(X)/64 - 1$ is up to equivalence the unique polynomial satisfying the hypothesis of (iv).

• In case (vi) we write $\widetilde{F}(X) = (X^2+20)^2(X-\alpha)$. Then $\widetilde{F}'(X) = 5(X^2+20)P(X)$ with $P(X) = X^2 - \frac{4}{5}\alpha X + 4$. As above, $P(X)$ must be a square, which happens only if $\alpha = \pm 5$; the two choices lead to equivalent polynomials so we choose $\alpha = 5$. Then $P(X) = (X-2)^2$, $\widetilde{F}(2) = -1728$, and we conclude that $F \sim C_2$.

• We now prove (vii) and also the last statement about $C_{3,j}$. Write $\widetilde{F}(X) = (X^2+a)^3(X+b)$ with $a \neq -b^2$ and $\widetilde{F}(X) \in K[X]$ where K is a field of characteristic zero. We infer that $a, b \in K$ (we can use the Galois action over K, which sends roots to roots of the same multiplicity). Up to equivalence, we assume that $b = 1$.

We have $\widetilde{F}'(X) = 7(X^2+a)^2P(X)$ where $P(X) = X^2 + \frac{6}{7}X + \frac{1}{7}a$. Now $F+1$ has two distinct double roots and they are roots of $\widetilde{F}'(X)$; thus they are the roots of $P(X)$. Let them be ϱ_1 and ϱ_2; the condition $\widetilde{F}(\varrho_1) = \widetilde{F}(\varrho_2)$ implies that the remainder of division of $\widetilde{F}(X)$ by $P(X)$ must be constant.

The coefficient of X in the remainder of the division of $\widetilde{F}(X)$ by $P(X)$ is

$$Q(a) = -\frac{6^3}{7^6}(9-7a)(49a^2+21a+4).$$

The equation $Q(a) = 0$ has three solutions: one is $a = 9/7$, which leads to $P(X)$ with a double root, and therefore is to be discarded; the other two are given by

$$a = (-3 \pm \sqrt{-7})/14. \tag{24}$$

Let α_1, α_2 be the two values of a in (24). We get the two polynomials $C_{3,j}$ for $j = 1, 2$ which are not equivalent (but are algebraic conjugates). In the above expression for the derivative we have $P(X) = X^2 + \frac{6}{7}X + \frac{1}{7}a$, and β_j is simply one of the two distinct solutions we get when $a = \alpha_j$ for $j = 1, 2$. Now, $\widetilde{C}_{3,j}(\beta_j)$ is just the remainder of the division of $\widetilde{C}_{3,j}(X)$ by $P(X)$,

which is in K as long as a is. Therefore we have proved (vii) and the last statement.

• Finally, we deal with case (viii). We start with $\widetilde{F}(X) = F_1(X)^3$, where $F_1(X) = X^3 + aX^2 + bX + c$. We can assume up to equivalence that $a = 0$, whence $\widetilde{F}(X) = (X^3 + bX + c)^3$ and $\widetilde{F}'(X) = (X^3 + bX + c)^2 P(X)$ where $P(X) = 9X^2 + 3b$. As above $P(X)$ must be square-free and the coefficient of X in the remainder of the division of $\widetilde{F}(X)$ by $P(X)$ must be 0; we get the equation

$$81bc^2 - 4b^4 = 0.$$

We want $b \neq 0$ such that $P(X)$ is not a square, and we get the following parametrization for the K-rational solutions:

$$b = 9t^2, \quad c = 6t^3 \quad \text{for } t \in K,\ t \neq 0.$$

Different choices of t lead to equivalent polynomials so we fix $t = 1$. Write $P(X) = 9(X - i\sqrt{3})(X + i\sqrt{3})$, we have $\widetilde{F}(i\sqrt{3}) = \widetilde{F}(-i\sqrt{3}) = -1728$.

Then $F(X) = \frac{1}{1728}\widetilde{F}(X) \in \mathbb{Q}[X]$ is up to equivalence the unique polynomial satisfying the hypothesis. ∎

Proposition 4.7. *If $S, T > 1$ and $n = 3 < m$ then (G, H) is equivalent to a pair in $\mathcal{F}_2$.*

Proof. Up to equivalence we can assume that $\lambda_1 = -2$ and $\lambda_2 = +2$, and since $T > 1$ we must have $\mathcal{M}(H - 2) = \mathcal{M}(H + 2) = [2, 1]$. Using the methods of Lemma 4.6 we conclude that $H(Y) \sim T_3(Y) = Y^3 - 3Y$.

Now, $s(y_i) = 2$ and $\sigma(y_i) = M_i$, thus (15) reads $2 = \{M_1 - 1\} + \{M_2 - 1\}$, i.e. $4 = M_1 + M_2$. Hence

$$(G(X) - 2)(G(X) + 2) = f(X) \cdot R(X)^2$$

for some $R(X), f(X) \in \Bbbk[X]$, where $f(X)$ is square-free and has degree 4. This concludes the proof. ∎

Proposition 4.8. *If $S, T > 1$ and $n = 4 < m$, then (G, H) is equivalent to a pair in $\mathcal{F}_3$ or to one of the pairs (B_1, C_1), (B_1, C_2), $(B_1, C_{3,j})$ for $j = 1$ or 2, and (B_1, C_4).*

