Max-Planck-Institut für Mathematik
Bonn

On the discriminator of Lucas sequences. II

by

Matteo Ferrari
Florian Luca
Pieter Moree

Max-Planck-Institut für Mathematik
Preprint Series 2023 (35)

Date of submission: December 21, 2023

On the discriminator of Lucas sequences. II

by

Matteo Ferrari
Florian Luca
Pieter Moree

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Politecnico di Torino
Corso Duca degli Abruzzi 24
10129 Torino
Italy

School of Mathematics
University of the Witwatersrand
P.O. Box Wits 2050
South Africa

MPIM 23-35

ON THE DISCRIMINATOR OF LUCAS SEQUENCES. II

M. FERRARI, F. LUCA AND P. MOREE

Abstract. The family of Shallit sequences consists of the Lucas sequences satisfying the recurrence $U_{n+2}(k) = (4k+2)U_{n+1}(k) - U_n(k)$, with initial values $U_0(k) = 0$ and $U_1(k) = 1$ and with $k \geq 1$ arbitrary. For every fixed k the integers $\{U_n(k)\}_{n\geq 0}$ are distinct, and hence for every $n \geq 1$ there exists a smallest integer $\mathcal{D}_k(n)$, called *discriminator*, such that $U_0(k), U_1(k), \ldots, U_{n-1}(k)$ are pairwise incongruent modulo $\mathcal{D}_k(n)$. In part I it was proved that there exists a constant n_k such that $\mathcal{D}_k(n)$ has a simple characterization for every $n \geq n_k$. Here, we study the values not following this characterization and provide an upper bound for n_k using Matveev's theorem and the Koksma-Erdős-Turán inequality. We completely determine the discriminator $\mathcal{D}_k(n)$ for every $n \geq 1$ and a set of integers k of natural density 68/75. We also correct an omission in the statement of Theorem 3 in part I.

1. Introduction

1.1. **Motivation.** The *discriminator* of a sequence $\mathbf{a} = \{a_n\}_{n\geq 0}$ of distinct integers is the sequence $\{\mathcal{D}_{\mathbf{a}}(n)\}_{n\geq 0}$ with

$$\mathcal{D}_{\mathbf{a}}(n) := \min\{m \geq 1 : a_0, \ldots, a_{n-1} \text{ are pairwise distinct modulo } m\}.$$

In other words, $\mathcal{D}_{\mathbf{a}}(n)$ is the smallest positive integer m that discriminates (tells apart) the integers $a_0, \ldots, a_{n-1}$ on reducing them modulo m.

Note that $n \leq \mathcal{D}_{\mathbf{a}}(n) \leq \max\{a_0, \ldots, a_{n-1}\} - \min\{a_0, \ldots, a_{n-1}\} + 1$. Put

$$\mathcal{D}_{\mathbf{a}} := \{\mathcal{D}_{\mathbf{a}}(n) : n \geq 1\}.$$

The main challenge is to give an easy description or characterization of $\mathcal{D}_{\mathbf{a}}(n)$. Unfortunately for most sequences $\mathbf{a}$ such a characterization does not seem to exist (see part I by Faye, Luca and Moree [4] for references to the earlier literature).

Let $\mathbf{U}(k)$ be the sequence $\{U_n(k)\}_{n\geq 0}$ with $U_0(k) = 0,\ U_1(k) = 1$ and

$$U_{n+2}(k) = (4k+2)U_{n+1}(k) - U_n(k).$$

It has Binet form as in (6) below. In this paper we continue the work of determining the discriminator $\mathcal{D}_{\mathbf{U}(k)}(n)$ (which for brevity we denote by $\mathcal{D}_k(n)$), which was initiated in part I. A typical example is provided in Tab. 1. The project is inspired by conjectures made by Jeffrey Shallit.

