ACTA ARITHMETICA
XCV.3 (2000)

The Diophantine equation $f(x) = g(y)$

by

Yuri F. Bilu (Basel) and Robert F. Tichy (Graz)

1. Introduction. Let $f(x)$ and $g(x)$ be polynomials with rational coefficients. We study the following question: does the equation

$$f(x) = g(y) \tag{1}$$

have finitely or infinitely many solutions in rational integers x and y?

Due to the classical theorem of Siegel (see Theorem 10.1 below), the finiteness problem for (1), and even for a more general equation $F(x, y) = 0$ with $F(x, y) \in \mathbb{Z}[x, y]$, is decidable ([1]). One has to:

- decompose the polynomial $F(x, y)$ into $\mathbb{Q}$-irreducible factors;
- for those factors which are not $\overline{\mathbb{Q}}$-reducible, determine the genus $\mathbf{g}$ and the number d of points at infinity of the corresponding plane curve;
- for the factors with $\mathbf{g} = 0$ and $d \leq 2$ determine whether the corresponding equation has finitely or infinitely many integral solutions (see [4, Section 1]).

Though this procedure completely solves the problem when the polynomials $f(x)$ and $g(x)$ are given numerically, it is not very helpful when they depend on unknown parameters, which often happens in applications.

In this paper we obtain a very explicit finiteness criterion for the equation (1). It turns out to be more convenient to study a slightly more general question: when does (1) have infinitely many rational solutions with a bounded denominator? We say that the equation $F(x, y) = 0$ *has infinitely*

2000 *Mathematics Subject Classification*: Primary 14H45; Secondary 11C08, 11D41, 11G30, 12E05, 12E10, 14H05, 14H25.

Key words and phrases: Ritt's second theorem, Dickson polynomials, reducibility, Diophantine equations.

The first author supported by the Lise Meitner Fellowship (Austria), grant M00421-MAT.

([1]) We mention in passing that the decidability of the *existence* problem (that is, whether or not $F(x, y) = 0$ has at least one solution) is still an open question. The answer, which is believed to be positive, is known only in particular cases.

many rational solutions with a bounded denominator if there exists a positive integer Δ such that $F(x,y)=0$ has infinitely many solutions $(x,y)\in\mathbb{Q}\times\mathbb{Q}$ with $\Delta x, \Delta y\in\mathbb{Z}$.

To formulate our criterion, we have to define five types of *standard pairs* $(f(x),g(x))$.

1.1. *Standard pairs.* In what follows a and b are *non-zero* elements of some field, m and n are positive integers, and $p(x)$ is a non-zero polynomial (which may be constant).

A *standard pair of the first kind* is

$$(x^m, ax^r p(x)^m)$$

or switched, $(ax^r p(x)^m, x^m)$, where $0\le r<m$, $(r,m)=1$ and $r+\deg p(x)>0$.

A *standard pair of the second kind* is

$$(x^2, (ax^2+b)p(x)^2)$$

(or switched).

Denote by $D_m(x,a)$ the mth Dickson polynomial, defined by

$$D_m(z+a/z,a)=z^m+(a/z)^m$$

(see Section 3). A *standard pair of the third kind* is

$$(D_m(x,a^n), D_n(x,a^m)),$$

where $\gcd(m,n)=1$.

A *standard pair of the fourth kind* is

$$(a^{-m/2}D_m(x,a), -b^{-n/2}D_n(x,b)),$$

where $\gcd(m,n)=2$.

A *standard pair of the fifth kind* is

$$((ax^2-1)^3, 3x^4-4x^3)$$

(or switched).

When we want to specify that the parameters a and b and the coefficients of the polynomial $p(x)$ belong to a field K we say *standard pair over* K.

If $(f(x),g(x))$ is a standard pair over $\mathbb{Q}$ of the first or third kind then (1) has infinitely many rational solutions with a bounded denominator. For the third kind, an infinite family of solutions is given by $x=D_n(t,a)$ and $y=D_m(t,a)$, where $t\in\mathbb{Z}$. For the first kind, find positive integers q and s with $qm-sr=1$. Then an infinite family of solutions is given by $x=a^q t^r p(a^s t^m)$ and $y=a^s t^m$, where $t\in\mathbb{Z}$.

If $(f(x),g(x))$ is a standard pair over $\mathbb{Q}$ of the second, fourth or fifth kind then (1) has infinitely many rational solutions with a bounded denominator for infinitely many choices of the parameters a and b.

For instance, for the second kind let (u, v) satisfy $u^2 = av^2 + b$. Then $x = up(v)$ and $y = v$ is a solution of (1). Hence (1) has infinitely many rational solutions with a bounded denominator whenever $u^2 = av^2 + b$ does, which happens for infinitely many choices of a and b.

For the fourth kind (where we assume, without loss of generality, that $n/2$ is odd), let (u, v) be a solution of $a^{m/2}u^2 + bv^2 = 4ab$. Then $x = a^{(2-n)/4}D_{n/2}(v, a)$ and $y = uE_{m/2}(v, a)$ (where $E_n(t, a)$ is defined in (8)) is a solution of (1), as follows from Proposition 3.1.

For the fifth kind, let (u, v) be a solution of $3au^2 = v^2 + 2$. Then $x = u(v + 2)$ and $y = ((v + 1)^3 + 4)/3$ is a solution of (1).

1.2. *The criterion*

THEOREM 1.1. *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent.*

(1.1.a) *The equation* (1) *has infinitely many rational solutions with a bounded denominator.*

(1.1.b) *We have $f = \varphi \circ f_1 \circ \lambda$ and $g = \varphi \circ g_1 \circ \mu$, where $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ are linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.*

We make several comments on this result.

REMARK 1.2. (i) The implication (1.1.b)⇒(1.1.a) is trivial. The non-trivial part is (1.1.a)⇒(1.1.b).

(ii) If $\gcd(\deg f, \deg g) = 1$ then in (1.1.b) we have $\deg \varphi = 1$, and $(f_1(x), g_1(x))$ is a standard pair of the first or third kind (over $\mathbb{Q}$). This reproduces a result of Schinzel [27, Theorem 8].

(iii) Write $f = a_p x^p + \ldots + a_0$ and $g = b_q x^q + \ldots + b_0$, and assume that a_p/b_q is not a perfect power in $\mathbb{Q}$. Then in (1.1.b) we have $\deg \varphi = 1$. (Indeed, $a_p/b_q = (a'/b')^{\deg \varphi}$, where a' and b' are the leading coefficients of f_1 and g_1, respectively.) Using this, one can easily prove, for instance, that the equation $\binom{x}{m} = y(y-1)\ldots(y-n+1)$ has finitely many solutions in integers x and y, when m and n are integers greater than 2. This was originally done by Brindza and Pintér [9].

(iv) One can express the assertion "$f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator" as an explicit arithmetical condition on the parameters a and b. For instance, for the second kind this means that a is positive, not a square, and $b = \mathcal{N}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}\beta$ for some $\beta \in \mathbb{Q}(\sqrt{a})$. For the other kinds one can proceed similarly. We do not go into this because we find Theorem 1.1 in its present form completely sufficient for applications.

(v) Actually, we obtain a more general result, on solutions of (1) in S-integers of an arbitrary number field (see Theorem 10.5). In this case one more kind of pairs can occur; to distinguish it from the standard pairs just defined, we call this new kind *specific pairs* (see Section 9).

(vi) Various applications of Theorem 1.1 will be given in the forthcoming papers [6, 8]. In particular, we solve the Diophantine problem involving Meixner polynomials, studied in [22]. (Beukers, Shorey and Tijdeman [3] considered another type of equations of the form (1), using methods very similar to ours.)

1.3. *Un peu d'histoire.* Finiteness conditions for the equation (1) were studied by many authors. For the equation $f(x) = y^n$ a finiteness theorem was established by Siegel [29] and LeVeque [24]. Evertse and Silverman [13] obtained a sharp estimate for the number of solutions. (See also a more recent paper of Voutier [34].)

Starting from Baker [2], methods for the effective analysis of the equation $f(x) = y^n$ were developed by Sprindžuk, Trelina, Brindza, Poulakis, Voutier and Bugeaud; see [31, 10] for the references. An efficient algorithm for the numerical solution of this equation was suggested in [7].

Davenport, Lewis and Schinzel [12] obtained a finiteness condition for the general equation (1). However, it was too restrictive for many applications.

Fried investigated the problem from various points of view in a remarkable series of paper [16, 17, 18]. In particular, he gave in [18, Corollary after Theorem 3] a new finiteness condition, much more general than that of [12], but still far from explicit.

Schinzel [27, Theorem 8] obtained a completely explicit finiteness criterion for the equation (1) under the assumption $(\deg f, \deg g) = 1$. His result is, basically, Remark 1.2(ii) of our paper.

Quite recently, Beukers, Shorey and Tijdeman [3] applied a similar approach to certain particular types of the equation (1).

1.4. *An overview of the paper.* The proof of Theorem 1.1 follows the main lines of the arguments of Fried [18] and Schinzel [27]. However, several substantially new ideas were required to drop Schinzel's assumption $(\deg f, \deg g) = 1$, retaining the explicit character of his result.

Call an absolutely irreducible polynomial $F(x, y) \in \mathbb{Q}[x, y]$ *exceptional* if the corresponding plane curve is of genus 0 and has at most 2 points at infinity. To deduce Theorem 1.1 from Siegel's theorem, one has to determine when the polynomial $f(x) - g(y)$ has an exceptional factor.

Our argument consists of two parts. In the first part (Sections 4–7) we show that if the polynomial $f(x) - g(y)$ itself is exceptional then (f, g) is a standard pair up to a linear transformation and linear change of variables. This generalizes the classical "Second theorem of Ritt".

In the second part (Sections 8–10) we classify pairs (f, g) such that $f(x) - g(y)$ has an exceptional factor. Due to a clever observation of Fried (see Theorem 8.1) this reduces to solving two independent problems.

(a) Determine when $f(x) - g(y)$ has a factor of degree at most 2.

(b) Given a polynomial $q(x, y)$ of degree at most two, determine for which $f(x)$ and $g(x)$ the polynomial $q(f(x), g(y))$ is exceptional.

Problem (a) is completely solved in [5]. The solution of (b) depends on whether $\partial^2 q/\partial x \partial y$ vanishes or not. If it does, then $q(f(x), g(y))$ can be written as $f_1(x) - g_1(y)$, reducing the problem to the generalized Ritt's second theorem, just proved. If $\partial^2 q/\partial x \partial y \neq 0$ then the solution of (b) is remarkably simple (see Proposition 9.2).

After all this work is done, our finiteness criterion becomes an (almost) immediate consequence of Siegel's theorem (see Section 10).