Proof. Since $T > 1$, we look at the possible $\mathcal{M}(H')$ where $H'(Y)$ is not equivalent to a monomial. Up to equivalence there are three possibilities for $H(Y)$:

$$\begin{aligned}
&\text{(I):} && \mathcal{M}(H - \lambda_1) = [3, 1] \quad \text{and} \quad \mathcal{M}(H - \lambda_2) = [2, 1^2];\\
&\text{(II):} && \mathcal{M}(H - \lambda_1) = \mathcal{M}(H - \lambda_2) = \mathcal{M}(H - \lambda_3) = [2, 1^2];\\
&\text{(III):} && \mathcal{M}(H - \lambda_1) = [2^2] \quad \text{and} \quad \mathcal{M}(H - \lambda_2) = [2, 1^2].
\end{aligned}$$

Let us consider first case (I). We assume that $\lambda_1 = 0$ and $\lambda_2 = -1$. Then $H(Y) \sim B_1(Y)$ by Lemma 4.6(i).

For $j = 1, 2$, let M_{1j} be the number of roots x_0 of $G(X)$ whose multiplicity $r(x_0)$ is such that $r(x_0) \equiv j \pmod 3$. Then $M_1 = M_{11} + M_{12}$.

We have $s(y_1) = 3,\ \sigma(y_1) = 2M_1,\ s(y_2) = 2$ and $\sigma(y_2) = M_2$, thus by (15) we get the relation

$$2M_1 + M_2 = 5. \tag{25}$$

We see immediately that M_2 is odd, which implies that m is odd.

By Remark 4.4 we have

$$\frac{2}{3}(m - M_1) + \frac{m - M_2}{2} \le \deg(V_1(X)) + \deg(V_2(X)) \le m - 1,$$

which implies, using (25), the inequality

$$5 \le m \le M_2 + 4 \le 9. \tag{26}$$

By (25) and (26) there are three possible subcases according to the value of M_1:

• $M_1 = 0$ and $M_2 = 5$. Then $G(X) = g_0 G_1(X)^3$ and $m = 9$. Since $\deg(V_1) = 6$ we must have $\deg(V_2) \le 2$, which implies that $G(X) + 1$ has at most one root of multiplicity at most 3 or at most two double roots. Since it has 5 roots of odd multiplicity, it is clear that $\mathcal{M}(G+1) = [2^2, 1^5]$. Moreover, $G_1(X)$ must be square-free as otherwise $G(X)$ would give a factor of $G'(X)$ of degree larger than 6. Hence $\mathcal{M}(G) = [3^3]$ and Lemma 4.6(viii) implies $(G, H) \approx (B_1, C_4)$.

• $M_1 = 1$ with $M_2 = 3$. If $M_{11} = 0$ and $M_{12} = 1$ then $m \equiv 2 \pmod 3$ so that $m = 5$. Now $\mathcal{M}(G)$ can be $[5]$ or $[3, 2]$ (which yield V_i of degree 4 and 3 respectively) whereas $\mathcal{M}(G + 1)$ can be $[2, 1^3]$ or $[3, 1^2]$ (giving V_2 of degree 1 and 2). Since by Remark 4.4 we have $4 \ge \sum_{i=1}^{2} \deg(V_i)$, we are left with the case satisfying the hypothesis of Lemma 4.6(v) with $F = G$. Hence $(G, H) \approx (B_1, C_1)$.

If $M_{11} = 1$ and $M_{12} = 0$ then $m \equiv 1 \pmod 3$, thus $m = 7$. Now $\mathcal{M}(G)$ can be one of $[7]$, $[3, 4]$, $[6, 1]$ and $[3^2, 1]$, whereas $\mathcal{M}(G + 1)$ can be one of $[5, 1^2]$, $[4, 1^3]$, $[3, 2, 1^2]$ and $[2^2, 1^3]$. We conclude that the only possible case is that of the hypothesis of Lemma 4.6(vii) with $F = G$, whence $(G, H) \approx (B_1, C_{3,j})$ for $j = 1$ or 2.

• $M_1 = 2$. Then $M_2 = 1$. By (25) and (26) we must have $m = 5$. Now $\mathcal{M}(G)$ can be $[4, 1]$ or $[3, 1^2]$ and $\mathcal{M}(G + 1)$ can only be $[5]$, $[3, 2]$, $[4, 1]$ or $[2^2, 1]$. It follows that $\mathcal{M}(G) = [3, 1^2]$, $\mathcal{M}(G + 1) = [2^2, 1]$ and by Lemma 4.6(vi) we get $(G, H) \approx (B_1, C_2)$.

We now show that case (II) cannot happen. In this case $T = 3$, and for $1 \le i \le 3$ we have $s(y_i) = 2$ and $\sigma(y_i) = M_i$. Then (15) gives $2 = \sum_{i=1}^{3} \{M_i - 1\}$, i.e. $5 = \sum_{i=1}^{3} M_i$. From Remark 4.4 (namely the bounds (23) and $\sum_{i=1}^{3} \deg(V_i) \le m - 1$) we obtain $m \le 3$, a contradiction.

Consider finally case (III). Here we choose $\lambda_1 = -2$ and $\lambda_2 = +2$. Denote the two double roots of $H(Y) + 2$ by y_{11} and y_{12}.

