Open Journal of Discrete Mathematics, 2019, 9, 11-16
http://www.scirp.org/journal/ojdm
ISSN Online: 2161-7643
ISSN Print: 2161-7635

On the Modular Erdös-Burgess Constant

Jun Hao[1], Haoli Wang[2*], Lizhen Zhang[1]

[1]Department of Mathematics, Tianjin Polytechnic University, Tianjin, China
[2]College of Computer and Information Engineering, Tianjin Normal University, Tianjin, China
Email: *bjpeuwanghaoli@163.com

How to cite this paper: Hao, J., Wang, H.L. and Zhang, L.Z. (2019) On the Modular Erdös-Burgess Constant. *Open Journal of Discrete Mathematics*, **9**, 11-16.
https://doi.org/10.4236/ojdm.2019.91003

Received: August 16, 2018
Accepted: December 26, 2018
Published: December 29, 2018

Abstract

Let n be a positive integer. For any integer a, we say that a is idempotent modulo n if $a^2 \equiv a \pmod{n}$. The n-modular Erdös-Burgess constant is the smallest positive integer ℓ such that any ℓ integers contain one or more integers, whose product is idempotent modulo n. We gave a sharp lower bound of the n-modular Erdös-Burgess constant, in particular, we determined the n-modular Erdös-Burgess constant in the case when n was a prime power or a product of pairwise distinct primes.

Keywords

Erdös-Burgess Constant, Davenport Constant, Modular Erdös-Burgess Constant

1. Introduction

Let $\mathcal{S}$ be a finite multiplicatively written commutative semigroup with identity $1_{\mathcal{S}}$. By a sequence over $\mathcal{S}$, we mean a finite unordered sequence of terms from $\mathcal{S}$ where repetition is allowed. For a sequence T over $\mathcal{S}$ we denote by $\pi(T) \in \mathcal{S}$ the product of its terms and we say that T is a product-one sequence if $\pi(T) = 1_{\mathcal{S}}$. If $\mathcal{S}$ is a finite abelian group, the Davenport constant $\mathrm{D}(\mathcal{S})$ of $\mathcal{S}$ is the smallest positive integer ℓ such that every sequence T over $\mathcal{S}$ of length $|T| \geq \ell$ has a nonempty product-one subsequence. The Davenport constant has mainly been studied for finite abelian groups but also in more general settings (we refer to [1] [2] [3] [4] [5] for work in the setting of abelian groups, to [6] [7] for work in case of non-abelian groups, and to [8] [9] [10] [11] [12] for work in commutative semigroups).

In the present paper we study the Erdös-Burgess constant $\mathrm{I}(\mathcal{S})$ of $\mathcal{S}$ which is defined as the smallest positive integer ℓ such that every sequence T over $\mathcal{S}$ of length $|T| \geq \ell$ has a non-empty subsequence T' whose product

$\pi(T')$ is an idempotent of $\mathcal{S}$. Clearly, if $\mathcal{S}$ happens to be a finite abelian group, then the unique idempotent of $\mathcal{S}$ is the identity $1_{\mathcal{S}}$, whence $\mathrm{I}(\mathcal{S}) = \mathrm{D}(\mathcal{S})$. The study of $\mathrm{I}(\mathcal{S})$ for general semigroups is initiated by a question of Erdös and has found renewed attention in recent years (e.g., [13] [14] [15] [16] [17]). For a commutative unitary ring *R*, let $\mathcal{S}_R$ be the multiplicative semigroup of the ring *R*, and $R^{\times}$ the group of units of *R*, noticing that the group $R^{\times}$ is a subsemigroup of the semigoup $\mathcal{S}_R$. We state our main result.

Theorem 1.1. *Let $n > 1$ be an integer, and let $R = \mathbb{Z}_n$ be the ring of integers modulon. Then*

$$\mathrm{I}(\mathcal{S}_R) \ge \mathrm{D}(R^{\times}) + \Omega(n) - \omega(n),$$

where $\Omega(n)$ is the number of primes occurring in the prime-power decomposition of n counted with multiplicity, and $\omega(n)$ is the number of distinct primes. Moreover, if n is a prime power or a product of pairwise distinct primes, then equality holds.