Acknowledgments. We are pleased to thank Roberto Maria Avanzi, Frits Beukers, Michael Fried, Peter Müller, Attila Pethő, Andrzej Schinzel, Robert Tijdeman, Gerhard Turnwald and Umberto Zannier for stimulating discussions and helpful suggestions. We are especially grateful to Andrzej Schinzel for detecting a number of inaccuracies in the text.

2. Terminology, notation, conventions

2.1. *General.* We use (a, b) for the greatest common divisor of a and b, when a and b are either integers or polynomials (in the latter case (a, b) is well defined up to a multiplicative constant). When it can be confused with (a, b) as an ordered pair, we write $\gcd(a, b)$.

We denote by $\lfloor x \rfloor$ the maximal integer not exceeding $x \in \mathbb{R}$.

2.2. *Fields.* All fields in this paper are of characteristic 0 (although some of the results are valid in arbitrary characteristic). The capital letter K (with or without indices) always stands for a field. We assume that all fields that occur in the paper are contained in one big algebraically closed (unnamed) field. In particular, any field K has a well defined algebraic closure $\overline{K}$, any two fields K and K' have well defined intersection $K \cap K'$ and composite KK', etc.

2.3. *Polynomials.* All polynomials are assumed non-constant, unless the contrary is stated explicitly. Given a polynomial $f(x)$ having s distinct roots (in an algebraically closed field), its *root type* is the array $(\mu_1, \ldots, \mu_s)$ formed of the multiplicities of its roots. Obviously, $\mu_1 + \ldots + \mu_s = \deg f$. The *$f$-type* of a scalar γ is the root type of the polynomial $f(x) - \gamma$. When it is clear which polynomial is referred to, we say simply "type" instead of "f-type". If $f(x) - \gamma$ has at least one multiple root (in other terms, if the f-type of γ is distinct from $(1, \ldots, 1)$) then γ is called an *extremum* of $f(x)$.

Given a polynomial $f(x) \in K[x]$ and $\gamma \in \overline{K}$ of type $(\mu_1, \dots, \mu_s)$, put

$$\delta_f(\gamma) = (\mu_1 - 1) + \dots + (\mu_s - 1) = \deg f - s$$

(so that $\delta_f(\gamma) > 0$ if and only if γ is an extremum of f). Then

$$\sum_{\gamma \in \overline{K}} \delta_f(\gamma) = \deg f - 1. \tag{2}$$

To see this, notice that $\delta_f(\gamma) = \deg \gcd(f - \gamma, f')$. Hence the sum in (2) is equal to $\deg f' = \deg f - 1$, as wanted. Equality (2) will often be used in the paper, sometimes without special reference.

2.4. *Curves and function fields.* Let $F(x, y) \in K[x, y]$ be an absolutely irreducible polynomial. By *points* of the plane curve $F(x, y) = 0$ we always mean *algebraic points*, i.e. places of its function field $\overline{K}(x, y)$. (With a standard abuse of notation, we use x, y for both independent variables and coordinate functions on the plane curve.) The place is *infinite* if it is a pole of x or y. The corresponding point of the plane curve is called a *point at infinity*.

Similarly, by the *genus* of a plane curve we always mean the genus of its function field.

3. Dickson polynomials. In this section, we collect miscellaneous facts about Dickson polynomials.

For $a \in K$, the nth *Dickson polynomial* $D_n(x, a)$ is defined from the relation

$$D_n(z + a/z, a) = z^n + (a/z)^n. \tag{3}$$

The following identities will often be used in the paper, sometimes without special reference:

$$D_1(x, a) = x; \qquad D_2(x, a) = x^2 - 2a; \tag{4}$$

$$D_{mn}(x, a) = D_m(D_n(x, a), a^n); \tag{5}$$

$$b^n D_n(x, a) = D_n(bx, b^2 a); \tag{6}$$

$$D_{2n}(x, a) - 2a^n = (x^2 - 4a) E_n(x, a)^2, \tag{7}$$

where the polynomial $E_n(x, a)$ is defined from the relation

$$E_n(z + a/z, a) = (z^n - (a/z)^n)/(z - a/z). \tag{8}$$

The proofs of (4)–(7) are immediate, upon substituting $x = z + a/z$ into both sides.

An important consequence of (6) is

$$(a, \cos 2\alpha \in K) \Rightarrow (D_n(x \cos \alpha, a) \in K[x]). \tag{9}$$

Here is a slightly less obvious consequence of (4)–(7).

PROPOSITION 3.1. *Let m, n be positive even numbers with $n/2$ odd. Then*

$$\begin{array}{c} a^{m/2}u^2 + bv^2 = 4ab \\ \Downarrow \\ a^{-m/2}D_m(a^{(2-n)/4}D_{n/2}(v,a),a) = -b^{-n/2}D_n(uE_{m/2}(v,a),b). \end{array} \tag{10}$$

P r o o f. This is just a calculation:

$$\begin{aligned} -b^{-n/2}D_n(uE_{m/2}(v,a),b) &= D_{n/2}(-D_2(uE_{m/2}(v,a)/\sqrt{b},1),1) \\ &= D_{n/2}(2 - b^{-1}u^2E_{m/2}(v,a)^2,1) \\ &= D_{n/2}(2 + a^{-m/2}(v^2-4a)E_{m/2}(v,a)^2,1) \\ &= D_{n/2}(a^{-m/2}D_m(v,a),1) \\ &= D_{mn/2}(v/\sqrt{a},1) \\ &= a^{-m/2}D_m(a^{(2-n)/4}D_{n/2}(v,a),a), \end{aligned}$$

as wanted. ∎

For further facts about Dickson polynomials, including equivalent definitions, differential equations, etc., see [25, Chapter 2] and [32].

3.1. *Factorization.* It is well known that $D_n(x,a) + D_n(y,a)$ splits into factors of degree at most two. More precisely, put

$$\Phi_n(x,y,a) = \prod_{\substack{1\le k<n \\ k\equiv 1 \bmod 2}} (x^2 - 2xy\cos(\pi k/n) + y^2 - 4a\sin^2(\pi k/n)). \tag{11}$$

Then

$$D_n(x,a) + D_n(y,a) = \begin{cases} \Phi_n(x,y,a) & \text{if } n \text{ is even,} \\ (x+y)\Phi_n(x,y,a) & \text{if } n \text{ is odd} \end{cases} \tag{12}$$

(see, for instance, [5, Proposition 3.1]). If $a \neq 0$ then the factors on the right-hand side of (11) are absolutely irreducible.

3.2. *Semi-definite polynomials.* Call a polynomial $F(x,y) \in \mathbb{R}[x,y]$ *semi-definite* if there exist positive constants X, C and A such that $|F(x,y)| \ge C\max(|x|,|y|)^A$ as soon as $\max(|x|,|y|) \ge X$. The following properties of semi-definite polynomials are immediate.

PROPOSITION 3.2. (i) *A product of semi-definite polynomials is semi-definite.*

(ii) *If $F(x,y)$ is semi-definite and $f(x), g(x)$ are non-constant real polynomials then $F(f(x),g(y))$ is semi-definite.*

(iii) *If $F(x,y)$ is semi-definite then the level set $\{(x,y) \in \mathbb{R}^2 : F(x,y) = C\}$ is bounded for any $C \in \mathbb{R}$.* ∎

PROPOSITION 3.3. *Let a be a real number. If $d = \gcd(m,n)$ is even then the polynomial*

$$D_m(x, a^{n/d}) + D_n(y, a^{m/d}) \tag{13}$$

is semi-definite. If $d = \gcd(m,n)$ is odd and greater than 1 then the polynomial

$$\frac{D_m(x, a^{n/d}) + D_n(y, a^{m/d})}{D_{m/d}(x, a^{n/d}) + D_{n/d}(y, a^{m/d})} \tag{14}$$

is semi-definite.

P r o o f. One immediately verifies that all the quadratic factors in (11) are semi-definite, which implies that the polynomial $\Phi_n(x,y,a)$ is semi-definite for $n > 1$. Since each of the polynomials (13) and (14) is equal to $\Phi_d(D_{m/d}(x, a^{n/d}), D_{n/d}(x, a^{m/d}), a^{mn/d})$, the result follows. ∎

4. The genus formula. Let $f(x)$, $g(x)$ be polynomials over a field K of degrees m, n respectively. Given $\gamma \in \overline{K}$ of f-type $(\mu_1, \dots, \mu_s)$ and g-type $(\nu_1, \dots, \nu_t)$, define the quantities

$$\begin{aligned}
\Omega(\gamma) &= \sum_{1 \le i \le s} \sum_{1 \le j \le t} (\mu_i, \nu_j), \\
\sigma(\gamma) &= \sum_{1 \le i \le s} \sum_{1 \le j \le t} (\mu_i - (\mu_i, \nu_j)) = mt - \Omega(\gamma), \\
\tau(\gamma) &= \sum_{1 \le i \le s} \sum_{1 \le j \le t} (\nu_j - (\mu_i, \nu_j)) = ns - \Omega(\gamma).
\end{aligned}$$

Obviously, $mn - \Omega(\gamma) = \sigma(\gamma) = \tau(\gamma) = 0$ for all but finitely many $\gamma \in \overline{K}$.

PROPOSITION 4.1. *Assume that $f(x) = g(y)$ is an absolutely irreducible plane curve of genus $\mathbf{g}$. Then*

$$\begin{aligned}
2\mathbf{g} - 2 &= \sum_{\gamma \in \overline{K}} \sigma(\gamma) - m - d = \sum_{\gamma \in \overline{K}} \tau(\gamma) - n - d \\
&= \sum_{\gamma \in \overline{K}} (mn - \Omega(\gamma)) - mn - d,
\end{aligned} \tag{15}$$

where $d = (m,n)$.

P r o o f. This is due to Fried [17, Proposition 2 on page 240]. Since our notation is very different from Fried's, we include a proof for the convenience of the reader.

We use the Riemann–Hurwitz formula

$$2\mathbf{g} - 2 = \sum_P (e_P - 1) - 2n, \tag{16}$$

where the sum extends to the places P of the function field $\overline{K}(x,y)$ and e_P is the ramification index of the place P over the field $\overline{K}(x)$.