Then $H(Y) \sim T_4(Y) = Y^4 - 4Y^2 + 2$. We have

$$s(y_{11}) = s(y_{12}) = s(y_2) = 2, \quad \sigma(y_{11}) = \sigma(y_{12}) = M_1, \quad \sigma(y_2) = M_2,$$

so we get $2 = 2\{M_1 - 1\} + \{M_2 - 1\}$, or $2M_1 + M_2 = 5$. As n is even, m must be odd and we have $M_1 = 1$, $M_2 = 3$. Reasoning as at the end of the proof of Proposition 4.7 we now conclude that (G, H) belongs to $\mathcal{F}_3$. ∎

Now if, say, $G(X) - \lambda$ is not a perfect power of a polynomial of smaller degree for all $\lambda \in \Bbbk$, then in (15) all summands are non-negative. Since their sum is 2, Lemma 4.2 limits the possibilities for T, the s_i and the M_i. The aim of the next proposition is to show that this is, essentially, always the case.

PROPOSITION 4.9. *If S and T are greater than 1 then for every choice of μ and λ in $\Bbbk$, the polynomials $G(X) - \mu$ and $H(Y) - \lambda$ cannot both be perfect powers of smaller degree polynomials.*

The proof of Proposition 4.9 uses the following

LEMMA 4.10. *Assumptions as in Proposition 4.9. Suppose further $G(X) = G_*(X)^r$ with $r > 1$. Then the curve $X^r = H(Y)$ has genus zero and $H(Y) \sim h_0 Y^q H_1(Y)^r$ with $(q, r) = 1$, where $H_1(Y)$ is a polynomial.*

Proof. Put $z = G_*(x)$ and $m_* = \deg(G_*)$. By doing this we embed the field $L = \Bbbk(z, y)$ of the curve defined by $Z^r = H(Y)$ in $F = \Bbbk(x, y)$, the function field of $\mathcal{C}$. Thus L has genus at most one. We want to prove that it is zero. Suppose L is elliptic; then the extension F/L is Galois and Abelian, and by the Riemann–Hurwitz formula it is also non-ramified. Now $[F : \Bbbk(x)] = [L : \Bbbk(z)] = \deg(H)$, thus it is also $[F : L] = [\Bbbk(x) : \Bbbk(z)] = m_*$. Consider the place w at infinity in $\Bbbk(z)$. It ramifies totally in $\Bbbk(x)$ with ramification index m_*, and the place at infinity in $\Bbbk(x)$ ramifies totally in F with index n. Therefore the ramification index of w in F is $m_* n$ which is maximal, being equal to the degree of the field extension. Therefore the place at infinity of L over w is also totally ramified in F with maximal index m_*, and, as the extension is non-ramified, it follows that $m_* = 1$. On the other hand $T > 1$ implies $m_* > 1$. This contradiction proves the first part of the statement.

The second part follows at once. ∎

Proof of Proposition 4.9. We prove the result by contradiction. Without loss of generality we can replace the pair (G, H) with an equivalent one, therefore we assume that our curve is given by $G(X) = H(Y)$ with $G(X) = G_*(X)^r$ and $r > 1$ an integer, and that for some $\lambda \in \Bbbk$ we have $H(Y) - \lambda = H_*(Y)^s$ with $s > 1$.

From Lemma 4.10 the curve

$$\mathcal{C}'/\Bbbk : \quad X^r = H(Y)$$

has genus zero and we can assume that $H(Y) = h_0 Y^q H_1(Y)^r$ with $(q, r) = 1$ and $H_1(Y) \in \Bbbk[Y]$ non-constant (because $T > 1$).

We now want to prove that $\lambda = 0$ and, implicitly, that $H(Y) - \delta$ for $\delta \neq 0$ is never a power of a smaller degree polynomial.

If $\lambda \neq 0$ then $Y^{q-1} H_1(Y)^{r-1} H_*(Y)^{s-1}$ would be a factor of $H'(Y)$, hence of degree $\leq n-1$, which would imply that $0 < n(1 - 1/r - 1/s) \leq -q/r$. Hence $\lambda = 0$ and we can write

$$H(Y) = h_0 Y^{as} H_0(Y)^{rs} \tag{27}$$

with $(a, r) = 1$, $H_0(0) \neq 0$ and $\deg(H_0) > 0$. One infers that the polynomial

$$Q(Y) = Y^{as-1} H_0(Y)^{rs-1}$$

is a factor of (H, H') of degree $\{n - 1 - (n - as)/(rs)\}$.

The same arguments applied to $G(X)$ yield

$$G(X) = g_0 X^{br} G_0(X)^{rs} \tag{28}$$

with $(b, s) = 1$, $G_0(0) \neq 0$ and $\deg(G_0) > 0$. Thus

$$P(X) = X^{br-1} G_0(X)^{rs-1}$$

is a factor of (G, G') of degree $\{m - 1 - (m - br)/(rs)\}$.

Exchanging G and H if necessary, we can assume without loss of generality that $m > n$.

From Lemma 4.2, if $H(y_0) \neq 0$ and $s(y_0) > 1$ then $\{\sigma(s_0) - (s(y_0) - 1)\} \geq 0$.

