International Electronic Journal of Algebra
Volume 30 (2021) 16-65
DOI: 10.24330/ieja.969577

THE LOEWY STRUCTURE OF CERTAIN FIXPOINT ALGEBRAS, PART II

T. Breuer, L. Héthelyi, E. Horváth and B. Külshammer

Received: 8 October 2019; Revised: 12 September 2020; Accepted: 20 December 2020
Communicated by A. Çiğdem Özcan

Abstract. In Part I of this paper, we introduced a class of certain algebras of finite dimension over a field. All these algebras are split, symmetric and local. Here we continue to investigate their Loewy structure. We show that in many cases their Loewy length is equal to an upper bound established in Part I, but we also construct examples where we have a strict inequality. The algebras considered here include certain rings of fixpoints under the action of particular finite groups. Thus we consider the results in this paper as a contribution to the general theory of fixpoint rings.

Mathematics Subject Classification (2020): 20C05, 11B13, 16P10
Keywords: Fixpoint algebra, symmetric algebra, Jacobson radical, Loewy length

1. Introduction

In Part I of this paper, we introduced a class of finite-dimensional algebras $A(q, n, e)$ over a field F, depending on parameters $q, n, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^n - 1$. All these algebras are split, local and symmetric. Moreover, they are all commutative and have a multiplicative basis in the sense that the product of any two basis elements is either a basis element or zero. Their dimension is $z + 1$ where $z := \frac{q^n-1}{e}$. When q is a prime p and F is algebraically closed of characteristic p then $A(q, n, e)$ is isomorphic to a fixpoint algebra $(FP)^H$ where FP is the group algebra of an elementary abelian p-group P of order p^n over F and H is a cyclic group of order e acting freely on $P \setminus \{1\}$.

The work on this paper was begun while the last author was visiting the Technical University of Budapest in October 2017. Part of the work was also done while the last author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2018 semester, supported by the National Science Foundation under Grant No. DMS-1440140. The first author gratefully acknowledges support by the German Research Foundation (DFG) – Project-ID 286237555 – within the SFB-TRR 195 *Symbolic Tools in Mathematics and their Applications*. The research in this paper was also supported by the NKFI-Grants No. 115288 and 115799.

In Part I, we presented an inductive procedure in order to compute the Loewy structure of $A(q,n,e)$, and we proved the following upper bound for the Loewy length of $A(q,n,e)$:

$$\mathrm{LL}(A(q,n,e)) \leq \left\lfloor n\frac{q-1}{m} \right\rfloor + 1; \tag{1}$$

here $m = m(q,e)$ is defined as the smallest positive integer t such that there exists a sum of t powers of q which is divisible by e. This number can be defined for arbitrary $q, e \in \mathbb{N}$ with $\gcd(q,e) = 1$.

In [3, Corollary 5.1] we proved that $A(q,n,e)$ is uniserial if and only if e is divisible by $\frac{q^n-1}{q-1}$. For an arbitrary finite-dimensional algebra A, the Loewy length $\mathrm{LL}(A)$ measures how far A is away from being semisimple.

The main purpose of this paper is to show that, in many cases, the inequality in (1) is in fact an equality. For example, we will show that

$$\mathrm{LL}(A(q,n,e)) = \left\lfloor n\frac{q-1}{m} \right\rfloor + 1 \tag{2}$$

whenever one of the following conditions is satisfied:

- $n \leq 3$, see [3, Corollary 7.1]. (There are examples for $n = 5$ where (2) does not hold, see Remark 7.13; the case $n = 4$ is still open. For $n = 4$ and $q \leq 100$, the equality (2) holds.)
- $e \leq 32$, see Proposition 6.1. (There are examples for $e = 33$ where (2) does not hold, see Proposition 6.2.)
- $e \mid \frac{q^d-1}{q-1}$ for $d \in \{1, \ldots, 5\}$, see Propositions 5.3 and 5.6. (There are examples for larger d where (2) does not hold, see Remark 7.13.)
- $e \mid \Phi_d(q)$ where d is a power of 2 or $d \in \{3, 5, 6, 9, 10\}$, see Remark 5.4. (Here $\Phi_d(X)$ denotes the d-th cyclotomic polynomial.)
- e is a power of a Pierpont prime, see Theorem 4.3. (A prime number p is called a Pierpont prime if it has the form $p = 1 + 2^a 3^b$ where $a, b \in \mathbb{N}_0$.)
- e is a divisor of $q^n - 1$ and a multiple of $q^{\frac{n}{2}} - 1$, see Lemma 5.8.
- $m(q,e) \mid q - 1$, see [3, Theorem 7.1].
- $m(q,e) = 2$, see [3, Lemma 6.3].
- $m(q,e) \geq \frac{e}{3}$, see Proposition 6.4.
- $z < 70$. (There is an example for $z = 70$ where (2) does not hold, see Example 7.11.)

More conditions and details can be found in the body of this paper.

We also define a certain equivalence relation on our set of algebras. Two equivalent algebras are isomorphic, and the upper bounds for their Loewy length in (1) are the same. One of us (T. B.) has computed a database with 768 511 equivalence classes of algebras, see [2]. These contain all algebras $A(q,n,e)$ with $z \leq 10\,000$. These algebras fall into at least 481 069 and at most 481 744 isomorphism classes, see Remark 7.13.

It turns out that the equality (2) holds for 757 790 of these equivalence classes. In only one of the equivalence classes the difference between both sides in (1) is bigger than 1 (namely 2). Thus, at least for algebras of dimension up to 10 000, the bound for the Loewy length in (1) appears to be reasonable. Many of the more general results below were inspired by the computations leading to our database.

In this paper, we will denote by $\mathrm{J}(A)$ the Jacobson radical and by $\mathrm{LL}(A)$ the Loewy length of a finite-dimensional algebra A. If $\mathrm{LL}(A) = l$ and $\dim \mathrm{J}(A)^{i-1}/\mathrm{J}(A)^i = d_i$ for $i = 1, \dots, l$ then $(d_1, \dots, d_l)$ is called the Loewy vector of A.

For $q, n, e \in \mathbb{N}$ with $q > 1$ and $e \mid q^n - 1$, the F-algebra $A(q,n,e)$ is constructed as follows. Consider the ideal $I := (X_1^q, \dots, X_n^q)$ of the polynomial algebra $F[X_1, \dots, X_n]$, and set $x_j := X_j + I$ for $j = 1, \dots, n$. Then $A(q,n,e)$ is the subalgebra of $F[X_1, \dots, X_n]/I = F[x_1, \dots, x_n]$ generated by all monomials $x_1^{i_1} \dots x_n^{i_n}$ such that $i_1 + qi_2 + \dots + q^{n-1}i_n \equiv 0 \pmod{e}$; note that $x_j^q = 0$ for $j = 1, \dots, n$. We showed in Part I that the elements $b_0, b_1, \dots, b_z$ constitute an F-basis of $A(q,n,e)$ where $b_k = x_1^{i_1} \dots x_n^{i_n}$ and $ke = i_1 + qi_2 + \dots + q^{n-1}i_n$ is the q-adic expansion of ke, for $k = 0, \dots, z$.

Our paper is structured as follows. In Section 2, we deal with the function $m(q,e)$ and prove several properties. Tables with the values of this function can be found at the end of the paper. In Section 3 we present various methods in order to obtain lower bounds for the Loewy length of $A(q,n,e)$. In Section 4 we investigate the validity of (2) in the situation where e is a prime power, and in Section 5 we consider the case where e divides $\frac{q^n-1}{q-1}$. Section 6 contains our results for the case when e is a small number. Here we also present a series of examples where the inequality in (1) is strict. Then we deal with algebras where $m(q,e)$ is large (relative to e) or q is small. In the last part of the paper, we change our perspective and consider all the algebras $A(q,n,e)$ of a fixed dimension $d = z + 1$.

Rings of fixed points under a group action have always been of interest to group and ring theorists (see for example, the book by S. Montgomery [7]). Our results and examples indicate that it will perhaps not be so easy to describe the Loewy structure, in particular the Loewy length and the Loewy vector, of such fixpoint algebras.

2. Congruence properties of sums of powers

Let $q, e \in \mathbb{N}$ such that $\gcd(q, e) = 1$. In [3, Section 6], we defined $m(q, e)$ as the smallest positive integer t with the property that there exists a sum of t powers of q which is divisible by e. Then $1 \le m(q, e) \le e$; moreover, $m(q, e) = e$ if and only if $q \equiv 1 \pmod e$, and $m(q, e) = 1$ if and only if $e = 1$ (cf. [3, Example 6.1]).

For $q > 1$, there is a slightly different description of $m(q, e)$. Recall that we denote by $s_q(x) = x_0 + x_1 + \ldots + x_n$ the q-adic digit sum of a nonnegative integer x with q-adic expansion $x = x_0 + x_1 q + \ldots + x_n q^n$. In [3, Proposition 6.1] we proved that

$$m(q, e) = \min\{s_q(ke) : k \in \mathbb{N}\} = \min\{s_q(ke) : k = 1, \ldots, z\}$$

where $z := \frac{q^n-1}{e}$ for any $n \in \mathbb{N}$ such that $e \mid q^n - 1$; usually we take $n := \mathrm{ord}_e(q)$ where $\mathrm{ord}_e(q)$ denotes the order of $q + e\mathbb{Z}$ in $(\mathbb{Z}/e\mathbb{Z})^\times$, the order of q modulo e.

Our first result is related to [3, Proposition 5.1].

Proposition 2.1. *Let $q, n, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^n - 1$. Moreover, let $n', e' \in \mathbb{N}$ such that $n' \mid n$ and $e = e' \frac{q^n-1}{q^{n'}-1}$. Then $m(q, e) = \frac{n}{n'} m(q, e')$.*

Proof. We set $z := \frac{q^n-1}{e} = \frac{q^{n'}-1}{e'}$. Since $m(q, e) = \min\{s_q(ke) : k = 1, \ldots, z\}$ and $m(q, e') = \min\{s_q(ke') : k = 1, \ldots, z\}$ it suffices to show that $s_q(ke) = \frac{n}{n'} s_q(ke')$ for $k = 1, \ldots, z$. Let $k \in \{1, \ldots, z\}$, and consider the q-adic expansion $ke' = \sum_{t=1}^{n'} q^{t-1} i_t$. Then

$$\begin{aligned} ke &= ke' \tfrac{q^n-1}{q^{n'}-1} = (\textstyle\sum_{t=1}^{n'} q^{t-1} i_t)(1 + q^{n'} + q^{2n'} + \ldots + q^{n-n'}) \\ &= \textstyle\sum_{t=1}^{n'} q^{t-1} i_t + \sum_{t=1}^{n'} q^{n'+t-1} i_t + \ldots + \sum_{t=1}^{n'} q^{n-n'+t-1} i_t \end{aligned}$$

is the q-adic expansion of ke. Hence $s_q(ke) = \frac{n}{n'} \sum_{t=1}^{n'} i_t = \frac{n}{n'} s_q(ke')$. □

We record two special cases.

Corollary 2.2. *Let $q, n, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^n - 1$.*

(i) *If $e' \in \mathbb{N}$ such that $e = e' \frac{q^n-1}{q-1}$ then $m(q, e) = ne'$.*
(ii) *If $n' \in \mathbb{N}$ such that $n' \mid n$ and $e = \frac{q^n-1}{q^{n'}-1}$ then $m(q, e) = \frac{n}{n'}$.*

Proof. Apply Proposition 2.1 with $n' = 1$ or $e' = 1$, respectively. In part (i), we get $m(q, e) = nm(q, e')$, and since $\frac{q-1}{e'} = \frac{q^n-1}{e} \in \mathbb{N}$, [3, Example 6.1 (i)] implies that $m(q, e') = e'$. In part (ii), we get $m(q, e) = \frac{n}{n'} m(q, 1)$, and [3, Example 6.1 (ii)] implies that $m(q, 1) = 1$. □

Example 2.3. Table 1 gives some of the numbers $m(q, e)$. The columns in this table are labelled by e, and the rows by q. The computations were done using the computer algebra system GAP [5].

Example 2.4. Let $q, e \in \mathbb{N}$ such that $1 \not\equiv q \equiv -1 \pmod{e}$. Then $m(q,e) = 2$; in fact, $m(q,e) \leq 2$ since $e \mid 1+q$, and $m(q,e) \neq 1$ since $e \neq 1$.

Next we investigate the situation where $m(q,e)$ is large.

Proposition 2.5. *Let $q, e \in \mathbb{N}$ such that $1 < q < e$ and $\gcd(q,e) = 1$. Then $m := m(q,e) \geq \frac{e}{3}$ if and only if one of the following holds:*

(i) *$q \geq 3$, $\gcd(2,q) = 1$, $e = 2q-2$ (where $m = \frac{e}{2} = q-1$).*
(ii) *$q \geq 4$, $\gcd(3,q) = 1$, $e = 3q-3$ (where $m = \frac{e}{3} = q-1$).*
(iii) *$q \geq 5$, $\gcd(6,q) = 1$, $e = \frac{3q-3}{2}$ (where $m = \frac{e}{3} = \frac{q-1}{2}$).*
(iv) *the pair (q,e) appears in the following table:*

q	2	2	2	3	3	4	4	4	5
e	3	5	7	5	8	5	7	15	24
m	2	2	3	2	4	2	3	6	8

Proof. For the "if" direction, observe that the claimed values of m for given q and e are equal to both $e_1 = \gcd(e, q-1)$ and $s_q(e)$ in the cases (i)–(iii), so that we can apply [3, Lemma 6.2 (i)] and [3, Proposition 6.1]. In case (iv), the values for m are given in Table 1. In each case, we have $3m(q,e) \geq e$.

For the "only if" direction, suppose that $m \geq e/3$. A careful inspection of Table 1 shows that we may assume $e > 30$. Consider the q-adic expansion $e = i_1 + qi_2 + \ldots + q^l i_{l+1}$ where $i_{l+1} \neq 0$. Then $m \leq s_q(e) = i_1 + i_2 + \ldots + i_{l+1}$, so $0 \leq 3m - e \leq 2i_1 + (3-q)i_2 + \cdots + (3-q^l)i_{l+1}$.

If $l \geq 2$ then $0 \leq 3m - e \leq 2i_1 + (3-q)i_2 + (3-q^l)i_{l+1}$. Assume first that $q \geq 3$. Then

$$\begin{aligned} 0 &\leq 2i_1 + (3-q^l)i_{l+1} \leq 2(q-1) + (3-q^l) = 2q + 1 - q^l \\ &= 1 - q\left(q^{l-1} - 2\right) \leq 1 - 3(3-2) < 0, \end{aligned}$$

a contradiction. Thus we must have $q = 2$. Then $0 \leq 2i_1 + i_2 + (3 - 2^l) \leq 6 - 2^l$. This implies that $l = 2$, and we have the contradiction $e = i_1 + 2i_2 + 4i_3 \leq 7$.

From now on, assume $l = 1$. Then $0 \leq 3m - e \leq 2i_1 + (3-q)i_2$, i. e., $(q-3)i_2 \leq 2i_1 \leq 2(q-1)$. Since $30 < e = i_1 + qi_2 < q^2$ this implies that $q \geq 6$.

$i_2 \geq 3$: Then $3(q-3) \leq 2i_1 \leq 2(q-1)$, i. e., $q \leq 7$.

If $q = 6$ then $9 \leq 3i_2 \leq 2i_1 \leq 10$, i. e., $i_2 = 3$ and $i_1 = 5$. Thus we have the contradiction $e = 23$.

If $q = 7$ then $12 \leq 4i_2 \leq 2i_1 \leq 12$, i. e., $i_2 = 3$ and $i_1 = 6$. Hence we have the contradiction $e = 27$.

$i_2 = 2$: Then $q-3 \le i_1 \le q-1$.

If $i_1 = q-1$ then $e = 2q + (q-1) = 3q-1$. Since $(q-1)(3q-1) = 3q^2-4q+1 = 2q^2+q(q-4)+1$, this leads to the contradiction $m \le q-1 < \frac{e}{3}$.

If $i_1 = q-2$ then $e = 2q + (q-2) = 3q-2$. Since $(q-1)(3q-2) = 3q^2-5q+2 = 2q^2+q(q-5)+2$, this leads to the contradiction $m \le q-1 < \frac{e}{3}$.

If $i_1 = q-3$ then $e = 2q + (q-3) = 3q-3$ and $m \le q-1 = \frac{e}{3}$, i.e. $m = \frac{e}{3} = q-1$. Since $\gcd(q,e) = 1$, we must have $3 \nmid q$. Thus we are in case (ii).

$i_2 = 1$: Then $30 < e = q + i_1$ and $\frac{q-3}{2} \le i_1 < q$, so that $q \ge 16$.

If $i_1 = \frac{q-3}{2}$ then q is odd, $e = q + \frac{q-3}{2} = \frac{3q-3}{2}$ and $m \le \frac{q-1}{2} = \frac{e}{3}$, i.e. $m = \frac{e}{3} = \frac{q-1}{2}$. Since $\gcd(q,e) = 1$ we also have $3 \nmid q$, so that $\gcd(q,6) = 1$. Thus we are in case (iii).

If $i_1 = \frac{q-2}{2}$ then q is even and $e = \frac{3q-2}{2}$. Since $\gcd(q,e) = 1$ this implies $4 \mid q$. Then $e^2 = 2q^2 + \frac{q-12}{4}q + 1$. This leads to the contradiction $m \le 2 + \frac{q-12}{4} + 1 = \frac{q}{4} < \frac{e}{3}$.

If $i_1 = \frac{q-1}{2}$ then q is odd and $30 < e = \frac{3q-1}{2}$, i.e. $q > 20$. If $q \equiv 1 \pmod 4$ then $\frac{3q-3}{2}e = 2q^2 + \frac{q-13}{4}q + \frac{q+3}{4}$. This leads to the contradiction $m \le 2 + \frac{q-13}{4} + \frac{q+3}{4} = \frac{q-1}{2} < \frac{e}{3}$. If $q \equiv 3 \pmod 4$ then $\frac{3q-5}{2}e = 2q^2 + \frac{q-19}{4}q + \frac{q+5}{4}$. This leads to the contradiction $m \le 2 + \frac{q-19}{4} + \frac{q+5}{4} = \frac{q-3}{2} < \frac{e}{3}$.

If $i_1 = \frac{q}{2}$ then q is even and $e = \frac{3q}{2}$. Since $\gcd(q,e) = 1$ this implies $4 \nmid q$. Then $\frac{3q-2}{2}e = 2q^2 + \frac{q-6}{4}q$. This leads to the contradiction $m \le 2 + \frac{q-6}{4} = \frac{q+2}{4} < \frac{e}{3}$.

If $\frac{q+1}{2} \le i_1 \le q-5$ then set $x := q - i_1$ and write $q = ax + k$ where $a, k \in \mathbb{N}_0$ and $0 \le k < x$. Then $5 \le x \le \frac{q-1}{2}$ and $a \ge 2$. Moreover, we have $ae = 2aq - ax = k + (2a-1)q$. Thus $m \le s_q(ae) \le k + (2a-1)$. This implies:

$$3k + 6a - 3 \ge 3m \ge e = 2q - x = 2(ax+k) - x = 2k + (2a-1)x.$$

Hence $6a - 3 \ge (2a-1)x - k > (2a-2)x \ge 10a - 10$, and we have the contradiction $4a < 7$.

If $i_1 = q-4$ then $e = 2q-4$. Since $\gcd(q,e) = 1$ this implies that q is odd. If $q \equiv 0 \pmod 3$ then $\frac{2q}{3}e = q^2 + \frac{q-9}{3}q + \frac{q}{3}$. This leads to the contradiction $m \le 1 + \frac{q-9}{3} + \frac{q}{3} = \frac{2q-6}{3} < \frac{e}{3}$. If $q \equiv 1 \pmod 3$ then $\frac{2q+1}{3}e = q^2 + \frac{q-7}{3}q + \frac{q-4}{3}$. This leads to the contradiction $m \le 1 + \frac{q-7}{3} + \frac{q-4}{3} = \frac{2q-8}{3} < \frac{e}{3}$. If $q \equiv 2 \pmod 3$ then $\frac{2q+2}{3}e = q^2 + \frac{q-5}{3}q + \frac{q-8}{3}$. This leads to the contradiction $m \le 1 + \frac{q-5}{3} + \frac{q-8}{3} = \frac{2q-10}{3} < \frac{e}{3}$.

If $i_1 = q-3$ then $e = 2q-3$. Since $\gcd(q,e) = 1$ we conclude that $q \not\equiv 0 \pmod 3$. If $q \equiv 1 \pmod 3$ then $\frac{2q-2}{3}e = q^2 + \frac{q-10}{3}q + 2$. This leads to the contradiction $m \leq 1 + \frac{q-10}{3} + 2 = \frac{q-1}{3} < \frac{e}{3}$. If $q \equiv 2 \pmod 3$ then $\frac{2q-1}{3}e = q^2 + \frac{q-8}{3}q + 1$. This leads to the contradiction $m \leq 1 + \frac{q-8}{3} + 1 = \frac{q-2}{3} < \frac{e}{3}$.

If $i_1 = q-2$ then $e = 2q-2$ and $m \leq 1 + (q-2) = q-1$. Since $\gcd(q,e) = 1$ we conclude that q is odd. Thus $q-1 = \gcd(e, q-1) \mid m$, so that $m = q-1$. Thus we are in case (i).