Fix $\alpha, \beta, \gamma \in K$ satisfying

$$f(\alpha) = g(\beta) = \gamma. \tag{17}$$

Let μ be the order of the root α of the polynomial $f - \gamma$, and ν the order of the root β of the polynomial $g - \gamma$. Then there are exactly (μ, ν) places P of $\overline{K}(x,y)$ with the property

$$x(P) = \alpha \quad \text{and} \quad y(P) = \beta, \tag{18}$$

and $e_P = \nu/(\mu,\nu)$ for every such P. It follows that

$$\sum_{P \text{ satisfies (18)}} (e_P - 1) = \nu - (\mu, \nu).$$

Defining $z \in \overline{K}(x,y)$ by $z = f(x) = g(y)$, we obtain

$$\sum_{z(P)=\gamma} (e_P - 1) = \sum_{\substack{(\alpha,\beta) \text{ satisfies (17)}}} \sum_{P \text{ satisfies (18)}} (e_P - 1) = \sum_{i=1}^{s} \sum_{j=1}^{t} (\nu_j - (\mu_i, \nu_j)) = \tau(\gamma).$$

Also, there exist $d = (m,n)$ places P with $x(P) = y(P) = \infty$, and $e_P = n/d$ for every such P. Hence

$$\sum_{z(P)=\infty} (e_P - 1) = n - d.$$

Now

$$2\mathbf{g} - 2 = \sum_{\gamma \in \overline{K}} \sum_{z(P)=\gamma} (e_P - 1) + \sum_{z(P)=\infty} (e_P - 1) - 2n = \sum_{\gamma \in \overline{K}} \tau(\gamma) - n - d,$$

which proves the second formula in (15). The first formula follows by symmetry. Finally, using (2), we obtain

$$\begin{aligned} \sum_{\gamma \in \overline{K}} \tau(\gamma) - n - d &= \sum_{\gamma \in \overline{K}} ((m - \delta_f(\gamma))n - \Omega(\gamma)) - n - d \\ &= \sum_{\gamma \in \overline{K}} (mn - \Omega(\gamma)) - n \sum_{\gamma \in \overline{K}} \delta_f(\gamma) - n - d \\ &= \sum_{\gamma \in \overline{K}} (mn - \Omega(\gamma)) - mn - d, \end{aligned}$$

which proves the last formula in (15). ∎

5. Polynomials with a few extrema. It is well known that Dickson polynomials $D_n(x,a)$ with $a \neq 0$ have exactly two extrema. More precisely, one has the following.

PROPOSITION 5.1. *If $a \neq 0$ and $n \geq 3$ then $D_n(x,a)$ has exactly two extrema $\pm 2a^{n/2}$. If n is odd then both are of type $(1,2,\dots,2)$. If n is even then $2a^{n/2}$ is of type $(1,1,2,\dots,2)$, and $-2a^{n/2}$ is of type $(2,\dots,2)$.*

For a proof see, for instance [5, Proposition 3.3].

It is of fundamental importance that, basically, the Dickson polynomials are characterized by this property. We shall use this classical fact in the following form.

THEOREM 5.2. *Let $f(x) \in K[x]$ be a polynomial of degree m having exactly two extrema in $\overline{K}$. Moreover, let its extrema be of one of the following types*:

$$(2,\dots,2), \quad (1,2,\dots,2), \quad (1,1,2,\dots,2). \tag{19}$$

Then $f(x) = \alpha D_m(x+\beta, a) + \gamma$, where $a, \alpha \in K^*$ and $\beta, \gamma \in K$.

Proof. We use induction on m. If m is odd then both the extrema are of the type $(1,2,\dots,2)$. In this case the assertion is a particular case of [32, Lemma 1.11] (reproduced in [25] as Lemma 6.16).

Now assume that m is even, and write $m = 2n$. Since $f(x)$ has two extrema, we have $m \geq 4$. By (2), one of the extrema is of type $(2,\dots,2)$ and the other is of type $(1,1,2,\dots,2)$. Since the extrema have distinct types, they both belong to K. Without loss of generality we may assume that the polynomial $f(x)$ is monic and that the extremum of type $(2,\dots,2)$ is 0. This means that $f(x) = g(x)^2$, where $g(x) \in K[x]$ is a monic polynomial of degree n.

If $n = 2$ then $g(x) = D_2(x+\beta, a)$, where $a, \beta \in K$. Moreover, $a \neq 0$, because $g(x)$ has simple roots.

Now assume that $n = \deg g > 2$. Let $\kappa \neq 0$ be the other extremum of $f(x)$. Then $(g(x) - \sqrt{\kappa})(g(x) + \sqrt{\kappa})$ has 2 simple roots, all the other roots being of order 2. It follows that $\pm\sqrt{\kappa}$ are extrema of $g(x)$, of one of the types from (19). Identity (2) applied to the polynomial $g(x)$ certifies that it has no other extrema. By induction, $g(x) = \alpha D_n(x+\beta, a) + \gamma$, where $a, \alpha \in K^*$ and $\beta, \gamma \in K$. Since $g(x)$ is monic, $\alpha = 1$. Since its extrema $\pm\sqrt{\kappa}$ are symmetric with respect to 0, we have $\gamma = 0$.

Thus, in either the case $n = 2$ or $n > 2$ we have $g(x) = D_n(x+\beta, a)$, where $a \in K^*$ and $\beta \in K$. It follows that $f(x) = g(x)^2 = D_m(x+\beta, a) + 2a^n$, as wanted. ∎

COROLLARY 5.3. *Let $f(x) \in K[x]$ and $\gamma_1, \gamma_2 \in \overline{K}$ be such that $f(x) - \gamma_i$ has at most s_i simple roots, where $s_1 + s_2 \leq 2$. (We assume that $\gamma_1 \neq \gamma_2$.) Then $f(x) = \alpha D_m(x+\beta, a) + \gamma$, where $a, \alpha \in K^*$ and $\beta, \gamma \in K$.*

Proof. We may assume that $m = \deg f \geq 3$, since otherwise there is nothing to prove. In particular, both γ_1 and γ_2 are extrema of f.

We have

$$\delta_f(\gamma_i) \geq (m - s_i)/2 \quad (i = 1, 2), \tag{20}$$

the equality being attained when $f(x) - \gamma_i$ has s_i simple and $(m - s_i)/2$ double roots. On the other hand, (2) implies that

$$(m - s_1)/2 + (m - s_2)/2 = m - 1 \geq \delta_f(\gamma_1) + \delta_f(\gamma_2).$$

Hence we have equalities in (20), and f has no extrema other than γ_i. We have shown that f satisfies the assumptions of Theorem 5.2. ∎

Corollary 5.4. *Let $f(x) \in K[x]$ be a polynomial of degree m such that for some $b \in K^*$, the polynomial $f(x)^2 - 4b$ has at most 2 roots of odd order. Then for some linear polynomial $\lambda(x) \in K[x]$ one of the following options takes place.*

(5.4.a) *The degree m is even, b is a perfect square in K, and $f(x) = \sqrt{b} D_m(\lambda(x)\sqrt{a}, 1)$, for some $a \in K$ and a suitable choice of the sign of $\sqrt{b}$.*

(5.4.b) *The degree m is odd, and $f(x) = \sqrt{b} D_m(\lambda(x)\sqrt{b}, 1)$.*

Proof. As $b \neq 0$, the polynomial $f(x)$ satisfies the assumption of Corollary 5.3. Hence $f(x) = \alpha D_m(x + \beta, a) + \gamma$, where $a, \alpha \in K^*$ and $\beta, \gamma \in K$. The extrema of $f(x)$ are $\pm 2\sqrt{b}$, which implies $\gamma = 0$ and $b = \alpha^2 a^m$. If m is even then $f(x) = \alpha a^{m/2} D_m(\lambda(x)\sqrt{a}, 1)$, where $\lambda(x) = (x + \beta)/a$. If m is odd then $f(x) = \sqrt{b} D_m(\lambda(x)\sqrt{b}, 1)$, where $\lambda(x) = (x + \beta)\alpha^{-1} a^{-(m+1)/2}$. ∎

Proposition 5.5. *If $f(x) \in K[x]$ has only one extremum then $f(x) = a(x - \alpha)^m + \gamma$, where $a, \alpha, \gamma \in K$ and $a \neq 0$.*

Proof. If γ is the extremum then (2) implies that its f-type is (n), and the result follows. ∎

6. Ritt's second theorem. Let $f_1(x)$, $g_1(x)$, $f_2(x)$, $g_2(x)$ be polynomials over K. We say that pairs (f_1, g_1) and (f_2, g_2) are *equivalent over K* (notation: $(f_1, g_1) \overset{K}{\sim} (f_2, g_2)$) if there exist (non-constant) linear polynomials $\ell(x), \lambda(x), \mu(x) \in K[x]$ such that $f_1 = \ell \circ f_2 \circ \lambda$ and $g_1 = \ell \circ g_2 \circ \mu$.

Theorem 6.1. *Let $f(x), g(x) \in K[x]$ be polynomials of degree m and n respectively. Assume that $d = \gcd(m, n) \leq 2$, and that*

$$f(x) = g(y) \tag{21}$$

is an absolutely irreducible plane curve of genus 0. Then $(f, g) \overset{K}{\sim} (f_1, g_1)$, where (f_1, g_1) is a standard pair over K.

The case $d = 1$ of this theorem follows from the classical "second theorem of Ritt" [26], as presented, for instance, in [27, Section 5]. The case $d = 2$

was examined by Fried [18, Theorem 3]. We give, however, a much more explicit classification of the possible pairs (f, g).

Recently, Avanzi and Zannier [1] classified the pairs (f, g) over an algebraically closed field and over $\mathbb{Q}$ such that $\gcd(\deg f, \deg g) = 1$ and the genus of $f(x) = g(y)$ is 1. Extending their result to number fields leads to interesting problems in the arithmetic of elliptic curves.

Theorem 6.1 will be proved in the next section. We conclude this section with several auxiliary statements required for the proof.

As the genus formula suggests, we have to deal with sums of the form $\sum(\mu_i, \nu_j)$. Some simple properties of such sums are listed in the following lemma.

LEMMA 6.2. *Let $\mu_1, \dots, \mu_s$ and $\nu_1, \dots, \nu_t$ be positive integers, and put*

$$m = \mu_1 + \dots + \mu_s, \quad n = \nu_1 + \dots + \nu_t, \quad \Omega = \sum_{1 \le i \le s} \sum_{1 \le j \le t} (\mu_i, \nu_j). \tag{22}$$

Then

(i) *We have $\Omega \le sn$, the equality being attained when every ν_j divides every μ_i.*

(ii) *If $\min(\mu_1, \dots, \mu_s) = 1$, then $\Omega \le n(s-1) + t$.*

(iii) (Schinzel) *If $\gcd(\mu_1, \dots, \mu_s, \nu_1, \dots, \nu_t) = 1$, then*

$$\Omega \le \max(m(t-1) + s, n(s-1) + n/2).$$

Proof. (i) For every i we have $(\mu_i, \nu_1) + \dots + (\mu_i, \nu_t) \le \nu_1 + \dots + \nu_t = n$, the equality being attained when every ν_j divides this μ_i. Summing up over i, we complete the proof.