We write (15) in the form

$$2 = \mathcal{A} + \mathcal{B} \tag{29}$$

where

$$\mathcal{A} = \{\sigma(0) - (s(0) - 1)\} + \sum_{y_0 \,:\, H_0(y_0) = 0} \{\sigma(s_0) - (s(y_0) - 1)\}$$

and

$$\mathcal{B} = \sum_{\substack{y_0 \,:\, H'(y_0) = 0 \\ H(y_0) \neq 0}} \{\sigma(s_0) - (s(y_0) - 1)\}.$$

The summands of $\mathcal{B}$ are non-negative; the same is not necessarily true of those of $\mathcal{A}$, but we can give lower bounds for them. For every root y_0 of H_0 let $\mu(y_0)$ be its multiplicity (thus $s(y_0) = rs\mu(y_0)$). By (27) and (28) we have

$$\sigma(0) - (s(0) - 1) \geq (as - (as, br)) - (as - 1) \geq 1 - a \tag{30}$$

(see the comment after (13)) and also, for every y_0 such that $H_0(y_0) = 0$,

$$\begin{aligned} \sigma(s_0) - (s(y_0) - 1) &\geq (rs\mu(y_0) - (rs\mu(y_0), br)) - (rs\mu(y_0) - 1) \\ &\geq 1 - r\mu(y_0). \end{aligned} \tag{31}$$

Summing (31) over the roots of $H_0(Y)$ we get

$$\sum_{y_0 \,:\, H_0(y_0)=0} \{\sigma(s_0) - (s(y_0) - 1)\} \geq 1 - r \deg(H_0) = 1 - n/s + a. \tag{32}$$

We combine (30) and (32) with (29) to obtain $2 = \mathcal{A} + \mathcal{B} \geq 2 - n/s + \mathcal{B}$, whence $\mathcal{B} \leq n/s$. In particular, for any y_0 such that $s(y_0) > 1$ and $G(y_0) \neq 0$ we have

$$\{\sigma(s_0) - (s(y_0) - 1)\} \leq n/s. \tag{33}$$

With the notation of 4.1, we can assume that $\lambda_1 = 0$ and that y_1 is a root of $H(Y)$. Since $T > 1$, we put $s_2 = s(y_2) > 1$ and see that $(Y - y_2)^{s_2 - 1}$ is a factor of $H'(Y)$ coprime to $Q(Y)$. Bounding the sum of their degrees by $n - 1$ we get

$$s_2 - 1 \leq \frac{n - as}{rs}. \tag{34}$$

Now, $P(X)$ and $V_2(X)$ are coprime factors of $G'(X)$. Bounding the sum of their degrees by $m - 1$ and using the fact that $\sum_{j=1}^{M_2} r(x_{2j}) \geq M_2$ we get

$$m\left(1 - \frac{1}{s_2} - \frac{1}{rs}\right) \leq M_2\left(1 - \frac{1}{s_2}\right) - \frac{b}{s}. \tag{35}$$

We now want to prove that $s_2 = 2$. Suppose $s_2 \geq 3$. In this case $\sigma(y_2) \geq 2M_2$, and we use (33) and (34) to write

$$\frac{n}{s} \geq \sigma(y_2) - (s_2 - 1) \geq 2M_2 - (s_2 - 1) \geq 2M_2 - \frac{n - as}{rs},$$

in other words, since $m > n$,

$$M_2 \leq \frac{1}{2}\left(\frac{n}{s} + \frac{n - as}{rs}\right) < \frac{m}{3}.$$

Using this inequality, (35) and the fact that $rs \geq 6$ we obtain the desired contradiction:

$$\frac{m}{2} \leq m\left(1 - \frac{1}{s_2} - \frac{1}{rs}\right) < M_2 < \frac{m}{3}.$$

Thus $s_2 = 2$, and (33) with $y_0 = y_2$ gives the bound $M_2 = \sigma(y_2) \leq n/s + 1$, which yields in turn

$$M_2 < m/s + 1.$$

This bound for M_2 and (35) with $s_2 = 2$ imply that

$$\frac{m}{3} < \frac{m-2b}{2s} + \frac{1}{2}.$$

Since $s \geq 2$ and $b \geq 1$, this is absurd.

This contradiction shows that *at least one* of the two polynomials G, H is *not* the power of a smaller degree polynomial plus a constant. ∎

The result just proved allows us to work without loss of generality under a following hypothesis:

(∗) *for every $\lambda \in \Bbbk$ the polynomial $G(X) - \lambda$ is not the perfect power of a polynomial of smaller degree.*

Moreover we can suppose that n and m are greater than or equal to 5 (and that T and S are greater than 1).

REMARK 4.11. Hypothesis (∗) and Lemma 4.2 imply that in (15) all summands are non-negative integers. Therefore only two cases are possible: either there exists some $y_0^* \in \Bbbk$ such that

$$\begin{cases} \sigma(y_0) = s(y_0) - 1 & \text{for all } y_0 \neq y_0^*, \\ \sigma(y_0^*) = s(y_0^*) + 1; \end{cases}$$

or there exist exactly two elements y_{01} and y_{02} in $\Bbbk$ such that

$$\begin{cases} \sigma(y_0) = s(y_0) - 1 & \text{for all } y_0 \notin \{y_{01}, y_{02}\}, \\ \sigma(y_{0i}) = s(y_{0j}) & \text{for } i = 1, 2. \end{cases}$$

In both cases using Lemma 4.2 one infers that, for any set of indices $\mathcal{T} \subseteq \{1, \ldots, T\}$, one has $\sum_{i \in \mathcal{T}} M_i \leq \#\mathcal{T} + 2$.