If $i_1 = q-1$ then $e = 2q-1$. If $q \equiv 0 \pmod 3$ then $\frac{2q-3}{3}e = q^2 + (\frac{q}{3} - 3)q + (\frac{q}{3} + 1)$. This leads to the contradiction $m \leq 1 + (\frac{q}{3} - 3) + (\frac{q}{3} + 1) = \frac{2q-3}{3} < \frac{e}{3}$. If $q \equiv 1 \pmod 3$ then $\frac{2q-2}{3}e = q^2 + \frac{q-7}{3}q + \frac{q+2}{3}$. This leads to the contradiction $m \leq 1 + \frac{q-7}{3} + \frac{q+2}{3} = \frac{2q-2}{3} < \frac{e}{3}$. If $q \equiv 2 \pmod 3$ then $\frac{2q-4}{3}e = q^2 + \frac{q-11}{3}q + \frac{q+4}{3}$. This leads to the contradiction $m \leq 1 + \frac{q-11}{3} + \frac{q+4}{3} = \frac{2q-4}{3} < \frac{e}{3}$.

This finishes the proof. □

Next we drop the assumption $q < e$ from Proposition 2.5. If $q \equiv 1 \pmod e$ then $m(q,e) = e \geq \frac{e}{3}$ by [3, Example 6.1]. Thus we can and will ignore this case.

Proposition 2.6. *Let $q, e \in \mathbb{N}$ such that $\gcd(q,e) = 1 \not\equiv q \pmod e$. Then $m := m(q,e) \geq \frac{e}{3}$ if and only if one of the following holds:*

(i) *$q \geq 3$, $\gcd(2,q) = 1$, $e = \frac{2q-2}{k}$ where k is an odd divisor of $q-1$ (where $m = \frac{e}{2}$).*

(ii) *$q \geq 4$, $\gcd(3,q) = 1$, $e = \frac{3q-3}{k}$ where k is a divisor of $q-1$ with $k \equiv 1 \pmod 3$ (where $m = \frac{e}{3}$).*

(iii) *$q \geq 5$, $\gcd(3,q) = 1$, $e = \frac{3q-3}{k}$ where k is a divisor of $q-1$ with $k \equiv 2 \pmod 3$ (where $m = \frac{e}{3}$).*

(iv) *$q \equiv b \pmod e$, and the pair (b,e) appears in the following table:*

b	2	2	2	3	3	4	4	4	5
e	3	5	7	5	8	5	7	15	24
m	2	2	3	2	4	2	3	6	8

Proof. Suppose first that $m := m(q,e) \geq \frac{e}{3}$, and write $q = ae + b$ where $a, b \in \mathbb{N}_0$ and $0 \leq b < e$. If $b = 0$ then $1 = \gcd(q,e) = e$ which is impossible since $q \not\equiv 1 \pmod e$. Thus $1 < b < e$. Since $\gcd(b,e) = \gcd(q,e) = 1$ and $m(b,e) = m(q,e) \geq \frac{e}{3}$ Proposition 2.5 applies, with b instead of q. We discuss the various cases.

(i) Let $b \geq 3$, $\gcd(2,b) = 1$, $e = 2b-2$, $m = \frac{e}{2} = b-1$. Then $q \geq b \geq 3$, and $\gcd(2,q) = \gcd(2,b) = 1$ since $2 \mid e$. Moreover, $e = 2(q-ae) - 2$, so that $e(1+2a) = 2q-2$ and $e = \frac{2q-2}{1+2a}$. Thus we are in case (i) of Proposition 2.6.

(ii) Let $b \geq 4$, $\gcd(3,b) = 1$, $e = 3b-3$, $m = \frac{e}{3} = b-1$. Then $q \geq b \geq 4$, and $\gcd(3,q) = \gcd(3,b) = 1$ since $3 \mid e$. Moreover, $e = 3(q-ae)-3$, so that $e(1+3a) = 3q-3$ and $e = \frac{3q-3}{1+3a}$. Thus we are in case (ii) of Proposition 2.6.

(iii) Let $b \geq 5$, $\gcd(6,b) = 1$, $e = \frac{3b-3}{2}$, $m = \frac{e}{3} = \frac{b-1}{2}$. Then $q \geq b \geq 5$, and $\gcd(3,q) = \gcd(3,b) = 1$ since $3 \mid e$. Moreover, $2e = 3(q-ae)-3$, so that $e(2+3a) = 3q-3$ and $e = \frac{3q-3}{2+3a}$. Thus we are in case (iii) of Proposition 2.6.

(iv) If one of these cases holds for b then we are clearly in the corresponding case of Proposition 2.6.

Now suppose, conversely, that we are in one of the cases of Proposition 2.6.

(i) Let $q \geq 3$, $\gcd(2,q) = 1$ and $e = \frac{2q-2}{k}$ where k is an odd divisor of $q-1$. We write $k = 2a+1$ with $a \in \mathbb{N}_0$. Then $e(2a+1) = 2q-2$, so that $e+2 = 2(q-ae)$ and $b := q-ae = \frac{e+2}{2} \in \mathbb{N}$. If $e = 2$ then we obtain the contradiction $k = q-1 \equiv 0 \pmod 2$. Thus $e \geq 4$ and $3 \leq b < e$. Moreover, $\gcd(b,e) = \gcd(q,e) = 1$. Since $2 \mid e$ this implies $\gcd(2,b) = 1$. Hence we are in case (i) of Proposition 2.5, with b instead of q. In particular, $m(q,e) = m(b,e) = \frac{e}{2} \geq \frac{e}{3}$.

(ii) Let $q \geq 4$, $\gcd(3,q) = 1$ and $e = \frac{3q-3}{k}$ where k is a divisor of $q-1$ with $k \equiv 1 \pmod 3$. We write $k = 3a+1$ with $a \in \mathbb{N}_0$. Then $e(3a+1) = 3q-3$, so that $e+3 = 3(q-ae)$ and $b := q-ae = \frac{e+3}{3} \in \mathbb{N}$; in particular, $\gcd(b,e) = \gcd(q,e) = 1$. Since $3 \mid e$ this implies $\gcd(3,b) = 1$. Obviously, $1 < \frac{e}{3}+1 < e$.

If $b = 2$ then $e = 3$. Thus we are in case (iv) of Proposition 2.5, with b instead of q. Hence $m(q,e) = m(b,e) = 2 \geq \frac{e}{3}$.

Thus we may assume $b \geq 4$. Then we are in case (ii) of Proposition 2.5, with b instead of q. Hence $m(q,e) = m(b,e) = \frac{e}{3}$.

(iii) Let $q \geq 5$, $\gcd(3,q) = 1$ and $e = \frac{3q-3}{k}$ where k is a divisor of $q-1$ with $k \equiv 2 \pmod 3$. We write $k = 3a+2$ with $a \in \mathbb{N}_0$. Then $e(3a+2) = 3q-3$, so that $2e+3 = 3(q-ae)$ and $b := q-ae = \frac{2e+3}{3} \in \mathbb{N}$; in particular, $\gcd(b,e) = \gcd(q,e) = 1$. Since $3 \mid e$ this implies $\gcd(3,b) = 1$. Since $b \equiv 3b = 2e+3 \equiv 1 \pmod 2$ we even have $\gcd(6,b) = 1$. Since $b = \frac{2e}{3}+1 > 1$ this implies $b \geq 5$ and $e \geq 6$. Thus $b = \frac{2e+3}{3} < e$. Hence we are in case (iii) of Proposition 2.5, with b instead of q. Hence $m(q,e) = m(b,e) = \frac{e}{3}$.

(iv) Let $q \equiv 2 \pmod e$ where $e = 3$. Then $m(q,e) = m(2,3) = 2 \geq \frac{e}{3}$.

The other cases are similar. □

Next we investigate the situation in the case where $\mathrm{ord}_e(q) = 2$. (The case $\mathrm{ord}_e(q) = 1$, i.e. $q \equiv 1 \pmod e$, is part of [3, Example 6.1].)

Proposition 2.7. *Let $q, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^2 - 1$, and set $e_1 := \gcd(e, q-1)$, $e_2 := \gcd(e, q+1), m := m(q, e)$. If $e_1 \geq e_2$ or both e and $\frac{q^2-1}{e}$ are even then $m = e_1$. Otherwise $m = 2e_1$.*

Proof. [3, Lemma 6.2] implies that $m \in \{e_1, 2e_1\}$.

Suppose first that both e and $\frac{q^2-1}{e}$ are even. Then q is odd, e_1 is even, and $l := \gcd(2, e_1, \frac{q^2-1}{e}) = 2$. Thus $m \leq \frac{2e_1}{l} = e_1$ by [3, Lemma 6.2 (iii)], i.e. $m = e_1$ by [3, Lemma 6.2 (i)].

Suppose next that $e_1 = e_2$. Then $e_1 \mid \gcd(q-1, q+1) \mid 2$, i.e. $e_1 = e_2 \in \{1, 2\}$. Thus $e = e_1 \mid q - 1$, and $m = e = e_1$ by [3, Example 6.1].

Now suppose that $e_1 > e_2$. If e is odd then there is $a \in \{0, \ldots, e_2 - 1\}$ such that $2a \equiv e_1 \pmod{e_2}$. Since $e = e_1 e_2$ one checks easily that $a + q(e_1 - a) \equiv 0 \pmod{e}$. Thus $m \leq e_1$, i.e. $m = e_1$.

If e is even then q is odd, and both e_1 and e_2 are even. Then $\frac{e_1 \pm e_2}{2} \in \mathbb{N}$. We claim that e divides $\frac{e_1+e_2}{2} + q\frac{e_1-e_2}{2} = e_1\frac{q+1}{2} - e_2\frac{q-1}{2}$. (Then $m \leq e_1$, i.e. $m = e_1$.) We write $e_1 = a_1(q-1) + b_1 e$ and $e_2 = a_2(q+1) + b_2 e$ with $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Then

$$e_1\frac{q+1}{2} - e_2\frac{q-1}{2} \equiv (a_1 - a_2)\frac{q^2-1}{2} \pmod{e}.$$

By the first part of the proof, we may assume that $\frac{q^2-1}{e}$ is odd. Then $q^2 - 1$ and e have equal 2-parts. Thus the 2-parts of e_1 and $q - 1$ are equal and smaller than the 2-part of e. Hence a_1 is odd. Similarly, the 2-parts of e_2 and $q + 1$ are equal and smaller than the 2-part of e. Thus a_2 is also odd. However, then $a_1 - a_2$ is even, and our claim follows. This finishes the proof of our first assertion.

In order to prove the second assertion, suppose that $m = e_1 < e_2$, and let $k \in \{1, \ldots, \frac{q^2-1}{e}\}$ such that $s_q(ke) = m$. Then $ke = a + q(e_1 - a)$ for some $a \in \{0, \ldots, e_1\}$. Hence $0 \equiv keq \equiv (e_1 - a) + qa \equiv e_1 + (q-1)a \pmod{e}$; in particular, $0 \equiv e_1 + (q-1)a \equiv e_1 - 2a \pmod{e_2}$, and $-e_1 \leq e_1 - 2a \leq e_1$. Thus $e_1 = 2a$ and e are even. Moreover, we have $0 \equiv 2a + (q-1)a \equiv (q+1)a \pmod{e}$. Thus $e \mid (q+1)a = (q+1)\frac{e_1}{2}$, so that $2e \mid (q+1)e_1 \mid q^2 - 1$. Hence $\frac{q^2-1}{e}$ is even. □

Example 2.8. Table 2 gives the values $m(q, e)$ for some larger values of q and e.

Next we present some infinite series of examples where $m(q, e)$ can be calculated directly. The following result is illustrated by Table 1 and Table 2.

Proposition 2.9. *Let $e = 2^k$ for some $k \in \mathbb{N}$ with $k \geq 3$. Moreover, let $q \in \mathbb{N}$ be odd. Then*

$$m(q,e) = \begin{cases} \gcd(e, q-1) = e/\mathrm{ord}_e(q)\,, & \text{if } q \equiv 1 \pmod 4, \\ 2\,, & \text{if } q \equiv -1 \pmod e, \\ 4\,, & \text{otherwise.} \end{cases}$$

Proof. It is well-known that $(\mathbb{Z}/e\mathbb{Z})^\times = \langle -1 + e\mathbb{Z}\rangle \times \langle 5 + e\mathbb{Z}\rangle$ and $\mathrm{ord}_e(5) = 2^{k-2}$, $\mathrm{ord}_e(-1) = 2$. Thus

$$\langle 5 + e\mathbb{Z}\rangle = \{b + e\mathbb{Z} \in \mathbb{Z}/e\mathbb{Z} : b \equiv 1 \pmod 4\}.$$

We also recall the well-known formula

$$5^{2^t} \equiv 1 + 2^{t+2} \pmod{2^{t+3}} \quad \text{for} \quad t \in \mathbb{N}_0.$$

(i) Let $q \in \mathbb{N}$ such that $q \equiv 1 \pmod 4$. Then $q \equiv 5^{2^r a} \pmod e$ where $r \in \{0, 1, \ldots, k-2\}$ and $a \in \mathbb{N}$ is odd, so that $\mathrm{ord}_e(q) = 2^{k-2-r}$. By [3, Lemma 6.1], we have $m := m(q,e) = m(5^{2^r a}, e) = m(5^{2^r}, e)$, and it is easy to see that $e_1 := \gcd(e, q-1) = \gcd(e, 5^{2^r a} - 1) = \gcd(e, 5^{2^r} - 1)$ and $\mathrm{ord}_e(q) = \mathrm{ord}_e(5^{2^r})$. Thus we may assume that $q = 5^{2^r}$. Then

$$\langle 5^{2^r} + e\mathbb{Z}\rangle = \{b + e\mathbb{Z} \in \mathbb{Z}/e\mathbb{Z} : b \equiv 1 \pmod{2^{r+2}}\},$$

and $e_1 = 2^{r+2}$; in particular, $2^{r+2} = e_1 \mid m$ by [3, Lemma 6.2], and $\gcd(e, q-1) = e/\mathrm{ord}_e(q)$. It remains to show that $m \leq 2^{r+2}$.

By the description of $\langle 5^{2^r} + e\mathbb{Z}\rangle$ above, there is $c \in \{0, 1, \ldots, 2^{k-2-r} - 1\}$ such that $(5^{2^r})^c \equiv 1 - 2^{r+2} \pmod e$. Then $e = 2^k \mid q^c + 2^{r+2} - 1$, and we conclude that $m(q,e) \leq s_q(q^c + 2^{r+2} - 1) \leq 2^{r+2}$.

(ii) Let $q \in \mathbb{N}$ such that $q \equiv -1 \pmod e$. Then $m(q,e) = 2$ by [3, Lemma 6.1] and Example 2.4.

(iii) Let $q \in \mathbb{N}$ such that $q \equiv 3 \pmod 4$ and $q \not\equiv -1 \pmod{2^k}$. Then $e_1 := \gcd(e, q-1) = 2$. Thus $m := m(q,e)$ is even by [3, Lemma 6.2]. Since $-1 + e\mathbb{Z} \notin \langle q + e\mathbb{Z}\rangle$ [3, Lemma 6.3] implies that $m > 2$, i.e. $m \geq 4$, and it remains to show that $m \leq 4$.

As above, we have $q \equiv -5^{2^r a} \pmod e$ where $r \in \{0, 1, \ldots, k-3\}$ and $a \in \mathbb{N}$ is odd. Moreover, we may assume again that $q \equiv -5^{2^r} \pmod e$. The formula above implies that

$$\begin{aligned} \langle q + e\mathbb{Z}\rangle &= \langle -5^{2^r} + e\mathbb{Z}\rangle \\ &= \{b + e\mathbb{Z} \in \mathbb{Z}/e\mathbb{Z} : b \equiv -1 - 2^{r+2} \pmod{2^{r+3}}\} \cup \\ &\qquad \{b + e\mathbb{Z} \in \mathbb{Z}/e\mathbb{Z} : b \equiv 1 \pmod{2^{r+3}}\}, \end{aligned}$$

where the first subset contains those powers of $q + e\mathbb{Z}$ where the exponents are odd and the second subset contains the powers with even exponents. Thus there are $c, d \in \{0, 1, \ldots, 2^{k-2-r} - 1\}$ such that

$$q^c \equiv -1 - 2^{r+2} \pmod{e} \text{ and } q^d \equiv 1 + 2^{r+3} \pmod{e}.$$

Note that c is odd and d is even, and that $2q^c + q^d + 1 \equiv -2 - 2^{r+3} + 1 + 2^{r+3} + 1 \equiv 0 \pmod{e}$ and $m(q, e) \leq s_q(2q^c + q^d + 1) \leq 4$. □

Now we turn to the situation where e is a power of an odd prime.

Proposition 2.10. *Let $e = p^k$ where p is an odd prime and $k \in \mathbb{N}$. Moreover, let $q \in \mathbb{N}$ such that $q \equiv 1 \pmod{p}$. Then $m(q, e) = \gcd(e, q - 1) = e/\mathrm{ord}_e(q)$.*

Proof. The hypothesis $q \equiv 1 \pmod{p}$ implies that $q + e\mathbb{Z}$ is a p-element in $(\mathbb{Z}/e\mathbb{Z})^\times$. Since p is odd the Sylow p-subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$ is generated by $1 + p + e\mathbb{Z}$. Since $\varphi(e) = p^{k-1}(p - 1)$ we have $q \equiv (1 + p)^{p^r a} \pmod{e}$ where $r \in \{0, 1, \ldots, k - 1\}$ and $a \in \mathbb{N} \setminus p\mathbb{N}$. [3, Lemma 6.1] implies that $m(q, e) = m((1 + p)^{p^r}, e)$. Since

$$(1 + p)^{p^r a} - 1 = \Big((1 + p)^{p^r} - 1\Big) \Big((1 + p)^{p^r(a-1)} + \ldots + (1 + p)^{p^r} + 1\Big)$$

where the second factor is not divisible by p we also have

$$\gcd(e, q - 1) = \gcd(e, (1 + p)^{p^r} - 1) \quad \text{and} \quad \mathrm{ord}_e(q) = \mathrm{ord}_e((1 + p)^{p^r}).$$

Thus we may assume that $q \equiv (1+p)^{p^r} \pmod{e}$ for some $r \in \{0, 1, \ldots, k-1\}$. We recall that

$$(1 + p)^{p^{t-1}} \equiv 1 + p^t \pmod{p^{t+1}} \quad \text{for} \quad t \in \mathbb{N}.$$

Thus

$$\langle (1 + p)^{p^r} + e\mathbb{Z} \rangle = \{b + e\mathbb{Z} \in \mathbb{Z}/e\mathbb{Z} : b \equiv 1 \pmod{p^{r+1}}\}.$$

Since $\mathrm{ord}_e((1 + p)^{p^r}) = p^{k-1-r}$ there is $c \in \{0, 1, \ldots, p^{k-1-r} - 1\}$ such that

$$\Big((1 + p)^{p^r}\Big)^c \equiv 1 - p^{r+1} \pmod{e}, \quad \text{i.e.} \quad e \mid q^c + p^{r+1} - 1.$$

Thus $m(q, e) \leq s_q(q^c + p^{r+1} - 1) \leq p^{r+1} = \gcd(e, q - 1)$. Now [3, Lemma 6.2] implies the first equality, and the second follows from $\mathrm{ord}_e(q) = e/p^{r+1} = \gcd(e, q - 1)$. □

Lemma 2.11. *Let $e = p^k$ where $p > 3$ is a prime and $k \in \mathbb{N}$, and assume that $\mathrm{ord}_e(q)$ is divisible by 3. Then $m(q, e) = 2$ if $\mathrm{ord}_e(q)$ is even, and $m(q, e) = 3$ otherwise.*

Proof. Let $n = \mathrm{ord}_e(q)$. We have $m(q,e) = 2$ if and only if n is even, by [3, Lemma 6.3] and [3, Remark 6.1] (cf. Table 1). By the assumption, $q^{n/3} + e\mathbb{Z}$ is not a p-element in $(\mathbb{Z}/e\mathbb{Z})^\times$, thus p does not divide $q^{n/3} - 1$, [3, Lemma 6.4] yields $m(q,e) \leq 3$, and equality holds because $m(q,e) \neq 2$. □

Corollary 2.12. *Let $e = p^k$ where p is an odd prime of the form $p = 1 + 2^a 3^b$ for some nonnegative integers a, b, and $k \in \mathbb{N}$. Then*

$$m(q,e) = \begin{cases} \gcd(e, q-1) = e/\mathrm{ord}_e(q), & \text{if } \mathrm{ord}_e(q) \text{ is a power of } p, \\ 2, & \text{if } \mathrm{ord}_e(q) \text{ is even}, \\ 3, & \text{otherwise.} \end{cases}$$

Proof. Proposition 2.10 yields $m(q,e) = \gcd(e, q-1) = e/\mathrm{ord}_e(q)$ if $q + e\mathbb{Z}$ is a p-element in $(\mathbb{Z}/e\mathbb{Z})^\times$. In the remaining cases, $\mathrm{ord}_e(q)$ is divisible by 2 or 3, and we can apply Lemma 2.11. □

Remark 2.13. (i) Primes of the form $1+2^a 3^b$ as above are called Pierpont primes, see [10]. It is conjectured that there are infinitely many Pierpont primes.

(ii) If $e = p^k$ where $k \in \mathbb{N}$ and p is a Fermat prime (e.g. $p \in \{3, 5, 17\}$) then only the first two cases in Corollary 2.12 occur.