(ii) Say, let $\mu_1 = 1$. Then

$$(\mu_i, \nu_1) + \dots + (\mu_i, \nu_t) \begin{cases} = t & \text{if } i = 1, \\ \le n & \text{if } i \ge 2. \end{cases}$$

We again complete the proof, summing up over i.

(iii) We consider two cases.

CASE 1: *For every i either*

$$\text{there exists a } j \text{ with } (\mu_i, \nu_j) = 1, \quad \text{or} \tag{23}$$

$$\text{there exist distinct } j_1 \text{ and } j_2 \text{ such that } \mu_i \text{ does not divide } \nu_{j_1} \text{ and } \nu_{j_2}. \tag{24}$$

If for a given i we have (23) then

$$(\mu_i, \nu_1) + \dots + (\mu_i, \nu_t) \le (t-1)\mu_i + 1.$$

If we have (24) then (μ_i, ν_{j_1}) and (μ_i, ν_{j_2}) do not exceed $\mu_i/2$, and

$$(\mu_i, \nu_1) + \dots + (\mu_i, \nu_t) \le (t-1)\mu_i < (t-1)\mu_i + 1.$$

Summing up over i, we obtain $\Omega \le (t-1)(\mu_1 + \dots + \mu_s) + s = (t-1)m + s$.

Case 2: *There exist i_0 and j_0 such that*

$$j \neq j_0 \Rightarrow \mu_{i_0} \mid \nu_j \quad \textit{and} \quad d := (\mu_{i_0}, \nu_{j_0}) > 1. \tag{25}$$

It follows from (25) that d divides $\nu_1, \ldots, \nu_t$. But

$$\gcd(\mu_1, \ldots, \mu_s, \nu_1, \ldots, \nu_t) = 1,$$

whence d does not divide at least one of the numbers μ_i, say, μ_1. It follows that none of the ν_j divides μ_1, which implies that $(\mu_1, \nu_j) \leq \nu_j/2$ for all j. Therefore

$$(\mu_i, \nu_1) + \ldots + (\mu_i, \nu_t) \leq \begin{cases} n/2 & \text{if } i = 1, \\ n & \text{if } i \geq 2. \end{cases}$$

Summing up over i, we obtain $\Omega \leq (s-1)n + n/2$. The proof is complete. ∎

The following trivial observation will often be used.

Proposition 6.3. *If $f(x) - \gamma$ has at least r simple roots then $\tau(\gamma) \geq r\delta_g(\gamma)$ (we use the notation of Section* 4*).*

Proof. At least r of the numbers $\mu_1, \ldots, \mu_s$ are equal to 1, say, $\mu_1 = \ldots = \mu_r = 1$. Hence

$$\tau(\gamma) \geq \sum_{i=1}^{r} \sum_{j=1}^{t} (\nu_j - (\mu_i, \nu_j)) = \sum_{i=1}^{r} \sum_{j=1}^{t} (\nu_j - 1) = r\delta_g(\gamma),$$

as wanted. ∎

Finally, we consider three simple particular cases of Theorem 6.1.

Proposition 6.4. *In the set-up of Theorem* 6.1 *assume that $m \geq 3$, $n \geq 2$ and $f(x) = a(x-\alpha)^m + \gamma$. Then $d = 1$ and $g(x) = b(x-\beta)^r g_1(x)^m + \gamma$, where $0 < r < m$, $b \in K^*$, $\beta \in K$ and the polynomial $g_1(x) \in K[x]$ may be constant.*

Proof. Plainly, $\gamma \in K$. Hence we may write $g(x) = g_2(x)g_1(x)^m + \gamma$, where $g_1, g_2 \in K[x]$ and the root type of g_1 is $(\nu_1, \ldots, \nu_t)$ with $\nu_i < m$. We have

$$\gcd(m, \nu_1, \ldots, \nu_t) = 1, \tag{26}$$

since otherwise the curve (21) would have been reducible.

The second formula in (15) implies that $-2 = 2\mathbf{g} - 2 = \sigma(\gamma) - m - d$ (because $\sigma(\gamma') = 0$ for $\gamma' \neq \gamma$). Further,

$$\sigma(\gamma) = \sum_{j=1}^{t} (m - (m, \nu_j)) > tm/2,$$

because $(m, \nu_j) \leq m/2$ for all j, and $(m, \nu_j) < m/2$ for at least one j (otherwise we violate (26)).

If $t \geq 2$ then $-2 > (t-2)m/2 - d$, a contradiction. Thus, $t = 1$, which completes the proof. ∎

PROPOSITION 6.5. *In the set-up of Theorem* 6.1 *assume that* $m = 2$ *and* $f(x) = a(x-\alpha)^2 + \gamma$. *Then* $g(x) = g_1(x)^2 g_2(x) + \gamma$, *where* $g_2(x) \in K[x]$ *is a separable polynomial of degree at most* 2, *and the polynomial* $g_1(x) \in K[x]$ *may be constant.*

Proof (similar to the proof of Proposition 6.4 and simpler). Now we have $\nu_1 = \ldots = \nu_t = 1$ and $\sigma(\gamma) = t$. The genus formula reads $-2 = t-2-d$, which yields $t = \deg g_2 = d \leq 2$, as desired. ∎

PROPOSITION 6.6. *In the set-up of Theorem* 6.1 *assume that* n *is odd*, $m, n \geq 3$ *and* $g(x) = D_n(x, b)$, *where* $b \in K^*$. *Then for some linear polynomial* $\lambda(x) \in K[x]$ *we have the following.*

(i) *If* m *is odd then* $f(x) = b^{(n-m)/2} D_m(\lambda(x), b)$.

(ii) *If* m *is even then* b *is a perfect square in* K, *and we have* $f(x) = a^{-m/2} b^{n/2} D_n(\lambda(x), a)$ *for some* $a \in K^*$ *and for a suitable choice of the sign of* $b^{n/2}$.

Proof. By Proposition 5.1, $g(x)$ has two extrema $\pm b^{n/2}$, both of type $(1, 2, \ldots, 2)$. Let s_+ (respectively, s_-) be the number of odd entries in the f-type of $b^{n/2}$ (respectively, $-b^{n/2}$). Then $\tau(\pm b^{n/2}) = s_\pm(n-1)/2$, and the second formula in (15) implies that $-2 \geq (s_+ + s_-)(n-1)/2 - n - 1$. It follows that $s_+ + s_- = 2$, and Corollary 5.3 implies that $f(x) = \alpha D_m(x + \beta, a) + \gamma$, where $\alpha, a \in K^*$ and $\beta, \gamma \in K$.

The extrema of f are $\pm \alpha a^{m/2} + \gamma$. On the other hand, they are $\pm b^{n/2}$. It follows that $\gamma = 0$ and

$$\alpha = \varepsilon a^{-m/2} b^{n/2}, \tag{27}$$

where $\varepsilon \in \{1, -1\}$ depends on the signs of $a^{-m/2}$ and $b^{n/2}$.

Now recall that $\alpha \in K$. If m is even, then (27) implies that b is a perfect square in K, say, $b = b_1^2$. The sign of b_1 can be defined to have $f(x) = a^{-m/2} b_1^n D_n(\lambda(x), a)$, which completes the proof in this case.

If m is odd then (27) implies that a/b is a perfect square in K, say, $b = ac^2$. We define that sign of c so that (27) turns to $f(x) = b^{(n-m)/2} D_n(\lambda(x), b)$ with $\lambda(x) = c(x + \beta)$. This completes the proof also in this case. ∎

7. Proof of Theorem 6.1. *Everywhere in this section "equivalent" means "equivalent over* K", *and "standard pair" means "standard pair over* K".

If $\min(m, n) = 1$ then (f, g) is equivalent to a standard pair of the first kind. If $\min(m, n) = 2$ then (f, g) is equivalent to a standard pair of the

first or second kind by Proposition 6.5. Hence we may assume that

$$\min(m, n) \geq 3.$$

We use the quantities $\sigma(\gamma)$, etc., defined at the beginning of Section 4. We start with the following observation.

ASSERTION 1. *Let* $\gamma \in \overline{K}$ *have* f*-type* $(\mu_1, \dots, \mu_s)$ *and* g*-type* $(\nu_1, \dots, \nu_t)$. *Then*

$$\gcd(\mu_1, \dots, \mu_s, \nu_1, \dots, \nu_t) = 1. \tag{28}$$

Indeed, assume that for some γ we have $q = \gcd(\mu_1, \dots, \mu_s, \nu_1, \dots, \nu_t) > 1$. Then both $f(x) - \gamma$ and $g(x) - \gamma$ are qth powers in the ring $\overline{K}[x]$, which contradicts the irreducibility of the curve (21).

The following assertion is just a reformulation of Lemma 6.2(iii).

ASSERTION 2. *For any* $\gamma \in \overline{K}$ *either* $\sigma(\gamma) \geq \delta_f(\gamma)$, *or* $\tau(\gamma) \geq n/2$.

We say that $\gamma \in \overline{K}$ is a σ*-point* (respectively, τ*-point*) ([2]) if $\delta_f(\gamma) > \sigma(\gamma)$ (respectively, $\delta_g(\gamma) > \tau(\gamma)$). Reformulating item (ii) of Lemma 6.2, we obtain the following.

ASSERTION 3. *If* γ *is a* τ*-point then* $f(x) - \gamma$ *has no simple roots. In particular*, $\delta_f(\gamma) \geq m/2$.

It follows that there can be at most one σ-point and at most one τ-point.

CASE 1: *There exist a* σ*-point* γ_1 *and a* τ*-point* γ_2.

SUBCASE 1.1: $\gamma_1 = \gamma_2$. We follow [27, pp. 37–38] with some changes. Assertion 2 implies that

$$\delta_f(\gamma_1) > \sigma(\gamma_1) \geq m/2, \qquad \delta_g(\gamma_1) > \tau(\gamma_1) \geq n/2.$$

Write $\delta_f(\gamma_1) = m/2 + \kappa$ and $\delta_g(\gamma_1) = n/2 + \lambda$. Without loss of generality $\kappa \geq \lambda$. Assume that $g(x)$ has an extremum $\gamma_3 \neq \gamma_1$. Since

$$\delta_f(\gamma_3) \leq m - 1 - \delta_f(\gamma_1) = m/2 - \kappa - 1,$$

the polynomial $f(x) - \gamma_3$ has at least $2\kappa + 2$ simple roots. By Proposition 6.3

$$\tau(\gamma_3) \geq (2\kappa + 2)\delta_g(\gamma_3) \geq \delta_g(\gamma_3) + 2\kappa + 1.$$

We also have

$$\tau(\gamma_1) \geq \delta_g(\gamma_1) - \lambda \geq \delta_g(\gamma_1) - \kappa,$$

and $\tau(\gamma) \geq \delta_g(\gamma)$ for $\gamma \neq \gamma_1, \gamma_3$. By the genus formula (15),

$$-2 = \sum_{\gamma \in \overline{K}} \tau(\gamma) - n - d \geq \sum_{\gamma \in \overline{K}} \delta_g(\gamma) + \kappa + 1 - n - d = \kappa - d > -d,$$

a contradiction.

