SEQUENCES OF CONSECUTIVE SMOOTH POLYNOMIALS OVER A FINITE FIELD

ARIANE MASUDA AND DANIEL PANARIO

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. Given $\varepsilon > 0$, we show that there are infinitely many sequences of consecutive εn -smooth polynomials over a finite field. The number of polynomials in each sequence is approximately $\ln \ln \ln n$.

1. INTRODUCTION

The ring of integers and the ring of polynomials over a finite field share elementary properties such as having the structure of a Euclidean ring and of a unique factorization domain. So, it is not very surprising that many authors have established analogues of ideas and results between these two rings. One could list a series of results about $\mathbb{Z}$ for which a $\mathbb{F}_q[x]$ version has been formulated. For example, Dirichlet's Theorem on primes in an arithmetic progression is established for polynomials in Kornblum [11]. Effinger in [2] proves a Goldbach-type theorem for polynomials of low degree over odd finite fields (see also [3] for another variant of this theorem). The well-known Twin Primes Conjecture also gives rise to a similar statement for polynomials by properly defining the notion of twin irreducible polynomials. The existence of infinitely many twin irreducible polynomials over a fixed finite field was conjectured by Effinger et al. [4], and has been recently proved by Hall [8] in the case of $\mathbb{F}_q$ with $q \neq 2$. In [4] one can find a polynomial version of Mertens' Theorem, which is another famous result over the integers. Results of this type are usually obtained by properly adjusting the concepts already in existence for integers to polynomials. One mimics the techniques as far as they work in the new context, and then employs some arguments from the theory of finite fields to complete the proof.

In this paper we also obtain results for polynomials following ideas developed for integers. In [1] Balog and Wooley investigate the existence of long strings of consecutive integers, all smooth, that is, having only small prime factors. They extend arguments given by Eggleton and Selfridge [5]. A key idea of the latter work is to use the fact that the polynomial $x^d - 1$ factors as a product of cyclotomic polynomials of degree at most $\phi(d)$. This observation appears again in [1], and also in this paper. In the case of polynomials over a finite field, the adaptation of

Received by the editors January 19, 2005 and, in revised form, December 14, 2005.

2000 *Mathematics Subject Classification*. Primary 11T06, 11T99.

Key words and phrases. Smooth polynomials, finite fields, sequences of polynomials.

©2006 American Mathematical Society
 Reverts to public domain 28 years from publication

techniques occurs naturally. The proof is elementary, and ends up being similar to the one given in [1], up to some adjustments.

Before we state our results, let us explain what we mean by *consecutive* and *smooth polynomials*. Suppose $\mathbb{F}_q$ is a finite field with $q = \ell^n$, ℓ prime, and the elements in $\mathbb{F}_q$ are written in terms of a root α of an irreducible polynomial of degree n over $\mathbb{F}_\ell$. To order all polynomials in $\mathbb{F}_q[x]$, we associate to

$$f(x) = a_m(\alpha)x^m + a_{m-1}(\alpha)x^{m-1} + \cdots + a_0(\alpha)$$

the integer $I_f = a_m(\ell)q^m + a_{m-1}(\ell)q^{m-1} + \cdots + a_0(\ell)$. If $|I_f - I_g| = 1$, we say that f and g are *consecutive polynomials*. This ordering has already been considered by some authors [10]. Here we are only interested in monic polynomials. Thus, two distinct monic polynomials f and g are said to be consecutive if there is no monic polynomial h over $\mathbb{F}_q$ with I_h between I_f and I_g . From now on, for simplicity, when we speak of polynomials over a finite field, it should be understood we mean monic polynomials. Another concept we need is smoothness. In analogy to the concept of smooth numbers, we say that a polynomial f is ρ -*smooth* if all irreducible factors of f have degree smaller than or equal to ρ . Smooth polynomials over a finite field play a crucial role in the discrete logarithm problem over finite field extensions [6, 13, 14]. The distribution of m -smooth polynomials over a finite field has also been studied in [7, 12, 13]. These papers provide estimates for the number of m -smooth polynomials of degree n over $\mathbb{F}_q$ by an application of the saddle point method. When m is large with respect to n , the estimation is given in terms of the Dickman function that underlies the estimation of smooth integers [14, 15].