2. Notation

Let $\mathcal{S}$ be a finite multiplicatively written commutative semigroup with the binary operation *. An element a of $\mathcal{S}$ is said to be idempotent if $a * a = a$. Let $\mathrm{E}(\mathcal{S})$ be the set of idempotents of $\mathcal{S}$. We introduce sequences over semigroups and follow the notation and terminology of Grynkiewicz and others (cf. [4], Chapter 10] or [6] [18]). Sequences over $\mathcal{S}$ are considered as elements in the free abelian monoid $\mathcal{F}(\mathcal{S})$ with basis $\mathcal{S}$. In order to avoid confusion between the multiplication in $\mathcal{S}$ and multiplication in $\mathcal{F}(\mathcal{S})$, we denote multiplication in $\mathcal{F}(\mathcal{S})$ by the boldsymbol $\cdot$ and we use brackets for all exponentiation in $\mathcal{F}(\mathcal{S})$. In particular, a sequence $S \in \mathcal{F}(\mathcal{S})$ has the form

$$T = a_1 a_2 \cdot \cdots \cdot a_\ell = \underset{i\in[1,\ell]}{\bullet} a_i = \underset{a\in\mathcal{S}}{\bullet} a^{[\mathrm{v}_a(T)]} \in \mathcal{F}(\mathcal{S}) \tag{1}$$

where $a_1, \cdots, a_\ell \in \mathcal{S}$ are the terms of *T*, and $\mathrm{v}_a(T)$ is the multiplicity of the term a in *T*. We call $|T| = \ell = \sum_{a\in\mathcal{S}} \mathrm{v}_a(T)$ the length of *T*. Moreover, if $T_1, T_2 \in \mathcal{F}(\mathcal{S})$ and $a_1, a_2 \in \mathcal{S}$, then $T_1 \cdot T_2 \in \mathcal{F}(\mathcal{S})$ has length $|T_1| + |T_2|, T_1 \cdot a_1 \in \mathcal{F}(\mathcal{S})$ has length $|T_1| + 1$, $a_1 \cdot a_2 \in \mathcal{F}(\mathcal{S})$ is a sequence of length 2. If $a \in \mathcal{S}$ and $k \in \mathbb{N}_0$, then $a^{[k]} = \underbrace{a \cdot \cdots \cdot a}_{k} \in \mathcal{F}(\mathcal{S})$. Any sequence $T_1 \in \mathcal{F}(\mathcal{S})$ is called a subsequence of T if $\mathrm{v}_a(T_1) \le \mathrm{v}_a(T)$ for every element $a \in \mathcal{S}$, denoted $T_1 \mid T$. In particular, if $T_1 \ne T$, we call T_1 a *proper* subsequence of *T*, and let $T \cdot T_1^{[-1]}$ denote the resulting sequence by removing the terms of T_1 from *T*.

Let *T* be a sequence as in (1). Then

- $\pi(T) = a_1 * \cdots * a_\ell$ is the product of all terms of *T*, and
- $\prod(T) = \left\{\prod_{j\in J} a_j : \varnothing \ne J \subset [1,\ell]\right\} \subset \mathcal{S}$ is the set of subsequence products of *T*.

We say that *T* is

- *a product-one sequence* if $\pi(T) = 1_{\mathcal{S}}$,
- *an idempotent-product sequence* if $\pi(T) \in \mathrm{E}(\mathcal{S})$,
- *product-one free* if $1_{\mathcal{S}} \notin \prod(T)$,
- *idempotent-product free* if $\mathrm{E}(\mathcal{S}) \cap \prod(T) = \varnothing$.