([2]) In Ritt's [26] terminology, *extra point* of f (respectively, g).

Thus, $g(x)$ cannot have an extremum distinct from γ_1. Proposition 5.5 implies that $g(x) = a(x-\alpha)^n + \gamma_1$, and Proposition 6.4 implies that (f, g) is equivalent to a standard pair of the first kind.

Subcase 1.2: $\gamma_1 \neq \gamma_2$. By Assertion 3,

$$\delta_f(\gamma_1) \geq m/2, \quad \delta_g(\gamma_2) \geq n/2, \tag{29}$$

and by Lemma 6.2,

$$\Omega(\gamma_1) \leq n(m - \delta_f(\gamma_1)), \quad \Omega(\gamma_2) \leq m(n - \delta_g(\gamma_2)). \tag{30}$$

Using (29), (30) and Proposition 4.1, we obtain

$$\begin{aligned} -2 &= \sum_{\gamma \in \overline{K}} (mn - \Omega(\gamma)) - mn - d \\ &\geq (mn - \Omega(\gamma_1)) + (mn - \Omega(\gamma_2)) - mn - d \qquad (31) \\ &\geq \delta_f(\gamma_1)n + \delta_g(\gamma_2)m - mn - d \\ &\geq -d. \qquad (32) \end{aligned}$$

Thus, $d = 2$, and inequalities (31) and (32) are equalities. This has the following consequences:

- $\Omega(\gamma) = mn$ for any $\gamma \neq \gamma_1, \gamma_2$. This implies that f and g have no extrema distinct from γ_1 and γ_2.
- Inequalities (29) are equalities, which implies that the f-type of γ_1 and the g-type of γ_2 are $(2, \dots, 2)$.
- Inequalities (30) are equalities. Hence Lemma 6.2(i) together with (2) implies that the f-type of γ_2 and the g-type of γ_1 are $(1, 1, 2, \dots, 2)$.

Now Theorem 5.2 implies

$$f(x) = \alpha D_n(x + \beta, a) + \gamma, \quad g(x) = \alpha' D_n(x + \beta', b) + \gamma'.$$

Since

$$\gamma_1 = -\alpha a^{m/2} + \gamma = \alpha' b^{n/2} + \gamma', \quad \gamma_2 = \alpha a^{m/2} + \gamma = -\alpha' b^{n/2} + \gamma',$$

we have $\gamma = \gamma'$ and $\alpha a^{m/2} = -\alpha' b^{n/2}$, which shows that (f, g) is equivalent to a standard pair of the fourth kind. This completes the proof in Case 1.

Case 2: *There exist no σ-point.* If f has a single extremum, then $f(x) = a(x-\alpha)^m + \gamma$ by Proposition 5.5, which reduces the theorem to Proposition 6.4.

From now on assume that

$$f \text{ has at least two distinct extrema.} \tag{33}$$

Subcase 2.1: *For every extremum γ of f, the polynomial $g - \gamma$ has at most one simple root.* Let γ_1 and γ_2 be two distinct extrema of f (which exist by (33)). Since $g - \gamma_1$ and $g - \gamma_2$ have at most one simple root, we

have $\delta_g(\gamma_1), \delta_g(\gamma_2) \geq (n-1)/2$. Since $\delta_g(\gamma_1) + \delta_g(\gamma_2) \leq n-1$, we have $\delta_g(\gamma_1) = \delta(\gamma_2) = (n-1)/2$ and the polynomial g has no extrema other than γ_1 and γ_2. Also, both γ_1 and γ_2 have g-type $(1, 2, \ldots, 2)$. In particular, n is odd and $d = 1$.

It follows from Theorem 5.2 that $g(x) = \alpha D_n(x + \beta, b) + \gamma$, where $\alpha, b \in K^*$ and $\beta, \gamma \in K$. If m is even then Proposition 6.6 implies that $b = b_1^2$, where $b_1 \in K^*$, and $f(x) = \alpha a^{-m/2} b_1^n D_m(\lambda(x), a) + \gamma$. Writing

$$f(x) = \alpha a^{-mn/2} b_1^n D_m(a^{(n-1)/2}\lambda(x), a^n) + \gamma,$$
$$g(x) = \alpha a^{-mn/2} b_1^n D_n(a^{(m-1)/2} b_1^{-1}(x + \beta), a^m) + \gamma,$$

we conclude that (f, g) is equivalent to a standard pair of the third kind.

If m is odd then Proposition 6.6 implies that

$$f(x) = \alpha b^{(n-m)/2} D_n(\lambda(x), b) + \gamma.$$

Writing

$$f(x) = \alpha b^{-n(m+1)/2} D_n(b^{(n-1)/2}\lambda(x), b^n) + \gamma,$$
$$g(x) = \alpha b^{-n(m+1)/2} D_n(b^{(m-1)/2}(x + \beta), b^m) + \gamma,$$

we again see that (f, g) is equivalent to a standard pair of the third kind.

SUBCASE 2.2: *For some extremum γ_1 of f, the polynomial $g - \gamma_1$ has at least two simple roots.* Since the argument in this subcase is rather lengthy, we divide it into short logically complete steps.

STEP 1: *The f-type and further properties of γ_1.* By Proposition 6.3 we have $\sigma(\gamma_1) \geq 2\delta_f(\gamma_1)$. Since there is no σ-point, $\sigma(\gamma) \geq \delta_f(\gamma)$ for all $\gamma \in \overline{K}$. By the genus formula,

$$-2 = \sigma(\gamma_1) + \sum_{\gamma \neq \gamma_1} \sigma(\gamma) - n - d \geq 2\delta_f(\gamma_1) + \sum_{\gamma \neq \gamma_1} \delta_f(\gamma) - n - d = \delta_f(\gamma_1) - 1 - d.$$

Since γ_1 is an extremum of f, we have $\delta_f(\gamma_1) \geq 1$. Hence

$$d = 2, \quad \delta_f(\gamma_1) = 1, \quad \sigma(\gamma_1) = 2, \tag{34}$$
$$\sigma(\gamma) = \delta_f(\gamma) \quad (\gamma \neq \gamma_1). \tag{35}$$

It follows from (34) that the f-type of γ_1 is $(2, 1, \ldots, 1)$.

STEP 2: *The definition of γ_2.* Equality (35) together with Proposition 6.3 implies that for any extremum γ of $f(x)$, distinct from γ_1, the polynomial $g(x) - \gamma$ has *at most one* simple root. Since n is even, $\delta_g(\gamma) \geq n/2$ for any such γ. Also, (34) and Proposition 6.3 imply that $g(x) - \gamma_1$ has *exactly two* simple roots, whence $\delta_g(\gamma_1) \geq (n-2)/2$. It follows that f has exactly two extrema, one of which is γ_1; denote the other by γ_2. Since $\delta_g(\gamma_1) + \delta_g(\gamma_2) \geq (n-2)/2 + n/2 = n - 1$, these γ_1 and γ_2 are the only extrema of g as well,

and

$$\delta_g(\gamma_1) = (n-2)/2, \quad \delta_g(\gamma_2) = n/2. \tag{36}$$

Step 3: *Possible g-types of γ_1 and γ_2.* As we have seen in the previous step, $g(x) - \gamma_2$ has at most one simple root, and $g(x) - \gamma_1$ has exactly two simple roots. Comparing this with (36), we conclude that the g-type of γ_1 is $(1, 1, 2, \dots, 2)$, and the g-type of γ_2 is either $(1, 3, 2, \dots, 2)$ or $(2, \dots, 2)$.

Step 4: *Possible m and n.* The third genus formula (15) implies that $-2 = mn - \Omega(\gamma_1) - \Omega(\gamma_2) - 2$. The f- and g-types of γ_1 being known, one finds $\Omega(\gamma_1) = mn/2 + m - 2$. Hence

$$\Omega(\gamma_2) = mn/2 - m + 2. \tag{37}$$

On the other hand, by Lemma 6.2(i),

$$\Omega(\gamma_2) \le n(m - \delta_f(\gamma_2)) = n(\delta_f(\gamma_1) + 1) = 2n. \tag{38}$$

Comparing (37) and (38), we obtain

$$m \le (2n-2)/(n/2-1), \tag{39}$$

which implies one of the following options:

$$m = 6, \quad n \ = 4, \tag{40}$$

$$m = 4, \quad n \ \equiv 2 \pmod 4. \tag{41}$$

Step 5: *Impossibility of* (41). In case (41) we have $\delta_f(\gamma_2) = 3 - \delta_f(\gamma_1) = 2$, and the f-type of γ_2 can be either $(2, 2)$ or $(1, 3)$.

Notice that the f-type $(2, 2)$ and the g-type $(2, \dots, 2)$ together violate (28). There remain three possibilities for the f- and g-types of γ_2, respectively:

$$(1,3) \text{ and } (1,3,2,\dots,2); \quad (2,2) \text{ and } (1,3,2,\dots,2); \quad (1,3) \text{ and } (2,\dots,2).$$

In the first case $\Omega(\gamma_2) = n + 2$, in the second case $\Omega(\gamma_2) = 2n - 4$, and in the third case $\Omega(\gamma_2) = n$. In any case, this contradicts (37), which shows that (41) is impossible.

Step 6: *The f- and g-types of γ_2.* Thus, we have (40). Moreover, we have equality in (38), which means, by Lemma 6.2(i), that

(42) every entry of the g-type of γ_2 divides every entry of its f-type.

This shows that the g-type $(2, 2)$ is impossible (it violates (28)), and the single possibility for the g-type of γ_2 is $(1, 3)$. By (42), the only possible f-type for γ_2 is $(3, 3)$.

Step 7: *Normalizing γ_1 and γ_2.* Since f has no extrema of type $(3, 3)$ other than γ_2, we have $\gamma_2 \in K$. Similarly, $\gamma_1 \in K$. Replacing f and g by $(f - \gamma_2)/(\gamma_2 - \gamma_1)$ and $(g - \gamma_2)/(\gamma_2 - \gamma_1)$, we may assume that $\gamma_1 = -1$ and $\gamma_2 = 0$.

