Available online at www.sciencedirect.com

ScienceDirect

C. R. Acad. Sci. Paris, Ser. I 346 (2008) 931–934

COMPTES RENDUS MATHEMATIQUE

http://france.elsevier.com/direct/CRASS1/

Number Theory

Decompositions into sums of two irreducibles in $\mathbf{F}_q[t]$

Andreas O. Bender [1]

Korea Institute for Advanced Study, Seoul 130-722, South Korea

Received 17 May 2008; accepted 28 July 2008

Available online 23 August 2008

Presented by Jean-Pierre Serre

Abstract

A monic polynomial in $\mathbf{F}_q[t]$ of degree n over a finite field $\mathbf{F}_q$ of odd characteristic is the sum of two monic irreducibles in $\mathbf{F}_q[t]$ of degrees n and $n-1$, provided q is larger than an explicitly given bound in terms of n. ***To cite this article: A.O. Bender, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

Décompositions en sommes de deux polynômes irréductibles dans $\mathbf{F}_q[t]$. Un polynôme unitaire $f \in \mathbf{F}_q[t]$ de degré n à coefficients dans un corps fini $\mathbf{F}_q$ de caractéristique différente de 2 s'écrit comme une somme $f = g + h$, où $g, h \in \mathbf{F}_q[t]$ sont des polynômes unitaires irréductibles de degrés n et $n-1$, dès que q est plus grand qu'une borne explicite dépendant uniquement de n. ***Pour citer cet article : A.O. Bender, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

1. Introduction

When is a polynomial of degree n in $\mathbf{F}_q[t]$ the sum of two irreducibles of unequal degrees at most n? This question is clearly motivated by the Goldbach conjecture which asserts that every even number greater than 2 is the sum of two primes.

In the function field case, it turns out that a distinction into even and odd elements only plays a role if $q = 2$ and that we want to consider only monic polynomials [3, conj. 1.20].

This Note outlines the proofs of the following two theorems, both of which rely heavily on the proof of Theorem 3 quoted below and proved in [2]. Complete proofs of both theorems are given in [1].

Theorem 1. *Let $\mathbf{F}_q$ be a finite field of odd characteristic and cardinality q and let F be a monic polynomial in $\mathbf{F}_q[t]$ whose degree is at least* 2.

E-mail address: andreas@kias.re.kr.

URL: http://homepage.mac.com/andreasobender.

[1] I thank Olivier Wittenberg for the translation of the abstract into French.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.07.025

Then for any sufficiently large integer s, there exist irreducible monic polynomials F_1 *and* F_2 *in* $\mathbf{F}_{q^s}[t]$ *with* $\deg(F_1) = \deg(F) - 1$ *and* $\deg(F_2) = \deg(F)$ *such that*

$$F = F_1 + F_2.$$

Theorem 2. *Let* $\mathbf{F}_q$ *be a finite field of odd characteristic and cardinality q and let F be a monic polynomial in* $\mathbf{F}_q[t]$ *whose degree n is at least* 2.

Then if $q > 8(n+6)^{2n^2}$, *there exist irreducible monic polynomials* F_1 *and* F_2 *in* $\mathbf{F}_q[t]$ *with* $\deg(F_1) = \deg(F) - 1$ *and* $\deg(F_2) = \deg(F)$ *such that*

$$F = F_1 + F_2.$$

2. The result over $\mathbf{F}_{q^s}[t]$

The main tool for the proof is a slight variant of the following theorem:

Theorem 3. *(Theorem 1.1 in [2].) Let* $\mathbf{F}_q$ *be a finite field of characteristic p and cardinality q. Let* $f_1, \ldots, f_n \in \mathbf{F}_q[t, x]$ *be irreducible polynomials whose total degrees* $\deg(f_i)$ *satisfy* $p \nmid \deg(f_i)(\deg(f_i) - 1)$ *for all i. Assume that the curves* $C_i \subseteq \mathbf{P}^2_{\mathbf{F}_q}$ *defined as the Zariski closures of the affine curves*

$$f_i(x, t) = 0$$

are smooth. Then, for any sufficiently large $s \in \mathbf{N}$, *there exist* $a, b \in \mathbf{F}_{q^s}$ *such that the polynomials* $f_1(at + b, t), \ldots, f_n(at + b, t) \in \mathbf{F}_{q^s}[t]$ *are all irreducible.*