Lemma 2.14. *Let $e = p^k$ where p is an odd prime and $k \in \mathbb{N}$. If $\mathrm{ord}_e(q) = \frac{\varphi(e)}{d}$ for a divisor d of $p-1$ then $m(q,e) = m(q,p)$.*

Proof. Since p is an odd prime and $k \in \mathbb{N}$, $(\mathbb{Z}/e\mathbb{Z})^\times$ is cyclic of order $\varphi(e) = p^{k-1}(p-1)$. If $q \in \mathbb{N}$ satisfies $\mathrm{ord}_e(q) = \frac{\varphi(e)}{d}$ for a divisor d of $p-1$ then $\langle q + e\mathbb{Z}\rangle = \{x^d + e\mathbb{Z} : x \in \mathbb{Z} \setminus p\mathbb{Z}\}$. Moreover, $\mathrm{ord}_p(q) = \frac{p-1}{d}$ and $\langle q + p\mathbb{Z}\rangle = \{x^d + p\mathbb{Z} : x \in \mathbb{Z} \setminus p\mathbb{Z}\}$. Let $m := m(q,p)$. Then there are $x_1, \ldots, x_m \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $x_1^d + \ldots + x_m^d \equiv 0 \pmod p$. Thus, by Hensel's Lemma (see II.2.2 in [8], for example), there are $y_1, \ldots, y_m \in \mathbb{Z}$ such that $y_1^d + \ldots + y_m^d \equiv 0 \pmod e$ and $y_i \equiv x_i \pmod p$ for $i = 1, \ldots, m$; in particular, $y_1, \ldots, y_m \notin p\mathbb{Z}$. This shows that $m(q,e) \leq m = m(q,p)$. Since $m(q,p) \leq m(q,e)$ by [3, Lemma 6.1], the result follows. □

Corollary 2.15. *Let $e = p^k$ where p is an odd prime and $k \in \mathbb{N}$. If $\mathrm{ord}_e(q) = \frac{\varphi(e)}{2}$ then*

$$m(q,e) = \begin{cases} 2, & \text{if } p \equiv 1 \pmod 4, \\ 3, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. By the lemma above and its proof, we have $m(q,e) = m(q,p)$ and $\mathrm{ord}_p(q) = \frac{p-1}{2}$. Thus we may assume that $k = 1$, i.e. $e = p$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $\varphi(p) = p-1$, $\langle q + p\mathbb{Z}\rangle$ consists of the squares in $(\mathbb{Z}/p\mathbb{Z})^\times$. It is well-known that there are $x_1, x_2 \in \mathbb{Z}$ such that $x_1^2+x_2^2 \equiv -1 \pmod p$ (cf. IV.1.7 in [8], for example), i.e. $x_1^2+x_2^2+1^2 \equiv 0 \pmod p$. Hence $m(q,p) \leq 3$. Moreover, by [3, Remark 6.1], we have $m(q,p) = 2$ if and only if $\mathrm{ord}_p(q)$ is even, i.e. if and only if $p \equiv 1 \pmod 4$. □

Remark 2.16. Let e be a prime, and let $q \in \mathbb{N}$ such that $\mathrm{ord}_e(q) = \frac{e-1}{k}$ where $k \in \mathbb{N}$ divides $e-1$ and $e > (k-1)^4$. Then, by the main theorem in [9], every element in $\mathbb{Z}/e\mathbb{Z}$ (in particular, $-1+e\mathbb{Z}$) is a sum of two k-th powers. Since $\langle q+e\mathbb{Z}\rangle$ is the set of all k-th powers in $(\mathbb{Z}/e\mathbb{Z})^\times$, this implies that $0+e\mathbb{Z}$ is a sum of at most three elements in $\langle q+e\mathbb{Z}\rangle$. Thus $m(q,e) \leq 3$.

For example, if $k = 4$ then $m(q,e) \leq 3$ for every prime $e > 81$. Explicit computations show that, for $k = 4$, the only cases where $m(q,e) > 3$ are as follows:

- $e = 5$, $q \equiv 1 \pmod 5$, $m(q,e) = 5$;
- $e = 29$, $\langle q+29\mathbb{Z}\rangle = \langle 7+29\mathbb{Z}\rangle$, $m(q,e) = 4$.

The smallest (odd) prime that is not a Pierpont prime is $p = 11$. Here we get the following.

Proposition 2.17. *Let $e = 11^k$ for some $k \in \mathbb{N}$. Then*

$$m(q,e) = \begin{cases} \gcd(e, q-1) = e/\mathrm{ord}_e(q), & \textit{if } \mathrm{ord}_e(q) \textit{ is a power of } 11, \\ 2, & \textit{if } \mathrm{ord}_e(q) \textit{ is even}, \\ 3, & \textit{if } \mathrm{ord}_e(q) = 5 \cdot 11^{k-1}, \\ 5, & \textit{otherwise.} \end{cases}$$

Proof. Note first that $(\mathbb{Z}/e\mathbb{Z})^\times$ is cyclic of order $2 \cdot 5 \cdot 11^{k-1}$ and generated by $2+e\mathbb{Z}$.

If $\mathrm{ord}_e(q)$ is a power of 11 then $m(q,e) = \gcd(e, q-1) = e/\mathrm{ord}_e(q)$ by Proposition 2.10, and if $\mathrm{ord}_e(q)$ is even then $m(q,e) = 2$ by [3, Lemma 6.3].

In all other cases, we have $\mathrm{ord}_e(q) = 5 \cdot 11^l$ for some $l < k$. Then $\gcd(11, q^{11^l} - 1) = \gcd(11, q-1) = 1$, and therefore $\gcd(e, q^{11^l} - 1) = 1$. Thus $m(q,e) \leq 5$ by [3, Lemma 6.4], and $m(q,e) > 2$ by [3, Lemma 6.3].

If $\mathrm{ord}_e(q) = 5 \cdot 11^{k-1} = \varphi(e)/2$ then the result follows from Lemma 2.15.

Thus we may assume that $k \geq 2$. Then [3, Lemma 6.1] and explicit computations show: $m(4^{11}, e) \geq m(4^{11}, 11^2) = 5$, i.e. $m(4^{11}, e) = 5$. Hence $m(4^{11^n}, e) \geq m(4^{11}, e) = 5$ for $n \in \mathbb{N}$, again by [3, Lemma 6.1], and the result follows. □

Our next result is similar to Proposition 2.10.

Proposition 2.18. *Let $e = 2p^k$ where p is an odd prime and $k \in \mathbb{N}$. Moreover, let $1 < q \in \mathbb{N}$ such that $\mathrm{ord}_e(q)$ is a power of p. Then $m(q,e) = \gcd(e, q-1) = e/\mathrm{ord}_e(q)$.*

Proof. Omitted. □

Remark 2.19. Suppose that $e = 2p^k$ where $p > 3$ is a prime and $k \in \mathbb{N}$. Moreover, let $q \in \mathbb{N}$ such that $\gcd(q, e) = 1$, and let $n := \mathrm{ord}_e(q)$.

Since q is odd, [3, Lemma 6.2 (i)] implies that $2 \mid \gcd(e, q-1) =: e_1 \mid m(q, e)$. Thus $m(q, e)$ is always even. Also, [3, Remark 6.1] implies that $m(q, e) = 2$ if and only if n is even.

Thus suppose now that n is odd, so that $m(q, e) \geq 4$, and suppose that $3 \mid n$. Then $\mathrm{ord}_e(q^{n/3}) = 3$, i. e., $q^{n/3} + e\mathbb{Z}$ is not a p-element in $(\mathbb{Z}/e\mathbb{Z})^\times$. Hence $q^{n/3} - 1$ is not divisible by p. Since $p^k \mid e \mid q^n - 1 = (q^{n/3} - 1)(q^{2n/3} + q^{n/3} + 1)$, this implies that $p^k \mid q^{2n/3} + q^{n/3} + 1$ and $e \mid 2(q^{2n/3} + q^{n/3} + 1)$. We conclude that $m(q, e) \leq 6$, i. e., $m(q, e) \in \{4, 6\}$.

We do not know when precisely we have $m(q, e) = 6$. However, it is easy to check that $m(q, e) = 6$ whenever $n = 3$ and $e > 14$.

We are interested in upper bounds for $m(q, e)$ which are cheap to compute. The following result improves the trivial bound $m(q, e) \leq e$.

Lemma 2.20. *Let $q, e \in \mathbb{N}$ such that $\gcd(q, e) = 1$, and set $H = \langle q + e\mathbb{Z} \rangle \leq (\mathbb{Z}/e\mathbb{Z})^\times$. For $l \in \mathbb{N}$, define*

$$\Sigma_l(H) := \{x_1 + x_2 + \cdots + x_k \mid x_1, x_2, \ldots, x_k \in H, 1 \leq k \leq l\}.$$

Then

$$m(q, e) = \min\{l \mid 0 + e\mathbb{Z} \in \Sigma_l(H)\} \leq \sum_{d \mid e} \frac{\varphi(d)}{\mathrm{ord}_d(q)} \leq e.$$

Proof. The group H acts on the set $A := \mathbb{Z}/e\mathbb{Z}$ by multiplication. We identify A with the disjoint union of the groups $(\mathbb{Z}/d\mathbb{Z})^\times$, for the divisors d of e, by mapping $a + e\mathbb{Z}$ to $\frac{a}{g} + \frac{e}{g}\mathbb{Z}$, where $g = \gcd(a, e)$ holds. The action of H on $(\mathbb{Z}/d\mathbb{Z})^\times$ is essentially the same as the action of $\langle q + d\mathbb{Z} \rangle$ on $(\mathbb{Z}/d\mathbb{Z})^\times$; the corresponding H-orbits are just the cosets of $\langle q + d\mathbb{Z} \rangle$ in $(\mathbb{Z}/d\mathbb{Z})^\times$. In particular, there are precisely $\varphi(d)/\mathrm{ord}_d(q)$ orbits of H on $(\mathbb{Z}/d\mathbb{Z})^\times$. Thus the total number of H-orbits on A is

$$\sum_{d \mid e} \frac{\varphi(d)}{\mathrm{ord}_d(q)} \leq \sum_{d \mid e} \varphi(d) = e.$$

Each of the sets $\Sigma_l(H)$ is H-invariant and thus a union of H-orbits, and the sequence $H = \Sigma_1(H) \subseteq \Sigma_2(H) \subseteq \cdots$ is strictly increasing until the first $\Sigma_l(H)$ with the property $0 + e\mathbb{Z} \in \Sigma_l(H)$. This implies that $m(q, e)$ is at most the number of H-orbits on A. □

Remark 2.21. By Propositions 2.9 and 2.10, we have $m(q,e) = e/\mathrm{ord}_e(q)$ when e is a power of 2 and $q \equiv 1 \pmod 4$, or when e is a power of an odd prime p and $q \equiv 1 \pmod p$.

If e is a power of 2 then $m(q,e) \leq e/\mathrm{ord}_e(q)$ holds for any q that is coprime to e. If e is a power of an odd prime p and $q \not\equiv 1 \pmod p$ then in general $\mathrm{ord}_e(q)$ does not divide e, and it can happen that $m(q,e) > e/\mathrm{ord}_e(q)$ holds; for example, take $(e,q) = (9,2)$, then $m(q,e) = 2 > 3/2 = e/\mathrm{ord}_e(q)$.

However, we can show that always $m(q,e) \leq \lceil e/\mathrm{ord}_e(q) \rceil$ holds.

Proposition 2.22. *Let $e = p^k$ where p is a prime and k is a positive integer, and let $q \in \mathbb{Z}$ such that* $\gcd(q,e) = 1$. *Then the following holds.*

$$m(q,e) \leq x(q,e) := \lceil e/\mathrm{ord}_e(q) \rceil.$$

Proof. By Remark 2.21, we may assume that p is odd and $q \not\equiv 1 \pmod p$. This means that $q + e\mathbb{Z}$ is not a p-element in $(\mathbb{Z}/e\mathbb{Z})^\times$. We choose a power $Q + e\mathbb{Z}$ of $q + e\mathbb{Z}$ whose order is a prime $r \neq p$. Since $p \nmid Q - 1$ we have $\gcd(e, Q-1) = 1$. Then [3, Lemma 6.4] implies that $m(q,e) \leq m(Q,e) \leq r$. On the other hand, we can write $\mathrm{ord}_e(q) = p^s t$ where $s, t \in \mathbb{N}_0$, $s \leq k-1$ and $r \mid t \mid p-1$. If $s \leq k$ then

$$\frac{e}{\mathrm{ord}_e(q)} = \frac{p^k}{p^s t} \geq \frac{p^2}{t} > p \geq r + 1 \geq m(q,e) + 1,$$

and the result follows in this case.

Thus we may assume that $s = k-1$, i. e., $\mathrm{ord}_e(q) = p^{k-1}t = \varphi(e)/t'$ where t' is a divisor of $p-1$. Then Lemma 2.14 implies that $m(q,e) = m(q,p)$. On the other hand, we have

$$\frac{e}{\mathrm{ord}_e(q)} = \frac{p^k}{p^{k-1}t} = \frac{p}{t} = \frac{p}{\mathrm{ord}_p(q)}.$$

Thus we may assume that $k = 1$, i. e., $e = p$ is a prime integer and $\mathrm{ord}_p(q) = t \mid p-1$. In this case, we have

$$m(q,p) \leq \sum_{d \mid p} \frac{\varphi(d)}{\mathrm{ord}_d(q)} = 1 + \frac{p-1}{t}$$

(see Lemma 2.20), and the result follows because of $x(q,p) = \lceil p/t \rceil = (p-1)/t + 1$. □

Remark 2.23. Does the relation $m(q,e) \leq x(q,e)$ hold also if e is not a prime power? There are no counterexamples for $e \leq 400$ and for pairs (q,e) such that $(q^n - 1)/e \leq 10\,000$ holds, where $n = \mathrm{ord}_e(q)$.

Example 2.24. Table 3 displays some more values $m(q,e)$. Here we list only one generator $q + e\mathbb{Z}$ for each cyclic subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$.

The following result may also be of interest; it is related to [3, Lemma 6.2 (iv)]. Here we denote by $\Phi_n \in \mathbb{Q}[X]$ the n-th cyclotomic polynomial.

Proposition 2.25. *Let n be a prime number. Then there are only finitely many $e \in \mathbb{N}$ such that $e \mid \Phi_n(q)$ (in particular, $\mathrm{ord}_e(q) \mid n$) and $m(q,e) < n$ for some $q \in \mathbb{N}$.*

Proof. We fix a prime number n and an integer $m \in \{1, \ldots, n-1\}$. Suppose that $q, e \in \mathbb{N}$ satisfy $e \mid \Phi_n(q)$ and $m(q,e) = m$. Then there are $i_1, \ldots, i_m \in \mathbb{N}_0$ such that

$$(*) \qquad q^{i_1} + \ldots + q^{i_m} \equiv 0 \pmod{e}.$$

Since $q^n \equiv 1 \pmod{e}$ we may assume that $i_1, \ldots, i_m \in \{0, \ldots, n-1\}$. Since $m < n$ there exists $j \in \{0, \ldots, n-1\} \setminus \{i_1, \ldots, i_m\}$. Since we can multiply $(*)$ by q^{n-1-j} we may assume that $j = n-1$, i.e. $i_1, \ldots, i_m \in \{0, \ldots, n-2\}$. (Of course, we may then also assume that $0 = i_1 \leq \ldots \leq i_m \leq n-2$.) Thus there are only finitely many possibilities for the m-tuple $(i_1, \ldots, i_m)$. Consider the polynomial $g(X) := X^{i_1} + \ldots + X^{i_m} \in \mathbb{Q}[X]$. Since $\Phi_n(X)$ is irreducible of degree $n-1$ there are $a(X), b(X) \in \mathbb{Q}[X]$ such that $a(X)\Phi_n(X) + b(X)g(X) = 1$. We fix $d \in \mathbb{N}$ such that $da(X), db(X) \in \mathbb{Z}[X]$. Then $e \mid da(q)\Phi_n(q) + db(q)g(q) = d$. Hence there are only finitely many possibilities for e, as claimed. □

Example 2.26. (i) Let $q, e \in \mathbb{N}$ such that $e \mid \Phi_5(q)$. Carrying out the calculations in the proof of Proposition 2.25 for $1 \leq m \leq 4$, we obtain the following values (d,m), where we choose the minimal possible d: $(1,m)$ and (m,m) for all m, $(2,4)$, $(11,3)$, $(11,4)$, and $(61,4)$. Since divisors of $\Phi_d(q)$ are odd for odd d (and are not divisible by 3 if additionally d is not divisible by 3), we get $e = 1$ if $m(q,e) = 1$, $e = 11$ if $m(q,e) = 3$, and $e \in \{11, 61\}$ if $m(q,e) = 4$. (And Proposition 2.17 or Table 1 shows that we cannot have $m(q,e) = 4$ in case $e = 11$.) We will need this result later on.

(ii) Let $q, e \in \mathbb{N}$ such that $1 < e \mid \Phi_7(q)$, and let $m = m(q,e)$. We proceed as in (i), and discard 2-parts and 3-parts of the values for d. Moreover, we can discard those candidates d with the property that 7 does not divide $\varphi(d)$, since the relevant divisors e of d must satisfy $\mathrm{ord}_e(q) = 7$ for some prime residue q modulo e; this criterion excludes $(d,m) \in \{(13,5), (41,6)\}$. We are left with the following list.

$m = 3: \quad e \in \{43\}$

$m = 4: \quad e \in \{29, 71, 547\}$

$m = 5: \quad e \in \{29, 43, 113, 197, 421, 463, 3277\}$

$m = 6: \quad e \in \{29, 43, 71, 113, 197, 211, 379, 449, 463, 757, 2689, 3053, 13021\}$

(Again, computing $m(q,e)$ shows that $e = 29$ occurs only for $m = 4$ (see Table 1), $e = 43$ occurs only for $m = 3$ (see Table 2), $e = 71$ occurs only for $m = 4$ (see Table 3), and $e \in \{113, 197, 463\}$ occur only for $m = 5$.)

Let again $q, e \in \mathbb{N}$ such that $\gcd(q,e) = 1$. Moreover, let $n \in \mathbb{N}$ such that $e \mid q^n - 1$ (e.g. $n = \mathrm{ord}_e(q)$), and set $z := \frac{q^n-1}{e}$. In order to avoid trivialities, we also suppose that $q > 1$ and $1 < e < q^n - 1$. Then [3, Proposition 6.1] implies that

$$m(q,e) = \min\{s_q(ke) : k = 1, \ldots, z\} = \min\{s_q(ke) : k = 1, \ldots, z-1\}.$$

Our next aim is to derive another description of $m(q,e)$. For this we introduce some more notation. For $x \in \mathbb{Z}$, we define $\overline{x} \in \mathbb{Z}$ by $\overline{x} \equiv x \pmod{z}$ and $0 \le \overline{x} < z$.

Proposition 2.27. *Let $k \in \mathbb{N}$ such that $k < z$. Then ke has the q-adic expansion*

$$ke = \sum_{i=1}^{n} \frac{\overline{kq^{n-i}}q - \overline{kq^{n-i+1}}}{z} q^{i-1} = \sum_{i=1}^{n} \left\lfloor \frac{\overline{kq^{n-i}}q}{z} \right\rfloor q^{i-1}.$$

Thus

$$s_q(ke) = \frac{q-1}{z} \sum_{i=1}^{n} \overline{kq^i} = \frac{q-1}{z} \frac{n}{\mathrm{ord}_z(q)} \sum_{i=1}^{\mathrm{ord}_z(q)} \overline{kq^i},$$

and

$$m(q,e) = \frac{q-1}{z} \frac{n}{\mathrm{ord}_z(q)} \min\left\{ \sum_{i=1}^{\mathrm{ord}_z(q)} \overline{kq^i} : 1 \le k < z \right\}.$$

Proof. Set $c_{k,i} = \overline{kq^{n-i}}$, for $0 \le i \le n$, and denote the coefficient of q^{i-1} in the above summation by $a_{k,i}$. Then $za_{k,i} = c_{k,i}q - c_{k,i-1}$ for $i = 1, \ldots, n$, $c_{k,0} = c_{k,n} = k$, and

$$z \sum_{i=1}^{n} a_{k,i} q^{i-1} = \sum_{i=1}^{n} c_{k,i} q^i - \sum_{i=1}^{n} c_{k,i-1} q^{i-1} = c_{k,n} q^n - c_{k,0} = k\,(q^n - 1) = zke$$

holds, as claimed.

The $a_{k,i}$ are integers because $\overline{kq^{n-i}}q - \overline{kq^{n-i+1}} \equiv 0 \pmod{z}$.

The $a_{k,i}$ are nonnegative because $\overline{kq^{n-i}}q \ge \overline{\overline{kq^{n-i}}q} = \overline{kq^{n-i+1}}$.

We have $a_{k,i} < q$ because $\overline{kq^{n-i}}q - \overline{kq^{n-i+1}} < zq$. Thus the q-adic expansion of ke has the desired form. Hence

$$s_q(ke) = \sum_{i=1}^{n} a_{k,i} = \frac{q-1}{z} \sum_{i=1}^{n} c_{k,i} = \frac{q-1}{z} \sum_{i=1}^{n} \overline{kq^i},$$

and $m(q,e)$ is the minimum of these values, for the admissible values of k. □

Remark 2.28. (i) A natural way to derive the statement of Proposition 2.27 is as follows. Dividing the obvious q-adic expansion of $q^n - 1$ by z, we get

$$\frac{q^n - 1}{z} = \frac{q-1}{z}q^{n-1} + \frac{q-1}{z}q^{n-2} + \cdots + \frac{q-1}{z}q^0.$$

If $q - 1$ is not divisible by z then these coefficients aren't integers, and we adjust them iteratively: Replacing $(q-1)/z$ by $(q - \overline{q})/z$ in the coefficient of q^{n-1} yields an integer, and can be compensated in the summation by choosing $(\overline{q}q - 1)/z$ as the coefficient of q^{n-2}. Next we replace this coefficient by $(\overline{q}q - \overline{q^2})/z$ and adjust the coefficient of q^{n-3} accordingly. Repeating this process, we get $(\overline{q^{n-1}}q - 1)/z$ as the coefficient of q^0, which is already an integer because $\operatorname{ord}_z(q)$ divides n.

(ii) Note that the cyclic subgroup $H := \langle q + z\mathbb{Z}\rangle$ of the multiplicative group $G := (\mathbb{Z}/z\mathbb{Z})^\times$ acts on the additive group $\mathbb{Z}/z\mathbb{Z}$ by multiplication, and that

$$\sum_{i=1}^{\operatorname{ord}_z(q)} \overline{kq^i} = |H_k| \sum_{x \in B} \overline{x}$$

where B is the H-orbit of $k + z\mathbb{Z}$ and

$$H_k := \{h + z\mathbb{Z} \in H : kh \equiv k \pmod{z}\}$$

is the stabilizer of $k + z\mathbb{Z}$ in H.