STEP 8: *The polynomial f.* Since $\gamma_2 = 0$ is an extremum of f of type $(3,3)$, we have $f(x) = \alpha f_1(x)^3$, where $\alpha \in K^*$ and $f_1(x) \in K[x]$ is a separable quadratic polynomial. After a linear change of the variable we may write $f_1(x) = a_1x^2 - a_2$, where $a_1, a_2 \in K^*$. The second extremum of f is $-\alpha a_2^3 = \gamma_1 = -1$. Thus, $\alpha = a_2^{-3}$ and $f(x) = (ax^2 - 1)^3$, where $a = a_1/a_2$.

STEP 9: *The polynomial g.* Since $\gamma_2 = 0$ has g-type $(1,3)$, we may write, after a linear change of variable, that $g(x) = (px - q)x^3$, where $p, q \in K^*$. The second extremum of g is $-27q^4/(256p^3) = -1$. Hence $(q/4)^4 = (p/3)^3 = \theta_1^{12}$, where $\theta_1 \in K^*$. Thus, $q/4 = \theta_1^3\xi_4$ and $p/3 = \theta_1^4\xi_3$, where ξ_3 and ξ_4 are third and fourth root of unity, respectively (not necessarily primitive). Notice that $\xi_3, \xi_4 \in K$. Putting $\theta = \theta_1\xi_3^{-1}\xi_4$, we obtain $q = 4\theta^3$ and $p = 3\theta^4$. Thus, $g(x) = 3(\theta x)^4 - 4(\theta x)^3$.

We have shown that (f, g) is equivalent to a standard pair of the fifth kind. The theorem is proved. ∎

8. Irreducible factors of $f(x) - g(y)$. *Everywhere in this section "irreducible" means "irreducible over K", and "factor" means "K-factor", unless the contrary is stated explicitly.*

Given $f(x) \in K[x]$, denote by $\mathfrak{V}_f$ the splitting field of $f(x) - t$ over $K(t)$ (where t is a new indeterminate). Two polynomials $f(x)$ and $g(x)$ are called *similar* if $\mathfrak{V}_f = \mathfrak{V}_g$.

A place of $\mathfrak{V}_f$ is called *infinite* if it lies over the infinite place of $K(t)$. The ramification index (over $K(t)$) of any infinite place of $\mathfrak{V}_f$ is equal to $\deg f$. It follows that

(43) similar polynomials have equal degrees.

Fried [16, Proposition 2] observed that the problem of factoring polynomials of the form $f(x) - g(y)$ reduces to the case of similar f and g.

THEOREM 8.1 (Fried). *Given $f(x), g(x) \in K[x]$, there exist similar polynomials $f_1(x), g_1(x) \in K[x]$, and polynomials $f_2(x), g_2(x) \in K[x]$ such that*

$$f = f_1 \circ f_2, \qquad g = g_1 \circ g_2,$$

and

- *for every irreducible factor $F_1(x, y)$ of $f_1(x) - g_1(y)$, the polynomial $F(x, y) := F_1(f_2(x), g_2(y))$ is irreducible;*
- *every irreducible factor of $f(x) - g(y)$ is of the form $F_1(f_2(x), g_2(y))$, where $F_1(x, y)$ is an irreducible factor of $f_1(x) - g_1(y)$.*

Thereby,

(44) $$F_1(x, y) \leftrightarrow F(x, y) := F_1(f_2(x), g_2(y))$$

gives a one-to-one correspondence between the irreducible factors of $f_1(x) - g_1(y)$ and of $f(x) - g(y)$.

P r o o f. We give a proof for the convenience of the reader. We use induction on $\deg f + \deg g$. If $f(x) - t$ has a root in $\mathcal{O}_g$ and $g(x) - t$ has a root in $\mathcal{O}_f$ then $\mathcal{O}_f = \mathcal{O}_g$ and there is nothing to prove. Therefore we may assume that, say, $g(x) - t$ has no root in $\mathcal{O}_f$.

Let y_1 be a root of $g(x) - t$. By assumption, $y_1 \notin \mathcal{O}_f$. We have a tower of rational fields:

$$K(t) \subseteq \mathcal{O}_f \cap K(y_1) \subsetneq K(y_1).$$

The infinite place of the field $K(t)$ totally ramifies in $K(y_1)$. Hence it totally ramifies in the intermediate field $\mathcal{O}_f \cap K(y_1)$. Therefore $\mathcal{O}_f \cap K(y_1) = K(y_2)$, where y_2 is integral over the ring $K[t]$. We have $t = \widetilde{g}(y_2) \in K[y_2]$ and $y_2 = \widehat{g}(y_1) \in K[y_1]$. It is important to notice that $\deg \widetilde{g} < \deg g$, because $K(y_2)$ is a proper subfield of $K(y_1)$.

Now let $F(x, y) = a_q(y)x^q + \ldots + a_0(y)$ be a factor of $f(x) - g(y)$. Then $a_0(y_1), \ldots, a_q(y_1)$ are polynomials in the roots of $f(x) - g(y_1) = f(x) - t$. Hence $a_0(y_1), \ldots, a_q(y_1) \in \mathcal{O}_f$. It follows that

$$a_0(y_1), \ldots, a_q(y_1) \in \mathcal{O}_f \cap K(y_1) = K(y_2).$$

Therefore $a_i(y) = \widetilde{a}_i(\widehat{g}(y))$, where $\widetilde{a}_0(y), \ldots, \widetilde{a}_q(y) \in K[y]$.

Obviously, $\widetilde{F}(x, y) := \widetilde{a}_q(y)x^q + \ldots + \widetilde{a}_0(y)$ is a factor of $f(x) - \widetilde{g}(y)$. We have proved that every factor of $f(x) - g(y)$ is of the form $\widetilde{F}(x, \widehat{g}(y))$, where $\widetilde{F}(x, y)$ is a factor of $f(x) - \widetilde{g}(y)$.

Conversely, for any factor $\widetilde{F}(x, y)$ of $f(x) - \widetilde{g}(y)$, the polynomial $F(x, y) = \widetilde{F}(x, \widehat{g}(y))$ is a factor of $f(x) - g(y)$, distinct $\widetilde{F}$ giving rise to distinct F. Hence

$$\widetilde{F}(x, y) \leftrightarrow F(x, y) := \widetilde{F}(x, \widehat{g}(y))$$

is a one-to-one correspondence between the factors of $f(x) - \widetilde{g}(y)$ and of $f(x) - g(y)$. Moreover, since this correspondence preserves the divisibility relation, it restricts to a one-to-one correspondence between the *irreducible* factors of $f(x) - \widetilde{g}(y)$ and of $f(x) - g(y)$.

Since $\deg \widetilde{g} < \deg g$, there exist, by induction, similar polynomials $f_1(x)$, $g_1(x) \in K[x]$, and polynomials $f_2(x), \widetilde{g}_2(x) \in K[x]$ such that $f = f_1 \circ f_2$, $\widetilde{g} = g_1 \circ \widetilde{g}_2$ and $F_1(x, y) \leftrightarrow \widetilde{F}(x, y) := F_1(f_2(x), \widetilde{g}_2(y))$ is a one-to-one correspondence between the irreducible factors of $f_1(x) - g_1(y)$ and of $f(x) - \widetilde{g}(y)$. Putting $g_2 = \widetilde{g}_2 \circ \widehat{g}$, we complete the proof. ∎

As Fried indicated in [18], the study of the Diophantine equation $f(x) = g(y)$ requires classification of polynomials of the form $f(x) - g(y)$ having quadratic factors. This problem is solved in [5].

THEOREM 8.2. *Let $f(x)$ and $g(x)$ be polynomials over K, and let $q(x, y) \in K[x, y]$ be an irreducible (over K) factor of $f(x) - g(y)$ of degree at most 2.*

Then there exist polynomials $\varphi(x), f_1(x), g_1(x) \in K[x]$ such that $f = \varphi \circ f_1$, $g = \varphi \circ g_1$ and one of the following two options takes place.

(8.2.a) *We have* $\max(\deg f_1, \deg g_1) = 2$ *and* $q(x,y) = f_1(x) - g_1(y)$.

(8.2.b) *There exists an integer $n > 2$ with $\cos(2\pi/n) \in K$ such that for some $\alpha \in K^*$ and $a, \beta, \gamma \in K$ we have*

$$f_1(x) = D_n(x + \beta, a), \qquad g_1(x) = -D_n((\alpha x + \gamma)\cos(\pi/n), a),$$

and $q(x,y)$ is a quadratic factor of $f_1(x) - g_1(y)$. If $q(x,y)$ is absolutely irreducible then $a \neq 0$.

P r o o f. See [5, Theorem 1.3]. ∎

Note in conclusion that the problem of factorization of $f(x) - g(y)$ has a long history, which cannot be presented here. We just mention that among the contributors were Cassels, Davenport, Feit, Fried, Lewis, Schinzel, Tverberg, and many others. In particular, Tverberg [33, Chapter 2] obtained some results complementary to Theorem 8.2. Fried [16, Theorem 1 on pp. 141–142] proved that if f is an *indecomposable* ([3]) polynomial of degree n and K contains no complex subfield of $\mathbb{Q}(e^{2\pi i/n})$ (in particular, if $K = \mathbb{Q}$), then $f(x) - g(y)$ is reducible (over $\overline{\mathbb{Q}}$) only in trivial cases. He also showed that the problem with indecomposable f and general K reduces to a certain problem in group theory, studied by Feit [14]. For further advances see [15, 19, 20]. Quite recently, Cassou-Noguès and Couveignes [11], essentially using the previous work of Fried and Feit, and assuming the classification of finite simple groups, completely classified the pairs of polynomials f, g with indecomposable f such that $f(x) - g(y)$ is reducible ([4]).

9. Exceptional factors of $f(x) - g(y)$ and specific pairs. An absolutely irreducible polynomial $F(x,y) \in K[x,y]$ is called *exceptional* if the plane curve $F(x,y) = 0$ is of genus 0 and has at most two points at infinity.

In this section we use Theorems 8.1 and 8.2 to classify polynomials of the form $f(x) - g(y)$ having exceptional factors.

Proposition 9.1. *Let $\Phi(x,y), f(x,y), g(x,y) \in K[x,y]$ be non-constant polynomials such that $\Phi(f(x,y), g(x,y))$ is an exceptional polynomial. Assume that f and g are algebraically independent over K. Then $\Phi(x,y)$ itself is an exceptional polynomial.*

P r o o f. First, since $\Psi(x,y) = \Phi(f(x,y), g(x,y))$ is absolutely irreducible, so is $\Phi(x,y)$.

([3]) A polynomial is *indecomposable* if it is not a composition of two polynomials of smaller degree.

