Publl. Math. Debrecen
79/3-4 (2011), 423–432
DOI: 10.5486/PMD.2011.5089

Smooth shifted monomial products

By ÉTIENNE FOUVRY (Orsay) and IGOR E. SHPARLINSKI (Sydney)

*Dedicated to our colleagues and friends Kálmán Győry, Attila Pethő,
János Pintz, András Sárközy*

Abstract. We use the large sieve inequality to show that if $a_1, \ldots, a_n$ are odd and coprime positive integers, then for a positive proportion of integral vectors $(m_1, \ldots, m_n)$ the values of the $m_1^{a_1} \ldots m_n^{a_n} - 1$ are rather smooth.

1. Introduction

Let $\mathbf{a} = (a_1, \ldots, a_n)$ be a fixed vector with positive integer components. We consider the polynomial in n variables X_i $(1 \leq i \leq n)$

$$F_{\mathbf{a}}(\mathbf{X}) = X_1^{a_1} \ldots X_n^{a_n} - 1.$$

of degree

$$d = a_1 + \cdots + a_n.$$

For $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n$, we define

$$F_{\mathbf{a}}(\mathbf{m}) = m_1^{a_1} \ldots m_n^{a_n} - 1.$$

Given real positive x and y consider the set

$$\mathcal{S}_{\mathbf{a}}(x, y) = \{\mathbf{m} \in \mathbb{Z}^n : 2 \leq \|\mathbf{m}\| \leq x,\ P(F_{\mathbf{a}}(\mathbf{m})) \leq y\}$$

Mathematics Subject Classification: Primary: 11N25; Secondary: 11L40, 11N36.

where

$$\|\mathbf{m}\| = \max_{1\le i\le n} |m_i|$$

and, as usual, $P(k)$ denotes the largest prime divisor of an integer $k \neq 0$.

Throughout the paper we always assume that $n \geq 2$ as in the case of $n = 1$ one gets stronger estimates from more general results about smooth values of polynomials, see [3], [7] and references therein. We also notice that smooth values of binary forms have been studied in [1].

As an application of a quite general result on smooth values of multivariate polynomials, it has been deduced in [4, Corollary 1] that if $d \geq 4$ and if $\gcd(a_1, \dots, a_n) = 1$, then for any fixed $\varepsilon > 0$ there exists two constants $c_{\mathbf{a}}(\varepsilon) > 0$ and $x_{\mathbf{a}}(\varepsilon)$ depending only on $\mathbf{a}$ and ε such that for

$$y = x^{d-2+2/(n+1)+\varepsilon}$$

we have

$$\sharp\, \mathcal{S}_{\mathbf{a}}(x, y) \geq c_{\mathbf{a}}(\varepsilon) x^n, \tag{1}$$

for every $x \geq x_{\mathbf{a}}(\varepsilon)$. The condition of coprimality of the a_i seems necessary for the method, since if $\delta = \gcd(a_1, \dots, a_n) > 1$, the polynomial $F_{\mathbf{a}}$ factorizes as

$$F_{\mathbf{a}}(\mathbf{X}) = \left(X_1^{\frac{a_1}{\delta}} \cdots X_n^{\frac{a_n}{\delta}}\right)^{\delta} - 1 = \left(X_1^{\frac{a_1}{\delta}} \cdots X_n^{\frac{a_n}{\delta}} - 1\right) Q(\mathbf{X}), \tag{2}$$

where Q is a polynomial, irreducible or not, of total degree $d(1-1/\delta)$. Hence the associated varieties are no more absolutely irreducible, which creates important difficulties for the involved methods of algebraic geometry.

The method of [4] is based on deep techniques on multidimensional exponential sums to study the number of solutions to the congruence

$$F_{\mathbf{a}}(\mathbf{m}) \equiv 0 \pmod p, \qquad \|\mathbf{m}\| \leq x, \tag{3}$$

for x that is reasonably small compared to the prime p.