n	$D_{16}(n)$	n	$D_{16}(n)$	n	D_{16}	n	$D_{16}(n)$
1	1	$257-272$	$2^4\cdot 17$	$2313-2400$	$2^5\cdot 5^3$	$19653-32768$	2^{15}
2	2	$273-300$	$2^2\cdot 5^3$	$2401-4096$	2^{12}	$32769-34816$	$2^{11}\cdot 17$
$3-4$	2^2	$301-512$	2^9	$4097-4352$	$2^8\cdot 17$	$34817-36992$	$2^7\cdot 17^2$
$5-8$	2^3	$513-544$	$2^5\cdot 17$	$4353-4624$	$2^4\cdot 17^2$	$36993-39304$	$2^3\cdot 17^3$
$9-16$	2^4	$545-578$	$2\cdot 17^2$	$4625-4800$	$2^6\cdot 5^3$	$39305-65536$	2^{16}
$17-32$	2^5	$579-600$	$2^3\cdot 5^3$	$4801-8192$	2^{13}	$65537-69632$	$2^{12}\cdot 17$
$33-34$	$2\cdot 17$	$601-1024$	2^{10}	$8193-8704$	$2^9\cdot 17$	$69633-73984$	$2^8\cdot 17^2$
$35-64$	2^6	$1025-1088$	$2^6\cdot 17$	$8705-9248$	$2^5\cdot 17^2$	$73985-78608$	$2^4\cdot 17^3$
$65-68$	$2^2\cdot 17$	$1089-1156$	$2^2\cdot 17^2$	$9249-9826$	$2\cdot 17^3$	$78609-131072$	2^{17}
$69-128$	2^7	$1157-1200$	$2^4\cdot 5^3$	$9827-16384$	2^{14}	$131073-139264$	$2^{13}\cdot 17$
$129-136$	$2^3\cdot 17$	$1201-2048$	2^{11}	$16385-17408$	$2^{10}\cdot 17$	$139265-147968$	$2^9\cdot 17^2$
$137-150$	$2\cdot 5^3$	$2049-2176$	$2^7\cdot 17$	$17409-18496$	$2^6\cdot 17^2$	$147969-157216$	$2^5\cdot 17^3$
$151-256$	2^8	$2177-2312$	$2^3\cdot 17^2$	$18497-19652$	$2^2\cdot 17^3$	$157217-167042$	$2\cdot 17^4$

Table 1. The discriminator for $k = 16$ and $1 \leq n \leq 167042$

Date: February 5, 2024.

We now recall the two main results from part I.

Theorem 1.

a) *Let s_n be the smallest power of 2 such that $s_n \geq n$. Let t_n be the smallest integer of the form $2^a \cdot 5^b$ satisfying $2^a \cdot 5^b \geq 5n/3$ with $a, b \geq 1$. Then*
$$\mathcal{D}_1(n) = \min\{s_n, t_n\}.$$

b) *Let $e \geq 0$ be the smallest integer such that $2^e \geq n$ and $f \geq 1$ the smallest integer such that $3 \cdot 2^f \geq n$. Then*
$$\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}.$$

The second main result shows that the behavior of the discriminator $\mathcal{D}_k$ with $k > 2$ is very different from that of $\mathcal{D}_1$. It corrects Theorem 3 in part I, where the conditions on k involving $6 \pmod 9$ in the definition of $\mathcal{B}_k$ were erroneously omitted. For details see Sec. 3.

Theorem 2 (Corrected version of Theorem 3 in [4])**.** *Put*
$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\} & \text{if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd},\ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k\} & \text{if } k \equiv 6 \pmod 9, \end{cases}$$
and
$$\mathcal{B}_k = \begin{cases} \{m \text{ even} : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \text{if } k \not\equiv 6 \pmod 9 \text{ and } k \not\equiv 2 \pmod 9; \\ \{m \text{ even},\ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \text{if } k \equiv 6 \pmod 9 \text{ or } k \equiv 2 \pmod 9. \end{cases}$$
Let $k > 2$ be fixed. We have
$$\mathcal{D}_k(n) = n \iff n \in \mathcal{A}_k \cup \mathcal{B}_k. \tag{1}$$
Furthermore,
$$\mathcal{D}_k(n) \leq \min\{m \geq n : m \in \mathcal{A}_k \cup \mathcal{B}_k\}, \tag{2}$$
with equality if the interval $[n, 3n/2)$ contains an integer $m \in \mathcal{A}_k \cup \mathcal{B}_k$. There are at most finitely many n for which in (2) strict inequality holds.

Corollary 1. *Let $k \geq 1$. Then $\mathcal{D}_k(n) \leq \min\{2^b : 2^b \geq n\}$.*

The corollary is rather trivial and can be easily proved directly ([4, Lemma 1]).

In (2) equality is more likely to hold if the set $\mathcal{A}_k \cup \mathcal{B}_k$ contains many elements. This will happen if $k(k+1)$ is divisible by a small odd prime. Related to this the following quantity will play a role.

Definition 1. Let $\alpha > 1$ be a given real number and $p \geq 3$ be an arbitrary prime. We denote by $n_p(\alpha)$ the smallest integer m such that the interval $[n, n\alpha)$ contains an *even* integer of the form $2^a \cdot p^b$ for every integer $n \geq m$. If we drop the evenness requirement, we will write $n_p^o(\alpha)$.