([4]) Cassou-Noguès and Couveignes assume that both f and g are indecomposable. But [16, assertion (2.38) on p. 142] implies that the assumption about g can be dropped.

Second, the field $K(u,v)$ of rational functions on the curve $\Phi(u,v)=0$ is contained in the field $K(x,y)$ of rational functions on the curve $\Psi(x,y)=0$, the embedding being defined by $u\mapsto f(x,y)$ and $v\mapsto g(x,y)$. By the Lüroth theorem, the curve $\Psi(x,y)=0$ is of genus 0.

Third, since $f(x,y)$ and $g(x,y)$ are polynomials, the infinite places of the field $K(x,y)$ restrict to the infinite places of the field $K(u,v)$. Since the former field has at most 2 infinite places, so does the latter. ∎

PROPOSITION 9.2. *Let $q(x,y)=\alpha x^2+2\beta xy+\gamma y^2+\delta\in K[x,y]$ be a quadratic polynomial with $\alpha\beta\gamma\delta(\beta^2-\alpha\gamma)\neq 0$. Let $f(x),g(x)\in K[x]$ be non-constant polynomials of degrees m and n, respectively, such that $q(f(x),g(y))$ is an exceptional polynomial. Then $(m,n)=1$. Furthermore, define $b=\delta\gamma/(4(\beta^2-\alpha\gamma))$. Then for some linear polynomial $\lambda(x)\in K[x]$ one of the following options takes place.*

(9.2.a) *The degree m is even, b is a perfect square in K, and $f(x)=\sqrt{b}D_m(\lambda(x)\sqrt{a},1)$ for some $a\in K$ and a suitable choice of the sign of $\sqrt{b}$.*

(9.2.b) *The degree m is odd and $f(x)=\sqrt{b}D_m(\lambda(x)\sqrt{b},1)$.*

We have similar options for $g(x)$ with $c=\delta\alpha/(4(\beta^2-\alpha\gamma))$ instead of b, and with another linear polynomial $\mu(x)$ instead of $\lambda(x)$.

Proof. The plane curve $q(f(x),g(y))=0$ has $2\gcd(m,n)$ points at infinity, which implies that $\gcd(m,n)=1$.

Further, since $q(f(x),g(y))$ is exceptional, so is

$$\gamma q(f(x),y)=(\gamma y-\beta\gamma y f(x))^2-(\beta^2-\alpha\gamma)(f(x)^2-4b),$$

as well as $y^2-(\beta^2-\alpha\gamma)(f(x)^2-4b)$. By Proposition 6.5, the polynomial $f(x)^2-4b$ has at most two roots of odd order. We complete the proof using Corollary 5.4. ∎

To formulate the main result of this section, we need to define one more kind of pairs, which we call *specific* ([5]). A *specific pair* over K is

$$(D_m(x,a^{m/d}),-D_n(x\cos(\pi/d),a^{n/d}))$$

(or switched), where $d=\gcd(m,n)\geq 3$ and $a,\cos(2\pi/d)\in K$. Notice that $-D_n(x\cos(\pi/d),a^{n/d})\in K[x]$ by (9).

THEOREM 9.3. *Let $f(x),g(x)\in K[x]$ be such that $f(x)-g(y)$ has an exceptional factor $E(x,y)$. Then there exist a standard or specific pair (f_1,g_1) over K, linear polynomials $\lambda(x),\mu(x)\in K[x]$, and a polynomial $\varphi(x)\in K[x]$ such that $f=\varphi\circ f_1\circ\lambda$ and $g=\varphi\circ g_1\circ\mu$. Also, $E(x,y)$ is equal to $f_1\circ\lambda(x)-g_1\circ\mu(y)$ times a constant if (f_1,g_1) is standard, and $E(x,y)$ divides $f_1\circ\lambda(x)-g_1\circ\mu(y)$ if (f_1,g_1) is specific.*

([5]) This term has no intuitive meaning: specific pairs are neither "less standard" nor "more specific" than standard pairs.

P r o o f. All polynomials that occur in the proof have coefficients in K unless the contrary is stated explicitly.

Let $f = f_3 \circ f_2$ and $g = g_3 \circ g_2$ be the decompositions from Theorem 8.1 (we write f_3 and g_3 instead of f_1 and g_1). In particular,

$$\deg f_3 = \deg g_3. \tag{45}$$

Then $E(x, y) = q(f_2(x), g_2(y))$, where $q(x, y)$ is an absolutely irreducible factor of $f_3(x) - g_3(y)$.

It follows from (45) that the curve $q(x, y) = 0$ has exactly $\deg q$ points at infinity. Since q is exceptional (by Proposition 9.1), we have $\deg q \le 2$. Theorem 8.2 implies that $f_3 = \varphi_1 \circ f_4$ and $g_3 = \varphi_1 \circ g_4$, where either

$$q(x, y) = f_4(x) - g_4(y), \tag{46}$$

or for some integer $\nu > 2$ we have

$$\begin{aligned} &f_4(x) = D_\nu(x + \beta, a), \quad g_4(x) = -D_\nu((\alpha x + \gamma)\cos(\pi/\nu), a), \\ &\nu > 2, \quad \cos(2\pi/\nu) \in K, \quad q(x, y) \,|\, (f_4(x) - g_4(y)), \end{aligned} \tag{47}$$

where $a, \alpha \in K^*$ and $\beta, \gamma \in K$. Put $f_5 = f_4 \circ f_2$ and $g_5 = g_4 \circ g_2$.

In the case (46) we have $E(x, y) = f_5(x) - g_5(y)$. Since $E(x, y)$ has $d = \gcd(\deg f_5, \deg g_5)$ points at infinity, we have $d \le 2$. Applying Theorem 6.1, we conclude that $f_5 = \ell \circ f_1 \circ \lambda$ and $g_5 = \ell \circ g_1 \circ \mu$, where $\ell(x), \lambda(x), \mu(x)$ are linear polynomials and (f_1, g_1) is a standard pair over K.

Obviously, $E(x, y)$ is equal to $f_1(\lambda(x)) - g_1(\mu(y))$ times a constant. Putting $\varphi = \varphi_1 \circ \ell$, we complete the proof in the case (46).

Now assume (47). By (11), for some positive integer k we have $q(x, y) = q_k(x + \beta, \alpha y + \gamma)$, where

$$q_k(x, y) = x^2 - 2xy\cos(\pi k/\nu)\cos(\pi/\nu) + y^2\cos^2(\pi/\nu) - 4a\sin^2(\pi k/\nu).$$

Put $f_6 = f_2 + \beta$ and $g_6 = \alpha g_2 + \gamma$. Then $E(x, y) = q_k(f_6(x), g_6(y))$ is an exceptional polynomial, which, by Proposition 9.2, implies that

$$\gcd(m', n') = 1, \tag{48}$$

where $m' = \deg f_6$ and $n' = \deg g_6$. Without loss of generality, n' is odd. Furthermore, Proposition 9.2 implies that

$$g_6(x) = (\cos(\pi/\nu))^{-1}\sqrt{a}D_{n'}(\mu_1(x)\cos(\pi/\nu)\sqrt{a}, 1),$$

and that either m' is odd and

$$f_6(x) = \sqrt{a}D_{m'}(\lambda_1(x)\sqrt{a}, 1),$$

or m' is even, a is a perfect square in K, and for some $a' \in K^*$ and a suitable choice of the sign of $\sqrt{a}$ we have

$$f_6(x) = \sqrt{a}D_{m'}(\lambda_1(x)\sqrt{a'}, 1).$$

Here $\lambda_1(x)$ and $\mu_1(x)$ are linear polynomials.

Putting $m = m'\nu$ and $n = n'\nu$, we obtain

$$\begin{aligned} g_5(x) &= -D_\nu(g_6(x)\cos(\pi/\nu), a) \\ &= -(\sqrt{a})^{-\nu} D_\nu((\sqrt{a})^{-1} g_6(x)\cos(\pi/\nu), 1) \\ &= -(\sqrt{a})^{-\nu} D_\nu(D_{n'}(\mu_1(x)\sqrt{a}\cos(\pi/\nu), 1), 1) \\ &= -(\sqrt{a})^{-\nu} D_n(\mu_1(x)\sqrt{a}\cos(\pi/\nu), 1) \\ &= \begin{cases} -a^{-(\nu+mn/\nu)/2} D_n(\mu(x)\cos(\pi/\nu), a^{m/\nu}) & \text{if } m' \text{ is odd,} \\ -(\sqrt{a})^{-\nu}(a')^{-mn/(2\nu)} D_n(\mu(x)\cos(\pi/\nu), (a')^{m/\nu}) & \text{if } m' \text{ is even.} \end{cases} \end{aligned}$$

(Recall that $\sqrt{a} \in K$ when m' is even.) Here

$$\mu(x) = \begin{cases} \mu_1(x) a^{(1+m/\nu)/2} & \text{if } m' \text{ is odd,} \\ \mu_1(x)(a')^{m/(2\nu)}\sqrt{a} & \text{if } m' \text{ is even.} \end{cases}$$

A similar calculation shows that

$$f_5(x) = \begin{cases} a^{-(\nu+mn/\nu)/2} D_m(\lambda(x), a^{n/\nu}) & \text{if } m' \text{ is odd,} \\ (\sqrt{a})^{-\nu}(a')^{-mn/(2\nu)} D_n(\lambda(x), (a')^{n/\nu}) & \text{if } m' \text{ is even,} \end{cases}$$

where

$$\lambda(x) = \begin{cases} \lambda_1(x) a^{(1+n/\nu)/2} & \text{if } m' \text{ is odd,} \\ \lambda_1(x)(a')^{(1+n/\nu)/2} & \text{if } m' \text{ is even.} \end{cases}$$

Further, $\nu = d = \gcd(m, n)$ by (48), which implies that $d > 2$ and $\cos(2\pi/d) \in K$ by (47). Thus, $f_5 = A f_1 \circ \lambda$ and $g_5 = A g_1 \circ \mu$, where

$$A = \begin{cases} a^{(\nu+mn/\nu)/2} & \text{if } m' \text{ is odd,} \\ (\sqrt{a})^{\nu}(a')^{mn/(2\nu)} & \text{if } m' \text{ is even,} \end{cases}$$

and (f_1, g_1) is a specific pair over K.

Finally, since $q(x, y) \,|\, (f_4(x) - g_4(y))$, the polynomial $E(x, y) = q(f_2(x), g_2(y))$ divides $f_5(x) - g_5(y) = A(f_1(\lambda(x)) - g_1(\mu(y)))$. Putting $\varphi(x) = \varphi_1(x/A)$, we complete the proof in the case (47) as well. ∎

10. The Diophantine equation. Let R be a commutative integral domain with quotient field K, and $F(x, y) \in K[x, y]$. We say that the equation $F(x, y) = 0$ *has infinitely many solutions with a bounded R-denominator* if there exists a non-zero $\Delta \in R$ such that $F(x, y) = 0$ has infinitely many solutions $(x, y) \in K \times K$ with $\Delta x, \Delta y \in R$.