Here we use a different approach to study (3) which, as in [8], [9], is based on multiplicative character sums. However instead of "individual" bounds of multiplicative character sums, such as Pólya–Vinogradov and Burgess bounds, see [6, Theorems 12.5 and 12.6], we use estimates on their average values given by the large sieve inequality, see [6, Theorem 7.13]. Such an approach already appears in the classical fact, sometimes called Motohashi's principle, that the convolution of two well-behaved sequences of integers satisfies an equidistribution theorem similar to the Bombieri–Vinogradov Theorem, see [2, Theorem 0 (b)], for instance. However, in the case when some of the integers $a_1, \dots, a_n$ are even we also need a bound of Heath-Brown [5, Theorem 1] on average values of sums of real characters. In particular, for $n \geq 4$ we obtain the bound (1) for much smaller values of y.

Theorem 1. *For any $n \geq 2$ and fixed $\varepsilon > 0$ there exist two constants $c_{\mathbf{a}}(\varepsilon) > 0$ and $x_{\mathbf{a}}(\varepsilon)$ depending only on $\mathbf{a}$ and ε such that for*

$$y = x^{d-n/2+\varepsilon}$$

the bound (1) *holds for $x \geq x_{\mathbf{a}}(\varepsilon)$.*

The fact that the proof of Theorem 1 is based on large sieve inequalities gives some flexibility to our method. For instance, the statement of Theorem 1 can be easily extended to the situation where for each $i = 1, \dots, n$, the values of the m_i are taken in a dense subset of integers $\mathcal{M}_i$ (for instance, the set of primes).

For a set of integers $\mathcal{M}$ and a real x, we denote by $\mathcal{M}(x)$ the set of elements of $\mathcal{M}$, which are up to x by absolute value, that is,

$$\mathcal{M}(x) = \mathcal{M} \cap [-x, x].$$

With these conventions, we enunciate, without proof

Theorem 2. *Let $n \geq 2$, let $\mathbf{a}$ as above and let $\mathcal{M}_i$ $(1 \leq i \leq n)$ be n subsets of non zero integers that satisfy*

$$\lim_{x\to\infty} \frac{\log\bigl(\sharp\, \mathcal{M}_i(x)\bigr)}{\log x} = 1.$$

Then, for every fixed $\varepsilon>0$, there exist constants $c_{\mathbf{a}}(\varepsilon, (\mathcal{M}_i))>0$ and $x_{\mathbf{a}}(\varepsilon, (\mathcal{M}_i))$, depending only on ε, $\mathbf{a}$ and the sets $\mathcal{M}_1, \dots \mathcal{M}_n$, such that for $x \geq x_{\mathbf{a}}(\varepsilon, (\mathcal{M}_i))$ one has the following lower bound

$$\sharp\,\{\mathbf{m} = (m_1, \dots, m_n) : m_i \in \mathcal{M}_i(x),\ P(F_{\mathbf{a}}(\mathbf{m})) \geq x^{d-n/2+\varepsilon}\} \geq c_{\mathbf{a}}(\varepsilon, (\mathcal{M}_i)) \prod_{i=1}^{n} \bigl(\sharp\, \mathcal{M}_i(x)\bigr).$$

Throughout the paper, the implied constants in symbols 'O' and '$\ll$' may depend on $\mathbf{a}$ (we recall that $U \ll V$ and $U = O(V)$ are both equivalent to the inequality $|U| \leq cV$ with some constant $c > 0$).

The letter p always denotes a prime number and k, m, n always denote positive integer numbers.

2. The case where the $a_1, \ldots, a_n$ are not coprime

As in § 1, let $\delta = \gcd(a_1, \ldots, a_n)$, and we suppose that $\delta \geq 2$.