The existence of $n_p(\alpha)$ is guaranteed by [4, Lemma 19]. Note that $n_p^o(\alpha) \leq n_p(\alpha)$. If $n_1, n_2, \ldots$ is an infinite sequence of integers of the required form with $1 < \frac{n_{j+1}}{n_j} < \alpha$ for every $j \geq 1$, then it is easy to see that $n_p^o(\alpha) \leq n_1$ (for further details see Sec. 2.8).

We do not need more than $n_p^o(\alpha)$ and $n_p(\alpha)$, but the same ideas apply to numbers of the form $p^a \cdot q^b$, with p and q distinct primes. If $m_1, m_2, \ldots$ is the ordered sequence of these numbers, then it was shown by Tijdeman [13] that there exist effectively computable constants c_1 and c_2 such that $(\log m_j)^{-c_1} \ll \frac{m_{j+1}}{m_j} - 1 \ll (\log m_j)^{-c_2}$. Later Langevin [7] gave explicit values for c_1 and c_2, which were recently improved by Languasco et al. [8].

Theorem 3 is our main result and gives a complete characterization of $\mathcal{D}_k(n)$ for every $n \geq 1$ and
$$k \not\equiv 2, 6, 7, 12, 17, 18, 22 \pmod{25}, \tag{3}$$
where for brevity we write $k \not\equiv a, b \pmod m$ for $k \not\equiv a \pmod m$ and $k \not\equiv b \pmod m$, and $k \equiv a, b \pmod m$ for $k \equiv a \pmod m$ or $k \equiv b \pmod m$. It sharpens Theorem 2 and will be proved in Sect. 5. The proof strategy is discussed in Sect. 1.3.

Theorem 3. *Let $k \geq 1$ be an arbitrary integer. Let $\mathcal{A}_k$ and $\mathcal{B}_k$ be as in Theorem 2 and define*
$$\mathcal{S}_{k,n} := \{m \in \mathcal{A}_k \cup \mathcal{B}_k : m \geq n\}.$$
Then
$$\mathcal{D}_k(n) = \min \mathcal{S}_{k,n} \text{ if } k \not\equiv 1 \pmod 3.$$

Next suppose that $k \equiv 1 \pmod 3$, $k \not\equiv 2 \pmod 5$ *and* $k \not\equiv 6, 18 \pmod{25}$. *Then*

$$\mathcal{D}_k(n) = \begin{cases} \min \mathcal{S}_{k,n} & \text{if } k \equiv 0, 4 \pmod 5, \\ \min\{\mathcal{S}_{k,n} \cup \{m \ge 5n/3 : m \in \mathcal{B}_{5,k}\}\} & \text{if } k \equiv 1 \pmod 5, \\ \min\{\mathcal{S}_{k,n} \cup \{m \ge 5n/3 : m \in \mathcal{A}_{5,k} \cup \mathcal{B}_{5,k}\}\} & \text{if } k \equiv 3 \pmod 5, \end{cases} \tag{4}$$

with

$$\mathcal{A}_{5,k} := \{m = a \cdot 5^b : a \in \mathcal{A}_k \text{ and } b \ge 1\}, \ \mathcal{B}_{5,k} := \{m = a \cdot 5^b : a \in \mathcal{B}_k \text{ and } b \ge 1\}.$$

If $k \equiv 1, 3 \pmod 5$, $k \not\equiv 6, 18 \pmod{25}$ *and* $k > 1$, *then* $\mathcal{D}_k(n) = \min \mathcal{S}_{k,n}$ *if* $n \ge n_p(\frac{5}{3})$ *for some odd prime divisor* p *of* $k(k+1)$. *If* $k > 1$ *is odd and* p *divides* k, *it suffices to require that* $n \ge n_p^o(\frac{5}{3})$.

Observe that on taking $k = 1$ and $k = 2$ we recover Theorem 1. Theorem 3 shows that the case $k \equiv 1 \pmod 3$ is considerably more subtle than $k \not\equiv 1 \pmod 3$. However, if $k \equiv 1 \pmod 3$ then $\mathcal{A}_k$ and $\mathcal{B}_k$ take the simpler form

$$\mathcal{A}_k = \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\}, \ \mathcal{B}_k = \{m \text{ even} : \text{if } p \mid m, \text{ then } p \mid k(k+1)\}.$$

Further using (3) we deduce that Theorem 3 gives a complete characterization of the discriminator for a set of integers k having density $1 - \frac{1}{3} \cdot \frac{7}{25} = \frac{68}{75}$.

If k is a power of two, then $\mathcal{A}_k \cup \mathcal{B}_k$ only contains 1 as an odd number. It is thus natural to wonder about the parity of $\mathcal{D}_{2^e}(n)$ for $n > 1$. In this direction Theorem 3 leads to the following corollary.