PROPOSITION 4.12. *If $S, T > 1$ and the polynomials G and H both have degree larger than 4, then (G, H) is equivalent to one of the following pairs: (B_2, C_1), $(B_2, C_{3,j})$ for $j = 1$ or 2, (B_3, C_5), (B_3, C_6) and (B_4, C_2).*

Proof. By Proposition 4.9 we can suppose that (∗) holds. Choose now $y_1, y_2, \ldots$ as in 4.1. Assume also that $s_1 \geq s_2$. We can also assume without loss of generality that $\lambda_1 = 0$ and $\lambda_2 = -1$.

Extend the notation of 4.1 putting $r_{ij} = r(x_{ij})$ and $r_i = \sum_{j=1}^{M_i} r_{ij}$.

• We claim that $T = 2$, $s_1 \geq 3$ and $M_1 \leq 2$. Suppose there exists a set of indices $\mathcal{T} \subseteq \{1, \ldots, T\}$ with $\#\mathcal{T} = 3$. By Lemma 4.5,

$$2m \leq \left(\sum_{i \in \mathcal{T}} \frac{m - M_i}{2} + M_i \right) - 1 = \frac{3}{2} m + \sum_{i \in \mathcal{T}} \frac{M_i}{2} - 1.$$

By Remark 4.11 we have $\sum_{i \in \mathcal{T}} M_i \leq 5$, therefore $m \leq 3$, a contradiction.

We prove the second claim: suppose $s_1 = 2$. Then also $s_2 = 2$. Moreover $M_1 \equiv M_2 \pmod 2$. If we had $M_1 = M_2 = 1$ then (since $T = 2$) all roots y_* of $H'(Y)$ would satisfy $s(y_*) = 2$ and $\sigma(y_*) = 1$, in contradiction with (15).

Assume then that $M_1 \neq 1$. By Lemma 4.2 and Remark 4.11 either $M_1 = M_2 = 2$ or $M_1 = 3$ and $M_2 = 1$. It is easy to see that in both cases $H(Y)$ has only one double root, all other roots being simple. For example, in the case $M_1 = M_2 = 2$, suppose $H(Y)$ has (at least) a multiple root y_1' other than y_1. By assumption then $s_1 = s(y_1') = s_2 = 2$ and $\sigma(y_1) = \sigma(y_1') = \sigma(y_2) = 2$. With these values one gets already a contradiction from (15), as all other summands in the genus formula are non-negative as we assume $(*)$. The other case is similar, but it suffices to consider the double roots of $H(Y)$.

Now $H(Y)$ contributes a degree 1 factor to $H'(Y)$ and $H(Y)+1$ contributes a factor of degree at most $n/2$, and the product of these factors is, up to a multiplicative constant, equal to $H'(Y)$. In other words $n-1 \leq n/2+1$, or $n \leq 4$. But $n > 4$, and this contradiction proves the second claim.

The third claim now follows by Remark 4.11 and Lemma 4.2.

• From Remark 4.4 and in particular from (23) we get

$$(m - M_1)\left(1 - \frac{1}{s_1}\right) + (m - M_2)\left(1 - \frac{1}{s_2}\right) \leq \deg(V_1) + \deg(V_2) \leq m - 1.$$

Using $r_i \geq M_i$ and the fact that $s_1 \geq 3$, we write

$$m \leq \frac{(M_1 + M_2 - 1)s_1 s_2 - (M_1 s_2 + M_2 s_1)}{s_1 s_2 - (s_1 + s_2)}. \tag{36}$$

• If $M_1 = 2$, since $s_1 \geq 3$ we have $\sigma(y_1) \geq s_1 + 1$. We fall in the first case of Remark 4.11 with $\sigma(y_1) = s_1 + 1$ and $\sigma(y_2) = s_2 - 1$. The last equality implies also $M_2 = 1$.

We have

$$5 \leq m \leq 2 + \frac{s_1}{s_1 s_2 - (s_1 + s_2)}, \tag{37}$$

which implies that $s_2 \leq \frac{4}{3} s_1/(s_1 - 1)$. The last inequality and $s_1 \geq 3$ imply that $s_2 = 2$. The same inequality and the fact that $s_2 = 2$ gives $s_1 = 3$. Now (37) implies that $m = 5$.

Bounding the sum of the degrees of coprime factors of $G'(X)$ as usual we infer that $r_{11} = r_{12} = r_{21} = 1$ and that G_1 and G_2 are square-free, so that $\mathcal{M}(G) = [3, 1^2]$ and $\mathcal{M}(G+1) = [2^2, 1]$. Thus $G(X) \sim C_2(X)$ by Lemma 4.6(vi).

Moreover, y_1 is also the only multiple root of $H(Y)$, since for any other such root y_1' we would also have $\sigma(y_1') \geq s(y_1') + 1$, contradicting Remark 4.11.

At this point we can write $\mathcal{M}(H) = [3, 1^{n-3}]$ and $\mathcal{M}(H+1) = [2^k, 1^{n-2k}]$. Thus $n - 1 = 2 + k$ with $n \geq 2k$ so that $n \leq 6$. As m and n are coprime $n = 6$. Finally $H(Y) \sim B_4(Y)$ by Lemma 4.6(iv) and $(G, H) \approx (B_4, C_2)$.