(iii) Now suppose, in addition, that $-1 + z\mathbb{Z} \in H = \langle q + z\mathbb{Z}\rangle$. Then $B = -B$ and $\overline{-x} = z - \overline{x}$ for $x \in B$. Thus

$$2\sum_{x\in B}\overline{x} = \sum_{x\in B}\overline{x} + \sum_{x\in B}\overline{-x} = \sum_{x\in B}\overline{x} + \sum_{x\in B} z - \overline{x} = |B|z,$$

and $\sum_{x\in B}\overline{x} = |H : H_k|\frac{z}{2}$. Hence Proposition 2.27 implies that

$$s_q(ke) = n\frac{q-1}{2}.$$

Since this expression is independent of k we conclude that

$$m(q,e) = n\frac{q-1}{2}$$

in this case.

(iv) The second expression for the q-adic expansion of ke that is stated in Proposition 2.27 can be used to compute the coefficients for $i = n, n-1, \ldots, 1$, without computing the number ke. Note that in typical examples (see Remark 7.13), q and z are small numbers, whereas e can be quite large.

Example 2.29. (i) If $q \equiv 1 \pmod{z}$ then $ke = \sum_{i=1}^{n} \frac{k(q-1)}{z} q^{i-1}$ for $k = 1, \ldots, z-1$, and $s_q(ke) = \frac{kn(q-1)}{z}$ for these k. Hence $m(q,e) = ne\frac{q-1}{q^n-1}$, as in Corollary 2.2.

(ii) If $q \equiv -1 \pmod z$, if $n = 2$ and $z > 2$ then

$$ke = \frac{(z-k)q-k}{z} + \frac{kq-(z-k)}{z}q,$$

so that $s_q(ke) = q-1$ for $k = 1, \ldots, z-1$, and $m(q,e) = q-1$.

(iii) Suppose that $(\mathbb{Z}/z\mathbb{Z})^\times$ is cyclic and generated by $q+z\mathbb{Z}$. Then $s_q(ke) = n\frac{q-1}{2}$ for $k = 1, \ldots, z-1$, and $m(q,e) = n\frac{q-1}{2}$.

(iv) Suppose that $z = p^a$ where p is a prime with $p \equiv 1 \pmod 4$, and $a \in \mathbb{N}$. Moreover, suppose that $\operatorname{ord}_z(q) = \frac{\varphi(z)}{2} = p^{a-1}\frac{p-1}{2}$. Then $(\mathbb{Z}/z\mathbb{Z})^\times$ is cyclic, and $-1 + z\mathbb{Z} \in \langle q + z\mathbb{Z}\rangle$. Thus Remark 2.28 implies that

$$m(q,e) = s_q(ke) = n\frac{q-1}{2} \quad \text{for} \quad k = 1, \ldots, z-1.$$

Proposition 2.30. *Suppose that z is a prime with $z \equiv -1 \pmod 4$, and that $\operatorname{ord}_z(q) = \frac{z-1}{2}$. Then $|\{s_q(ke); 1 \leq k \leq z-1\}| = 2$.*

Proof. Let $k \in \{1, \ldots, z-1\}$. Then Proposition 2.27 implies:

$$s_q(ke) = \frac{q-1}{z}\frac{2n}{z-1}\sum_{i=1}^{\operatorname{ord}_z(q)} \overline{kq^i}.$$

For $\epsilon \in \{\pm 1\}$, we set $G_\epsilon := \{x + z\mathbb{Z} \in (\mathbb{Z}/z\mathbb{Z})^\times : \left(\frac{x}{z}\right) = \epsilon\}$ where $\left(\frac{x}{z}\right)$ denotes the Legendre symbol. Then

$$\{kq^i + z\mathbb{Z} : i = 1, \ldots, \operatorname{ord}_z(q)\} \in \{G_+, G_-\}.$$

Moreover, by a result of Dirichlet (cf. [4, Chap. 6, equ. (19)]), we have

$$\sum_{x+z\mathbb{Z}\in G_+} \overline{x} < \sum_{x+z\mathbb{Z}\in G_-} \overline{x}.$$

The result follows. □

3. Lower bounds

Let $q, n, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^n - 1$. We set $z := \frac{q^n-1}{e}$. Moreover, let F be a field, and let $A = A(q,n,e)$ be the F-algebra of [3], Section 3. We denote by $J := \mathrm{J}(A)$ the Jacobson radical of A. In this section we establish certain lower bounds for $\mathrm{LL}(A)$. In certain cases, these lower bounds coincide with the upper bound established in [3, Theorem 7.1].

Proposition 3.1. *Let $n_1, n_2 \in \mathbb{N}$ such that $e \mid q^{n_1} - 1$ and $e \mid q^{n_2} - 1$. Then*

$$\mathrm{LL}(A(q, n_1 + n_2, e)) \geq \mathrm{LL}(A(q, n_1, e)) + \mathrm{LL}(A(q, n_2, e)) - 1.$$

Thus $\mathrm{LL}(A(q, rn, e)) \geq r \cdot \mathrm{LL}(A(q, n, e)) - r + 1$, *for* $r \in \mathbb{N}$.

Proof. Note first that $q^{n_1+n_2} = q^{n_1}q^{n_2} \equiv 1 \cdot 1 \equiv 1 \pmod e$. Then observe that the F-algebra $F[x_1, \ldots, x_{n_1}, x_{n_1+1}, \ldots, x_{n_1+n_2}]$ contains the subalgebras $F[x_1, \ldots, x_{n_1}]$ and $F[x_{n_1+1}, \ldots, x_{n_1+n_2}]$. We consider $A(q, n_1, e)$ as a subalgebra of $F[x_1, \ldots, x_{n_1}]$, as usual, and $A(q, n_2, e)$ as a subalgebra of $F[x_{n_1+1}, \ldots, x_{n_1+n_2}]$, via a shift of indices. Then $A(q, n_1, e)$ and $A(q, n_2, e)$ become subalgebras of $A(q, n_1 + n_2, e)$; this is obvious for $A(q, n_1, e)$, and if a monomial $x_{n_1+1}^{i_1} \ldots x_{n_1+n_2}^{i_{n_2}}$ satisfies

$$i_1 + qi_2 + \ldots + q^{n_2-1}i_{n_2} \equiv 0 \pmod e$$

then also $q^{n_1}i_1 + q^{n_1+1}i_2 + \ldots + q^{n_1+n_2-1}i_{n_2} \equiv 0 \pmod e$.

For $j = 1, 2$, let $t_j := \mathrm{LL}(A(q, n_j, e)) - 1$, and let y_j be a nonzero product of t_j basis elements in $\mathrm{J}(A(q, n_j, e))$. Then y_1y_2 is a nonzero product of t_1t_2 basis elements in $\mathrm{J}(A(q, n_1 + n_2, e))$. Thus $\mathrm{LL}(A(q, n_1 + n_2, e)) > t_1 + t_2$ which implies the first inequality in Proposition 3.1. The second inequality follows by induction on r. □

We obtain the following consequence.

Corollary 3.2. *For $i = 1, 2$, let $n_i \in \mathbb{N}$ such that $e \mid q^{n_i} - 1$. Moreover, suppose that $\mathrm{LL}(A(q, n_i, e)) = \lfloor n_i \frac{q-1}{m} \rfloor + 1$ for $i = 1, 2$ where $m = m(q, e)$. If $m \mid n_1(q - 1)$ then $\mathrm{LL}(A(q, n_1 + n_2, e)) = \lfloor (n_1 + n_2)\frac{q-1}{m} \rfloor + 1$.*

Proof. By Proposition 3.1, the hypotheses of Corollary 3.2 imply:

$$\begin{aligned}
\mathrm{LL}(A(q, n_1 + n_2, e)) &\geq \mathrm{LL}(A(q, n_1, e)) + \mathrm{LL}(A(q, n_2, e)) - 1 \\
&= \left\lfloor n_1 \frac{q-1}{m} \right\rfloor + \left\lfloor n_2 \frac{q-1}{m} \right\rfloor + 1 \\
&= \left\lfloor n_1 \frac{q-1}{m} + n_2 \frac{q-1}{m} \right\rfloor + 1 = \left\lfloor (n_1 + n_2)\frac{q-1}{m} \right\rfloor + 1.
\end{aligned}$$

Thus the result follows from [3, Theorem 7.1 (i)]. □

Remark 3.3. Suppose that $m := m(q, e) \mid n(q - 1)$ and e divides $q^n - 1$. Then Corollary 3.2 implies, by induction: If $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$, then we have $\mathrm{LL}(A(q, rn, e)) = \lfloor rn\frac{q-1}{m} \rfloor + 1$, for $r \in \mathbb{N}$.

These results lead to the following reduction:

Proposition 3.4. *Let $q, e \in \mathbb{N}$ such that $q > 1$ and $\gcd(q, e) = 1$. Moreover, let $m := m(q, e)$, and let $N \in \mathbb{N}$ such that $\mathrm{ord}_e(q) \mid N$ and $m \mid N(q - 1)$. If $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ for all $n \in \mathbb{N}$ with $\mathrm{ord}_e(q) \mid n \leq N$ then $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ for all $n \in \mathbb{N}$ with $e \mid q^n - 1$.*

Proof. Suppose that $\mathrm{LL}(A(q,n,e)) = \lfloor n\frac{q-1}{m}\rfloor + 1$ for all $n \in \mathbb{N}$ with $\mathrm{ord}_e(q) \mid n \leq N$. Moreover, let $n \in \mathbb{N}$ with $e \mid q^n - 1$ and $n > N$. Then there are $a, r \in \mathbb{N}$ such that $n = aN + r$ and $1 \leq r \leq N$. Thus $1 \equiv q^n \equiv (q^N)^a q^r \equiv q^r \pmod{e}$. By our assumption and Remark 3.3, this implies that $\mathrm{LL}(A(q,r,e)) = \lfloor r\frac{q-1}{m}\rfloor + 1$ and $\mathrm{LL}(A(q,aN,e)) = \lfloor aN\frac{q-1}{m}\rfloor + 1$. Hence $\mathrm{LL}(A(q,n,e)) = \lfloor (aN+r)\frac{q-1}{m}\rfloor + 1 = \lfloor n\frac{q-1}{m}\rfloor + 1$, by Corollary 3.2. □

It is easy to see that one may take $N := \frac{m}{d}\mathrm{ord}_e(q)$ where $d := \gcd(m, (q-1)\mathrm{ord}_e(q))$, so that $N \mid \frac{m}{e_1}\mathrm{ord}_e(q)$ where $e_1 := \gcd(e, q-1)$.

Proposition 3.5. *Let $q, Q, e \in \mathbb{N}$ such that $\gcd(q,e) = 1 = \gcd(Q,e)$, and suppose that $q+e\mathbb{Z}$ and $Q+e\mathbb{Z}$ generate the same subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$. Let n be a multiple of $\mathrm{ord}_e(q)$ and $1 \leq a < \min\{q,Q\}$. Then $0 \neq (x_1x_2\cdots x_n)^a \in \mathrm{J}(A(q,n,e))$ is a product of k monomials in $\mathrm{J}(A(q,n,e))$ if and only if $0 \neq (x_1x_2\cdots x_n)^a \in \mathrm{J}(A(Q,n,e))$ is a product of k monomials in $\mathrm{J}(A(Q,n,e))$.*

Proof. There is a permutation π of $\{0,1,\ldots,n-1\}$ such that $q^t \equiv Q^{\pi(t)} \pmod{e}$ for $t = 0,1,\ldots,n-1$. For any choice of exponents $a_0, a_1, \ldots, a_{n-1}$ in $\{0,1,\ldots,a\}$, we have

$$x_1^{a_0}x_2^{a_1}\cdots x_n^{a_{n-1}} \in \mathrm{J}(A(Q,n,e)) \text{ if and only if } 0 \equiv \sum_{i=0}^{n-1} a_iQ^i \equiv \sum_{i=0}^{n-1} a_{\pi(i)}q^i \pmod{e},$$

which happens if and only if $x_1^{a_{\pi(0)}}x_2^{a_{\pi(1)}}\cdots x_n^{a_{\pi(n-1)}} \in \mathrm{J}(A(q,n,e))$. Given a factorization of $(x_1x_2\cdots x_n)^a$ into k factors in $\mathrm{J}(A(Q,n,e))$, permuting the exponents of each factor with π yields a factorization into k factors in $\mathrm{J}(A(q,n,e))$. The same argument works in the other direction. □

Remark 3.6. Suppose that we are in the situation of Proposition 3.5, that is, $q + e\mathbb{Z}$ and $Q + e\mathbb{Z}$ generate the same subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$. If $Q = q + ma$, with $m = m(q,e) = m(Q,e)$ and $a \in \mathbb{N}$, then we have

$$\left\lfloor \frac{n(Q-1)}{m} \right\rfloor = \left\lfloor \frac{n(q-1)}{m} \right\rfloor + na.$$

Setting $t = \mathrm{LL}(A(q,n,e)) - 1$, we have $0 \neq (x_1x_2\cdots x_n)^{q-1} \in \mathrm{J}(A(q,n,e))^t$. By Proposition 3.5, this implies

$$0 \neq (y_1\ldots y_n)^{Q-1} = (y_1\ldots y_n)^{q-1}(y_1\ldots y_n)^{ma} \in \mathrm{J}(A(Q,n,e))^t\mathrm{J}(A(Q,n,e))^{na}$$

where we consider $A(Q,n,e)$ as a subalgebra of the F-algebra $F[y_1,\ldots,y_n] = F[Y_1,\ldots,Y_n]/(Y_1^q,\ldots,Y_n^q)$. Thus $\mathrm{LL}(A(Q,n,e)) \geq t+1+na = \mathrm{LL}(A(q,n,e))+na$. This implies: If the upper bound from [3, Theorem 7.1] is attained for $A(q,n,e)$ then it is also attained for $A(Q,n,e)$.

Proposition 3.7. *Let q, n, e, m be as usual, and let $l := \operatorname{lcm}(e, m)$. Then*

$$\mathrm{LL}(A(q+l, n, e)) \geq \frac{nl}{m} + \mathrm{LL}(A(q, n, e)).$$

Thus, if $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ *then* $\mathrm{LL}(A(q+l, n, e)) = \lfloor n\frac{q+l-1}{m} \rfloor + 1$.

Proof. We write the nonzero monomial $x_1^{q+l-1} \ldots x_n^{q+l-1} \in A(q+l, n, e)$ as a product of the two monomials $x_1^{q-1} \ldots x_n^{q-1}$ and $x_1^l \ldots x_n^l$ in $A(q+l, n, e)$. Let $x_1^{i_1} \ldots x_n^{i_n}$ be a monomial of degree $m := m(q, e) = m(q+l, e)$. The product of the n cyclic shifts of $x_1^{i_1} \ldots x_n^{i_n}$ is $x_1^m \ldots x_n^m$, so that $x_1^l \ldots x_n^l = (x_1^m \ldots x_n^m)^{l/m}$ is a product of $\frac{nl}{m}$ monomials in $\mathrm{J}(A(q+l, n, e))$.

In order to distinguish between $A(q, n, e)$ and $A(q+l, n, e)$ we consider $A(q, n, e)$ as a subalgebra of $F[y_1, \ldots, y_n] = F[Y_1, \ldots, Y_n]/(Y_1^q, \ldots, Y_n^q)$. The nonzero monomial $y_1^{q-1} \ldots y_n^{q-1} \in A(q, n, e)$ can be written as a product of $t := \mathrm{LL}(A(q, n, e)) - 1$ monomials in $\mathrm{J}(A(q, n, e))$. Thus the monomial $x_1^{q-1} \ldots x_n^{q-1} \in A(q+l, n, e)$ can be written as a product of the corresponding t monomials in $\mathrm{J}(A(q+l, n, e))$; note that

$$j_1 + (q+l)j_2 + \ldots + (q+l)^{n-1}j_n \equiv j_1 + qj_2 + \ldots + q^{n-1}j_n \pmod{e}$$

for $j_1, \ldots, j_n \in \mathbb{Z}$. Thus $x_1^{q+l-1} \ldots x_n^{q+l-1}$ can be written as a product of $\frac{nl}{m} + t$ monomials in $\mathrm{J}(A(q+l, n, e))$. Hence

$$\mathrm{LL}(A(q+l, n, e)) \geq \frac{nl}{m} + t + 1 = \frac{nl}{m} + \mathrm{LL}(A(q, n, e)).$$

If $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ then this implies

$$\mathrm{LL}(A(q+l, n, e)) \geq \frac{nl}{m} + \left\lfloor n\frac{q-1}{m} \right\rfloor + 1 = \left\lfloor \frac{nl}{m} + n\frac{q-1}{m} \right\rfloor + 1 = \left\lfloor n\frac{q+l-1}{m} \right\rfloor + 1,$$

and the result follows from [3, Theorem 7.1]. □

Remark 3.8. Let $n, e, Q \in \mathbb{N}$ such that $Q \not\equiv 1 \equiv Q^n \pmod{e}$, and let $m := m(Q, e)$. Then, by Proposition 3.7, we have $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ for all $q \in \mathbb{N}$ with $q \equiv Q \pmod{e}$ if and only if $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ for all $q \in \mathbb{N}$ with $q \equiv Q \pmod{e}$ and $q \leq \operatorname{lcm}(e, m)$.

Proposition 3.9. *Let q, n, e be as usual, and let $f \mid e$. Then $A(q, n, e)$ can be viewed as a subalgebra of $A(q, n, f)$; in particular,* $\mathrm{LL}(A(q, n, e)) \leq \mathrm{LL}(A(q, n, f))$.

Proof. By definition, $A(q, n, e)$ is the F-subalgebra of $F[x_1, \ldots, x_n]$ generated by all monomials $x_1^{i_1} \ldots x_n^{i_n}$ such that $i_1 + qi_2 + \ldots + q^{n-1}i_n \equiv 0 \pmod{e}$. (Recall that $x_1^q = \ldots = x_n^q = 0$.) Similarly, $A(q, n, f)$ is the F-subalgebra of $F[x_1, \ldots, x_n]$ generated by all monomials $x_1^{i_1} \ldots x_n^{i_n}$ such that $i_1 + qi_2 + \ldots + q^{n-1}i_n \equiv 0 \pmod{f}$. Thus

$A(q,n,e) \subseteq A(q,n,f)$ and $\mathrm{J}(A(q,n,e)) \subseteq \mathrm{J}(A(q,n,f))$; in particular, $\mathrm{LL}(A(q,n,e)) \leq \mathrm{LL}(A(q,n,f))$. □

Proposition 3.10. *Let q,n,e be as usual, and let $k \in \mathbb{N}$. Then*

$$\mathrm{LL}(A(q,kn,e)) \leq \mathrm{LL}(A(q^k,n,e)).$$

Proof. Note first that both $A(q,kn,e)$ and $A(q^k,n,e)$ have dimension $z+1$ where

$$z := (q^{kn}-1)/e.$$

We set $Q := q^k$ and denote the standard bases of $A(q,kn,e)$ and $A(Q,n,e)$ by $b_0,b_1,\ldots,b_z$ and $B_0,B_1,\ldots,B_z$, respectively. Now let $r,s \in \{0,1,\ldots,z\}$, and consider the Q-adic expansions

$$re = \sum_{t=1}^{n} Q^{t-1} I_t \quad \text{and} \quad se = \sum_{t=1}^{n} Q^{t-1} J_t$$

($I_t, J_t \in \{0,1,\ldots,Q-1\}$ for $t=1,\ldots,n$). Then I_t and J_t have q-adic expansions

$$I_t = \sum_{u=1}^{k} q^{u-1} i_{tu} \quad \text{and} \quad J_t = \sum_{u=1}^{k} q^{u-1} j_{tu}$$

($i_{tu}, j_{tu} \in \{0,1,\ldots,q-1\}$ for $t=1,\ldots,n$ and $u=1,\ldots,k$). Thus the q-adic expansions of re and se are

$$re = \sum_{t=1}^{n}\sum_{u=1}^{k} q^{u-1+k(t-1)} i_{tu} \quad \text{and} \quad se = \sum_{t=1}^{n}\sum_{u=1}^{k} q^{u-1+k(t-1)} j_{tu}.$$

If $b_r b_s \neq 0$ then $i_{tu} + j_{tu} < q$ for all t,u. But then also $I_t + J_t < Q$ for all t, i.e. $B_r B_s \neq 0$. Similarly, $b_{r_1} \cdots b_{r_v} \neq 0$ implies $B_{r_1} \cdots B_{r_v} \neq 0$. This shows that $\mathrm{LL}(A(q,kn,e)) \leq \mathrm{LL}(A(Q,n,e))$. □

Remark 3.11. In general, $A(q,kn,e)$ and $A(q^k,n,e)$ are not isomorphic. Computational experiments show that if they have the same Loewy vector and if $z \leq 10\,000$ holds then mapping the basis vectors b_i to the corresponding basis vectors B_i defines an isomorphism.

Next we improve a little on [3, Theorem 7.1 (ii)].