We use the same notational conventions as Balog and Wooley in [1]. Our main result is Theorem 2.1. We prove that there exist infinitely many sequences of consecutive smooth polynomials of length approximately $\ln \ln \ln n$. In other words, given $\varepsilon > 0$, we show explicitly that there are infinitely many polynomials f such that $f - b$ has all irreducible factors of degree at most εn , where b is any polynomial of degree less than $\ln \ln \ln \ln n$, approximately. To prove this we need two lemmas. The first one (Lemma 2.1) is proved in [1]. The second one (Lemma 2.2) is actually a more general form of Theorem 2.1. We also provide infinitely many sets of smooth polynomials of a special form (Theorem 2.2), as another consequence of Lemma 2.2. There is an $\ln$ difference between Balog and Wooley's result [1] for integers and our result for polynomials over a finite field. This is typical when studying similar problems for integers and polynomials over a finite field.

2. SMOOTH POLYNOMIALS

In this paper, $\ln$ denotes the natural logarithm, $\log$ denotes the logarithm in base q , and $\log_k x$ denotes the k -fold iterated logarithm. We need the following result from [1].

Lemma 2.1 ([1]). *Let y be a large real number, and let t and k be positive integers. Then, one can partition the prime numbers not exceeding y , and coprime with k , into sets $\mathcal{P}_1, \dots, \mathcal{P}_t$ with the property that for each i ,*

$$\prod_{p \in \mathcal{P}_i} \left(1 - \frac{1}{p}\right) < 2 \left(\frac{k}{\phi(k) \ln y}\right)^{1/t}$$

and

$$\prod_{p \in \mathcal{P}_i} p < y^2 \exp\left(\frac{5y}{4t}\right).$$

Lemma 2.2. Suppose $\mathbb{F}_q$ has characteristic ℓ . Let (t_n) be an increasing sequence of integers (possibly constant) such that $t_n \geq 2$ for all n sufficiently large, let (a_n) and (b_n) be sequences of non-zero polynomials over $\mathbb{F}_q$ with at least one b_i non-constant, and let (k_n) be a sequence of positive integers. We define for each $n \in \mathbb{N}$

$$(1) \quad \Delta_n = \sum_{i=1}^{t_n} (\deg a_i + \deg b_i), \quad K_n = \prod_{i=1}^{t_n} k_i, \quad \kappa_n = \max_{1 \leq i \leq t_n} k_i,$$

$$(2) \quad \alpha_n = \max_{1 \leq i \leq t_n} \{\deg a_i - \deg b_i\}, \quad \text{and} \quad y_n = \frac{4}{5} \ln \left(\frac{n}{\Delta_n} \right).$$

Then, for each natural number n , for which y_n is sufficiently large and $\deg b_i > 0$ for some $i \leq t_n$, there is a polynomial f_n over $\mathbb{F}_q$ with

$$(3) \quad \frac{n^{1/11}}{\ell K_n} < \deg f_n < n,$$

which satisfies the property that the largest degree among the irreducible factors over $\mathbb{F}_q$ of the polynomial $f_n \prod_{i=1}^{t_n} (a_i f_n^{k_i} - b_i)$ is at most

$$\max \left\{ \max_{1 \leq i \leq t_n} \{\deg a_i, \deg b_i\}, 2(\kappa_n n + \alpha_n) \left(\frac{\phi(\ell K_n)}{\ell K_n} \ln y_n \right)^{-1/t_n} \right\}.$$

Proof. For convenience, from now on we shall drop the subscripts n . Suppose y is very large. It follows from Lemma 2.1 that we can partition all prime numbers not exceeding y , and coprime with ℓK , into sets $\mathcal{P}_1, \dots, \mathcal{P}_t$ with the property that

$$(4) \quad \prod_{p \in \mathcal{P}_i} \left(1 - \frac{1}{p}\right) < 2 \left(\frac{\ell K}{\phi(\ell K) \ln y} \right)^{1/t}$$

and

$$(5) \quad \prod_{p \in \mathcal{P}_i} p < y^2 \exp\left(\frac{5y}{4t}\right).$$

For $1 \leq i \leq t$, we define

$$\gamma_i = \prod_{p \in \mathcal{P}_i} p, \quad \Gamma_i = \prod_{\substack{1 \leq j \leq t \\ j \neq i}} \gamma_j, \quad \text{and} \quad \Gamma = \gamma_1 \cdots \gamma_t.$$