We let $F(t)$ be a monic polynomial in $\mathbf{F}_q[t]$ of degree n at least 2. Now suppose there exists an $f_1 \in \mathbf{F}_q[x, t]$ of total degree $n - 1$ such that both f_1 and $f_2 = -f_1 + F(t)$ satisfy the assumptions of Theorem 3. Then we can apply that theorem and get a and b in some $\mathbf{F}_{q^s}$ for which both $f_i(at + b, t)$ are irreducible in $\mathbf{F}_{q^s}[t]$. In view of $F = f_1 + (-f_1 + F)$, we then have a representation of $F(t)$ as the sum of two irreducibles in $\mathbf{F}_{q^s}[t]$, one of degree at most $n - 1$ and the other of degree n.

For the construction of such an f_1, we observe that both irreducibility and smoothness are genericity conditions. The proof of Theorem 3 shows that the conditions $p \nmid \deg(f_i)(\deg(f_i) - 1)$ are imposed to ensure separability of the Gauss maps of the curves C_i, which is a genericity condition as well.

The polynomial $f_2(at + b, t)$ is always monic, but $f_1(at + b, t)$ will in general not be. In order to ensure monicity of f_1, the proof of Theorem 3 has to be suitably modified.

We start with a short review of the proof of Theorem 3, for which the following definition is pivotal.

If k is a field, a finite k-scheme X is said to have *at most one double point* if $n(X) \geqslant r(X) - 1$, where $r(X)$ denotes the rank and $n(X)$ the geometric number of points of X (this paragraph is quoted from [2]).

Definition 4. (See [5].) A finite morphism $f : C \to \mathbf{P}^1_k$ is called generic if $f^{-1}(x)$ has at most one double point for all $x \in \mathbf{P}^1_k$.

The proof shows that projections of the curves C_i to $\mathbf{P}^1$ from a generically chosen point in $\mathbf{P}^2$ are generic morphisms β_i with pairwise disjoint ramification loci. This leads to the conclusion that the function field extensions associated to the β_i have the full symmetric group as Galois group. Then the Cebotarev Density Theorem is used to find irreducible fibres of the β_i which in turn give rise to irreducible polynomials $f_i(at + b, t)$.

If, without loss of generality, we fix $a = 1$, the leading coefficient of $f_1(t + b, t)$ is the sum of the coefficients of the terms of total degree $n - 1$. We parametrize the polynomials $f_{1(c)}$ in two variables x, t of total degree $n - 1$ by their coefficient vectors (c) in an affine space $\mathbf{A}^I$. Then every element in the family $\mathfrak{F}$ of such polynomials $f_{1(c)}$ for which $f(t + b, t)$ is monic for all b has coefficients (c) in an affine subspace $H \subset \mathbf{A}^I$ of codimension one.

For any $f_1 \in \mathfrak{F}$, we set $f_2 = -f_1 + F$ and let C_i be the Zariski closure of $f_i = 0$ in the projective plane. In the projectivised coordinates (x, t, z), we denote by β_i the projections from the point $M = (1, 1, 0)$ to $\mathbf{P}^1(x, z)$. All affine lines containing the point M are of the form $x = t + b$. One easily checks that the monicity assumption implies that $M \notin C_i$ and so the projections β_i are morphisms.

There are two groups of conditions we need to impose on the coordinate vector (c) parametrizing the two f_i. The first group consists of the properties listed as assumptions in Theorem 3 and these are smoothness, irreducibility and separability of the Gauss maps of both curves C_i. The second group of conditions is needed to ensure that the proof of Theorem 3 goes through with the fixed value of $a = 1$. In this group we have the conditions that the projection β_1 be generic and that β_2 be generic with the exception of the point at infinity whose fibre intersects C_2 in a point of order n. Furthermore, we have to demand that no line of the form $x = t + b$ be tangent to both curves C_i and that the line at infinity, which is tangent to C_2, not be tangent to C_1.