In this section K is a number field, and S a finite set of places of K containing all Archimedean places. We denote by $\mathcal{O}_S$ the ring of S-integers of the field K.

Recall the classical theorem of Siegel [30] (see also [23, 28]).

THEOREM 10.1 (Siegel). *Let $F(x, y) \in K[x, y]$ be an absolutely irreducible polynomial. If the equation $F(x, y) = 0$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator, then the polynomial $F(x, y)$ is exceptional, as defined at the beginning of Section* 9. ∎

We need several simple auxiliary results.

PROPOSITION 10.2. *Let $F(x,y) \in K[x,y]$ be irreducible over K but reducible over $\overline{K}$. Then the equation $F(x,y) = 0$ has at most finitely many solutions $(x,y) \in K \times K$.*

P r o o f. This is well known (and very simple); see, for instance, [31, beginning of Section 9.6]. ∎

PROPOSITION 10.3. *Let K be a totally real number field, $\mathcal{O}$ its ring of integers, and let $F(x,y) \in K(x,y)$ have the following property: for any embedding $\sigma : K \to \mathbb{R}$, the polynomial σF is semi-definite (see Subsection 3.2). Then the equation $F(x,y) = 0$ has only finitely many solutions with a bounded $\mathcal{O}$-denominator.*

P r o o f. By Proposition 3.2(iii), there is a constant $c = c(F)$ such that $\max(|\sigma(x)|, |\sigma(y)|) \le c(F)$ for any $(x,y) \in K^2$ satisfying $F(x,y) = 0$ and for any embedding $\sigma : K \to \mathbb{R}$.

Fix $\Delta \in \mathcal{O}$. Let $(x,y) \in K^2$ be a solution of $F(x,y) = 0$ with $\Delta x, \Delta y \in \mathcal{O}$. Then $\Delta x, \Delta y$ are algebraic integers with all conjugates bounded. Hence there are only finitely many possibilities for x and y. This completes the proof. ∎

COROLLARY 10.4. *Let K be a totally real number field, $\mathcal{O}$ its ring of integers and $a \in K^*$. Then we have the following.*

(i) *If $d = \gcd(m,n)$ is even then the equation*

$$D_m(x, a^{n/d}) + D_n(y\cos(\pi/d), a^{m/d}) = 0$$

has only finitely many solutions with a bounded $\mathcal{O}$-denominator.

(ii) *If $d = \gcd(m,n)$ is odd and the equation*

$$D_m(x, a^{n/d}) + D_n(y, a^{m/d}) = 0$$

has infinitely many solutions with a bounded $\mathcal{O}$-denominator, then all of them with finitely many exceptions satisfy

$$D_{m/d}(x, a^{n/d}) + D_{n/d}(y, a^{m/d}) = 0.$$

P r o o f. This follows from Propositions 3.3 and 10.3. ∎

Now we are ready to prove the main result of this paper.

THEOREM 10.5. *Let K be number field, S a finite set of places of K containing all Archimedean places, and $f(x), g(x) \in K[x]$. Then the following two assertions are equivalent.*

(10.5.a) *The equation $f(x) = g(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator.*

(10.5.b) *We have $f = \varphi \circ f_1 \circ \lambda$ and $g = \varphi \circ g_1 \circ \mu$, where $\lambda(x), \mu(x) \in K[x]$ are linear polynomials, $\varphi(x) \in K[x]$, and $(f_1(x), g_1(x))$ is a standard or specific pair over K such that the equation $f_1(x) = g_1(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator.*

If K is totally real and S is the set of Archimedean places (in particular, if $K = \mathbb{Q}$ and $\mathcal{O}_S = \mathbb{Z}$) then the word "specific" in (10.5.b) *may be skipped.*

P r o o f. Only (10.5.a)⇒(10.5.b) is to be proved (the converse is obvious).

Thus, assume (10.5.a). Then there exists a K-irreducible factor $E(x, y)$ of $f(x) - g(y)$ such that the equation $E(x, y) = 0$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator. By Proposition 10.2, the polynomial $E(x, y)$ is absolutely irreducible. By Siegel's theorem, $E(x, y)$ is exceptional. Now Theorem 9.3 implies that $f = \varphi \circ f_1 \circ \lambda$ and $g = \varphi \circ g_1 \circ \mu$, where φ, f_1, g_1, λ and μ are as required.

Further, since $E(x, y)$ divides $f_1 \circ \lambda(x) - g_1 \circ \mu(y)$, the equation $f_1 \circ \lambda(x) = g_1 \circ \mu(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator. Hence so does the equation $f_1(x) = g_1(y)$.

Now assume that K is totally real, S the set of its Archimedean places, and (f_1, g_1) a specific pair. That is,

$$f_1(x) = D_m(x, a^{n/d}) \quad \text{and} \quad g_1(x) = -D_n(x \cos(\pi/d), a^{m/d}),$$

where $d = \gcd(m, n) \geq 3$ and $a, \cos(2\pi/d) \in K$.

Since $f_1(x) = g_1(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator, Corollary 10.4(i) implies that d is odd. Therefore $\cos(\pi/d) \in K$. Now, $f = \widetilde{\varphi} \circ \widetilde{f}_1 \circ \widetilde{\lambda}$ and $g = \widetilde{\varphi} \circ \widetilde{g}_1 \circ \widetilde{\mu}$ with

$$\widetilde{\varphi}(x) = \varphi(D_d(\varepsilon x, a^{mn/d^2})),$$
$$\widetilde{f}_1(x) = D_{m/d}(x, a^{n/d}), \quad \widetilde{g}_1(x) = D_{n/d}(x, a^{m/d}),$$
$$\widetilde{\lambda}(x) = \varepsilon \lambda(x), \quad \widetilde{\mu}(x) = -\varepsilon \mu(x) \cos(\pi/d),$$

where $\varepsilon = (-1)^m$. Notice that $(\widetilde{f}_1, \widetilde{g}_1)$ is a standard pair (of the third kind).

It remains to show that $\widetilde{f}_1(x) = \widetilde{g}_1(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator. Since $\cos(\pi/d) \in K$, the equation

$$f_1(x) - g_1(y/\cos(\pi/d)) = D_m(x, a^{n/d}) + D_n(x, a^{m/d}) = 0$$

has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator. By Corollary 10.4(ii), so does the equation $D_{m/d}(x, a^{n/d}) = -D_{n/d}(x, a^{m/d})$. Since either m/d or n/d is odd, the equation $\widetilde{f}_1(x) = \widetilde{g}_1(y)$ has the same property. The theorem is proved. ∎

Theorem 1.1 is a particular case of Theorem 10.5.

References

[1] R. M. Avanzi and U. Zannier, *Genus one curves defined by separated variable polynomials*, Acta Arith., to appear.

[2] A. Baker, *Bounds for solutions of superelliptic equations*, Proc. Cambridge Philos. Soc. 65 (1969), 439–444.

[3] F. Beukers, T. N. Shorey and R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal product of terms*, in: [21], pp. 11–26.

[4] Yu. Bilu, *Integral points and Galois covers*, Mat. Contemp. 14 (1998), 1–11.

[5] —, *Quadratic factors of* $f(x) - g(y)$, Acta Arith. 90 (1999), 341–355.

[6] Yu. F. Bilu, B. Brindza, Á. Pintér and R. F. Tichy, *On some diophantine problems related to power sums and binomial coefficients*, in preparation.

[7] Yu. Bilu and G. Hanrot, *Solving superelliptic Diophantine equations by Baker's method*, Compositio Math. 112 (1998), 273–312.

[8] Yu. F. Bilu, T. Stoll and R. F. Tichy, *Diophantine equations for the Meixner polynomials*, in preparation.

[9] B. Brindza and Á. Pintér, *On the irreducibility of some polynomials in two variables*, Acta Arith. 82 (1997), 303–307.

[10] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Math. 107 (1997), 187–219.

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

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

[13] J.-H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to* $Y^n = f(X)$, Math. Proc. Cambridge Philos. Soc. 100 (1986), 237–248.

[14] W. Feit, *On symmetric balanced incomplete block designs with doubly transitive automorphism groups*, J. Combin. Theory Ser. A 14 (1973), 221–247.

[15] —, *Some consequences of the classification of finite simple groups*, in: Proc. Sympos. Pure Math. 37, Amer. Math. Soc., 1980, 175–181.

[16] M. Fried, *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.

[17] —, *Arithmetical properties of function fields (II). The generalized Schur problem*, Acta Arith. 25 (1973/74), 225–258.

[18] —, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. 264 (1974), 40–55.

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

[20] —, *Variables separated polynomials, the genus* 0 *problem, and moduli spaces*, in: [21], pp. 169–228.

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

[22] P. Kirschenhofer, A. Pethő and R. F. Tichy, *On analytical and Diophantine properties of a family of counting polynomials*, Acta Sci. Math. (Szeged) 65 (1999), 47–59.

[23] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[24] W. J. LeVeque, *On the equation* $y^m = f(x)$, Acta Arith. 9 (1964), 209–219.

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

[26] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), 51–66.
[27] A. Schinzel, *Selected Topics on Polynomials*, The Univ. of Michigan Press, Ann Arbor, 1982.
[28] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, Aspects Math. E15, Vieweg, Braunschweig, 1989.
[29] C. L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc. 1 (1926), 66–68; also: *Gesammelte Abhandlungen*, Band 1, 207–208.
[30] —, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl., 1929, Nr. 1; also: *Gesammelte Abhandlungen*, Band 1, 209–266.
[31] V. G. Sprindžuk, *Classical Diophantine Equations in Two Unknowns*, Nauka, Moscow, 1982 (in Russian); English transl.: Lecture Notes in Math. 1559, Springer, 1994.
[32] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. 58 (1995), 312–357.
[33] H. A. Tverberg, *A study in irreducibility of polynomials*, Ph.D. thesis, Dept. of Math., Univ. of Bergen, 1968.
[34] P. M. Voutier, *On the number of S-integral solutions to* $Y^m = f(X)$, Monatsh. Math. 119 (1995), 125–139.

Mathematisches Institut
Universität Basel
Rheinsprung 21
4051 Basel, Switzerland
E-mail: yuri@math.unibas.ch

Institut für Mathematik (A)
Technische Universität Graz
Steyrergasse 30
8010 Graz, Austria
E-mail: tichy@weyl.math.tu-graz.ac.at

Received on 17.12.1999 (3730)