By (2), we deduce the inequality

$$P(F_{\mathbf{a}}(\mathbf{m})) \ll \max\{\|\mathbf{m}\|^{d\delta^{-1}},\ \|\mathbf{m}\|^{d(1-\delta^{-1})}\} \ll \|\mathbf{m}\|^{d(1-\delta^{-1})},$$

for every $\mathbf{m}$, with $\inf m_i \geq 2$. If we suppose that $\|\mathbf{m}\| \leq x$, we see that, as $x \to \infty$, a positive proportion of these $\mathbf{m}$ is such that $P(F_{\mathbf{a}}(\mathbf{m})) \ll x^{d(1-\delta^{-1})}$. From the trivial equality $\delta n \leq d$, we deduce the inequality $d(1-\delta^{-1}) \leq d - n/2$. This gives the proof of Theorem 1 in the case where the a_i are not coprime.

The remaining case, corresponding to the situation where

$$\gcd(a_1, \ldots, a_n) = 1, \tag{4}$$

is more interesting.

3. Some analytic number theory tools

For a prime p we denote by $\mathcal{X}_p$ the set of all multiplicative characters χ modulo p and by $\mathcal{X}_p^*$ the set of all non principal characters modulo p, see [6, Section 3.2] for a background on multiplicative characters. In particular, we have the following orthogonality relations

$$\frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \chi(r) = \begin{cases} 1 & \text{if } r \equiv 1 \pmod p, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Our principal tool is the following special case of the large sieve inequality, see [6, Theorem 7.13].

Lemma 3. *For any real $Q \geq 2$ and sequence of $L \geq 1$ complex numbers $\alpha_1, \ldots, \alpha_L$, we have*

$$\sum_{p \leq Q} \sum_{\chi \in \mathcal{X}_p^*} \left| \sum_{\ell=1}^{L} \alpha_\ell \chi(\ell) \right|^2 \leq (Q^2 + L)A,$$

where

$$A = \sum_{\ell=1}^{L} |\alpha_\ell|^2.$$

We also recall the result of Heath-Brown [5, Corollary 3], about sums of Legendre symbols (ℓ/p) modulo a prime $p \geq 3$.

Lemma 4. *For any real numbers $\varepsilon > 0$, $Q \ge 2$ and for any sequence of $L \ge 1$ complex numbers $\alpha_1, \dots, \alpha_L$, we have*

$$\sum_{p \le Q} \left| \sum_{\ell=1}^{L} \alpha_\ell \left(\frac{\ell}{p} \right) \right|^2 \ll_\varepsilon (QL)^\varepsilon (Q+L) L A_0^2,$$

where

$$A_0 = \max_{1 \le \ell \le L} |\alpha_\ell|.$$

Note that in fact the result of [5, Corollary 3] is more general and the external summation can be extended to all odd square-free integers $s \le L$.

Finally, we recall the following simple form of the Mertens theorem for arithmetic progressions, which follows instantly from the prime number theorem for arithmetic progressions, see [6, Corollary 5.29], via partial summation. As usual, φ is the Euler function.

Lemma 5. *For any fixed integers $q > c \ge 1$ with $\gcd(q, c) = 1$, and real $z > w > 1$, we have*

$$\sum_{\substack{w \le p \le z \\ p \equiv c \pmod q}} \frac{1}{p} = \frac{1}{\varphi(q)} \log \frac{\log z}{\log w} + o(1),$$

as $w \to \infty$.

4. Average number of solutions of monomial congruences

Instead of (3) it is technically easier to work only with positive solutions, so we consider the congruence

$$F_{\mathbf{a}}(\mathbf{m}) \equiv 0 \pmod p \qquad 2 \le m_1, \dots, m_n \le x, \tag{6}$$

We denote by $T_p(x)$ the number of solutions to (6).

Now for a vector $\mathbf{a} = (a_1, \dots, a_n)$ and real $z > w \ge 3$, we denote by $\mathcal{P}_{\mathbf{a}}(w, z)$, the set of primes $p \in [w, z]$ with

$$\gcd \left(\frac{p-1}{2}, a_1 \dots a_n \right) = 1.$$

Also for a real $u \ge 1$, we denote by $\mathcal{P}_{\mathbf{a}}(u) = \mathcal{P}_{\mathbf{a}}(u, 2u)$.