Corollary 2. *If* $n > 1$, $e \ge 0$ *with* $e \not\equiv 4 \pmod{10}$, *then* $\mathcal{D}_{4^e}(n)$ *is even.*

Finally, we observe that the interval $[n, 3n/2)$ in Theorem 2 can often be replaced by a larger one. Theorem 5 gives the details.

1.2. **The exceptional set $\mathcal{F}_k$.** By (1) we know that $\mathcal{A}_k \cup \mathcal{B}_k \subseteq \mathcal{D}_k$. Inequality (2) suggests to consider the *exceptional set*

$$\mathcal{F}_k := \mathcal{D}_k \setminus (\mathcal{A}_k \cup \mathcal{B}_k),$$

that is,

$$\mathcal{D}_k = \mathcal{A}_k \cup \mathcal{B}_k \cup \mathcal{F}_k, \tag{5}$$

with $\mathcal{F}_k$ disjoint from both $\mathcal{A}_k$ and $\mathcal{B}_k$.

Lemma 1. *Let* $k > 1$ *be an integer.*
a) *The set* $\mathcal{F}_k$ *is finite.*
b) *There are infinitely many* k *for which the set* $\mathcal{F}_k$ *is non-empty.*
c) *The cardinality of the set* $\mathcal{F}_k$ *can be larger than any given bound.*

Proof. a) For $k > 2$ this is a direct consequence of Theorem 2 and the definition of $\mathcal{F}_k$. For $k = 2$ it follows from Theorem 1b.
b)+c). The idea is to take $k \equiv 1 \pmod{N!}$ with $N \ge 5$ large enough. Then $\mathcal{D}_k(n) = \mathcal{D}_1(n)$ for $n = 1, \ldots, N$, and thus the values involving 5 will appear (cf. part a) of Theorem 1). As $5 \nmid k(k+1)$, these are not in $\mathcal{A}_k \cup \mathcal{B}_k$, and so they must be in $\mathcal{F}_k$. Since it can be shown that infinitely many values of $\mathcal{D}_1$ are divisible by 5, the proof is completed. □

k	mod 25	$\mathcal{F}_k$ $(a = 125)$	$k(k+1)$	$n_p(5/3)$
16	16	$\{2a, 4a, 8a, 16a, 32a, 64a\}$	$2^4 \cdot \mathbf{17}$	78644
73	23	$\{a, 2a, 4a, 8a, 16a\}$	$2 \cdot \mathbf{37} \cdot 73$	1229
136	11	$\{2a, 4a, 8a, 16a, 32a\}$	$2^3 \cdot \mathbf{17} \cdot 137$	78644
148	23	$\{a, 2a, 4a, 8a\}$	$2^2 \cdot \mathbf{37} \cdot 149$	1229
271	21	$\{2a, 4a, 8a, 16a, 32a, 64a\}$	$2^4 \cdot \mathbf{17} \cdot 271$	78644
283	8	$\{a, 2a, 4a, 8a, 16a, 32a\}$	$2^2 \cdot \mathbf{71} \cdot 283$	4916
313	13	$\{a, 2a\}$	$2 \cdot \mathbf{157} \cdot 313$	154

TABLE 2. Some non-empty exceptional sets $\mathcal{F}_k$

Tab. 2 demonstrates Lemma 1a. Every number appearing in it is of the form $2^b \cdot 5^3$ and explained by Theorem 3 (which covers all the congruence classes mod 25 appearing in the table). The final column gives $n_p(\frac{5}{3})$ for a prime p indicated in bold in the column headed $k(k+1)$. The number $\frac{5}{3}n_p(\frac{5}{3})$ is an upper bound for the largest number in $\mathcal{F}_k$. It is of crucial importance here to choose the right p, if for $k=136$ for example we would choose $p=137$, then we end up with $n_{137}(5/3)=2516583$, whereas for $p=17$ we obtain $n_{17}(5/3)=78644$. The set given in the first row of Tab. 2 is certainly a subset of $\mathcal{F}_{16}$ by Tab. 1.

In Sec. 6 we establish an effective, but unfortunately huge, upper bound for $\max \mathcal{F}_k$.

Theorem 4. *For $k>3$ we have*

$$\max \mathcal{F}_k \le 2^{k^{10^{10}\log\log k}}.$$

1.3. **Outline of the proof of Theorem 3.** For m to be a potential discriminator value its *rank of appearance* $z(m)$ (see Def. 2) has to be large. The idea is now to first identify those values of m. This is the object of Secs. 2.3–2.5, with basic properties of $z(m)$ being recalled in Sec. 2.2.