• Consider now the case $M_1 = 1$. We necessarily have $M_2 > 1$ otherwise by (36) we would get $m \leq 1$, a contradiction. Then, by Remark 4.11 and Lemma 4.2, either $s_2 = 2$ and $M_2 \leq 3$ or $s_2 \geq 3$ and $M_2 = 2$.

If $s_2 \geq 3$ then $5 \leq m \leq 2 + s_2/(s_1 s_2 - (s_1 + s_2))$ whence $3 \leq s_2/(s_1 s_2 - (s_1 + s_2))$ and $s_2(3s_1 - 4) \leq 3s_1$; this and $s_2 \geq 3$ now would imply that $s_1 \leq 2$, a contradiction.

Hence $s_2 = 2$ and (36) simplifies to

$$m \leq \frac{M_2 s_1 - 2}{s_1 - 2} = M_2 + 2\frac{M_2 - 1}{s_1 - 2}. \tag{38}$$

We cannot have $M_2 = 2$ (in the last inequality, if $M_2 = 2$ we get $m \leq 4$), so $M_2 = 3$ and (38) is satisfied only in the following cases: $s_1 = 4$ with $m = 5$ and $s_1 = 3$ with $m \leq 7$. Since $M_2 = 3$ and $s_2 = 2$ the root type of $H(Y) + 1$ is $[2, 1^{n-2}]$, as we fall in the first case of Remark 4.11.

Consider first the case $s_1 = 4$. Then $\mathcal{M}(G) = [4, 1]$ and $\mathcal{M}(G + 1) = [2, 1^3]$, whence $G(X) \sim B_3(X)$ by Lemma 4.6(iii). Since $H(Y)$ cannot have triple roots by Remark 4.11, we write $\mathcal{M}(H) = [4^l, 2^k, 1^{n-2k-4l}]$ with $l \geq 1$. Counting the roots of $H'(Y)$ from the root types of H and $H + 1$ we get $n - 1 = 3l + k + 1$. Clearly $4l + 2k \leq n$. The last two relations imply that $l + k \leq 2$ and $n \leq 8 - 2k$.

If $k = 0$ then $n \leq 8$ and we have thus two possibilities: $n = 6$ and $n = 8$. If $n = 6$ then $\mathcal{M}(H) = [4, 1^2]$ and $\mathcal{M}(H + 1) = [2, 1^4]$ with $T = 2$, which is absurd. Then $n = 8$ and $l = 2$ (the case $l = 1$ is discarded in the same way we have discarded $n = 6$), hence by Lemma 4.6(ix) it is $H(Y) \sim C_5(Y)$, and finally $(G, H) \approx (B_3, C_5)$.

If $k = 1$ then $n = 6$ and $l = 1$. By Lemma 4.6(x) we have $H(Y) \sim C_6(Y)$ and $(G, H) \approx (B_3, C_6)$.

Now consider the case $s_1 = 3$. From Lemma 4.5 follows that

$$\begin{gathered} m - 3 \leq \deg(G_1) + \deg(G_2), \quad \text{with} \\ \deg(G_1) \leq \left\lfloor \frac{m-1}{3} \right\rfloor \quad \text{and} \quad \deg(G_2) \leq \left\lfloor \frac{m-3}{2} \right\rfloor. \end{gathered} \tag{39}$$

This allows us to discard the case $m = 6$ at once.

If $m = 5$, then (39) implies $\deg(G_1) = \deg(G_2) = 1$, so that we can write $\mathcal{M}(G) = [3, 2]$ and $\mathcal{M}(G + 1) = [2, 1^3]$. By Lemma 4.6(v) we have $G \sim C_1$. Write $\mathcal{M}(H) = [3^l, 2^k, 1^{n-2k-3l}]$ with $l \geq 1$ (recall that $\mathcal{M}(H+1) = [2, 1^{n-2}]$). Then $n - 1 = 2l + k + 1$ with $3l + 2k \leq n$. Thus $l + k \leq 2$ and $n \leq 6 - k$. Since $m = 5$ we must have $n = 6$, and the relations just

proved imply $k = 0$ and $l = 2$. Using Lemma 4.6(ii) we conclude that $(G, H) \approx (B_2, C_1)$.

Lastly, if $m = 7$ by (39) we must have $\deg(G_1) = \deg(G_2) = 2$. Then $\mathcal{M}(G) = [3^2, 1]$ and $\mathcal{M}(G+1) = [2^2, 1^3]$. By Lemma 4.6(vii) we have $G \sim C_{3,j}$ for $j = 1$ or 2. To prove that $H(Y)$ has no double roots we observe that $\sigma(y_2) = s(y_2)+1$ and that for any double root y_1' of $H(Y)$ we would also have $\sigma(y_1') = s(y_1')+1$, contradicting Remark 4.11. Write then $\mathcal{M}(H) = [3^l, 1^{n-3l}]$ with $l \geq 1$. Hence $n-1 = 2l+1$ and since $l \leq n/3$ we get $n \leq 6$, but $n = 2l+2$ is even, so $n = 6$ and $l = 2$. Then $H(Y)$ is as in the case $m = 5$ above. Finally we infer that $(G, H) \approx (B_2, C_{3,j})$ for $j = 1$ or 2. ∎

We can now give the

Proof of the Main Theorem. It is immediate to see that any pair (G, H), possibly exchanging G and H, falls under the hypothesis of one of Propositions 4.3, 4.7, 4.8 or 4.12.