Proposition 3.12. *Let q,n,e be as usual, and let $\nu := \mathrm{ord}_e(q)$. If $m := m(q,e) \nmid q-1$ then $\mathrm{LL}(A(q,n,e)) \geq n\lfloor \frac{q-1}{m} \rfloor + \frac{n}{\nu} + 1$.*

Proof. Let $r \in \mathbb{N}$ such that $n = \nu r$. Then Proposition 3.1 and [3, Theorem 7.1 (ii)] imply:

$$\mathrm{LL}(A(q,n,e)) \quad \geq \quad r \cdot \mathrm{LL}(A(q,\nu,e)) - r + 1 \geq r\left(\nu \left\lfloor \frac{q-1}{m} \right\rfloor + 2\right) - r + 1$$

$$= \quad n\left\lfloor\frac{q-1}{m}\right\rfloor + r + 1.$$

□

Remark 3.13. If $m = m(q,e) \nmid q-1$ then, by [3, Theorem 7.1] and Proposition 3.12, we have

$$n\left\lfloor\frac{q-1}{m}\right\rfloor + \frac{n}{\nu} + 1 \leq \mathrm{LL}(A(q,n,e)) \leq \left\lfloor n\frac{q-1}{m}\right\rfloor + 1.$$

Let $a, r \in \mathbb{N}_0$ such that $q-1 = am + r$ and $0 \leq r < m$. It is routine to check that the upper and lower bound for $\mathrm{LL}(A(q,n,e))$ coincide if and only if $r < \frac{m}{\nu} + \frac{m}{n}$. Thus in this case we have $\mathrm{LL}(A(q,n,e)) = \lfloor n\frac{q-1}{m}\rfloor + 1$.

Here is an example where $(x_1x_2\cdots x_n)^{q-1}$ can be decomposed into $\lfloor n(q-1)/m\rfloor$ monomials in $\mathrm{J}(A(q,n,e))$ but where no factor of degree m can occur. (There are not very many such examples of dimension up to 10 000, and this is the example of smallest dimension.)

Example 3.14. Let $q = 55$ and $e = (q^n-1)/123 = 680\,763\,722\,688$. Then $n = \mathrm{ord}_e(q) = 8$ and $m = m(q,e) = 126$.

We have $(x_1x_2\cdots x_8)^{18} \in \mathrm{J}(A(q,n,e))$, which implies that $\mathrm{LL}(A(q,n,e)) \geq 4$ holds. Since this is equal to the upper bound $\lfloor n(q-1)/m\rfloor + 1$, we have equality.

The monomials in $\mathrm{J}(A(q,n,e))$ have the degrees (and multiplicities) 126 (8), 144 (1), 198 (32), 216 (40), 234 (32), 288 (1), 306 (8), and 432 (1). Thus monomials of degree larger than 144 cannot occur in a decomposition of $(x_1x_2\cdots x_8)^{q-1}$ into three factors. Hence monomials of degree 126 cannot occur in such a decomposition, either.

This means that no monomial of degree m can occur in a decomposition of $(x_1x_2\cdots x_8)^{q-1}$ into three factors.

Proposition 3.15. *Let $q, q', e, n \in \mathbb{N}$ such that $q > 1$, $e \mid q^n-1$ and $q' \equiv q \pmod{m}$ where $m := m(q,e)$. If $\lfloor n(q'-1)/m\rfloor = 1$ then* $\mathrm{LL}(A(q,n,e)) = \lfloor n(q-1)/m\rfloor + 1$.

Proof. Let $q = q' + am$ for some nonnegative integer a. We have to show that $(x_1x_2\cdots x_n)^{q-1} \in J = \mathrm{J}(A(q,n,e))$ is a product of $\lfloor n(q-1)/m\rfloor = an + 1$ monomials in J. This follows from the facts that $(x_1x_2\cdots x_n)^{am}$ is a product of an monomials in J (take a times the n cyclic shifts of a monomial of degree m) and that $(x_1x_2\cdots x_n)^{q'-1} \in J$. □

Our next result is similar to Remark 3.3.

Lemma 3.16. *Let $q, n, e \in \mathbb{N}$ such that $q > 1$, $e > 1$ and $e \mid q^n - 1$. Moreover, let $m = m(q, e)$, and suppose that $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ and $n(q-1) \equiv 1 \pmod{m}$. Then $\mathrm{LL}(A(q, kn, e)) = \lfloor kn\frac{q-1}{m} \rfloor + 1$ for $k = 1, \ldots, m-1$.*

Proof. Let $a \in \mathbb{N}_0$ such that $n(q-1) = am + 1$, and let $k \in \{1, \ldots, m-1\}$. Then $\lfloor n\frac{q-1}{m} \rfloor = \lfloor \frac{am+1}{m} \rfloor = a$ and $\lfloor kn\frac{q-1}{m} \rfloor = ka$. Since $\mathrm{LL}(A(q, n, e)) = a + 1$, the monomial $(x_1 \ldots x_n)^{q-1}$ can be written as a product of a monomials in $\mathrm{J}(A(q, n, e))$. Thus the monomial $(x_1 \ldots x_{kn})^{q-1}$ can be written as a product of ka monomials in $\mathrm{J}(A(q, kn, e))$. The result follows. □

4. The case that e is a prime power

As before, let $q, n, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^n - 1$. We set $A := A(q, n, e)$, $J := \mathrm{J}(A)$ and $m := m(q, e)$. In this section, we will give several conditions which imply that $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$.

Lemma 4.1. *If $m = m(q, e)$ divides n/r, for some divisor r of n, and e divides $\sum_{i=0}^{m-1} q^{ni/(mr)}$ then $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$.*

Proof. Let $a = n/(mr)$. We have $x_1 x_{a+1} x_{2a+1} \cdots x_{(m-1)a+1} \in \mathrm{J}(A)$ of degree m. The product of a cyclic shifts of this monomial yields $x_1 x_2 \cdots x_{ma} = x_1 x_2 \cdots x_{n/r}$, and r cyclic shifts by n/r positions of this product yield $x_1 x_2 \cdots x_n$. Thus we have found a decomposition of $(x_1 x_2 \cdots x_n)^{q-1}$ into $ar(q-1) = n(q-1)/m$ factors in $\mathrm{J}(A)$. Hence

$$\mathrm{LL}(A) \geq \frac{n(q-1)}{m} + 1 = \left\lfloor \frac{n(q-1)}{m} \right\rfloor + 1 \geq \mathrm{LL}(A).$$

□

We apply this in the proof of our next result.

Proposition 4.2. *If e divides $q^k + 1$ or $q^{2k} + q^k + 1$ for some $k \in \mathbb{N}$ then*

$$\mathrm{LL}(A(q, n, e)) = \left\lfloor n\frac{q-1}{m} \right\rfloor + 1.$$

Proof. Suppose first that $e \mid q^k + 1$ for some $k \in \mathbb{N}$. Then also $e \mid q^{2k} - 1$, and $2 \geq m(q, e)$. Hence the result follows from [3, Lemma 7.1 (iv)].

Now suppose that $e \mid q^{2k} + q^k + 1$ for some $k \in \mathbb{N}$, and set $n = 3k$. Then $e \mid q^n - 1$ and $m(q, e) \leq 3$. By [3, Lemma 7.1 (iv)], we may assume that $m(q, e) = 3$. Since m divides n and e divides $1 + q^k + q^{2k} = \sum_{i=0}^{m-1} q^{ni/m}$, we can apply Lemma 4.1. □

Now we come to the proof of the main result of this section.

Theorem 4.3. *We have* $\mathrm{LL}(A(q,n,e)) = \left\lfloor \frac{n(q-1)}{m(q,e)} \right\rfloor + 1$ *in each of the following cases.*

(i) $e = p^k$ *for an odd prime* p *and* $k \in \mathbb{N}$, *and* $q \equiv 1 \pmod{p}$, *or*
$e = 2p^k$ *for an odd prime* p *and* $k \in \mathbb{N}$, *and* $q \equiv 1 \pmod{2p}$*;*

(ii) e *is a power of an odd Pierpont prime (cf. Remark 2.13);*

(iii) e *is a power of* 2.

Proof.

(i) Proposition 2.10 yields that $m(q,e) = \gcd(e, q-1)$ in this case. Now apply [3, Theorem 7.1 (iii)].

(ii) Let p be the prime that divides e. Apply part (i) in the cases where $q \equiv 1 \pmod{p}$, and Corollary 2.12 and [3, Lemma 7.1] in the cases where $\mathrm{ord}_e(q)$ is even.

In the remaining cases, $\mathrm{ord}_e(q) = 3^c p^l$ with $c > 0$. Set $t := \mathrm{ord}_e(q)/3$ and note that e divides $q^{3t} - 1 = (q^t - 1)(1 + q^t + q^{2t})$. Since $\mathrm{ord}_p(q) = 3^c$ holds, p does not divide $q^t - 1$, thus e divides $1 + q^t + q^{2t}$, and Proposition 4.2 can be applied.

(iii) We follow the proof of Proposition 2.9. Apply [3, Theorem 7.1 (iii)] if $q \equiv 1 \pmod{4}$, and [3, Lemma 7.1] if $q \equiv -1 \pmod{e}$.

In all other cases, we have $m(q,e) = 4$, $e = 2^k$ for some $k \in \mathbb{N}$, and $q \equiv -5^{2^r a} \pmod{e}$ for some $r \in \{0, 1, \ldots, k-2\}$ and some odd $a \in \mathbb{N}$. Let $Q \equiv -5^{2^r} \pmod{e}$. The proof of Proposition 2.9 (iii) shows that e divides $2Q^c + Q^d + 1$, for suitable $c, d \in \{0, 1, \ldots, \mathrm{ord}_e(q) - 1\}$, where c is odd and d is even. Since $\langle q + e\mathbb{Z} \rangle = \langle Q + e\mathbb{Z} \rangle$, there is an odd $t \in \mathbb{Z}$ with $q^t \equiv Q \pmod{e}$, which implies that e divides $2q^{ct} + q^{dt} + 1$. Note that ct is odd and dt is even. Thus the $n/2$ cyclic shifts of $x_1 x_{dt+1} x_{ct+1}^2$ by an even number of positions yield a decomposition of $(x_1 x_2 \cdots x_n)^2$ into monomials of degree $m(q,e)$ in $\mathrm{J}(A(q,n,e))$.

□

5. The case that e divides $(q^n - 1)/(q-1)$

We keep the notation of the preceding sections.

Proposition 5.1. *Let* e *be a divisor of* $\frac{q^n-1}{q-1}$ *(so that* $m = m(q,e) \leq n$ *by* [3, Lemma 6.2]*). Then* $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$ *holds in the following cases.*

(i) $n - m \mid \lfloor (n-m)\frac{q-1}{m} \rfloor$,

(ii) $m \geq n - 1$,

(iii) $m = n - 2$ *and* $q \equiv a \pmod{m}$ *for some* $a \in \{1, \dots, \lfloor \frac{m+1}{2} \rfloor\}$.

Proof. (i) We set $k := \lfloor (n-m)\frac{q-1}{m} \rfloor / (n-m)$ if $n > m$, and $k := 0$ if $n = m$. Then $0 \leq k \leq \frac{q-1}{m}$. Let $x_1^{i_1} \dots x_n^{i_n}$ be a monomial of degree m in A. The product of the n cyclic shifts of $x_1^{i_1} \dots x_n^{i_n}$ is $x_1^m \dots x_n^m$, and the k-th power of this monomial is $x_1^{km} \dots x_n^{km}$. We multiply this with the $(q-1-km)$-th power of the monomial $x_1 \dots x_n \in A$ to obtain the nonzero monomial $x_1^{q-1} \dots x_n^{q-1} \in A$, a product of

$$kn + q - 1 - km = q - 1 + k(n-m) = \left\lfloor n \frac{q-1}{m} \right\rfloor$$

monomials in $\mathrm{J}(A)$. Thus $\mathrm{LL}(A) \geq \lfloor n\frac{q-1}{m} \rfloor + 1$, and the result follows from [3, Theorem 7.1].

(ii) This is an immediate consequence of (i).

(iii) We write $q = a + cm$ for some $c \in \mathbb{N}_0$. Then

$$\left\lfloor (n-m)\frac{q-1}{m} \right\rfloor = \left\lfloor 2\frac{a-1+cm}{m} \right\rfloor = 2c + \left\lfloor 2\frac{a-1}{m} \right\rfloor = 2c$$

is divisible by $2 = n - m$. Thus the result follows again from (i). □

Lemma 5.2. (i) *Let* $q, e, k \in \mathbb{N}$ *such that* $\gcd(q,e) = 1$ *and* $k < q$. *Moreover, let* $n = \mathrm{ord}_e(q)$, *and let* N *be a multiple of* n. *Then the monomial* $(x_1 x_2 \cdots x_N)^k \in J = \mathrm{J}(A(q,N,e))$ *is a product of* M *monomials* $m_1, m_2, \dots, m_M \in J$ *if and only if the monomial* $(Y_1 Y_2 \cdots Y_n)^{kN/n}$ *in the polynomial ring* $F[Y_1, \dots, Y_n]$ *is a product of* M *monomials* $p_1, p_2, \dots, p_M$ *with the property that* $p_i = Y_1^{c_{i,1}} \cdots Y_n^{c_{i,n}}$ *such that* $\sum_{j=1}^n c_{i,j} q^{j-1} \equiv 0 \pmod{e}$ *holds for* $1 \leq i \leq M$. *Furthermore, the factors may be chosen such that the total degrees of* m_i *and* p_i *are equal, for* $1 \leq i \leq M$.

(ii) *Let* $q, e \in \mathbb{N}$ *such that* $q > 1$ *and* $\gcd(q,e) = 1$. *Moreover, let* $n := \mathrm{ord}_e(q)$, $m := m(q,e)$ *and* $m_1 := \gcd(m, q-1)$. *If* N *is a multiple of* $\frac{m}{m_1}n$ *then* $\mathrm{LL}(A(q,N,e)) = N\frac{q-1}{m} + 1$.

Proof. (i) If the factors m_i are given by $m_i = x_1^{a_{i,1}} \cdots x_N^{a_{i,N}}$ then define $p_i = Y_1^{c_{i,1}} \cdots Y_n^{c_{i,n}}$ by setting $c_{i,j} = \sum_{l=0}^{N/n-1} a_{i,j+ln}$.

If the factors p_i are given by $p_i = Y_1^{c_{i,1}} \cdots Y_n^{c_{i,n}}$ then define $m_1, m_2, \dots, m_M$ inductively: For m_1, distribute the exponents $c_{1,1}$ to $x_1, x_{n+1}, \dots, x_{N-n+1}$, $c_{1,2}$ to $x_2, x_{n+2}, \dots, x_{N-n+2}$, etc., such that all values are less than q. Then construct the exponent vector of m_2 by distributing $c_{2,1}, \dots, c_{2,n}$ such that the sum of the exponent vectors of m_1 and m_2 does not exceed $q-1$, and continue in this way.

(ii) It suffices to show that the monomial $(x_1 x_2 \cdots x_N)^{q-1} \in A(q,N,e)$ decomposes into a product of $\frac{N(q-1)}{m}$ factors in $\mathrm{J}(A(q,N,e))$. By part (i), it suffices to show that $(Y_1 Y_2 \cdots Y_n)^{N(q-1)/n}$ decomposes into a product of $\frac{N(q-1)}{m}$ admissible factors. Since m divides $N(q-1)/n$, such a factorization is given by $N(q-1)/(mn)$ times the n cyclic shifts of a monomial of degree m in $A(q,n,e)$. □

Note that Lemma 5.2 (ii) generalizes part of [3, Theorem 7.1].

Proposition 5.3. *If* $e \mid \frac{q^d-1}{q-1}$ *for some* $d \in \{2,3,4\}$ *then* $\mathrm{LL}(A(q,n,e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$.

Proof. If $e \mid q+1$ then the assertion follows from [3, Lemma 7.1].

If $e \mid q^2+q+1$ then the assertion is a special case of Proposition 4.2.

Finally, suppose that $e \mid q^3+q^2+q+1$. Since $e \mid q^4-1$ and $e \mid q^n-1$, we also have $e \mid q^g-1$ where $g := \gcd(4,n)$.

If $g=1$ then $e \mid q-1$, and there is nothing to prove.

If $g=2$ then $e \mid \gcd(q^2-1, q^3+q^2+q+1) \mid 2q+2$. Suppose first that e is odd. Then $e \mid q+1$, so that $m \leq 2$, and the result follows. Suppose therefore that e is even. Then q is odd. Moreover, $e_1 = \gcd(e, q-1)$ and m are even. Since $m \leq 4$ we may assume that $m=4$. Then $x_1^2x_2^2 \in J := \mathrm{J}(A(q,n,e))$. Since n is also even we can write $x_1^{q-1}\dots x_n^{q-1}$ as a product of $\frac{n}{2}\frac{q-1}{2}$ shifts of the monomial $x_1^2x_2^2$. The result follows in this case.

This leaves the case $g=4$. If $m=4$ then $x_1x_2x_3x_4 \in J$, and we can write $x_1^{q-1}\dots x_n^{q-1}$ as a product of $x_1x_2x_3x_4$ and its cyclic shifts since $4 \mid n$. The result follows in this case.

Thus we may assume that $m=3$. In this case, J contains one of the following monomials:

$$x_1^3, x_1^2x_2, x_1^2x_3, x_1^2x_4, x_1x_2x_3, x_1x_2x_4, x_1x_3x_4.$$

In the first case, we have $e=3$, and the result follows from Table 1 and [3, Lemma 7.1 (iv)]. In the next three cases, we have

$$\begin{aligned} e &\mid \gcd(q^3+q^2+q+1, q+2) \mid 5, \\ e &\mid \gcd(q^3+q^2+q+1, q^2+2) \mid 3, \\ e &\mid \gcd(q^3+q^2+q+1, q^3+2) \mid 5, \end{aligned}$$

and we know that the claimed result holds. In the last three cases, e divides $1+q+q^2$, $1+q+q^3$ or $1+q^2+q^3$. Since also $e \mid 1+q+q^2+q^3$ we obtain $e=1$, and the result holds trivially. □

As before, for $d \in \mathbb{N}$, we denote by $\Phi_d \in \mathbb{Q}[X]$ the d-th cyclotomic polynomial.

Remark 5.4. Proposition 4.2 implies:

If $e \mid \Phi_d(q)$ for some $d \in \{6,9,10\}$ or for a 2-power d then $\mathrm{LL}(A(q,n,e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$.

Our next result extends Proposition 5.3 to the case $d = 5$. First we deal with a special case.

Example 5.5. Let $e = 11$. We show the equality $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m(q,e)}\rfloor + 1 \quad (*)$.

If $q \equiv k \pmod{e}$ with $k \notin \{3, 4, 5, 9\}$ then we are done by [3, Remark 7.1] and [3, Lemma 7.1], so we can assume $k \in \{3, 4, 5, 9\}$. Then $m = 3$ and $\mathrm{ord}_e(q) = 5$. We apply Proposition 3.4 with $N = 15$. Thus it suffices to prove $(*)$ for $n \in \{5, 10, 15\}$. By Lemma 5.2 (ii), $(*)$ holds for $n = 15$. Thus we may assume $n \in \{5, 10\}$.

By Remark 3.8, it suffices to prove $(*)$ for $q \leq \mathrm{lcm}(e, m) = 33$. For two such values of q that differ by a multiple of m, only the smaller one has to be verified, by Remark 3.6. Thus we may assume that $q \in \{3, 4, 5\}$. If $q = 4$ then $m \mid q - 1$, so that $(*)$ holds by [3, Theorem 7.1 (iii)].

Suppose that $n = 5$. If $q = 5$ then $(*)$ holds by Proposition 3.15. If $q = 3$ then $x_1^2 \ldots x_5^2$ is the product of the 3 monomials $x_1^2x_3$, $x_2^2x_4$ and $x_3x_4x_5^2$ in $\mathrm{J}(A(3, 5, 11))$. Thus $(*)$ holds in this case. Hence we may now assume that $n = 10$ and $q \in \{3, 5\}$.

If $q = 3$ then $x_1^2 \ldots x_{10}^2$ is the product of the 6 monomials $x_1^2x_3$, $x_2^2x_4$, $x_3x_4x_5^2$, $x_6^2x_8$, $x_7^2x_9$, $x_8x_9x_{10}^2$ in $\mathrm{J}(A(3, 10, 11))$. Thus $\mathrm{LL}(A(3, 10, 11)) > 6 = \lfloor 10\frac{2}{3}\rfloor$.

If $q = 5$ then $x_1^3 \ldots x_{10}^3$ is the product of the 10 cyclic shifts of a monomial of degree $m = 3$ in $J := \mathrm{J}(A(5, 10, 11))$, and $x_1 \ldots x_{10}$ is the product of the 3 monomials $x_1x_5x_6$, $x_3x_7x_8$ and $x_2x_4x_9x_{10}$ in J. Thus $x_1^4 \ldots x_{10}^4$ is a product of 13 monomials in J. Hence $\mathrm{LL}(A(5, 10, 11)) > 13 = \lfloor 10\frac{4}{3}\rfloor$.

Proposition 5.6. *If e divides $\Phi_d(q)$ for some $d \in \{1, 2, 3, 4, 5\}$ then*

$$\mathrm{LL}(A(q, n, e)) = \left\lfloor n\frac{q-1}{m}\right\rfloor + 1.$$

Proof. By Proposition 5.3, we may assume that $d = 5$. Since $e \mid \Phi_5(q) = \frac{q^5-1}{q-1}$, [3, Lemma 6.2] implies that $m \leq 5$. By [3, Lemma 7.1 (iv)], we may also assume that $m \geq 3$, i.e. $m \in \{3, 4, 5\}$. Moreover, by [3, Theorem 7.1], we may assume that $q \not\equiv 1 \pmod{m}$. Furthermore, by [3, Remark 7.1], we may assume that $q \not\equiv 1 \pmod{e}$. Since $q^5 - 1 = (q - 1)\Phi_5(q) \equiv 0 \pmod{e}$ this implies that $\nu := \mathrm{ord}_e(q) = 5$; in particular, we have $5 \mid n$. Now we discuss the three possibilities for m separately.

(i) Suppose first that $m = 5$. Since $e_1 := \gcd(e, q-1) \mid m = 5$ by [3, Lemma 6.2], this implies $e_1 \in \{1, 5\}$. Since the assumption $e_1 = 5$ would lead to the contradiction $m = 5 = e_1 \mid q - 1$ we must have $e_1 = 1$. Then $\mathrm{LL}(A(q, 5, e)) = \lfloor 5\frac{q-1}{m}\rfloor + 1$ by [3, Theorem 7.1 (iii)]. But then Remark 3.3 implies that $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m}\rfloor + 1$ whenever $5 \mid n \in \mathbb{N}$.