Let $n > 1$ be an integer. For any integer a, we denote $\overline{a}$ the congruence class of a modulo *n*. Any integer a is said to be *idempotent modulo n* if $aa \equiv a \pmod{n}$, *i.e.*, $\overline{aa} = \overline{a}$ in $\mathbb{Z}_n$. A sequence T of integers is said to be *idempotent-product free modulo n* provided that T contains no nonempty subsequence T' with $\pi(T')$ being idempotent modulo *n*. We remark that saying a sequence T of integers is idempotent-product free modulo n is equivalent to saying the sequence $\bullet_{a|T} \overline{a}$ is idempotent-product free in the multiplicative semigroup of the ring $\mathbb{Z}_n$.

3. Proof of Theorem 1.1

Lemma 3.1. *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *be a positive integer where* $r \geq 1$, $k_1, k_2, \cdots, k_r \geq 1$, *and* $p_1, p_2, \cdots, p_r$ *are distinct primes. For any integer* a, *the congruence* $a^2 \equiv a \pmod{n}$ *holds if and only if* $a \equiv 0 \pmod{p_i^{k_i}}$ *or* $a \equiv 1 \pmod{p_i^{k_i}}$ *for every* $i \in [1, r]$.

Proof. Noted that $a^2 \equiv a \pmod{n}$ if and only if $p_i^{k_i}$ divides $a(a-1)$ for all $i \in [1, r]$, since $\gcd(a, a-1) = 1$, it follows that $a^2 \equiv a \pmod{n}$ holds if and only if $p_i^{k_i}$ divides a or $a-1$, *i.e.*, $a \equiv 0 \pmod{p_i^{k_i}}$ or $a \equiv 1 \pmod{p_i^{k_i}}$ for every $i \in [1, r]$, completing the proof.

Proof of Theorem 1. 1. Say

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \tag{2}$$

where $p_1, p_2, \cdots, p_r$ are distinct primes and $k_i \geq 1$ for all $i \in [1, r]$. It is observed that

$$\Omega(n) = \sum_{i=1}^{r} k_i \tag{3}$$

and

$$\omega(n) = r. \tag{4}$$

taking a sequence V of integers of length $\mathrm{D}(R^\times) - 1$ such that

$$\bullet_{a|V} \overline{a} \in \mathcal{F}(R^\times) \tag{5}$$

and

$$\overline{1} \notin \prod\left(\bullet_{a|V} \overline{a}\right). \tag{6}$$

Now we show that the sequence $V \cdot \left(\bullet_{i \in [1,r]} p_i^{[k_i - 1]}\right)$ is idempotent-product free modulo *n*, supposing to the contrary that $V \cdot \left(\bullet_{i \in [1,r]} p_i^{[k_i - 1]}\right)$ contains a **nonempty** subsequence *W*, say $W = V' \cdot \left(\bullet_{i \in [1,r]} p_i^{[\beta_i]} \right)$, such that $\pi(W)$ is idempotent modulo *n*, where V' is a subsequence of *V* and

$$\beta_i \in [0, k_i - 1] \text{ for all } i \in [1, r].$$

It follows that

$$\pi(W) = \pi(V') p_1^{\beta_1} \cdots p_r^{\beta_r}. \tag{7}$$

If $\sum_{i=1}^{r} \beta_i = 0$, then $W = V'$ is a *nonempty* subsequence of *V*. By (5) and (6), there exists some $t \in [1, r]$ such that $\pi(W) \not\equiv 0 \left(\bmod p_t^{k_t} \right)$ and $\pi(W) \not\equiv 1 \left(\bmod p_t^{k_t} \right)$. By Lemma 3.1, $\pi(W)$ is not idempotent modulo *n*, a contradiction. Otherwise, $\beta_j > 0$ for some $j \in [1, r]$, say

$$\beta_1 \in [1, k_1 - 1]. \tag{8}$$

Since $\gcd(\pi(V'), p_1) = 1$, it follows from (7) that $\gcd\left(\pi(W), p_1^{k_1}\right) = p_1^{\beta_1}$. Combined with (8), we have that $\pi(W) \not\equiv 0 \left(\bmod p_1^{k_1} \right)$ and $\pi(W) \not\equiv 1 \left(\bmod p_1^{k_1} \right)$. By Lemma 3.1, we conclude that $\pi(W)$ is not idempotent modulo *n*, a contradiction. This proves that the sequence $V \cdot \left(\bullet_{i \in [1,r]} p_i^{[k_i - 1]} \right)$ is idempotent-product free modulo *n*. Combined with (3) and (4), we have that

