Journal of Number Theory 135 (2014) 60–66

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Square-free values of polynomials over the rational function field ☆

Zeév Rudnick

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

ARTICLE INFO

Article history:
Received 23 August 2013
Accepted 23 August 2013
Available online 15 October 2013
Communicated by K. Soundararajan

Keywords:
Square-free
Finite fields
Function fields

ABSTRACT

We study representation of square-free polynomials in the polynomial ring $\mathbb{F}_q[t]$ over a finite field $\mathbb{F}_q$ by polynomials in $\mathbb{F}_q[t][x]$. This is a function field version of the well-studied problem of representing square-free integers by integer polynomials, where it is conjectured that a separable polynomial $f \in \mathbb{Z}[x]$ takes infinitely many square-free values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is square-free have a positive density. We show that if $f(x) \in \mathbb{F}_q[t][x]$ is separable, with square-free content, of bounded degree and height, and n is fixed, then as $q \to \infty$, for almost all monic polynomials $a(t)$ of degree n, the polynomial $f(a)$ is square-free.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. We wish to study representation of square-free polynomials in the polynomial ring $\mathbb{F}_q[t]$ by polynomials in $\mathbb{F}_q[t][x]$. This is a function field version of the well-studied problem of representing square-free integers by integer polynomials, where it is conjectured that a separable polynomial (that is, without

☆ We thank Lior Rosenzweig for his comments. This work was conceived during the ERC Research Period on Diophantine Geometry in Pisa during September 2012. The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ERC grant agreement No. 320755.

E-mail address: rudnick@post.tau.ac.il.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.08.014

repeated roots) $f \in \mathbb{Z}[x]$ takes infinitely many square-free values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is square-free have a positive density. The problem is most difficult when f is irreducible. The quadratic case was solved by Ricci [13]. For cubics, Erdös [2] showed that there are infinitely many square-free values, and Hooley [6] gave the result about positive density. Beyond that nothing seems known unconditionally for irreducible f, for instance it is still not known that a^4+2 is infinitely often square-free. Granville [3] showed that the ABC conjecture completely settles this problem. An easier problem which has recently been solved is to ask how often an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree d attains values which are free of $(d-1)$-th powers, either when evaluated at integers or at primes, see [2,7–9,5,1,4,12].

In this note we study a function field version of this problem. Given a polynomial $f(x)=\sum_j \gamma_j(t)x^j \in \mathbb{F}_q[t][x]$ which is separable, that is with no repeated roots in any extension of $\mathbb{F}_q(t)$, we want to know how often is $f(a)$ square-free in $\mathbb{F}_q[t]$ as a runs over (monic) polynomials in $\mathbb{F}_q[t]$.

We want to rule out polynomials like $f(x,t)=t^2x$ for which $f(a(t),t)$ can never be square-free. To do so, recall that the content $c \in \mathbb{F}_q[t]$ of a polynomial $f \in \mathbb{F}_q[t][x]$ as above is defined as the greatest common divisor of the coefficients of f: $c=\gcd(\gamma_0,\dots,\gamma_\ell)$. A polynomial is *primitive* if $c=1$, and any $f \in \mathbb{F}_q[t][x]$ can be written as $f=cf_0$ where f_0 is primitive. If the content c is not square-free then $f(a)$ can never be square-free.

For any field $\mathbb{F}$, let

$$\mathcal{M}_n(\mathbb{F})=\{a \in \mathbb{F}[t]:\ \deg a=n,\ a \text{ monic}\}, \tag{1.1}$$

so that $\#\mathcal{M}_n(\mathbb{F}_q)=q^n$. Defining

$$\mathcal{S}_f(n)(\mathbb{F})=\{a \in \mathcal{M}_n(\mathbb{F}):\ f(a) \text{ is square-free}\}, \tag{1.2}$$

we want to study the frequency

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#\mathcal{M}_n(\mathbb{F}_q)} \tag{1.3}$$

in an appropriate limit.

There are two possible limits to take: Large degree ($n \to \infty$) while keeping the constant field $\mathbb{F}_q$ fixed, or large constant field ($q \to \infty$) while keeping n fixed. The large degree limit (q fixed, $n \to \infty$) was investigated by Ramsay [11] and Poonen [10] who showed[1] that for $f \in \mathbb{F}_q[t][x]$ separable,

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#\mathcal{M}_n(\mathbb{F}_q)}=c_f+O_{f,q}\left(\frac{1}{n}\right), \quad \text{as } n \to \infty, \tag{1.4}$$

[1] They actually count all polynomials up to degree n, and do not impose the monic condition.