(ii) Suppose next that $m = 3$. Then $e = 11$ by Example 2.26. By Example 5.5, the result follows in this case.

(iii) Thus we are left with the case $m = 4$. Then $e = 61$ by Example 2.26. Thus $\mathrm{ord}_e(q) = 5$ implies that $q \equiv a \pmod{61}$ for some $a \in \{9, 20, 34, 58\}$ (cf. Table 3). By Remark 3.8, we may assume that $q = a + 61k$ for some $k \in \{0, 1, 2, 3\}$. By Proposition 3.4, we may also assume that $n \in \{5, 10, 15, 20\}$.

If $n = 5$ then Proposition 5.1 implies the result. If $n = 20$ then the result holds by Remark 3.3. Thus it remains to prove the result for $A(q, 10, 61)$ and $A(q, 15, 61)$.

Our hypothesis $q \not\equiv 1 \pmod{m}$ implies that we can ignore $q \in \{9, 81, 217, 241\}$.

For $q \in \{34, 58, 70, 142\}$ we have $5(q-1) \equiv 1 \pmod 4$. In this case the (known) result for $n = 5$ implies the result for $n = 10$ and $n = 15$, by Proposition 3.1.

Suppose that $q \in \{95, 119, 131, 203\}$. If $n = 10$ then the result follows from Lemma 5.2, and Corollary 3.2 implies the result for $n = 15$.

It remains to deal with the cases $q \in \{20, 156, 180, 192\}$ and $n \in \{10, 15\}$. In these cases we have $q \equiv 0 \pmod 4$ and write

$$x_1^{q-1} \cdots x_n^{q-1} = x_1^{q-4} \cdots x_n^{q-4} \cdot x_1^3 \cdots x_n^3.$$

As usual, we can write $x_1^{q-4} \cdots x_n^{q-4}$ as a product of $n\frac{q-4}{4}$ monomials of degree 4 in A. Thus it suffices to write $x_1^3 \cdots x_{10}^3$ as a product of $\lfloor \frac{30}{4} \rfloor = 7$ monomials in $\mathrm{J}(A)$, and to write $x_1^3 \cdots x_{15}^3$ as a product of $\lfloor \frac{45}{4} \rfloor = 11$ monomials in $\mathrm{J}(A)$. Now the proof of Lemma 5.2 shows that it suffices to write $x_1^6 \cdots x_5^6$ as a product of 7 monomials in $\mathrm{J}(A(q, 5, 61))$, and $x_1^9 \cdots x_5^9$ as a product of 11 monomials in $\mathrm{J}(A(q, 5, 61))$.

Now observe that $x_1^6 \cdots x_5^6 = x_1^4 \cdots x_5^4 \cdot x_1^2 \cdots x_5^2$ where $x_1^4 \cdots x_5^4$ is a product of 5 monomials of degree 4 in $A(q, 5, 61)$, and $x_1^2 \cdots x_5^2$ is a product of 2 monomials of degree 5 in $A(q, 5, 61)$.

Similarly, we have $x_1^9 \cdots x_5^9 = x_1^8 \cdots x_5^8 \cdot x_1 \cdots x_5$ where $x_1^8 \cdots x_5^8$ is a product of 10 monomials of degree $m = 4$ in $A(q, 5, 61)$. This finishes the proof of the proposition. □

Proposition 5.7. *Let n be a prime number. Then there are at most finitely many $e \in \mathbb{N}$ such that $e \mid \Phi_n(q)$ and $\mathrm{LL}(A(q, n, e)) \leq \lfloor n\frac{q-1}{m} \rfloor$ for some $q \in \mathbb{N}$.*

Proof. If $q, e \in \mathbb{N}$ satisfy $q > 1$, $e \mid \Phi_n(q)$ and $m := m(q, e) = n$ then $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ by Proposition 5.1. Thus the result follows from Proposition 2.25. □

For $d = 7$, Example 2.26 gives a list of pairs (m, e).

Lemma 5.8. *Let n be even, and let e be a proper divisor of q^n-1 and a multiple of $q^{\frac{n}{2}}-1$. Then $s_q(ke)=n\frac{q-1}{2}$ for $k=1,\dots,z-1$; in particular, we have $m(q,e)=n\frac{q-1}{2}$ and $\mathrm{LL}(A(q,n,e))=3=n\frac{q-1}{m(q,e)}+1$.*

Proof. Let $r\in\{1,\dots,q^{\frac{n}{2}}\}$, and consider the q-adic expansion $\sum_{i=0}^{\frac{n}{2}-1}a_iq^i$ of $q^{\frac{n}{2}}-r$. Then $\sum_{i=0}^{\frac{n}{2}-1}a_iq^i+\sum_{i=0}^{\frac{n}{2}-1}(q-1-a_i)q^{\frac{n}{2}+i}$ is the q-adic expansion of $r(q^{\frac{n}{2}}-1)$. Thus $s_q(r(q^{\frac{n}{2}}-1))=\frac{n}{2}(q-1)$; in particular, $m(q,e)=\frac{n}{2}(q-1)$ and $\mathrm{LL}(A(q,n,e))\leq\lfloor n\frac{q-1}{m(q,e)}\rfloor+1=3$. Since $e\neq q^n-1$ we conclude that $\mathrm{LL}(A(q,n,e))=3$. □

6. Small values of e

Let $e\in\mathbb{N}$ be fixed. Then Proposition 3.4 and Remark 3.8 imply that, in order to show that

$$\mathrm{LL}(A(q,n,e))=\left\lfloor n\frac{q-1}{m}\right\rfloor+1$$

for all $q,n\in\mathbb{N}$ with $q>1$ and $e\mid q^n-1$ it suffices to check a finite number of pairs (q,n).

Proposition 6.1. *If $e\leq 32$ then $\mathrm{LL}(A)=\lfloor n\frac{q-1}{m}\rfloor+1\quad(*)$.*

Proof. Consider the set of all pairs $(e,q+e\mathbb{Z})$ with $e,q\in\mathbb{N}$, $e\leq 32$ and $\gcd(q,e)=1$. If $q\equiv 1\pmod{e}$ then $(*)$ holds, by [3, Remark 7.1 (viii)]. Thus we can eliminate the corresponding pairs $(e,q+e\mathbb{Z})$. If e is a power of 2 or a power of an odd Pierpont prime then $(*)$ also holds, by Theorem 4.3. Thus we can also remove the corresponding pairs. Similarly, we can eliminate the pairs where $m(q,e)=2$, by [3, Lemma 7.1 (iv)]. Also, by [3, Theorem 7.1 (iii)], we can remove the pairs $(e,q+e\mathbb{Z})$ where $m=e_1:=\gcd(e,q-1)$. If e divides $\Phi_d(q)$ for some $d\in\{1,2,3,4,6,8,9,10\}$, or if e divides q^3+q^2+q+1 or q^4+q^2+1 or q^6+q^3+1 or $q^{10}+q^5+1$ then $(*)$ holds, by the results in Section 4 and Section 5. Hence we can also eliminate these pairs. The case $e=11$ has been treated in Example 5.5. The remaining pairs $(e,q+e\mathbb{Z})$ are given by the following table:

e	14	15	21	22	23
q	$9,11$	4	13	$3,5,9,15$	$2,3,4,6,8,9,12,13,16,18$

e	24	26	28	29	31
q	5	$3,9$	$11,23$	$7,16,20,23,24,25$	$2,4,8,16$

Now consider a pair $(e,q+e\mathbb{Z})$ where $\mathrm{ord}_e(q)\leq 3$ and $m\mid\mathrm{ord}_e(q)(q-1+er)$ for all $r\in\mathbb{N}$. Since $(*)$ holds for $n\leq 3$ by [3, Corollary 7.1], $(*)$ holds for all admissible n, by Proposition 3.4. By this argument, we can eliminate the pairs $(15,4+15\mathbb{Z})$, $(21,13+21\mathbb{Z})$, $(24,5+24\mathbb{Z})$, $(26,3+26\mathbb{Z})$, and $(26,9+26\mathbb{Z})$.

Next consider the pair $(14, 9 + 14\mathbb{Z})$. Then $m = 4$ and $\mathrm{ord}_{14}(9) = 3$. By Remark 3.8, it suffices to prove $(*)$ for $q \leq \mathrm{lcm}(e, m) = 28$, i. e., for $q \in \{9, 23\}$. By [3, Theorem 7.1 (iii)], $(*)$ holds for $q = 9$ since $m \mid q - 1$ in this case. Thus we may assume that $q = 23$. Now, by an application of Proposition 3.4 with $N = 6$, we may assume that $n \in \{3, 6\}$. If $n = 3$ then $(*)$ holds by [3, Corollary 7.1]. Thus we may assume that $n = 6$. But now $(*)$ holds, by Lemma 5.2 (ii).

In a similar way, we can eliminate the pair $(14, 11 + 14\mathbb{Z})$.

Let $e = 22$. In the relevant cases, we have $m = 4$ and $\mathrm{ord}_e(q) = 5$. By Proposition 3.4 (with $N = 10$) we may assume that $n \in \{5, 10\}$. By Remark 3.8, we may also assume that $q \leq \mathrm{lcm}(e, m) = 44$, i. e., $q \in \{3, 5, 9, 15, 25, 27, 31, 37\}$. By [3, Theorem 7.1], we may further assume that $m \nmid q - 1$, i. e., $q \in \{3, 15, 27, 31\}$. Then $m_1 := \gcd(m, q - 1) = 2$. Hence, by Lemma 5.2, we may assume that $n = 5$.

For $q = 3$, we need to write $(x_1 x_2 \ldots x_5)^2$ as a product of 2 monomials in $J := \mathrm{J}(A(q, n, e))$, and $(x_1^2 x_4 x_5)(x_2^2 x_3^2 x_4 x_5)$ is such a decomposition. For $q \in \{15, 27, 31\}$, we need to write $(x_1 x_2 \ldots x_5)^{q-1}$ as a product of $\lfloor 5\frac{q-1}{4} \rfloor = \frac{5q-7}{4}$ monomials in $J := \mathrm{J}(A(q, n, e))$. As usual, we can write $(x_1 x_2 \ldots x_5)^4$ as a product of the 5 cyclic shifts of a monomial of degree 4 in J. Thus we can write $x_1^{q-3} \ldots x_5^{q-3}$ as a product of $5\frac{q-3}{4} = \frac{5q-15}{4}$ monomials of degree 4 in J. Hence it suffices to write $(x_1 x_2 \ldots x_5)^2$ as a product of 2 monomials in J, which can be constructed from the above decomposition for $q = 3$ with the help of Proposition 3.5.

Let $e = 23$. In the relevant cases, we have $m = 3$ and $\mathrm{ord}_e(q) = 11$. We may assume that $2 \leq q < em = 69$ and $n \in \{11, 22\}$. For two such q that differ by a multiple of m, only the smaller one must be verified, thus we have to consider only $q \in \{2, 3, 4\}$. Moreover, we can ignore the case $q = 4$ since then m divides $q - 1$.

- $q = 2$, $n = 11$: Write $x_1 \cdots x_{11} = x_1 x_3 x_7 \cdot x_2 x_4 x_8 \cdot x_5 x_6 x_9 x_{10} x_{11}$.
- $q = 2$, $n = 22$: Write $x_1 \cdots x_{22} = x_1 x_3 x_7 \cdot x_2 x_4 x_8 \cdot x_9 x_{11} x_{15} \cdot x_{10} x_{12} x_{16} \cdot x_5 x_{14} x_{20} \cdot x_{13} x_{17} x_{22} \cdot x_6 x_{18} x_{19} x_{21}$.
- $q = 3$, $n = 11$: A decomposition of $x_1 \cdots x_{22}$ into 7 monomials as for $q = 2$ exists also for $q = 3$, by Proposition 3.5, and can be turned into a decomposition of $(x_1 \cdots x_{11})^2$ into 7 monomials, as in Lemma 5.2 (i).
- $q = 3$, $n = 22$: In this case Lemma 3.16 gives the result.

Let $e = 29$. For the relevant values of q, we have $m(q, e) = 4$ and $\mathrm{ord}_e(q) = 7$, thus all relevant values of q generate the same group of residues modulo e.

It is enough to verify $(*)$ for $2 \leq q < em = 116$ and $n \in \{7, 14, 21\}$. For two such q that differ by a multiple of m, only the smaller one must be verified, thus we have to consider only q congruent to one of $7, 16, 25$ modulo e. This leaves

$q \in \{7, 16, 25, 54\}$ to be considered. Moreover, we can ignore the case $q = 25$ since then m divides $q - 1$.

- For $q = 7$, $n = 7$ is done by decomposing

  $$(x_1x_2\cdots x_7)^3 = (x_1^2x_2x_3)(x_2^2x_3x_4)(x_4^2x_5x_6)(x_5^2x_6x_7)(x_1x_3x_6x_7^2),$$

  which establishes a decomposition of $(x_1x_2\cdots x_7)^6$ into 10 invariant monomials, and $n = 14$ is done by Lemma 5.2. Moreover, $n = 21$ need not be considered by Corollary 3.2.
- Let $q = 16$. For $n = 7$, Proposition 3.5 and the above decomposition of $(x_1x_2\cdots x_7)^3$ for $q = 7$ yield the required decomposition of $(x_1x_2\cdots x_7)^{15}$, using the generic decomposition of $(x_1x_2\cdots x_7)^{12}$ into cyclic shifts of a monomial of minimal degree. The cases $n = 14$ and $n = 21$ follow by Lemma 3.16.
- Let $q = 54$. For $n = 7$, Proposition 3.15 strikes. For $n = 14$, write

  $$(x_1x_2\cdots x_{14})^1 = (x_1x_4x_7x_8)(x_2x_3x_6x_{10})(x_9x_{11}x_5x_{12}x_{13}x_{14}).$$

  For $n = 21$, construct a decomposition of $(x_1x_2\cdots x_7)^3$ into 5 monomials from one for $q = 7$ and $n = 7$, again using Proposition 3.5, and distribute it to $n = 21$ as in Lemma 5.2 (i).

Suppose that $e = 31$. In each case, $m = 5 = \mathrm{ord}_e(q)$. By Remark 3.3, it suffices to prove $(*)$ for $n = 5$. Since $e \mid \frac{q^5-1}{q-1}$, Proposition 5.1 implies $(*)$.

Suppose that $e = 28$ and $q + e\mathbb{Z} \in \{11 + e\mathbb{Z}, 23 + e\mathbb{Z}\}$. Then $m = 4$ and $\mathrm{ord}_e(q) = 6$. Thus, by Remark 3.3, it suffices to prove $(*)$ for $n = 6$. If $q \equiv 11 \pmod{e}$ (resp. $q \equiv 23 \pmod{e}$) then $x_1^2 \dots x_6^2$ is the product of the 3 monomials $x_1^2x_2x_4$, $x_3^2x_4x_6$ and $x_2x_5^2x_6$ (resp. $x_1x_3x_4^2$, $x_3x_5x_6^2$ and $x_1x_2^2x_5$) in $J := \mathrm{J}(A(q, 6, e))$. Thus $x_1^{q-1} \dots x_6^{q-1}$ is the product of $3\frac{q-1}{2}$ elements in J, so that $\mathrm{LL}(A(q, 6, e)) > \lfloor 6\frac{q-1}{m} \rfloor$. □

The following result establishes an infinite series of examples $A(q, n, e)$, with $e = 33$, for which the upper bound on the Loewy length from [3, Theorem 7.1] is not attained.

Proposition 6.2. *Let* $(q, e) = (5, 33)$. *Then* $m = m(q, e) = 3$, *and* $\mathrm{LL}(A(q, n, e)) = \lfloor \frac{(q-1)n}{m} \rfloor + \epsilon$, *where* $\epsilon = 0$ *if* $n \equiv 10 \pmod{30}$, *and* $\epsilon = 1$ *otherwise.*

Proof. We have $\mathrm{ord}_e(q) = 10$, $m = m(q, e) > 2$ because $q^5 \equiv 23 \not\equiv -1 \pmod{e}$, and $2 + q^4 = 627 = 19e$ establishes $m = 3$.

Let $n = 10$. The values $(1 + q^i + q^j) \pmod e$, for $0 \leq i \leq j < n$, are as follows.

	0	1	2	3	4	5	6	7	8	9
0	3	7	27	28	0	25	18	16	6	22
1		11	31	32	4	29	22	20	10	26
2			18	19	24	16	9	7	30	13
3				20	25	17	10	8	31	14
4					30	22	15	13	3	19
5						14	7	5	28	11
6							0	31	21	4
7								29	19	2
8									9	25
9										8

We see that the only possibilities for $1 + q^i + q^j \equiv 0 \pmod e$ are $2 + q^4$ and $1 + 2q^6$. Thus all monomials of degree m in $A = A(q, n, e)$ are $x_1^2 x_5$ and its cyclic shifts.

We show that $(x_1 x_2 \cdots x_n)^{q-1} \in A$ is a product of 12 monomials in A but not a product of 13 such monomials.

A decomposition into 12 factors is given by decomposing $(x_1 x_2 \cdots x_n)^3$ into 10 factors of degree 3 (taking each cyclic shift of $x_1^2 x_5$ with multiplicity one), and then writing $x_1 x_2 \cdots x_{10}$ as a product of $x_1 x_4 x_6 x_7$ (since $1 + q^3 + q^5 + q^6 = 572e$) and $x_2 x_3 x_5 x_8 x_9 x_{10}$.

In any factorization of $(x_1 x_2 \cdots x_n)^{q-1}$, each of the cyclic shifts of $x_1^2 x_5$ can appear with multiplicity at most two. For each monomial $x_i^2 x_{\overline{i+4}}$ with multiplicity two, the monomial $x_{\overline{i+6}}^2 x_i$ cannot appear at all, hence the number of cyclic shifts with multiplicity one is at most $10-2k$. Thus the multiplicity of degree 3 monomials in a factorization is at most $2k+(10-2k) = 10$, which is too small for a factorization into 13 monomials.

Let $n = 20$. We have to decompose $(x_1 \cdots x_{20})^4 \in A = A(q, n, e)$ into 26 monomials in A. For that, decompose $(x_1 \cdots x_{20})^3$ into 20 monomials (take the cyclic shifts of a monomial of degree 3) and decompose $(y_1 \cdots y_{10})^2$ with the following exponent vectors:

$$\begin{gathered}(2,0,0,0,1,0,0,0,0,0),\\(0,2,0,0,0,1,0,0,0,0),\\(0,0,1,0,1,1,0,0,0,1),\\(0,0,0,2,0,0,0,1,0,0),\\(0,0,0,0,0,0,2,1,0,1),\\(0,0,1,0,0,0,0,0,2,0).\end{gathered}$$

For $n = 30$, the maximal decomposition follows from Lemma 5.2.

Applying Corollary 3.2 to the above results yields the claim for $n \equiv 0 \pmod{30}$ and $n \equiv 20 \pmod{30}$.

It remains to compute the Loewy length for $n \equiv 10 \pmod{30}$ and $n > 10$. The above proof for $n = 10$ can be generalized, as follows. Let $n = 30a + 10$, for a nonnegative integer a. We claim that the Loewy length of $A = A(5, n, 33)$ is $40a + 13$. By Proposition 3.1, this value is a lower bound: Take $n_1 = 10, n_2 = 30a$. Thus we have to show that $(x_1 \cdots x_n)^4$ cannot be decomposed into $40a + 13$ factors in A. As in the case $n = 10$, we show that $(y_1 \cdots y_{10})^{4N/n}$ cannot be decomposed into $40a + 13$ allowed monomials. Since $4N = 120a + 40 = (40a + 12) \cdot 3 + 1 \cdot 4$, we would need $40a + 12$ factors of degree 3 for such a factorization. The possible factors of degree 3 are the 10 cyclic shifts of $y_1^2 y_5$, each with multiplicity at most $2N/n = 6a + 2$. Set $k_0 = 4a + 1$. If the multiplicity of a degree 3 monomial $y_i^2 y_{\overline{i+4}}$ as a factor is $k > k_0$ then the multiplicity of the monomial $y^2_{\overline{i+6}} y_i$ is at most $k_1 \leq 4N/n - 2k \geq 0$. Thus

$$k + k_1 \leq 4N/n - k < 4N/n - k_0 = 12a + 4 - (4a + 1) = 8a + 3 \leq 2k_0 + 1,$$

which means $k + k_1 \leq 2k_0$. Thus we can consider the ten cyclic shifts in pairs, and the total number of degree 3 monomials is at most $10k_0 < 40a + 12$. This is too small for a factorization into $40a + 13$ monomials. □

Remark 6.3. Explicit computations show that the Loewy vector of $A(5, 10, 33)$ is

$$(1, 440, 4296, 17770, 42595, 66482, 71186, 53392, 27865, 9710, 2011, 180, 1).$$

Proposition 6.4. *If $m = m(q, e) \geq e/3$ then $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$.*

Proof. As mentioned in the proof of Proposition 2.6, we have $m = e_1 = \gcd(e, q-1)$ in the cases (i)–(iii), and $e \leq 32$ in case (iv). Thus the claim follows from [3, Theorem 7.1] and Proposition 6.1. □

Remark 6.5. Fix $q \in \mathbb{N}$ such that $q > 1$. By [3, Theorem 7.1], we have

$$\mathrm{LL}(A(q, n, e)) \leq \left\lfloor n \frac{q-1}{m(q, e)} \right\rfloor + 1,$$

and equality holds for $n \leq 3$, by [3, Corollary 7.1].

In order to find the smallest n such that some divisor e of $q^n - 1$ exists for which the above inequality is strict, we may proceed as follows.