Lemma 6. *Assume that the positive integers $a_1, \dots, a_n$ satisfy* (4). *Then as $x \to \infty$, we have*

$$\sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \left| T_p(x) - \frac{x^n}{p} \right| \le \left(u x^{n/2} + x^{n-1/2} \right) u^{o(1)},$$

uniformly for $u \ge x$.

Proof. Using (5) to detect solutions we express the number $T_p(x)$ of solutions to (6) as

$$T_p(x) = \sum_{2 \le m_1, \dots, m_n \le x} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \chi\left(m_1^{a_1} \dots m_n^{a_n}\right).$$

Changing the order of summation and then separating the contribution $(\lfloor x \rfloor - 1)^n/(p-1)$ of the principal character, we obtain the inequality

$$\left| T_p(x) - \frac{(\lfloor x \rfloor - 1)^n}{p-1} \right| \le \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p^*} \prod_{j=1}^{n} |S(\chi^{a_j}, x)|,$$

where

$$S(\chi^{a_j}, x) = \sum_{2 \le m \le x} \chi(m^{a_j}) = \sum_{2 \le m \le x} \chi^{a_j}(m).$$

Let

$$W = \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \left| T_p(x) - \frac{(\lfloor x \rfloor - 1)^n}{p-1} \right|, \tag{7}$$

we have

$$W \ll u^{-1} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\chi \in \mathcal{X}_p^*} \prod_{j=1}^{n} |S(\chi^{a_j}, x)|.$$

We now separate from the sum on the right hand side of the above inequality the contribution of Legendre symbols $(\cdot/p)$, getting

$$W \ll \sigma_1 + \sigma_2 \tag{8}$$

where

$$\sigma_1 = u^{-1} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \chi \ne (\cdot/p)}} \prod_{j=1}^{n} |S(\chi^{a_j}, x)|,$$

and

$$\sigma_2 = u^{-1} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \prod_{j=1}^{n} |S((\cdot/p)^{a_j}, x)|.$$

To estimate σ_1, we use the Hölder inequality, to derive

$$\sigma_1^n \le u^{-n} \prod_{j=1}^{n} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \chi \ne (\cdot/p)}} |S(\chi^{a_j}, x)|^n.$$

The coprimality condition $\gcd((p-1)/2, a_j) = 1$ implies that when χ runs through all other characters of $\mathcal{X}_p^*$ with $\chi \ne (\cdot/p)$ then the character χ^{a_j} is never principal and takes the same value at most two times, $j = 1, \ldots, n$. From these considerations, we deduce the inequality

$$\sum_{\substack{\chi \in \mathcal{X}_p^* \\ \chi \ne (\cdot/p)}} |S(\chi^{a_j}, x)|^n \le 2 \sum_{\chi \in \mathcal{X}_p^*} |S(\chi, x)|^n$$

and we obtain

$$\sigma_1^n \ll u^{-n} \left(\sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\chi \in \mathcal{X}_p^*} |S(\chi, x)|^n \right)^n,$$

which reduces to

$$\sigma_1 \ll u^{-1} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\chi \in \mathcal{X}_p^*} |S(\chi, x)|^n.$$

To apply the large sieve inequality, we want to deal with squares of trigonometric sums. We write $n = 1 + (n-1)$ and apply the Cauchy–Schwarz inequality to derive

$$\sigma_1^2 \ll u^{-2} \left(\sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\chi \in \mathcal{X}_p^*} |S(\chi, x)|^2 \right) \cdot \left(\sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \sum_{\chi \in \mathcal{X}_p^*} |S(\chi, x)|^{2n-2} \right).$$