$$\mathrm{I}(\mathcal{S}_R) \geq \left| V \cdot \left(\bullet_{i \in [1,r]} p_i^{[k_i - 1]} \right) \right| + 1 = (|V| + 1) + \sum_{i=1}^{r} (k_i - 1) = \mathrm{D}(R^\times) + \Omega(n) - \omega(n). \tag{9}$$

Now we assume that *n* is a prime power or a product of pairwise distinct primes, *i.e.*, either $r = 1$ or $k_1 = \cdots = k_r = 1$ in (2). It remains to show the equality $\mathrm{I}(\mathcal{S}_R) = \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$ holds. We distinguish two cases.

Case 1. $r = 1$ in (2), *i.e.*, $n = p_1^{k_1}$.

Taking an arbitrary sequence *T* of integers of length $|T| = \mathrm{D}(R^\times) + k_1 - 1 = \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$, let $T_1 = \bullet_{\substack{a | T \\ a \equiv 0 (\bmod p_1)}} a$ and $T_2 = T \cdot T_1^{[-1]}$. By the Pigeonhole Principle, we see that either $|T_1| \geq k_1$ or $|T_2| \geq \mathrm{D}(R^\times)$. It follows either $\pi(T_1) \equiv 0 \left(\bmod p_1^{k_1} \right)$, or $\overline{1} \in \prod \left(\bullet_{a | T_2} \overline{a} \right)$. By Lemma 3.1, the sequence *T* is not idempotent-product free modulo *n*, which implies that $\mathrm{I}(\mathcal{S}_R) \leq \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$. Combined with (9), we have that $\mathrm{I}(\mathcal{S}_R) = \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$.

Case 2. $k_1 = \cdots = k_r = 1$ in (2), *i.e.*, $n = p_1 p_2 \cdots p_r$.

Then

$$\Omega(n) = \omega(n) = r. \tag{10}$$

Taking an arbitrary sequence T of integers of length $|T| = \mathrm{D}(R^\times)$, by the Chinese Remainder Theorem, for any term a of *T* we can take an integer a' such that for each $i \in [1, r]$,

$$a' \equiv \begin{cases} 1 \pmod{p_i} & \text{if } a \equiv 0 \pmod{p_i}; \\ a \pmod{p_i} & \text{otherwise.} \end{cases} \tag{11}$$

Note that $\gcd(a', n) = 1$ and thus $\bullet_{a|T} \overline{a}' \in \mathcal{F}(R^\times)$. Since $\left|\bullet_{a|T} \overline{a}'\right| = |T| = \mathrm{D}(R^\times)$, it follows that $\overline{1} \in \prod\left(\bullet_{a|T} \overline{a}'\right)$, and so there exists a **nonempty** subsequence W of T such that $\prod_{a|W} a' \equiv 1 \pmod{p_i}$ for each $i \in [1, r]$. Combined with (11), we derive that $\pi(W) \equiv 0 \pmod{p_i}$ or $\pi(W) \equiv 1 \pmod{p_i}$, where $i \in [1, r]$. By Lemma 3.1, we conclude that $\pi(W)$ is idempotent modulo *n*. Combined with (10), we have that $\mathrm{I}(\mathcal{S}_R) \le \mathrm{D}(R^\times) = \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$. It follows from (9) that $\mathrm{I}(\mathcal{S}_R) = \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$, completing the proof.

We close this paper with the following conjecture.

Conjecture 3.2. *Let* $n > 1$ *be an integer, and let* $R = \mathbb{Z}_n$ *be the ring of integers modulo n. Then* $\mathrm{I}(\mathcal{S}_R) = \mathrm{D}(R^\times) + \Omega(n) - \omega(n)$.