Then, it follows from the Prime Number Theorem [9] that

$$(6) \quad (\ell K)^{-1} e^{3y/4} < \Gamma < e^{5y/4}.$$

Moreover, $(k_j \Gamma_j, \gamma_j) = 1$ for $1 \leq j \leq t$. So, for each j , let $\tilde{\lambda}_j$ and $\tilde{\mu}_j$ satisfy the property that

$$\begin{aligned} k_j \Gamma_j \tilde{\lambda}_j &\equiv -1 \pmod{\gamma_j}, \\ k_j \Gamma_j \tilde{\mu}_j &\equiv 1 \pmod{\gamma_j}, \end{aligned}$$

and

$$(7) \quad 1 \leq \tilde{\lambda}_j, \tilde{\mu}_j < \gamma_j.$$

Let $\lambda_j = \Gamma_j \tilde{\lambda}_j$ and $\mu_j = \Gamma_j \tilde{\mu}_j$, for $1 \leq j \leq t$. We also define the integers

$$\Lambda_{ij} = \begin{cases} \frac{\lambda_i k_j}{\gamma_j} & \text{if } i \neq j, \\ \frac{\gamma_j k_j + 1}{\gamma_j} & \text{if } i = j, \end{cases} \quad \text{and} \quad M_{ij} = \begin{cases} \frac{\mu_i k_j}{\gamma_j} & \text{if } i \neq j, \\ \frac{\mu_j k_j - 1}{\gamma_j} & \text{if } i = j, \end{cases}$$

where $1 \leq i, j \leq t$. Let $f = \prod_{j=1}^t a_j^{\lambda_j} b_j^{\mu_j}$. We first prove that such f satisfies (3). From (6) and (7), we get

$$\deg f = \sum_{j=1}^t (\lambda_j \deg a_j + \mu_j \deg b_j) < \Gamma \Delta < e^{5y/4} \Delta = n.$$

On the other hand, if $\tilde{\gamma} = \max\{\gamma_j : 1 \leq j \leq t\}$, then from the fact that $t \geq 2$ and from (5), (6) and (7), we have that, for y sufficiently large,

$$\begin{aligned} \deg f &\geq \frac{\Gamma \Delta}{\tilde{\gamma}} > \frac{\Gamma \Delta}{y^2} \exp\left(-\frac{5y}{4t}\right) > \frac{\Delta}{\ell K y^2} \exp\left(\frac{3y}{4} - \frac{5y}{4t}\right) \\ &\geq \frac{\Delta}{\ell K y^2} \left(\frac{n}{\Delta}\right)^{1/10} > \frac{n^{1/11}}{\ell K}. \end{aligned}$$

The rest of the proof concentrates on the smoothness of the polynomial

$$f \prod_{j=1}^t (a_j f^{k_j} - b_j).$$

For $1 \leq j \leq t$, we have

$$a_j f^{k_j} - b_j = b_j (z_j^{\gamma_j} - 1),$$

where $z_j = \prod_{i=1}^t a_i^{\Lambda_{ij}} b_i^{M_{ij}}$. The polynomial $z_j^{\gamma_j} - 1$ factors as a product of cyclotomic polynomials of degree at most $\phi(\gamma_j)$ over $\mathbb{F}_q$, since $\ell = \text{char}(\mathbb{F}_q)$ does not divide γ_j . So the polynomial $f \prod_{j=1}^t (a_j f^{k_j} - b_j)$ is ρ -smooth, where

$$\rho = \max_{1 \leq j \leq t} \left\{ \deg a_j, \deg b_j, \phi(\gamma_j) \left(\sum_{i=1}^t (\Lambda_{ij} \deg a_i + M_{ij} \deg b_i) \right) \right\}.$$

Now, by (4), (6) and (7), we get

$$\begin{aligned} &\phi(\gamma_j) \left(\sum_{i=1}^t (\Lambda_{ij} \deg a_i + M_{ij} \deg b_i) \right) < \frac{\phi(\gamma_j)}{\gamma_j} (\kappa \Gamma \Delta + \alpha) \\ &< \prod_{p \in \mathcal{P}_j} \left(1 - \frac{1}{p} \right) (\kappa e^{5y/4} \Delta + \alpha) < 2 \left(\frac{\ell K}{\phi(\ell K) \ln y} \right)^{1/t} (\kappa n + \alpha). \end{aligned}$$

This completes the proof. $\square$

We choose specific values for the parameters in Lemma 2.2 to get our main result.