If m is in $\mathcal{F}_k$, then there is a unique prime power p^e with $p \nmid k(k+1)$ such that p^e exactly divides m. We call p^e a *wild prime power*[1] for k (the smallest one being 125, cf. Tab. 2). The major part of the proof of Theorem 3 consists of showing that $p=5$. This is the content of Theorem 6. The proof idea is to replace a wild prime power by a suitable number of the form $2^a\cdot 5^b$ and thus get a smaller, but still discriminating, number. For this we need to ensure the existence of numbers of the form $2^a\cdot 5^b$ in small enough intervals, a problem in the realm of Diophantine approximation. This is studied in Sec. 2.8 (and in greater generality in Languasco et al. [8]).

Once we know that $p=5$ we are left with a very restricted set of potential discriminator values. The even ones have good discriminating properties, but in general not the odd ones. To weed these further out we use a more refined quantity, *the incongruence index*, which unfortunately is more awkward to work with than $z(m)$. It is studied in Secs. 2.6–2.7, culminating in Lemma 20. The proof of Theorem 3 now follows (in essence) on combining this lemma with Theorem 6.

Remark 1. The congruence classes modulo 25 covered by Theorem 3 are precisely the congruence classes for which $z(25)=15$ (see Tab. 3) or $z(25)=25$.

1.4. **Outline of the proof of Theorem 4.** Let $m\in\mathcal{F}_k$. Write $m=p_1^{e_1}\cdot m_1$, where $p_1\nmid k(k+1)$, $p_1^{e_1}$ exactly divides m, and m_1 consists only of prime factors of $k(k+1)$. We need to bound $p_1^{e_1}$ and m_1. We explain only the case when m_1 is odd as the even case is similar. Let p be any odd prime factor of $k(k+1)$. It follows from uniform distribution theory that there exists u such that

$$\left\{(u+1)\frac{\log 2}{\log p}\right\}\in\left(\frac{\log(4/3)}{\log p},\frac{\log(3/2)}{\log p}\right).$$

This is containment (18). We show by an elementary argument that $p_1^{e_1}<2^{u+1}$. Thus, it suffices to bound u. This we do using the Koksma-Erdős-Turán inequality which bounds the discrepancy of a sequence modulo 1 by an exponential sum involving the distances to nearest integers of the members of our sequence. In our case, the members of our sequence are the multiples of $\log 2/\log p$, so we can bound the distances to the nearest integer using a version of Baker's lower bounds for linear forms in logarithms due to Matveev (Theorem 7). Putting everything together gives a bound on u in terms of p which is exponential in $(\log p)(\log\log p)$ (see Lemma 25). The argument can be iterated. Namely one writes $m_1=\prod_{i=1}^s q_i^{a_i}$, with $q_1,\ldots,q_s$ divisors of $k(k+1)$, and one uses a similar argument to bound the exponents $a_1,\ldots,a_s$. A similar extra step is needed to bound the exponent of 2 in case m_1 is even.

1.5. **Related work on other discriminators.** Apart from the infinite family of recurrence discriminators dealt with here, only one other infinite family has been studied, namely by Ciolan and Moree [1]. Also in this case the associated discriminators $\mathcal{D}$ have the property that $\mathcal{D}(2^b)=2^b$ for every $b\ge 1$. De Clercq and his (many!) coauthors [2] have classified all binary linear recurrences for which the discriminator has this property. It is expected that for all of them a rather simple characterization of the discriminator should be possible. However, very little is known for second order linear recurrences not of this form.

The work of de Clercq et al. [2] was partly generalized by Ferrari [5], who, given any fixed odd prime p, found a large class of binary recurrences $\mathbf{a}$ for which $\mathcal{D}_{\mathbf{a}}(p^k)=p^k$ for every $k\ge 1$.

[1]This terminology is inspired by the novel "The Wild Numbers: a Novel" by Philibert Schogt.

2. Preliminaries

2.1. **Notation.** The characteristic equation of the Shallit recurrence $\mathbf{U}(k)$ is

$$x^2-(4k+2)x+1=0.$$

Its roots are $\alpha(k)$ and $\alpha(k)^{-1}$, where

$$\alpha(k)=2k+1+2\sqrt{k(k+1)},\quad \alpha^{-1}(k)=2k+1-2\sqrt{k(k+1)}.$$

Note that

$$\alpha(k)=\beta^2(k),\quad \text{with}\quad \beta(k)=\sqrt{k+1}+\sqrt{k}.$$

The discriminant of the Shallit sequence is

$$\Delta(k):=(\alpha(k)-\alpha(k)^{-1})^2=16k(k+1),$$

and we easily verify that

$$U_n(k)=\frac{\alpha^n(k)-\alpha^{-n}(k)}{\alpha(k)-\alpha^{-1}(k)}=\frac{\beta^{2n}(k)-\beta^{-2n}(k)}{\beta^2(k)-\beta^{-2}(k)}. \tag{6}$$

Given a prime p, we define

$$e_p(k):=\left(\frac{k(k+1)}{p}\right), \tag{7}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol.