The fact that the defined pairs of polynomials indeed give genus one curves should be clear from the same arguments that led to them, or by a direct checking using (16) and (15). ∎

5. Computations for the arithmetic case. In this section we describe a method for performing the computations which are used to prove Corollary 1.3 and Theorem 3.

The interested reader can then reproduce our computations, or ask the authors to send the data by email. One will also find the complete tables in [Av].

The first assertion of Corollary 1.3 is clear by Theorem 2 and Mazur's celebrated theorem, which we quote here:

Mazur's Theorem (Maz1, Maz2). *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\mathrm{tors}}(\mathbb{Q})$ is one of the following fifteen groups*:

$$\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 10 \text{ or } N = 12;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4.$$

Further, each of these groups occurs as $E_{\mathrm{tors}}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

If $G(X), f(X), R(X) \in \mathbb{Q}[X]$ satisfy (4) for some γ, we can assume, by a linear change of variable over $\mathbb{Q}$, that $f(X) = X^4 + cX^2 + bX + a$.

We first determine the admissible $f(X)$, that is, those such that the point π on Δ is a torsion point. We get families of polynomials $f_N(X, \mathbf{t})$ for $2 \leq N \leq 10$ or $N = 12$ where $\mathbf{t}$ is a set of parameters. Then we solve the equation (4) as a system of equations in the coefficients of the polynomials $G(X)$ and $R(X)$ and in γ; the solutions will then be given by a CAS (Computer Algebra System) as rational functions in $\mathbf{t}$. We need

to do it only for the solutions with $G(X)$ of minimal degree N and with $f(X) = f_N(X, \mathbf{t})$.

In order to do this we bring the curve Δ into a normal form equivalent to that given by Tate. If $b \neq 0$ the birational morphism defined by

$$z = 2(X^2 + Y) + c, \quad w = (2X - d)z + 2b \quad \text{where} \quad d = \frac{4a - c^2}{2b}$$

maps Δ to the curve

$$E: \quad w^2 + 2dwz - 2bw = z^3 - (2c + d^2)z^2 \tag{40}$$

and the points ∞_0, resp. $\pi = \infty_1$ on Δ are mapped to the point at infinity, resp. $(0, 0)$ on E.

In what follows we implicitly use the methods and results of [Hu, §2] for a generic elliptic curve determined by a cubic equation

$$w^2 + a_1wz + a_3w = z^3 + a_2z^2.$$

The rational point $(0, 0)$ has order 3 if and only if $a_2 = 0$ and $a_3 \neq 0$. If it has finite order greater than 3 we can take a change of variables defined over the ground field so that $a_3 = a_2$, and get the Tate parametrization of coefficients

$$w^2 + (1 - P)wz - Qw = z^3 - Qz^2. \tag{41}$$

Instead of doing this we prefer to use the following form:

$$w^2 + L(1 - P)wz - L^3Qw = z^3 - L^2Qz^2, \tag{42}$$

which can be obtained from (41) via the transformation $(w, z) \mapsto (w/L^3, z/L^2)$ and is best suited to our computations. Suitable parametrizations of P and Q give all the elliptic curves over $\mathbb{Q}$ in Tate's form where the origin is a torsion point.

The needed parametrizations of P and Q are well known. For example if $P = t^2(t - 1)$ and $Q = t^2(t - 1)(t^2 - t + 1)$, then (41) and (42) describe all curves in Tate's normal form such that $(0, 0)$ is a point of order 9 as t runs through $\mathbb{Q} \setminus \{0, 1\}$. The method to determine them is sketched in [Hu, pp. 88–90]. They are also given in the online help system of Connell's MAPLE package **apecs**, available from [Co].

We then equate the coefficients of (42) and (40) and solve the resulting system for a, b, and c. In this way, when N is greater than 3, we parametrize all possible $f(X)$. Different choices of L yield equivalent polynomial $f(X)$, and thus lead to equivalent values of $G(X)$. Thus one can fix an arbitrary non-zero value of L.

If the order is 3 then we have $2c + d^2 = 0$ in (40). We express b as a function of a and c which are the parameters.

The case when the point has order 2 is easily handled. By Theorem 2 if we can solve (4) with $\deg(G) = 2$ then π on Δ has order 2. If $b = 0$ this actually happens for any choice of a and c since a general solution is given by $G(X; \{a, c\}) = X^2 + c/2$. Moreover, this can happen only if $b = 0$, because if $b \neq 0$ then the tangent to E at the origin has slope 0, which means that the order of π is not 2.

We thus compute polynomials $f_N(X; \mathbf{t}) \in \mathbb{Q}(\mathbf{t})[X]$ where $\mathbf{t}$ is the parameter set and $2 \leq N \leq 10$ or $N = 12$. If $N = 2$ or 3 then $\#\mathbf{t} = 2$, otherwise $\#\mathbf{t} = 1$.

Denote by $\mathrm{Coeff}(P(X), j)$ the coefficient of X^j in the polynomial $P(X)$.

Now we can use a computer to solve the system

$$\mathrm{Coeff}(G(X)^2, j) = \mathrm{Coeff}(f(X; \mathbf{t})R(X)^2, j) \quad \text{for } 1 \leq j \leq 2N - 1 \tag{43}$$

where the unknowns are the coefficients of the monic polynomials $G(X)$ and $R(X)$ (of course we do not equate the constant terms of the two sides).