We apply the large sieve inequality to each of the sums in the above expression. For the second one we put $L = \lfloor x^{n-1} \rfloor$ and write

$$S(\chi, x)^{n-1} = \sum_{\ell=1}^{L} \alpha_\ell \chi(\ell),$$

where α_ℓ is the number of representations of ℓ in the form $\ell = m_1 \ldots m_{n-1}$ with $2 \le m_1, \ldots, m_{n-1} \le x$. By the well known bound on the divisor function, see [6, Bound 1.81], we have $\alpha_\ell = x^{o(1)}$. Thus applying twice Lemma 3 we obtain

$$\sigma_1^2 \le u^{-2} \big((u^2 + x)x \big) \cdot \big((u^2 + x^{n-1})x^{n-1} \big) x^{o(1)},$$

which finally gives

$$\sigma_1 \ll \left(ux^{n/2} + x^{n-1/2}\right)x^{o(1)}. \tag{9}$$

since we supposed $u \geq x$.

Now, for the study of σ_2 we note that (4) implies that at least one of the exponents $a_1, \ldots, a_n$, say, a_1 is odd. Then we trivially have the inequality

$$\sigma_2 \leq u^{-1}x^{n-1} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} \prod_{j=1}^{n} |S((\cdot/p)^{a_1}, x)| = u^{-1}x^{n-1} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} |S((\cdot/p), x)|.$$

Using the Cauchy–Schwarz inequality and Lemma 4, we derive

$$\begin{aligned} \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} |S((\cdot/p), x)| &\leq \left(u \sum_{p \in \mathcal{P}_{\mathbf{a}}(u)} |S((\cdot/p), x)|^2\right)^{1/2} \\ &\leq (u+x)^{1/2}u^{1/2+o(1)}x^{1/2+o(1)}. \end{aligned}$$

Therefore, recalling that $u > x$, we obtain

$$\sigma_2 \leq u^{o(1)}x^{n-1/2}. \tag{10}$$

Substituting (9) and (10) in (8), we derive

$$W \leq \left(ux^{n/2} + x^{n-1/2}\right)u^{o(1)}. \tag{11}$$

We now remark that, for $p \in \mathcal{P}_{\mathbf{a}}(u)$ and $u \geq x$, we have the equality

$$\frac{(\lfloor x \rfloor - 1)^n}{p-1} = \frac{x^n}{p} + O(x^{n-1}p^{-1} + x^n p^{-2}) = \frac{x^n}{p} + O(x^{n-1}u^{-1}).$$

Combining with (7) and (11), we complete the proof of Lemma 6 . $\square$

Via dyadic dissection we immediately derive:

Corollary 7. *Assume that the integers $a_1 \ldots, a_n$ satisfy (4). Then for any real $z > w \geq x > 1$ we have*

$$\sum_{p \in \mathcal{P}_{\mathbf{a}}(w,z)} \left| T_p(x) - \frac{x^n}{p} \right| \leq \left(zx^{n/2} + x^{n-1/2}\right)z^{o(1)}.$$

5. Proof of Theorem 1

Following the idea of [4] we consider the sum

$$\Sigma_{\mathbf{a}}(x;w,z) = \sum_{p\in\mathcal{P}(w,z)} \sum_{\substack{2\le m_1,\ldots,m_n\le x\\ p\mid F_{\mathbf{a}}(m_1,\ldots,m_n)}} 1 = \sum_{p\in\mathcal{P}(w,z)} T_p(x).$$

Applying Corollary 7, we see that

$$\Sigma_{\mathbf{a}}(x;w,z) = x^n \sum_{p\in\mathcal{P}(w,z)} \frac{1}{p} + O\big((zx^{n/2}+x^{n-1/2})z^{o(1)}\big). \tag{12}$$