For increasing values of $n \geq 4$, run through all divisors e of $q^n - 1$. If none of the results from [3] or from this paper implies that equality holds for the triple (q, n, e)

then explicitly compute $\mathrm{LL}(A(q,n,e))$ (for example using [3, Proposition 3.2]) and $m(q,e)$, and check.

Here is the list for $2 \leq q \leq 9$ which includes the algebra $A(5,10,33)$ of Proposition 6.2.

q	min. n	e such that the min. n yields strict inequality
2	20	8 525
3	12	35, 1 168, 7 592
4	10	275
5	10	33
6	13	3 433
7	12	2 241 504, 3 735 840, 23 660 320, 29 139 552, 70 980 960, 133 089 300, and perhaps others
8	12	72 412 515, 278 216 505, 723 362 913, and perhaps others
9	9	247

Note that the “brute force” computation of the Loewy length can be expensive for high dimensional algebras $A(q,n,e)$, i. e., small values of e. We used a combination of programs in GAP [5] and Julia [1] for these computations.

The following result gives more direct information concerning the Loewy length of $A(q,2,e)$. However, it seems to be difficult to prove similar results for $A(q,n,e)$ in case $n \geq 3$.

Corollary 6.6. *Let e be a divisor of q^2-1, and set $e_1 = \gcd(e,q-1)$, $e_2 = \gcd(e,q+1)$, and $A = A(q,2,e)$. Then $\mathrm{LL}(A) = 2\frac{q-1}{e_1}+1$ if $e_1 \geq e_2$ or both e and $\frac{q^2-1}{e}$ are even, and $\mathrm{LL}(A) = \frac{q-1}{e_1}+1$ otherwise.*

Proof. Let $m = m(q,e)$. We know from [3, Corollary 7.1] that $\mathrm{LL}(A) = \lfloor 2\cdot\frac{q-1}{m}\rfloor+1$ in the case $n=2$. Now apply Proposition 2.7. □

7. Small values of z

Now we change our perspective, and focus on $z = (q^n-1)/e$ instead of e. For convenience, we introduce the notation $A[q,n,z]$ and $m[q,n,z]$ for $A(q,n,e)$ and $m(q,e)$, respectively.

Let us fix a number z. Since $z+1$ is the dimension of $A[q,n,z]$, a finite set of parameters (q,n) suffices to cover all $A[q,n,z]$, up to isomorphism.

First we observe that only the smallest possible n has to be considered, which is the multiplicative order $\mathrm{ord}_z(q)$ of q modulo z.

Lemma 7.1. *If z divides q^n-1 and N is a multiple of n then $A[q,n,z] \cong A[q,N,z]$.*

Proof. By [3, Theorem 5.1],

$$\begin{aligned} A[q,N,z] &= A(q,N,(q^N-1)/z) = A(q,N,(q^N-1)/(q^n-1)\cdot(q^n-1)/z) \\ &\cong A(q,n,(q^n-1)/z) = A[q,n,z]. \end{aligned}$$

□

Remark 7.2. Note that the upper bound from [3, Theorem 7.1 (i)] on the Loewy length of $A[q,N,z]$ is attained if and only if it is attained for $A[q,n,z]$, by [3, Remark 7.1 (v)].

Example 7.3. (1) By [3, Corollary 5.1], $A[q,n,z]$ is uniserial if and only if $(q^n-1)/z$ is a multiple of $(q^n-1)/(q-1)$, that is, if $q \equiv 1 \pmod{z}$. In this case, Example 2.29 (i) shows that $s_q(ke) = kn\frac{q-1}{z}$, for $1 \leq k < z$.

(2) Let $q \equiv -1 \pmod{z}$ and $z > 2$. Then n is even, and we may choose $n = 2$, by Lemma 7.1. As in Example 2.29 (ii), we have $s_q(ke) = q-1$, for $1 \leq k < z$. (If we admit larger values of n then we get $s_q(ke) = n(q-1)/2$.) Thus all monomials b_k, with $1 \leq k < z$, have the same degree and therefore belong to the same Loewy layer. In particular, we get $m[q,n,z] = n(q-1)/2$ and $\mathrm{LL}(A[q,n,z]) = 3$, which is equal to the upper bound $\lfloor n(q-1)/m[q,n,z]\rfloor + 1$.

In the above examples, we have seen that the structure of $A[q,n,z]$ depends only on the residue class of q modulo z. The following corollary will show that this holds in general, which means that we have to consider only prime residues q modulo z. (As before, we replace $q = 1$ by $q = z+1$.)

For that, we need a technical lemma that describes, in terms of residues modulo z, whether the product of two basis vectors b_k, b_l in $A[q,n,z]$ is zero.

Lemma 7.4. *In the situation of Proposition 2.27, there is a carry in the addition of the vectors of q-adic coefficients of ke and le if and only if there is an index $i \in \{1,2,\ldots,n\}$ such that $\overline{kq^i}+\overline{lq^i} \geq z$ holds and not all values $\overline{kq^j}+\overline{lq^j}$, $1 \leq j \leq n$, are equal to z.*

Proof. Set $c_{k,i} = \overline{kq^{n-i}}$, for $0 \leq i \leq n$, as in the proof of Proposition 2.27. By this lemma, we know that a carry occurs if and only if

$$\frac{(c_{k,i}+c_{l,i})q - (c_{k,i-1}+c_{l.i-1})}{z} \geq q$$

holds for some $i \in \{1,2,\ldots,n\}$.

In this case we have $(c_{k,i}+c_{l,i})q \geq zq$, and some $c_{k,j}+c_{l,j}$ is different from z because otherwise all coefficients of $ke+le$ would be equal to $q-1$, contradicting the assumption that a carry occurs.

Conversely, assume that not all $c_{k,i}+c_{l,i}$ are equal and that $c_{k,i}+c_{l,i} \geq z$ holds for some i. Then we can choose $i \in \{1,2,\ldots,n\}$ such that $c_{k,i}+c_{l,i} \geq z$ and $c_{k,i-1}+c_{l,i-1} < c_{k,i}+c_{l,i}$. (Start with the largest index i for which $c_{k,i}+c_{l,i}$ is maximal, and decrease i until $c_{k,i-1}+c_{l,i-1} < c_{k,i}+c_{l,i}$ holds. Since $c_{k,0}=c_{k,n}$ and $c_{l,0}=c_{l,n}$, there is a positive index i with the required property.) Thus

$$(c_{k,i}+c_{l,i})q-(c_{k,i-1}+c_{l.i-1}) > (c_{k,i}+c_{l,i})(q-1) \geq z(q-1)$$

holds. The left hand side is divisible by z, hence it is at least zq, which means that there is a carry at i. □

Lemma 7.5. *Let z be a positive integer and let q and Q be two prime residues modulo z that generate the same subgroup of order n, say, in the group of prime residues modulo z. Then $A[q,n,z]$ and $A[Q,n,z]$ are isomorphic.*

In particular, if $q \equiv Q \pmod{z}$ then $A[q,n,z] \cong A[Q,n,z]$.

Proof. We want to show that the two algebras have the same multiplication table with respect to their natural bases. We know that

$$\left\{\overline{kq^i}; 0 \leq i \leq n-1\right\} = \left\{\overline{kQ^i}; 0 \leq i \leq n-1\right\}$$

holds for $1 \leq k < z$, thus there is a permutation π of $\{0,1,\ldots,n-1\}$ such that $q^t \equiv Q^{\pi(t)} \pmod{z}$ for $t=0,\ldots,n-1$. Hence the statement follows from Lemma 7.4: The product of b_k and b_l in $A[q,n,z]$ is zero if and only if there is an $i \in \{1,2,\ldots,n\}$ such that $\overline{kq^i}+\overline{lq^i} \geq z$ holds, and that not all $\overline{kq^i}+\overline{lq^i}$ are equal to z. Since $\overline{kq^i}+\overline{lq^i} = \overline{kQ^{\pi(i)}}+\overline{lQ^{\pi(i)}}$, this condition is satisfied if and only if it is satisfied for Q instead of q, and this holds if and only if the product of b_k and b_l in $A[Q,n,z]$ is zero. □

Remark 7.6. In the situation of Lemma 7.5, Proposition 2.27 yields that the upper bound from [3, Theorem 7.1 (i)] for the Loewy length is the same for $A[q,n,z]$ and $A[Q,n,z]$.

Example 7.7. (1) For $z \in \{2,3,4,6\}$, only the cases $q \equiv \pm 1 \pmod{z}$ occur, which were handled in Example 7.3.

(2) Consider $z=5$. The cases $q \equiv \pm 1 \pmod{z}$ are known, they yield the algebras $A[6,1,5]=A(6,1,1)$ and $A[4,2,5]=A(4,2,3)$. Lemma 7.5 tells

us that we have the isomorphisms

$$\begin{array}{lllllll} A[6,1,5] & \cong & A[11,1,5] & \cong & A[16,1,5] & \cong & \cdots \cong \\ A(6,1,1) & \cong & A(11,1,2) & \cong & A(16,1,3) & \cong & \cdots \end{array}$$

and

$$\begin{array}{lllllll} A[4,2,5] & \cong & A[9,2,5] & \cong & A[14,2,5] & \cong & \cdots \cong \\ A(4,2,3) & \cong & A(9,2,16) & \cong & A(14,2,65) & \cong & \cdots \end{array}$$

and also that the only other cases are

$$\begin{array}{lllllll} A[2,4,5] & \cong & A[7,4,5] & \cong & A[12,4,5] & \cong & \cdots \cong \\ A(2,4,3) & \cong & A(7,4,480) & \cong & A(12,4,4147) & \cong & \cdots \end{array}$$

and

$$\begin{array}{lllllll} A[3,4,5] & \cong & A[8,4,5] & \cong & A[13,4,5] & \cong & \cdots \cong \\ A(3,4,16) & \cong & A(8,4,819) & \cong & A(13,4,5712) & \cong & \cdots \end{array}$$

By Lemma 7.5, the latter two algebras, $A[2,4,5]$ and $A[3,4,5]$, are isomorphic, and have Loewy length 3. Note that $s_q(ke) = \frac{q-1}{z}\sum_{i=1}^{4}\overline{kq^i}$, and $\{\overline{kq^i}; 1 \leq i \leq 4\} = \{1,2,3,4\}$ is the set of all prime residues modulo z, for any $k \in \{1,2,3,4\}$; thus $s_q(ke) = 2(q-1)$.

(3) Consider $z = 7$. The cases $q \equiv \pm 1 \pmod{z}$ are known. The same arguments as in the case $z = 5$ show that $q \in \{3,5\}$ yields two isomorphic algebras $A[q,n,7]$ of Loewy length 3, because the sum of all prime residues modulo z appears in the formula for $s_q(ke)$.

The remaining cases are $q \equiv 2 \pmod{z}$ and $q \equiv 4 \pmod{z}$. Here the situation is different. We choose $n = \mathrm{ord}_z(q) = 3$ and compute $c_{k,i}$ and $a_{k,i}$; the rows in the following tables are indexed by k and the columns by i.

(We know that it is sufficient to consider $q \in \{2,4\}$, and that the two values yield isomorphic algebras, but here we show the general case.)

$q \equiv 2 \pmod{z}$:

$c_{k,i}$	0	1	2	3
1	1	4	2	1
2	2	1	4	2
3	3	5	6	3
4	4	2	1	4
5	5	6	3	5
6	6	3	5	6

$za_{k,i}$	1	2	3
1	$4q-1$	$2q-4$	$q-2$
2	$q-2$	$4q-1$	$2q-1$
3	$5q-3$	$6q-5$	$3q-6$
4	$2q-4$	$q-2$	$4q-1$
5	$6q-5$	$3q-6$	$5q-3$
6	$3q-6$	$5q-3$	$6q-5$

$q \equiv 4 \pmod{z}$:

$c_{k,i}$	0	1	2	3	$za_{k,i}$	1	2	3
1	1	2	4	1	1	$2q-1$	$4q-1$	$q-4$
2	2	4	1	2	2	$4q-2$	$q-4$	$2q-1$
3	3	6	5	3	3	$6q-3$	$5q-6$	$3q-5$
4	4	1	2	4	4	$q-4$	$2q-1$	$4q-2$
5	5	3	6	5	5	$3q-5$	$6q-3$	$5q-6$
6	6	5	3	6	6	$5q-6$	$3q-5$	$6q-3$

We see that the following holds in both cases:

The exponent sums of b_1, b_2, b_4 are $q-1$, and the exponent sums of b_3, b_5, b_6 are $2(q-1)$. We have $b_3 = b_1 b_2$, $b_5 = b_1 b_4$, and $b_6 = b_2 b_4$. Since $m[q, 3, z] = q-1$, the upper bound for the Loewy length of $A[q, 3, z]$ is 4, and thus $\mathrm{LL}(A[q, 3, z]) = 4$ holds.

We can generalize an observation from Example 7.7.

Proposition 7.8. *Let z be an odd prime power. If $\mathrm{ord}_z(q) = \varphi(z)$ then we have*

$$\mathrm{LL}(A[q, \varphi(z), z]) = 3.$$

Proof. Apply Remark 2.28 (iii). □

Proposition 7.9. *Let z be an odd prime. If $\mathrm{ord}_z(q) = (z-1)/2$ then*

$$\mathrm{LL}(A[q, (z-1)/2, z]) = \begin{cases} 4, & \textit{if } z \in \{3, 7\} \\ 3, & \textit{otherwise} \end{cases}$$

Proof. In the case $z \equiv 1 \pmod 4$, Remark 2.28 (iii) yields $\mathrm{LL}(A[q, (z-1)/2, z]) = 3$, so assume $z \equiv -1 \pmod 4$. By Proposition 2.30, exactly two different values occur for $s_q(ke)$, $1 \le k \le z-1$. Thus $\mathrm{LL}(A[q, (z-1)/2, z]) \in \{3, 4\}$ holds, and if the value is 4 then $s_q(ke) = 2s_q(e)$ must hold for quadratic nonresidues k modulo z, which means that the sum N, say, of quadratic nonresidues modulo z is twice as large as the sum Q, say, of quadratic residues modulo z. This holds for $z \in \{3, 7\}$, and indeed we have $\mathrm{LL}(A[4, 1, 3]) = \mathrm{LL}(A[2, 3, 7]) = 4$.

The class number formula [4, Chap. 6, equ. (19)] (which has been used in the proof of Proposition 2.30) states that the ideal class number $h(-z)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-z})$ equals $(N-Q)/z$. Since $N + Q = z(z-1)/2$ holds, the condition $N = 2Q$ implies $h(-z) = (z-1)/6$. Hence it suffices to show that this equality cannot hold for primes z with $z \equiv -1 \pmod 4$ and $z > 7$.

For that, note that $h(-z) = \sqrt{z} L(1, \chi)/\pi$ (see [4, Chap. 6, equ. (15)]) for $z > 3$, where χ is a primitive Dirichlet character modulo z and $L(1, \chi)$ is the value of the Dirichlet L function for χ at 1. Now [6, Theorem A] (with $N = 0$) states that

$L(1,\chi) \leq 1+\log(\sqrt{z})$, which implies $h(-z) \leq \sqrt{z}(1+\log(\sqrt{z}))/\pi$. It is easy to check that $\sqrt{z}(1+\log(\sqrt{z}))/\pi < (z-1)/6$ holds for $z > 27$, and that $h(-z) \neq (z-1)/6$ for the relevant $z \in \{8, \dots, 27\}$. □

Remark 7.10. In the situation of Proposition 7.8, the upper bound from [3, Theorem 7.1 (i)] is

$$\left\lfloor \frac{n(q-1)}{m[q,n,z]} \right\rfloor + 1 = \left\lfloor \frac{\varphi(z)(q-1)}{\varphi(z)(q-1)/2} \right\rfloor + 1 = 3,$$

hence it is equal to the Loewy length. In the situation of Proposition 7.9, we have $m[q,n,z] = (z-1)(q-1)/4 = n(q-1)/2$ in the case $z \equiv 1 \pmod 4$, $m[q,n,z] = n(q-1)/3$ in the cases $z \in \{3,7\}$; in the remaining cases, we have $m[q,n,z] = (q-1)Q/z$, by the proof of Proposition 2.30, and $N < 2Q$ implies $Q > z(z-1)/6 = zn/3$ and thus $m[q,n,z] > n(q-1)/3$. Together with the obvious inequality $m[q,n,z] \leq n(q-1)/2$, we get that the upper bound is attained in each case.

We can compute, for fixed z, the Loewy length of all $A[q,n,z]$. The smallest value of z for which this Loewy length differs from the upper bound from [3, Theorem 7.1 (i)] is $z = 70$.

Example 7.11. Let $n = 12$, $q = 3$, and $z = 70$; then $e = 7\,592$. The exponent vectors of $b_1, b_2, \dots, b_{z-1}$, up to cyclic shifts, are as follows. We list the value k for which the shown vector belongs to ke, the vector itself, the length of its orbit under cyclic shifts, and $s_q(ke)$.

1	[2, 1, 0, 2, 0, 1, 1, 0, 1, 0, 0, 0]	12	8
2	[1, 0, 1, 1, 1, 2, 2, 0, 2, 0, 0, 0]	12	10
5	[1, 2, 2, 1, 0, 0, 1, 2, 2, 1, 0, 0]	6	12
7	[2, 2, 0, 0, 2, 2, 0, 0, 2, 2, 0, 0]	4	12
10	[2, 1, 2, 0, 1, 0, 2, 1, 2, 0, 1, 0]	6	12
14	[1, 2, 1, 0, 1, 2, 1, 0, 1, 2, 1, 0]	4	12
35	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]	1	12
68	[1, 2, 1, 1, 1, 0, 0, 2, 0, 2, 2, 2]	12	14
69	[0, 1, 2, 0, 2, 1, 1, 2, 1, 2, 2, 2]	12	16

Since $m[q,n,z] = 8$, the upper bound for $\mathrm{LL}(A[q,n,z])$ is $\frac{n(q-1)}{m[q,n,z]} + 1 = 4$. If this bound would be attained then the above vector with coefficient sum 16 would be the sum of two cyclic shifts of the vector with coefficient sum 8. However, no such decomposition is possible, and thus $\mathrm{LL}(A[q,n,z]) = 3$.

The following example shows nonisomorphic algebras $A[q,n,z]$ which have the same Loewy vector.

Example 7.12. (i) The algebras of smallest dimension with this property are $A[3,4,40]$ and $A[19,2,40]$. They have the Loewy vector $(1,10,19,10,1)$, and they can be distinguished as follows. View $A[q,n,z]$ as an algebra over the ring of integers, and let $A[q,n,z]_p$ denote its reduction modulo p. Then $U[q,n,z] := \{x^2; x \in \mathrm{J}(A[q,n,z]_2)\}$ is a subspace of $A[q,n,z]_2$. We have $\dim(U[3,4,40]) = 7$ and $\dim(U[19,2,40]) = 11$.

(ii) The algebras $A[29,6,117]$ and $A[35,6,117]$ both have the Loewy vector $(1,104,12,1)$, and the vector spaces $U[q,n,z]$ defined above have dimension 3.

We compute the cardinality of $\{(x,y); x,y \in A[q,n,z]_2, xy \in U[q,n,z] + \langle b_z \rangle\}$ for the two parameter sets and get $2^{221} \cdot 119$ and $2^{216} \cdot 1069$, respectively.

Checking more examples, we get the following.

Remark 7.13. Using GAP [5], we have computed the Loewy vectors of all $A[q,n,z]$ with $1 \leq z \leq 10\,000$, where q runs over representatives of cyclic subgroups of the group of prime residues modulo z and $n = \mathrm{ord}_z(q)$.

- There are 768 512 such parameter pairs (q,z), the number of pairwise different Loewy vectors is 475 581.
- $\mathrm{LL}(A[q,n,z]) = 3$ occurs in 191 608 cases, and Loewy vectors of the form $(1,k,1,\ldots,1)$ and of length larger than 3 occur in 37 400 cases; here the isomorphism type of $A[q,n,z]$ is determined by the dimension, by [3, Proposition 5.2].
- Moreover, it happens in many cases that mapping corresponding basis vectors b_i of two algebras with equal Loewy vector to each other defines an isomorphism, see Remark 3.11.

  More generally, mapping the basis vectors b_i of one algebra to the basis vectors $b_{\pi(i)}$ of another algebra, for a permutation π, may define an isomorphism.

  Checking for these special kinds of isomorphism reduces the possible number of isomorphism types to at most 481 744. At this stage, we know that at most 5 174 Loewy vectors can belong to more than one isomorphism type.
- Nonisomorphic algebras $A[q,n,z]$ with the same Loewy vector can occur, see Example 7.12.

- Using invariants such as the dimensions of the subspaces $V_{p,k} = \{x \in \mathrm{J}(A[q,n,z]_p); x^{p^k} = 0\}$ in the reduction modulo p, and the dimensions of the ideals $V_{p,k}A[q,n,z]_p$, $J^i + S_j$, and J^iS_j, where $J = \mathrm{J}(A[q,n,z])$ and S_j is the j-th member of the socle series of $A[q,n,z]$, we can show that several of the remaining candidates are nonisomorphic. Note that the subspaces in question have bases consisting of some of the b_i and are thus easy to handle.

  More nonisomorphisms can be shown using other invariants, such as the dimension of the algebra of derivations of suitable subquotients. At this stage, we know that the number of possible isomorphism types is at least 481 069.
- The smallest algebras $A[q,n,z]$ for which we currently do not know whether they are isomorphic are $A[100,3,259]$ and $A[121,3,259]$, they have the Loewy vector $(1,129,129,1)$.

The upper bound from [3, Theorem 7.1] is not attained for 10 721 parameter pairs; some properties of these cases are listed below.