Acknowledgements

This work is supported by NSFC (Grant No. 61303023, 11301381, 11501561).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Gao, W. and Geroldinger, A. (2006) Zero-Sum Problems in Finite Abelian Groups: A Survey. *Expositiones Mathematicae*, **24**, 337-369. https://doi.org/10.1016/j.exmath.2006.07.002

[2] Geroldinger, A. and Halter-Koch, F. (2006) Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory. Pure Appl. Math., Vol. 278, Chapman & Hall/CRC.

[3] Geroldinger, A. and Ruzsa, I. (2009) Combinatorial Number Theory and Additive Group Theory. In *Advanced Courses in Mathematics CRM Barcelona*, Springer, Birkhäuser. https://doi.org/10.1007/978-3-7643-8962-8

[4] Grynkiewicz, D.J. (2013) Structural Additive Theory, Developments in Mathematics. Vol. 30, Springer, Cham. https://doi.org/10.1007/978-3-319-00416-7

[5] Tao, T. and Van Vu, H. (2006) Additive Combinatorics. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511755149

[6] Cziszter, K., Domokos, M. and Geroldinger, A. (2016) The Interplay of Invariant Theory with Multiplicative Ideal Theory and with Arithmetic Combinatorics, Multiplicative Ideal Theory and Factorization Theory. Springer, Berlin, 43-95.

[7] Gao, W., Li, Y. and Peng, J. (2014) An Upper Bound for the Davenport Constant of Finite Groups. *Journal of Pure and Applied Algebra*, **218**, 1838-1844. https://doi.org/10.1016/j.jpaa.2014.02.009

[8] Wang, G. (2015) Davenport Constant for Semigroups II. *Journal of Number Theory*, **153**, 124-134. https://doi.org/10.1016/j.jnt.2015.01.007

[9] Wang, G. (2017) Additively Irreducible Sequences in Commutative Semigroups. *Journal of Combinatorial Theory*, *Series A*, **152**, 380-397. https://doi.org/10.1016/j.jcta.2017.07.001

[10] Wang, G. and Gao, W. (2008) Davenport Constant for Semigroups. *Semigroup Forum*, **76**, 234-238. https://doi.org/10.1007/s00233-007-9019-3

[11] Wang, G. and Gao, W. (2016) Davenport Constant of the Multiplicative Semigroup of the Ring $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$. arXiv:1603.06030

[12] Zhang, L., Wang, H. and Qu, Y. (2017) A Problem of Wang on Davenport Constant for the Multiplicative Semigroup of the Quotient Ring of $\mathbb{F}_2[x]$. *Colloquium Mathematicum*, **148**, 123-130. https://doi.org/10.4064/cm6707-6-2016

[13] Burgess, D.A. (1969) A Problem on Semi-Groups. *Studia Sci. Math. Hungar.*, **4**, 9-11.

[14] Gillam, D.W.H., Hall, T.E. and Williams, N.H. (1972) On Finite Semigroups and Idempotents. *Bulletin of the London Mathematical Society*, **4**, 143-144. https://doi.org/10.1112/blms/4.2.143

[15] Wang, G. (2019) Structure of the Largest Idempotent-Product Free Sequences in Semigroups. *Journal of Number Theory*, **195**, 84-95. https://doi.org/10.1016/j.jnt.2018.05.020

[16] Wang, G. (2018) Erdös-Burgess Constant of the Direct Product of Cyclic Semigroups. arXiv:1802.08791.

[17] Wang, H., Hao, J. and Zhang, L. (2018) On the Erdös-Burgess Constant of the Multiplicative Semigroup of a Factor Ring of $\mathbb{F}_q[x]$. *International Journal of Number Theory*. (To Appear)

[18] Grynkiewicz, D.J. (2013) The Large Davenport Constant II: General Upper Bounds. *Journal of Pure and Applied Algebra*, **217**, 2221-2246. https://doi.org/10.1016/j.jpaa.2013.03.002