For any one of these conditions, we need to show that the subscheme of H whose associated $f_{i(c)}$ satisfy it is both Zariski open and nonempty. The argument for showing openness uses the following classical result from elimination theory [4, Cor. 14.3]: The condition for a polynomial of fixed degree and fixed number of variables to split into factors of specified degree and multiplicity is the vanishing of certain polynomials in the polynomial's coefficients. For every condition, nonemptiness is ensured by constructing examples of the f_i which satisfy that particular condition for any given $F(t)$. Since the intersection of nonempty open subschemes of H is nonempty, openness and nonemptyness for each one of the conditions show that there exist (c) whose associated polynomials f_i satisfy all of them.

Smoothness and irreducibility are straightforward to check along the lines sketched in the previous paragraph.

Separability of the Gauss maps for the case of $p \nmid \deg(f_i)(\deg(f_i) - 1)$ is proved in the last paragraph of the proof of Proposition 3.1 in [2]. For $p \mid \deg(f_i)(\deg(f_i) - 1)$, we need to consider the splitting behaviour of the polynomials describing the intersection of the curves C_i with a tangent.

As for the conditions on the morphisms β_i, part of the proof of Theorem 3 shows that by separability of the Gauss maps, there are only finitely many tangents to the C_i which intersect these curves other than in at most one double point. A rescaling of one of the variables therefore suffices to let all of them assume a form different from $x = t + b$.

The condition on the tangent at infinity is again straightforward.

Now let s be large enough such that $(c) \in H_{\mathbf{F}_{q^s}}$ exists with all conditions in both groups satisfied.

Since the projection β_1 of C_1 is generic, the rest of the proof of Theorem 3 goes through for f_1 and we can conclude that the Galois group associated to β_1 is indeed the full symmetric group. As for C_2, the projection has one ramification point of order n above the point at infinity and is generic otherwise. We note that the symmetric group of n elements is generated by one element of order n and one transposition, so as in the case of generic projection to $\mathbf{P}^1$, we get the full symmetric group as Galois group.

The two conditions on the tangents to the curves C_i were chosen precisely to ensure that the ramification loci of the β_i do not intersect, which is necessary for proceeding with the proof of Theorem 3.

Finally we need to let s be large enough for the application of the Cebotarev Density Theorem and then we find b_0 such that both $f_i(t + b_0, t)$ in $\mathbf{F}_{q^s}[t]$ are monic and irreducible.

3. Application to the case $\mathbf{F}_q[t]$

We have to derive explicit lower bounds for the size of q^s in Theorem 1 and then show that a q larger than the stated bound satisfies them.

For every condition on the f_i we pursue the following approach. We estimate the degree of the closed subscheme of H which consists of the unusable points (c) for which the associated C_i do not satisfy the respective condition. Using the fact that this closed subscheme is contained in a hypersurface of that degree, we remove from H an upper bound for the number of points over $\mathbf{F}_q$ on such a hypersurface.

Doing this for every condition imposed on the f_i, we show that the given lower bound on q implies that there is at least one point (c) in H over $\mathbf{F}_q$ for which the associated C_i satisfy all conditions.

Finally, we have to check that the given lower bound on q suffices to apply the Cebotarev Density Theorem at the end of the proof of Theorem 3.

References

[1] A.O. Bender, Representing an element in $\mathbf{F}_q[t]$ as the sum of two irreducibles in $\mathbf{F}_{q^s}[t]$, submitted for publication.

[2] A.O. Bender, O. Wittenberg, A potential analogue of Schinzel's hypothesis for polynomials with coefficients in $\mathbf{F}_q[t]$, Int. Math. Res. Not. 36 (2005) 2237–2248, also available from http://arxiv.org/abs/math/0412303.

[3] G.W. Effinger, D.R. Hayes, Additive Number Theory of Polynomials Over a Finite Field, Oxford University Press, New York, NY, 1991.
[4] D. Eisenbud, Commutative Algebra With a View Toward Algebraic Geometry, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, NY, 1995.
[5] A. Hurwitz, Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten, Math. Ann. 39 (1891) 1–61 and Math. Werke, Band 1/XXI, Birkhäuser, Basel, 1932.