Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 1157–1181
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Complete decomposition of Dickson-type polynomials and related Diophantine equations ☆

Thomas Stoll

Institute of Discrete Mathematics and Geometry, TU Vienna, Wiedner Hauptstrasse 8–10, A-1040 Vienna, Austria

Received 4 December 2006; revised 22 January 2007

Available online 5 May 2007

Communicated by David Goss

Abstract

We characterize decomposition over $\mathbb{C}$ of polynomials $f_n^{(a,B)}(x)$ defined by the generalized Dickson-type recursive relation ($n \geqslant 1$)

$$f_0^{(a,B)}(x) = B, \quad f_1^{(a,B)}(x) = x, \quad f_{n+1}^{(a,B)}(x) = x f_n^{(a,B)}(x) - a f_{n-1}^{(a,B)}(x),$$

where $B, a \in \mathbb{Q}$ or $\mathbb{R}$. As a direct application of the uniform decomposition result, we fully settle the finiteness problem for the Diophantine equation

$$f_n^{(a,B)}(x) = f_m^{(\hat{a},\hat{B})}(y).$$

This extends and completes work of Dujella/Tichy and Dujella/Gusić concerning Dickson polynomials of the second kind. The method of the proof involves a new sufficient criterion for indecomposability of polynomials with fixed degree of the right component.

MSC: 30D05; 11B39; 11D45; 12E10

Keywords: Polynomial decomposition; Dickson-type polynomials; Diophantine equations

☆ Research supported by the Austrian Science Foundation (FWF), project S9604, “Analytic and Probabilistic Methods in Combinatorics”.

E-mail address: stoll@dmg.tuwien.ac.at.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.02.004

1. Introduction

1.1. Indecomposability and Diophantine equations

In what follows, by a (binary) *decomposition* of $f \in \mathbb{C}[x]$ we mean a representation $f = r \circ q$ with some non-constant polynomials $r, q \in \mathbb{C}[x]$, where the operation is the usual functional composition. The theory of polynomial decompositions has a long history and dates back to the work of J.F. Ritt [20,21]. If $\deg r, \deg q > 1$, then the decomposition is called a *non-trivial* decomposition. We call r the *left* and q the *right component* of the decomposition. It is clear, that $(\mathbb{C}[x], \circ)$ forms a non-commutative monoid, where the units are exactly the polynomials over $\mathbb{C}$ of degree 1. Two decompositions $f = r_1 \circ q_1 = r_2 \circ q_2$ are said to be *equivalent* if there is a unit κ such that $r_2 = r_1 \circ \kappa$ and $q_2 = \kappa^{-1} \circ q_1$. A polynomial f is called *decomposable* over $\mathbb{C}$ if it has at least one non-trivial decomposition, and *indecomposable* (or *prime*) otherwise. It is well known that indecomposability over $\mathbb{Q}$ or $\mathbb{R}$ implies indecomposability over $\mathbb{C}$ (see [23, p. 14]).

Indecomposability results are closely related to finiteness statements for Diophantine equations of the form

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

with $f, g \in \mathbb{Q}[x]$ in unknowns $(x, y) \in \mathbb{Q}^2$. In 2000, Bilu and Tichy [3] succeeded in fully joining polynomial decomposition theory with the classical finiteness theorem of Siegel [24] on finiteness of integral points of curves of genus > 0.

Theorem 1 *(Bilu/Tichy [3]). Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent*:

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

$$f = \varphi \circ \mathfrak{f}_1 \circ \kappa_1 \quad \textit{and} \quad g = \varphi \circ \mathfrak{g}_1 \circ \kappa_2,$$

where $\kappa_1, \kappa_2 \in \mathbb{Q}[x]$ are linear, $\varphi(x) \in \mathbb{Q}[x]$, and $(\mathfrak{f}_1, \mathfrak{g}_1)$ is a standard pair over $\mathbb{Q}$ such that the equation $\mathfrak{f}_1(x) = \mathfrak{g}_1(y)$ has infinitely many rational solutions (x, y) with a bounded denominator.

We say that the equation $f(x) = g(y)$ has *infinitely many rational solutions with a bounded denominator*, if there is $\nu \in \mathbb{Z}^+$ such that $f(x) = g(y)$ has infinitely many rational solutions (x, y) with $\nu x, \nu y \in \mathbb{Z}$. The list of *standard pairs*, which is referred to in Theorem 1, includes five different pairs of polynomials $(\mathfrak{f}_1, \mathfrak{g}_1)$ which are defined in the sequel.

Let γ, δ denote some non-zero rational numbers, r, q, s and t some non-negative integers and $v(x) \in \mathbb{Q}[x]$ a non-zero polynomial (which may also be constant). Furthermore, denote by $D_s(x, \gamma)$ the *Dickson polynomial of the first kind* (for short: *Dickson polynomial*) of degree s defined by

$$D_s(x, \gamma) = \sum_{i=0}^{\lfloor s/2 \rfloor} \frac{s}{s-i} \binom{s-i}{i} (-\gamma)^i x^{s-2i},$$