Theorem 2.1. *Let $\mathbb{F}_q$ be of characteristic ℓ , let u be a fixed real number with $u > 1$, and let (m_n) be a sequence of positive integers defined by*

$$m_n = \left\lfloor \log \left(\frac{\ln_3 n}{\ln(3u)} \right) \right\rfloor.$$

Then, in $\mathbb{F}_q[x]$, there are infinitely many polynomials f_n such that $f_n - b$ is n/u -smooth for every polynomial b of degree $< m_n$.

Proof. First we observe that $m_n \geq 2$ for n sufficiently large. Let

$$T_n = \{b \in \mathbb{F}_q[x] : b \neq 0 \text{ and } 0 \leq \deg b < m_n\},$$

for $n \in \mathbb{N}$. We apply Lemma 2.2 with

$$t_n = \#T_n, \quad k_n = 1, \quad a_n = 1,$$

for $n \in \mathbb{N}$. Thus,

$$t_n = q^{m_n} - 1.$$

We also note that $t_n \geq 2$, for n sufficiently large. In the notation defined by (1) and (2), we have for $b_i \in T_n$

$$\begin{aligned} \Delta_n &= \sum_{i=1}^{t_n} \deg b_i = (q-1) \sum_{i=1}^{m_n-1} iq^i = \frac{q((m_n-1)q^{m_n} - m_n q^{m_n-1} + 1)}{(q-1)}, \\ K_n &= 1, \quad \kappa_n = 1, \quad \alpha_n = 0, \quad \text{and} \quad y_n = \frac{4}{5} \ln \left(\frac{n}{\Delta_n} \right). \end{aligned}$$

Therefore, provided that n is sufficiently large, we conclude that there is a polynomial f_n , namely, $f_n = \prod_{j=1}^{t_n} b_j^{\mu_j}$, where $b_1, \dots, b_{t_n}$ are all polynomials in T_n and $n^{1/11}\ell^{-1} < \deg f_n < n$. Furthermore, the largest degree among the irreducible factors of the polynomial $f_n \prod_{i=1}^{t_n} (f_n - b_i)$ is at most

$$\max \left\{ m_n - 1, 2n \left(\frac{\ell}{\phi(\ell) \ln y_n} \right)^{1/t_n} \right\}.$$

As $m_n \geq 2$ and ℓ is a prime ≥ 2 , we get

$$\begin{aligned} 2 \left(\frac{\ell}{\phi(\ell) \ln y_n} \right)^{1/t_n} &< 2.6 \left(\frac{1}{\ln y_n} \right)^{1/t_n} = 2.6 \exp \left(-\frac{1}{t_n} \ln_2 y_n \right) \\ &< 2.6 \exp \left(-\frac{1}{q^m} \ln_2 y_n \right) = \frac{2.6}{(3u)^{\frac{\ln_2 y_n}{\ln_3 n}}} < \frac{1}{u}, \end{aligned}$$

for n sufficiently large. □

Another application of Lemma 2.2 provides families of smooth polynomials of a special type.

Theorem 2.2. *Let $\mathbb{F}_q$ be of characteristic ℓ , and let t be an integer with $t \geq 2$. For $1 \leq i \leq t$, let A_i and B_i be non-zero polynomials over $\mathbb{F}_q$ with some $\deg B_i > 0$. Then, there are infinitely many polynomials f_n with $\frac{n^{1/11}}{2^t \ell} < \deg f_n < n$, for which the polynomials f_n and $A_i f_n \pm B_i$, $1 \leq i \leq t$, are simultaneously ρ -smooth, where*

$$\rho = \frac{5n}{\left(\frac{1}{3} \ln_2 n^{3/4} \right)^{1/t}}.$$

Proof. Following the notation of Lemma 2.2, let $t_n = t$, for each $n \in \mathbb{N}$, and

$$k_i = 2, \quad a_i = A_i^2, \quad b_i = B_i^2,$$

for each $1 \leq i \leq t$. Thus, we have

$$\Delta_n = 2 \sum_{i=1}^t (\deg A_i + \deg B_i), \quad K_n = 2^t, \quad \kappa_n = 2,$$

$$\alpha_n = \max_{1 \leq i \leq t} \{\deg A_i^2 - \deg B_i^2\}, \quad y_n = \frac{4}{5} \ln \left(\frac{n}{\Delta_n} \right).$$