Clearly, the set $\mathcal{P}(w,z)$ contains all primes $p\in[w,z]$ in the arithmetic progression

$$p \equiv -1 \pmod{2a_1\ldots a_n}$$

since we have

$$\frac{p-1}{2} \equiv -1 \pmod{a_1\ldots a_n}$$

for such primes. We now fix some sufficiently small $\varepsilon>0$ and choose

$$w = x^{n/2-\varepsilon} \qquad \text{and} \qquad z = x^{n/2-\varepsilon/2}.$$

Since we always have $\varphi(n)\le n$, Lemma 5 implies the lower bound

$$\sum_{p\in\mathcal{P}(w,z)} \frac{1}{p} \ge \frac{1}{2a_1\ldots a_n}\log\frac{n/2-\varepsilon/2}{n/2-\varepsilon} + o(1),$$

and with the above choice of w and z, we deduce from (12) the following

$$\Sigma_{\mathbf{a}}(x;w,z) \gg x^n. \tag{13}$$

Now, let $\mathcal{M}$ be the set of vectors $\mathbf{m}\in\mathbb{Z}^n$ with $2\le\|\mathbf{m}\|\le x$ and such that $p\mid F_{\mathbf{a}}(\mathbf{m})$ for some $p\in\mathcal{P}_{\mathbf{a}}(w,z)$. For every such vector $\mathbf{m}$ we have $F_{\mathbf{a}}(\mathbf{m})\ne 0$. Thus we have the following trivial estimate

$$\sum_{\substack{p\ge w\\ p\mid F_{\mathbf{a}}(\mathbf{m})}} 1 \ll \frac{\log|F_{\mathbf{a}}(\mathbf{m})|}{\log w} \ll \frac{\log x}{\log w} \ll 1,$$

which implies

$$\Sigma_{\mathbf{a}}(x;w,z) \ll \sharp\mathcal{M}. \tag{14}$$

Comparing (13) and (14), we see that $\sharp\mathcal{M}\gg x^n$.

It remains to notice that for every $\mathbf{m}\in\mathcal{M}$ we have $F_{\mathbf{a}}(\mathbf{m}) = pM$ with $p\in[w,z]$. Thus

$$P(F_{\mathbf{a}}(\mathbf{m})) \ll \max\{z, x^d/w\}$$

which concludes the proof of Theorem 1.

References

[1] A. Balog, V. Blomer, C. Dartyge and G. Tenenbaum, Friable values of binary forms, *Comm. Math. Helv.* (*to appear*).

[2] E. Bombieri, J. Friedlander and H. Iwaniec, Primes in arithmetic progressions, *Acta Math.* **156** (1986), 203–251.

[3] C. Dartyge, G. Martin and G. Tenenbaum, Polynomial values free of large prime factors, *Periodica Math. Hungar.* **43** (2001), 111–119.

[4] E. Fouvry, Friabilité des valeurs d'un polynôme, *Archiv der Math.* **95** (2010), 411–421.

[5] D. R. Heath-Brown, A mean value estimate for real character sums, *Acta Arith.* **72** (1995), 235–275.

[6] H. Iwaniec and E. Kowalski, Analytic number theory, American Mathematical Society Colloquium Publications, 53., *American Mathematical Society, Providence, RI*, 2004.

[7] G. Martin, An asymptotic formula for the number of smooth values of a polynomial, *J. Number Theory* **93** (2002), 108–182.

[8] I. E. Shparlinski, On the distribution of points on multidimensional modular hyperbolas, *Proc. Japan Acad. Sci., Ser.A* **83** (2007), 5–9.

[9] I. E. Shparlinski, On a generalisation of a Lehmer problem, *Math. Zeitschrift* **263** (2009), 619–631.

ÉTIENNE FOUVRY
UNIVIRSITY PARIS-SUD 11
LABORATOIRE DE MATHÉMATIQUES
UMR 8628 CNRS
ORSAY F-91405 ORSAY CEDEX
FRANCE

E-mail: etienne.fouvry@math.u-psud.fr

IGOR E. SHPARLINSKI
DEPARTMENT OF COMPUTING
MACQUARIE UNIVERSITY
SYDNEY, NSW 2109
AUSTRALIA

E-mail: igor.shparlinski@mq.edu.au

(Received January 10, 2011; revised May 9, 2011)