2.2. **The index of appearance.** A crucial role in our considerations is played by the *index of appearance.*

Definition 2 (Index of appearance)**.** Let $k\ge 1$ be fixed. Given m, the smallest $n\ge 1$ such that m divides $U_n(k)$ exists and is called the *index of appearance* of m in $\mathbf{U}(k)$ and is denoted by $z_k(m)$.

For notational convenience we suppress the dependence of $z_k(m)$ on k and, when there is no danger of confusion, we denote it simply by $z(m)$. The following result is trivial, but we will use it time and again.

Lemma 2. *If $m=\mathcal{D}_k(n)$, then $z(m)\ge n$ and $z(m)>m/2$.*

Proof. Since $U_{z(m)}\equiv U_0 \pmod m$ it follows that $z(m)\ge n$. The second assertion we prove by contradiction and so suppose that $z(m)\le m/2$. The interval $[z(m),2z(m))$ contains a power of two, say $z(m)\le 2^b<2z(m)\le m$. Since $2^b\ge z(m)\ge n$, it follows from Corollary 1 that $U_0(k),\ldots,U_{n-1}(k)$ are pairwise distinct modulo 2^b. As $2^b<m$, this contradicts the definition of the discriminator. □

Thus a way to characterize discriminator values would be to first characterize those integers m for which $z(m)>m/2$ (note that in part I we already determined the integers m for which $z(m)=m$, cf. Lemma 13). This we address in Sec. 2.4. The next step is then to investigate the discriminatory properties of these m (see Sec. 2.7).

If p divides $k(k+1)$ we have $z(p)=p$. This follows from the following trivial lemma.

Lemma 3. *If $p\mid k$, then $U_n(k)\equiv n \bmod p$. If $p\mid (k+1)$, then $U_n(k)\equiv(-1)^{n+2}n \bmod p$.*

Corollary 3. *If $p\mid(k+1)$ is odd, then $U_{\frac{p-1}{2}}(k)\equiv U_{\frac{p+1}{2}}(k) \pmod p$ and for $0\le i<j\le(p-1)/2$ we have $U_i(k)\not\equiv U_j(k) \pmod p$.*

2.3. **The index of appearance in prime powers.** The index of appearance in a prime power p^b is related to the multiplicative order of α modulo p^b.

Lemma 4. *Let p be odd such that $e_p(k)=-1$ and let $b\ge 1$ be an integer. Then $z(p^b)$ is the minimal $m\ge 1$ such that $\alpha^m\equiv\pm 1 \pmod{p^b}$.*

Proof. The proof of [4, Lemma 5] applies here verbatim, but with 32 replaced by $\Delta(k)$, and $\mathbb{Z}[\sqrt{2}]$ by $\mathbb{Z}[\sqrt{k(k+1)}]$. □

The following lemma is basic and will be taken for granted in all our arguments involving the index of appearance.

Lemma 5 ([4, Lemma 2])**.** *The index of appearance z of the sequence $\mathbf{U}(k)$ has the following properties.*

(1) *If* $p \mid U_m(k)$, *then* $z(p)|m$;
(2) *If* $p \mid k(k+1)$, *then* $z(p) = p$;
(3) *If* $p \nmid k(k+1)$, *then* $z(p)|p - e_p(k)$;
(4) $z(p^b) = p^{\max\{b-\nu_p(U_{z(p)}(k)),0\}} z(p)$. *In particular,* $z(p^b) \mid p^{b-1}z(p)$;
(5) *If* $n = m_1 \cdots m_s$ *with* $m_1, \ldots, m_s$ *pairwise coprime, then*

$$z(m_1 \cdots m_s) = \operatorname{lcm}[z(m_1), \ldots, z(m_s)].$$

In part 4 we mostly have $z(p^b) = p^{b-1}z(p)$. In order to determine whether there can be exceptions to this, we introduce the notion of *special prime.*

Definition 3 (special prime)**.** A prime p is said to be special if $p \mid k(k+1)$ and $p^2 \mid U_p(k)$.

If p is special, then $z(p^b) \mid p^{b-2}z(p)$ for every $b \geq 2$, otherwise $z(p^b) = p^{b-1}z(p)$. In part I (Lemma 3) it is shown that if p is special, then we must have $p = 3$. It is easy to check that 3 is special if and only if $k \equiv 2 \pmod 9$ or $k \equiv 6 \pmod 9$. If 3 is special and 9 divides m, then $z(m) < m$. This together with Theorem 2 shows that

$$\mathcal{A}_k = \{m \text{ odd} : z(m) = m,\ m \in \mathcal{P}(k)\} \quad \text{and} \quad \mathcal{B}_k = \{m \text{ even} : z(m) = m\}, \tag{8}$$

where

$$\mathcal{P}(k) := \{m \geq 1 : p \mid m \Rightarrow p \mid k\}$$

is the set of positive integers m composed only of prime factors dividing k.