- The only examples of dimension up to 100 are $A[3,12,70]$, $A[5,12,91]$, and $A[8,12,95]$.
- The unique example for $z \leq 10\,000$ where $\mathrm{LL}(A[q,n,z])$ is strictly smaller than $\lfloor \frac{n(q-1)}{m[q,n,z]} \rfloor$ is $A[9,15,5\,551]$. In this case we have $m[q,n,z] = 24$ and $\mathrm{LL}(A[q,n,z]) = 4$.
- The unique example for $z \leq 10\,000$ where the upper bound is not attained and $e = (q^n-1)/z$ is a prime power is $A[3,43,862]$, where $e = 380\,808\,546\,861\,411\,923$ is actually a prime. Note that e divides $(q^n-1)/(q-1)$.
- The unique example of smallest dimension with Loewy length at least 4 is $A[7,12,195]$.
- The smallest value of n is 5, it occurs in 13 cases, the one of smallest dimension is $A[223,5,1\,353]$.
- The smallest value of e is 275, it occurs exactly for $A[4,10,3\,813]$. Note that e divides $(q^n-1)/(q-1)$.

Of course the chosen enumeration may be misleading, since it is based on selecting certain parameter pairs. However, this way we can get at least some measure how good the upper bound from [3, Theorem 7.1 (i)] is.

8. Concluding remarks

The results and examples presented in this paper suggest the following more general problems:

- Given a finite-dimensional algebra A over a field F and a finite group G of automorphisms of A, describe the Loewy structure (in particular, the Loewy length and the Loewy vector) of the fixpoint algebra A^G in terms of the Loewy structure of A, the structure of G and the action of G on A.
- Find a list of numerical invariants which determine the isomorphism type of the algebra $A(q,n,e)$, and describe the Loewy length of $A(q,n,e)$ by an explicit formula in terms of the three parameters q, n, and e.
- Design a fast algorithm in order to test whether two algebras $A(q,n,e)$ and $A(q',n',e')$ are isomorphic or not.
- Give at least easily computable invariants which "often" distinguish between nonisomorphic algebras $A(q,n,e)$ and $A(q',n',e')$; see [2] for examples.
- Give at least necessary and sufficient conditions for when the Loewy length of $A(q,n,e)$ equals $\lfloor n(q-1)/m(q,e)\rfloor + 1$.
- Does this equality always hold in the case $\mathrm{ord}_e(q) = 4$?
- Prove more general properties of our number-theoretic function $m(.,.)$.

Note added in proof

In his bachelor thesis ("Über Summen von Potenzen einer natürlichen Zahl", University of Jena, Jena 2020) Leif Jacob proves the following:

Theorem 8.1. *Let q, e be relatively prime positive integers. Then $m(q,e) \leq \lceil e/\mathrm{ord}_e(q)\rceil$.*

He also obtains:

Proposition 8.2. *Let q, e be positive integers such that $\gcd(q,e) = 1$ and $1 < q < e$.*

(i) *If there are positive integers a, b such that $\gcd(a,b) = 1$, $b < a \leq n$, $q \geq ab$, and $e = a(q-1)/b$ then $m(q,e) = \gcd(e, q-1) \geq e/n$.*

(ii) *If $e > n^4 - 2n^2$ and $m(q,e) \geq e/4$ then, conversely, there are positive integers a, b such that $\gcd(a,b) = 1$, $b < a \leq n$, $q \geq ab$ and $e = a(q-1)/b$.*

In addition, he conjectures that the bound $n^4 - 2n^2$ in (ii) can be replaced by $4n^2 - 4n$. As a consequence, he proves the following result in the special case $n = 4$:

Corollary 8.3. *Let q, e be positive integers such that* $\gcd(q, e) = 1$ *and* $q \not\equiv 1 \pmod{e}$. *Moreover, let b be the positive integer such that* $b \equiv q \pmod{e}$ *and* $1 < b < e$. *Then $m := m(q, e) \geq e/4$ if and only if one of the following holds:*

(i) $b \geq 3, \gcd(2, b) = 1, e = 2(b - 1)$ *(where $m = e/2 = b - 1$);*

(ii) $b \geq 4, \gcd(3, b) = 1, e = 3(b - 1)$ *(where $m = e/3 = b - 1$);*

(iii) $b \geq 5, \gcd(6, b) = 1, e = 3(b - 1)/2$ *(where $m = e/3 = (b - 1)/2$);*

(iv) $b \geq 5, \gcd(2, b) = 1, e = 4(b - 1)$ *(where $m = e/4 = b - 1$);*

(v) $b \geq 7, b \equiv 1 \pmod{6}, e = 4(b - 1)/3$ *(where $m = e/4 = (b - 1)/3$);*

(vi) *the pair (b,e) appears in the following table:*

b	2	2	2	2	3	3	3	3	3	4	4	4	4
e	3	5	7	15	5	7	8	11	16	5	7	11	15
m	2	2	3	4	2	2	4	3	4	2	3	3	6

b	5	5	5	6	6	7	7	8	9	9	11	11
e	7	11	24	7	35	16	48	15	11	14	14	16
m	2	3	8	2	10	4	12	4	3	4	4	4

These results extend some of the facts obtained in Section 2 above.

Acknowledgement. We thank the referees of an earlier version of this paper for several helpful comments.

Table 1. $m(q,e)$ for $e \leq 30$

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1
2		2		2		3		2		2		2		4		2		2		3		3		2		2		2		2
3			2	2		2	4		2	3		3	2		4	2		2	4		4	3		2	6		2	2		3
4				2		3		3		3		2		6		2		3		3		3		2		3		2		4
5					2	2	4	2		3	4	2	2		4	2	2	3		2	4	2	8		2	2	4	2		5
6						2				2		2				2		3				3		5				2		6
7							2	3	2	2	6	2		3	4	2	6	3	4		2	2	6	2	2	3		4	6	7
8								2		2		2		4		2		2		7		3		2		2		2		8
9									2	3		3	4		8	2		3	4		4	3		2	6		4	2		9
10										2		2				2		2		3		2				9		2		10
11											2	2	4	5	4	2	2	3	10	3		2	4	5	2	2	4	2	10	11
12												2				2		2				3		2				2		12
13													2	3	4	2	6	2	4	6	2	3	12	2		3	4	2	6	13
14														2		2		2				2		2		2		2		14
15															2	2		2			4	2			2		14	2		15
16																2		3		3		3		5		3		4		16
17																	2	3	4	2	2	2	8	2	2	2	4	2	4	17
18																		2				3		2				2		18
19																			2	3	2	2	6	2	2	9	2	2	6	19
20																				2		2				2		4		20
21																					2	2		5	2			2		21
22																						2		2		3		2		22
23																							2	2	2	2	4	4	4	23
24																								2				4		24
25																									2	3	4	4		25
26																										2		2		26
27																											2	2		27
28																												2		28
29																													2	29
30																														30

TABLE 2. $m(q, e)$ for $31 \leq e \leq 60$

e	**m** for sets of residues $\neq 1$ mod e
31	**2**: { 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30 }, **3**: { 5, 7, 9, 10, 14, 18, 19, 20, 25, 28 }, **5**: { 2, 4, 8, 16 }
32	**2**: { 31 }, **4**: { 3, 5, 7, 11, 13, 15, 19, 21, 23, 27, 29 }, **8**: { 9, 25 }, **16**: { 17 }
33	**2**: { 2, 8, 17, 29, 32 }, **3**: { 4, 5, 7, 13, 14, 16, 19, 20, 25, 26, 28, 31 }, **6**: { 10 }, **11**: { 23 }
34	**2**: { 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33 }
35	**2**: { 19, 24, 34 }, **3**: { 2, 3, 12, 17, 18, 23, 32, 33 }, **4**: { 4, 9, 13, 27 }, **5**: { 11, 16, 26, 31 }, **7**: { 8, 22, 29 }, **10**: { 6 }
36	**2**: { 11, 23, 35 }, **4**: { 5, 17, 29 }, **6**: { 7, 31 }, **12**: { 13, 25 }, **18**: { 19 }
37	**2**: { 2, 3, 4, 5, 6, 8, 11, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 35, 36 }, **3**: { 7, 9, 10, 12, 16, 26, 33, 34 }
38	**2**: { 3, 13, 15, 21, 27, 29, 31, 33, 37 }, **4**: { 5, 9, 17, 23, 25, 35 }, **6**: { 7, 11 }
39	**2**: { 17, 23, 38 }, **3**: { 2, 4, 7, 10, 11, 16, 19, 20, 22, 28, 29, 32, 35, 37 }, **4**: { 5, 8 }, **6**: { 25, 31, 34 }, **13**: { 14 }
40	**2**: { 39 }, **4**: { 3, 7, 13, 19, 23, 27, 37 }, **8**: { 9, 17, 29, 33 }, **10**: { 11, 31 }, **20**: { 21 }
41	**2**: { 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40 }, **5**: { 10, 16, 18, 37 }
42	**2**: { 5, 17, 41 }, **4**: { 11, 23 }, **6**: { 13, 19, 25, 31, 37 }, **14**: { 29 }
43	**2**: { 2, 3, 5, 7, 8, 12, 18, 19, 20, 22, 26, 27, 28, 29, 30, 32, 33, 34, 37, 39, 42 }, **3**: { 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41 }
44	**2**: { 7, 19, 35, 39, 43 }, **4**: { 3, 5, 9, 13, 15, 17, 21, 25, 27, 29, 31, 37, 41 }, **22**: { 23 }
45	**2**: { 14, 29, 44 }, **3**: { 7, 13, 22, 43 }, **4**: { 2, 8, 17, 23, 32, 38 }, **5**: { 11, 41 }, **6**: { 4, 34 }, **9**: { 19, 28, 37 }, **10**: { 26 }, **15**: { 16, 31 }
46	**2**: { 5, 7, 11, 15, 17, 19, 21, 33, 37, 43, 45 }, **4**: { 3, 9, 13, 25, 27, 29, 31, 35, 39, 41 }
47	**2**: { 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46 }, **3**: { 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42 }
48	**2**: { 47 }, **4**: { 11, 23, 35 }, **6**: { 19, 31, 43 }, **8**: { 5, 29, 41 }, **12**: { 7, 13, 37 }, **16**: { 17 }, **24**: { 25 }
49	**2**: { 3, 5, 6, 10, 12, 13, 17, 19, 20, 24, 26, 27, 31, 33, 34, 38, 40, 41, 45, 47, 48 }, **3**: { 2, 4, 9, 11, 16, 18, 23, 25, 30, 32, 37, 39, 44, 46 }, **7**: { 8, 15, 22, 29, 36, 43 }
50	**2**: { 3, 7, 9, 13, 17, 19, 23, 27, 29, 33, 37, 39, 43, 47, 49 }, **10**: { 11, 21, 31, 41 }
51	**2**: { 50 }, **3**: { 5, 7, 10, 11, 14, 19, 20, 22, 23, 25, 28, 29, 31, 37, 40, 41, 43, 44, 46, 49 }, **4**: { 2, 8, 26, 32, 38, 47 }, **6**: { 4, 13, 16 }, **17**: { 35 }
52	**2**: { 23, 43, 51 }, **4**: { 5, 7, 11, 15, 17, 19, 21, 25, 31, 33, 37, 41, 45, 47, 49 }, **6**: { 3, 35 }, **8**: { 9, 29 }, **26**: { 27 }
53	**2**: { 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 14, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 29, 30, 31, 32, 33, 34, 35, 37, 38, 39, 40, 41, 43, 45, 48, 50, 51, 52 }, **3**: { 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49 }
54	**2**: { 5, 11, 17, 23, 29, 35, 41, 47, 53 }, **6**: { 7, 13, 25, 31, 43, 49 }, **18**: { 19, 37 }
55	**2**: { 19, 24, 29, 39, 54 }, **3**: { 2, 3, 7, 8, 13, 17, 18, 27, 28, 37, 38, 42, 47, 48, 52, 53 }, **4**: { 4, 9, 14, 32, 43, 49 }, **5**: { 6, 16, 26, 31, 36, 41, 46, 51 }, **10**: { 21 }, **11**: { 12, 23, 34 }
56	**2**: { 31, 47, 55 }, **4**: { 3, 5, 11, 19, 23, 27, 37, 39, 45, 51, 53 }, **8**: { 9, 13, 17, 25, 33, 41 }, **14**: { 15, 43 }, **28**: { 29 }
57	**2**: { 2, 8, 14, 29, 32, 41, 50, 53, 56 }, **3**: { 4, 5, 7, 10, 11, 13, 16, 17, 22, 23, 25, 26, 28, 31, 34, 35, 40, 43, 44, 46, 47, 49, 52, 55 }, **6**: { 37 }, **19**: { 20 }
58	**2**: { 3, 5, 9, 11, 13, 15, 17, 19, 21, 27, 31, 33, 35, 37, 39, 41, 43, 47, 51, 55, 57 }, **4**: { 7, 23, 25, 45, 49, 53 }
59	**2**: { 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56, 58 }, **3**: { 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57 }
60	**2**: { 59 }, **4**: { 17, 23, 29, 47, 53 }, **6**: { 7, 19, 43 }, **10**: { 11 }, **12**: { 13, 37, 49 }, **20**: { 41 }, **30**: { 31 }

Table 3. $m(q, e)$ for $61 \leq e \leq 100$

e	**m** for smallest generators of residues $\neq 1 \pmod{e}$
61	**2**: { 2, 3, 4, 8, 11, 14, 21, 60 }, **3**: { 12, 13 }, **4**: { 9 }
62	**2**: { 3, 15, 37, 61 }, **4**: { 7 }, **6**: { 5, 33 }
63	**2**: { 5, 17, 20, 47, 62 }, **3**: { 31 }, **4**: { 44 }, **5**: { 11 }, **6**: { 2, 13, 25, 40 }, **7**: { 29 }, **9**: { 4, 10, 37, 55 }, **14**: { 8 }, **21**: { 22 }
64	**2**: { 63 }, **4**: { 3, 5, 7, 15, 31 }, **8**: { 9 }, **16**: { 17 }, **32**: { 33 }
65	**2**: { 2, 4, 7, 8, 18, 64 }, **3**: { 3 }, **4**: { 12, 17, 19, 34 }, **5**: { 6, 9, 16, 21, 36 }, **10**: { 51 }, **13**: { 14, 27 }
66	**2**: { 17, 65 }, **4**: { 5 }, **6**: { 7, 25, 43 }, **22**: { 23 }
67	**2**: { 2, 3, 30, 66 }, **3**: { 4, 29 }, **4**: { 9 }
68	**2**: { 67 }, **4**: { 3, 5, 9, 13, 15, 33, 47 }, **34**: { 35 }
69	**2**: { 5, 68 }, **3**: { 2, 4, 7 }, **6**: { 22 }, **23**: { 47 }
70	**2**: { 19, 69 }, **4**: { 3, 9, 13, 23 }, **10**: { 11, 31, 41 }, **14**: { 29, 43 }
71	**2**: { 7, 14, 23, 70 }, **3**: { 2 }, **4**: { 20 }, **5**: { 5 }
72	**2**: { 23, 71 }, **4**: { 11, 35 }, **6**: { 7, 43 }, **8**: { 5, 17, 41, 53 }, **12**: { 13 }, **18**: { 19, 55 }, **24**: { 25 }, **36**: { 37 }
73	**2**: { 3, 5, 6, 7, 9, 10, 18, 27, 72 }, **3**: { 2, 8 }
74	**2**: { 3, 5, 11, 23, 31, 73 }, **4**: { 7 }, **6**: { 47 }
75	**2**: { 14, 74 }, **3**: { 13 }, **4**: { 2, 32 }, **5**: { 11 }, **6**: { 4, 7, 49 }, **15**: { 16 }, **25**: { 26 }
76	**2**: { 3, 27, 75 }, **4**: { 5, 13, 23, 37, 65 }, **6**: { 7 }, **8**: { 45 }, **38**: { 39 }
77	**2**: { 6, 10, 17, 76 }, **3**: { 2, 3, 4 }, **4**: { 20, 32 }, **7**: { 8, 15 }, **11**: { 12, 23, 34 }, **14**: { 43 }
78	**2**: { 17, 77 }, **4**: { 5, 11 }, **6**: { 7, 25, 29, 31, 43, 55 }, **26**: { 53 }
79	**2**: { 3, 12, 24, 78 }, **3**: { 2, 23 }, **4**: { 8 }
80	**2**: { 79 }, **4**: { 7, 19, 39, 47, 53 }, **6**: { 43 }, **8**: { 3, 13, 29, 57 }, **10**: { 11, 31, 71 }, **16**: { 9, 17, 49 }, **20**: { 21 }, **40**: { 41 }
81	**2**: { 2, 8, 26, 80 }, **3**: { 4 }, **9**: { 10 }, **27**: { 28 }
82	**2**: { 3, 5, 7, 9, 23, 81 }, **6**: { 37 }
83	**2**: { 2, 82 }, **3**: { 3 }
84	**2**: { 47, 83 }, **4**: { 5, 11, 41, 53 }, **6**: { 19, 55, 67 }, **12**: { 13, 25, 61 }, **14**: { 71 }, **28**: { 29 }, **42**: { 43 }
85	**2**: { 13, 38, 84 }, **3**: { 3, 42 }, **4**: { 2, 4, 9, 12, 14, 33 }, **5**: { 6, 21, 26 }, **10**: { 16 }, **17**: { 18, 69 }
86	**2**: { 3, 7, 27, 85 }, **4**: { 9 }, **6**: { 11, 49 }
87	**2**: { 5, 86 }, **3**: { 2, 4, 10 }, **4**: { 17, 20 }, **6**: { 7, 28, 46 }, **29**: { 59 }
88	**2**: { 7, 87 }, **4**: { 3, 5, 13, 15, 19, 43 }, **8**: { 9, 17, 21, 65 }, **22**: { 23, 67 }, **44**: { 45 }
89	**2**: { 3, 5, 11, 12, 34, 88 }, **4**: { 2 }
90	**2**: { 29, 89 }, **4**: { 17, 23 }, **6**: { 7, 49 }, **10**: { 11, 71 }, **18**: { 19, 37 }, **30**: { 31 }
91	**2**: { 10, 12, 17, 62, 90 }, **3**: { 2, 3, 4, 9, 11, 16, 19, 30, 45, 68 }, **4**: { 5, 6, 18, 25, 34 }, **6**: { 48 }, **7**: { 8, 15, 22, 36 }, **13**: { 27, 40, 53 }, **14**: { 64 }
92	**2**: { 7, 91 }, **4**: { 3, 5, 9, 45 }, **46**: { 47 }
93	**2**: { 11, 23, 26, 92 }, **3**: { 5, 7, 13, 14, 25, 37, 46 }, **5**: { 2 }, **6**: { 4, 61 }, **31**: { 32 }
94	**2**: { 5, 93 }, **4**: { 3 }
95	**2**: { 14, 69, 94 }, **3**: { 2, 7, 17 }, **4**: { 4, 8, 18 }, **5**: { 6, 21, 31 }, **6**: { 49 }, **10**: { 11, 56 }, **19**: { 39, 58 }
96	**2**: { 95 }, **4**: { 11, 23, 47 }, **6**: { 19, 31 }, **8**: { 5, 41 }, **12**: { 7, 13, 79 }, **16**: { 17 }, **24**: { 25 }, **32**: { 65 }, **48**: { 49 }
97	**2**: { 2, 4, 5, 6, 8, 19, 22, 33, 36, 96 }, **3**: { 35 }
98	**2**: { 3, 13, 19, 97 }, **4**: { 9 }, **6**: { 67 }, **14**: { 15 }
99	**2**: { 2, 8, 32, 98 }, **3**: { 4, 5, 7 }, **4**: { 26 }, **6**: { 43 }, **9**: { 19, 37 }, **11**: { 23, 89 }, **18**: { 10 }, **33**: { 34 }
100	**2**: { 19, 99 }, **4**: { 3, 7, 9, 13, 49, 57 }, **10**: { 11 }, **20**: { 21 }, **50**: { 51 }

References

[1] J. Bezanson, A. Edelman, S. Karpinski, and V. B. Shah, *Julia: a fresh approach to numerical computing*, SIAM Review, 59 (2017), 65-98.

[2] T. Breuer, SingerAlg, Loewy lengths of certain algebras, Version 1.0.1, (`http://www.math.rwth-aachen.de/~Thomas.Breuer/singeralg/`), Jan 2021, GAP package.

[3] T. Breuer, L. Héthelyi, E. Horváth, and B. Külshammer, *The Loewy structure of certain fixpoint algebras, Part I*, J. Algebra, 558 (2020), 199-220.

[4] Harold Davenport, Multiplicative Number Theory, Second Edition, Springer-Verlag, New York-Berlin, 1980.

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.0, 2020. (`https://www.gap-system.org`)

[6] S. Louboutin, *Majoration au point* 1 *des fonctions L associées aux caractères de Dirichlet primitifs, ou au caractère d'une extension quadratique d'un corps quadratique imaginaire principal*, J. Reine Angew. Math., 419 (1991), 213-219.

[7] S. Montgomery, Fixed Rings of Finite Automorphism Groups of Associative Rings, Lecture Notes in Math. 818, Springer-Verlag, Berlin, 1980.

[8] J.-P. Serre, A Course in Arithmetic, Springer-Verlag, New York, 1973.

[9] C. Small, *Sums of powers in large finite fields*, Proc. Amer. Math. Soc., 65 (1977), 35-36.

[10] I. N. Stewart, Galois Theory, Fourth Edition, CRC Press, Boca Raton, 2015.

T. Breuer (Corresponding Author)
Lehrstuhl D für Mathematik
RWTH Aachen University
Pontdriesch 14-16
D-52062 Aachen, Germany
e-mail: sam@math.rwth-aachen.de

L. Héthelyi and **E. Horváth**
Department of Algebra
Budapest University of Technology and Economics
Műegyetem rkp. 3-9
H-1111 Budapest, Hungary
e-mails: fobaba@t-online.hu (L. Héthelyi)
he@math.bme.hu (E. Horváth)

B. Külshammer
Institut für Mathematik
Friedrich-Schiller-Universität
D-07737 Jena, Germany
e-mail: kuelshammer@uni-jena.de