We get, for each N, two polynomials $G_N(X; \mathbf{t})$ and $R_N(X; \mathbf{t}) \in \mathbb{Q}(\mathbf{t})[X]$. Next we compute

$$\gamma_N(\mathbf{t}) = G_N(X; \mathbf{t})^2 - f_N(X; \mathbf{t})R_N(X; \mathbf{t})^2. \tag{44}$$

Now $\gamma_N(\mathbf{t})$ is a square in $\mathbb{Q}(\mathbf{t})$ for odd N, which means that in Theorem 3(ii,b) we can fix a square root of $\gamma_N(\mathbf{t})$ in $\mathbb{Q}(\mathbf{t})$ as required and that $G(X)$ is actually a polynomial with rational coefficients.

The constants in Theorem 3 are chosen so that $G(X)$ is monic, the extrema of $H(Y)$ are $\pm 2(\gamma_N(\mathbf{t})/4)^{d/2}$ and the pairs are equivalent to the corresponding pairs given in Theorem 1.

This completes our description of the methods followed in our calculations. ∎

References

[A] N. I. Akhiezer, *Elements of the Theory of Elliptic Functions*, Providence, 1990.

[Av] R. M. Avanzi, *A study on polynomials in separated variables with low genus factors*, Dissertation, Fachbereich 6 (Mathematik und Informatik), University of Essen, 2001.

[BST] F. Beukers, T. N. Shorey and R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal product of terms*, in [GIU], 11–26.

[B] Yu. F. Bilu, *Quadratic factors of $f(x) - g(y)$*, Acta Arith. 90 (1999), 341–355.

[BT] Yu. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) - g(y)$*, ibid. 95 (2000), 261–288.

[CC] P. Cassou-Noguès et J.-M. Couveignes, *Factorisations explicites de $g(y) - h(z)$*, ibid. 87 (1999), 291–317.

[CGG$^+$] B. W. Char, K. O. Geddes, G. H. Gonnet, B. L. Leong, M. B. Monagan and S. M. Watt, *Maple V Language Reference Manual*, Springer, 1991.

[Co] I. G. Connell, *Elliptic Curve Handbook*, http://www.math.mcgill.ca/~connell/. At the same URL one can also download **apecs**.

[DLS] H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Math. Oxford (2) 12 (1961), 304–312.

[E] A. Ehrenfeucht, *A criterion of absolute irreducibility of polynomials*, Prace Mat. 2 (1958), 167–169 (in Polish).

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366. Erratum, ibid. 75 (1984), 381.

[Fr1] M. Fried, *On a theorem of Ritt and related diophantine problems*, J. Reine Angew. Math. 264 (1973), 40–55.

[Fr2] —, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. 17 (1973), 128–146.

[Fr3] —, *Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem*, in: Proc. Sympos. Pure Math. 37, Amer. Math. Soc., 1980, 571–601.

[Fr4] —, *Variables separated polynomials, the genus* 0 *problem and moduli spaces*, in [GIU], 169–228.

[GIU] K. Győry, H. Iwaniec and J. Urbanowicz (eds.), *Number Theory in Progress*, Proc. Intern. Conf. on Number Theory in Honor of A. Schinzel (Zakopane, 1997), de Gruyter, Berlin, 1999.

[HL] Y. Hellegouarch et M. Lozach, *Equation de Pell et points d'ordre fini*, Publ. Math. Orsay 86/01 (1986), 72–92; Appendix 93–95.

[Hu] D. Husemöller, *Elliptic Curves*, New York, 1987.

[La] S. Lang, *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. (N.S.) 23 (1990), 37–75.

[LMT] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman Monographs Surveys Pure Math. 65, Longman Sci. Tech., 1993.

[Maz1] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[Maz2] —, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.

[Me] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, ibid. 124 (1996), 437–449.

[Mü] P. F. Müller, *Primitive monodromy groups of polynomials*, in: Recent Developments in the Inverse Galois Problem, M. Fried (ed.), Contemp. Math. 186, Amer. Math. Soc., 1995, 385–401.

[Oe] J. Oesterlé, *Torsion des courbes elliptiques sur le corps de nombres*, in preparation.

[P] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur le corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116.

[Ri] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), 51–66.

[Sch1] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1961), 393–413.

[Sch2] —, *On some problems of the arithmetical theory of continued fractions II*, ibid. 7 (1962), 287–298. Corrigendum, ibid. 47 (1986), 295.

[Sch3] —, *Selected Topics on Polynomials*, Ann Arbor, 1982.

[Sie] C. L. Siegel, *Über einige Anwendungen diophantischer Approximation*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. 1 (1929), 41–69.

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, New York, 1986.

[Tv] H. Tverberg, *A remark on Ehrenfeucht's criterion for the irreducibility of polynomials*, Prace Mat. 8 (1963/64), 117–118.

[Z] U. Zannier, *Ritt's Second Theorem in arbitrary characteristic*, J. Reine Angew. Math. 445 (1993), 175–203.

Institut für Experimentelle Mathematik
Universität Gesamthochschule Essen
Ellernstr. 29
D-45326 Essen, Germany
E-mail: mocenigo@exp-math.uni-essen.de

Istituto Universitario di Architettura D.C.A.
Santa Croce 191
30135 Venezia, Italy
E-mail: zannier@dimi.uniud.it

Received on 11.5.1999
and in revised form on 29.6.2000 (3598)