The next lemma is formulated and proved in [4, Sec. 6.2.2], but not stated as a lemma there.

Lemma 6. *Let* $p \nmid k(k+1)$ *and* $b \geq 1$. *Then*

$$z(p^b) \mid p^{b-1}(p - e_p(k))/2; \tag{9}$$

moreover if $p \equiv 3 \pmod 4$ *and we assume*

$$\left(\frac{k+1}{p}\right) = 1 \quad \textit{and} \quad \left(\frac{k}{p}\right) = -1,$$

then

$$z(p^b) \mid p^{b-1}(p+1)/4.$$

The next proposition shows that (9) is sometimes sharp. The various congruence classes of k counted in parts b,c and d are explicitly worked out in Tab. 3 for the primes $3 \leq p \leq 17$ (with a few exceptions where the table margins would be too small).

Proposition 1. *Let* $p \geq 5$ *be a prime not dividing* $k(k+1)$. *Put* $f = \varphi(\frac{p+1}{2})$, *with* φ *Euler's totient function.*

(a) *For* k *there are exactly* f *classes modulo* p *such that* $z_k(p) = (p+1)/2$;
(b) *For* k *there are exactly* f *congruence classes modulo* p^2 *such that* $z_k(p^2) = (p+1)/2$;
(c) *For* k *there are exactly* $(p-1)f$ *congruence classes modulo* p^2 *such that* $z_k(p^2) = p(p+1)/2$;
(d) *For* k *there are exactly* $p - f - 2$ *congruence classes modulo* p *such that* $z_k(p) < (p+1)/2$.

Proof. (a) We observe that if $k(k+1)$ is not a square modulo p, then $\alpha(k) = 2k + 1 + 2\sqrt{k(k+1)}$ is quadratic modulo p. Here, by $\sqrt{\ }$ we mean any fixed determination of the square root. Thus, $\alpha(k) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$, where $\mathbb{F}_{p^2}$ is the unique quadratic field over p with p^2 elements. The Frobenius automorphism sends $\alpha(k)$ into its conjugate $2k + 1 - 2\sqrt{k(k+1)} = \alpha(k)^{-1}$. Hence, $\alpha(k)^p = \alpha(k)^{-1}$ in $\mathbb{F}_{p^2}$, and so $\alpha(k)^{p+1} = 1$ in $\mathbb{F}_{p^2}$. In particular, $\alpha(k)^{(p+1)/2} = \pm 1$ in $\mathbb{F}_{p^2}$. Further, by Lemma 4, $(p+1)/2$ must be the minimal m such that $\alpha(k)^m = \pm 1$ in $\mathbb{F}_{p^2}$. Let ρ be a primitive root modulo p. Write $\alpha(k) = \rho^d$ for some integer d. Then $\alpha(k)^{(p+1)/2} = \pm 1$ implies $\rho^{d(p+1)/2} = \pm 1$. Since ρ is a primitive root, it follows that $p - 1 \mid d$. Thus, $d = (p-1)w$. Since $(p+1)/2$ is minimal such that $\alpha(k)^{(p+1)/2} = \pm 1$, it follows that w is coprime to $(p+1)/2$. But $w \in [0, p+1]$. Each of the intervals $[0, (p+1)/2 - 1]$ and $[(p+1)/2, p+1]$ contains exactly $\phi((p+1)/2)$ numbers of the form w which are coprime to $(p+1)/2$. For each one of these, $\alpha = \rho^{(p-1)w}$ is an element of $\mathbb{F}_{p^2}$. Then, keeping in mind that $\alpha^{p^2-1} = 1$, we see that $\alpha^p = \alpha^{p(p-1)w} = \alpha^{(p-1)(p+1-w)}$ and $p + 1 - w$ is also coprime to $p + 1$. Thus, the $2\phi((p+1)/2)$ numbers get grouped into $\phi((p+1)/2)$ non-overlapping unordered pairs $\{\alpha, \alpha^p\}$. Let $t = \alpha + \alpha^p$. Then $t \in \mathbb{F}_p$ and (α, α^p) are roots of

$$x^2 - tx + 1 = 0.$$

It remains to see that we can choose k such that $4k+2 = t \pmod p$, which is clear since 2 is invertible modulo p. This gives the statement.
(b) If k is such that $z_k(p^2) = (p+1)/2$, then certainly $z_k(p) = (p+1)/2$. Thus, $k \pmod p$ is one of the classes counted at part (a). It remains to prove that each such class can be lifted uniquely to a class modulo p^2 such that $z_k(p^2) = (p+1)/2$. But with a fixed k, putting $x := 2k+1$, we have

$$\begin{aligned} U_1(k) &= 1; \\ U_2(k) &= 2x; \\ U_3(k) &= 4x^2 - 1; \\ U_4(k) &= 8x^3 - 4x; \\ U_{n+2}(k) &= 2xU_{n+1}(k) - U_n(k) \qquad \text{for all} \qquad n \geq 3. \end{aligned}$$