Therefore, there exists a polynomial f_n such that

$$\frac{n^{1/11}}{2^{t\ell}} < \deg f_n < n,$$

satisfying the property that the largest degree among the irreducible factors of $f_n \prod_{i=1}^t (A_i^2 f_n^2 - B_i^2) = f_n \prod_{i=1}^t (A_i f_n + B_i)(A_i f_n - B_i)$ is at most

$$\max \left\{ 2 \max_{1 \leq i \leq t} \{\deg A_i, \deg B_i\}, 2(2n + \alpha_n) \left(\frac{\phi(2^{t\ell})}{2^{t\ell}} \ln y_n \right)^{-1/t} \right\}.$$

We recall that α_n and Δ_n do not depend on n in this theorem. Hence, there is a sequence (f_{n_k}) of non-zero polynomials satisfying the property that for each k the polynomials f_{n_k} and $A_i f_{n_k} \pm B_i$, $1 \leq i \leq t$, are simultaneously ρ -smooth, where

$$\begin{aligned} \rho &= 2(2n_k + \alpha_{n_k}) \left(\frac{\phi(2^{t\ell})}{2^{t\ell}} \ln_2 \left(\frac{n_k}{\Delta_{n_k}} \right)^{4/5} \right)^{-1/t} \\ &\leq \frac{5n_k}{\left(\frac{1}{3} \ln_2 n_k^{3/4} \right)^{1/t}}. \end{aligned}$$

□

ACKNOWLEDGMENTS

The authors would like to thank Igor Shparlinski for suggesting the problem and for his helpful comments. The second author was supported in part by NSERC grant 238757.

REFERENCES

1. A. Balog and T. D. Wooley, On strings of consecutive integers with no large prime factors, *J. Austral. Math. Soc. Ser. A* **64** (1998), 266-276. MR1619809 (99g:11109)
2. G. Effinger, A Goldbach theorem for polynomials of low degree over odd finite fields, *Acta Arith.* **42** (1983), 329-365. MR0736718 (85f:11092)
3. G. Effinger, A Goldbach 3-primes theorem for polynomials of low degree over finite fields of characteristic 2, *J. Number Theory* **29** (1988), 345-363. MR0955958 (89j:11119)
4. G. Effinger, K. Hicks and G. L. Mullen, Twin irreducible polynomials over finite fields, *Finite fields with applications to coding theory, cryptography and related fields*, Springer, 2002, 94-111. MR1995330 (2004h:11104)
5. R. B. Eggleton and J. L. Selfridge, Consecutive integers with no large prime factors, *J. Austral. Math. Soc. Ser. A* **22** (1976), 1-11. MR0439778 (55:12662)
6. T. Garefalakis and D. Panario, The index calculus method using non-smooth polynomials, *Math. Comp.* **70** (2001), 1253-1264. MR1826581 (2002a:11140)
7. T. Garefalakis and D. Panario, Polynomials over finite fields free from large and small degree irreducible factors, *J. Algorithms* **44** (2002), 98-120. MR1932679 (2003j:12001)
8. C. J. Hall, *L-functions of Twisted Curves*, Ph.D. Thesis, Princeton University, 2003.
9. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Clarendon Press, Oxford, 1989. MR0568909 (81i:10002)

10. K. H. Hicks, G. L. Mullen and I. Sato, Distribution of irreducible polynomials over $\mathbb{F}_2$, *Finite fields with applications in coding theory, cryptography and related fields*, Springer, 2002, 177-186. MR1995335 (2004h:11105)
11. H. Kornblum, Über die Primfunktionen in einer arithmetischen Progression, *Math. Z.* **5** (1919), 100-111. MR1544375
12. R. Lovorn, *Rigorous, Subexponential Algorithms for Discrete Logarithms over Finite Fields*, Ph.D. Thesis, University of Georgia, 1992.
13. A. M. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance, *Advances in cryptology: Proceeding of Eurocrypt'84* (T. Beth, N. Cot, I. Ingemarsson, eds.), Lecture Notes in Comput. Sci., **209**, Springer-Verlag (1985), 224-314. MR0825593 (87g:11022)
14. A. M. Odlyzko, Discrete logarithms and smooth polynomials, *Finite fields: theory, applications, and algorithms*, G. L. Mullen and P. Shiue, eds., Amer. Math. Soc., Contemp. Math. **168** (1994), 269-278. MR1291435 (95f:11107)
15. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, 1995. MR1366197 (97e:11005a)

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO,
CANADA K1S 5B6

E-mail address: ariane@math.carleton.ca

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO,
CANADA K1S 5B6

E-mail address: daniel@math.carleton.ca