We recognize that $U_n(x)$ is the Chebyshev polynomial $\sin(n\theta)/\sin(\theta)$ as a polynomial in $\cos(\theta)$, which has discriminant $2^{(n-1)^2} n^{n-2}$, cf. Dilcher and Stolarsky [3]. So, for us we have that $x = 2k+1$ is a solution of $U_{(p+1)/2}(x) \equiv 0 \pmod p$, and we would like to extend it to a unique solution of the above congruence modulo p^2. This is possible via Hensel's lemma provided that p does not divide the discriminant of $U_{(p+1)/2}(x)$ as a polynomial, which is the case since this discriminant is $2^{((p-1)/2)^2}((p+1)/2)^{(p-5)/2}$. This proves (b).

(c) is also immediate. By part (a), there are f classes k modulo p for which $z_k(p) = (p+1)/2$. These f classes give pf lifts to classes modulo p^2. Exactly f of them have the property that $z_k(p^2) = (p+1)/2$. Thus, for the remaining $(p-1)f$ classes, it must be the case that $z_k(p^2) = p(p+1)/2$.

(d) is also immediate. There are $p-2$ classes for k modulo p as we need to exclude $k \equiv 0, -1 \pmod p$ for which $k(k+1)$ is a multiple of p. By (a), there are f of them for which $z_k(p) = (p+1)/2$. So there are $p - f - 2$ of them for which $z_k(p) < (p+1)/2$. ☐

Corollary 4. *For every odd prime p there exists at least one congruence class modulo p^2 for k such that $z_k(p^2) = (p+1)/2$ and one such that $z_k(p^2) = p(p+1)/2$.*

p	k	congruence classes	mod
3	b	4	9
	c	1, 7	9
	d	none	3
5	b	6, 18	25
	c	1, 3, 8, 11, 13, 16, 21, 23	25
	d	2	5
7	b	2, 46	49
	c	4, 9, 10, 16, 18, 23, 25, 30, 32, 37, 39, 44	49
	d	1, 3, 5	7
11	b	23, 97	121
	c	$c_1, \ldots, c_{20}$	121
	d	2, 3, 4, 5, 6, 7, 8	11
13	b	1, 8, 49, 119, 160, 167	169
	c	$c_1, \ldots, c_{72}$	169
	d	3, 5, 6, 7, 9	13
17	b	20, 53, 111, 177, 235, 268	289
	c	$c_1, \ldots, c_{196}$	289
	d	1, 4, 5, 6, 8, 10, 11, 12, 15	17

TABLE 3. Congruence classes related to $z_k(p^2)$ (cf. Proposition 1)

Remark 2. For $p \geq 5$ we have $p - \varphi((p+1)/2) - 2 \geq p - (p-1)/2 - 2 \geq (p-3)/2 \geq 1$ and so by Proposition 1 there is at least one congruence class modulo p for k such that $z_k(p) < (p+1)/2$.

Remark 3. Proposition 1 suggests considering Artin primitive root type problems such as whether given k the set of primes p such that $z_k(p) = (p+1)/2$ has a natural density. Likely these questions can be answered assuming the Generalized Riemann Hypothesis. These issues also play a role in understanding the behavior of ρ_k, σ_k and τ_k (see Sec. 2.5.1). We might come back to this in a sequel to this paper.

2.4. **Integers for which the index of appearance** $z(m)$ **satisfies** $z(m) > m/2$**.** In this section we characterize the integers m for which $z(m) > m/2$.

Lemma 7. *If $m/2 < z(m) < m$, then there exists a prime $p \nmid k(k+1)$, such that*

$$z(m) = \frac{m(p+1)}{2p}. \tag{10}$$

Further, $z(p) = (p+1)/2$ and $e_p(k) = -1$. The integer m can be written as $m = a \cdot p^b$ with $a \in \mathcal{P}(k(k+1))$, $z(a) = a$, $(a, p(p+1)/2) = 1$ and $b \geq 1$. If $b \geq 2$, then $z(p^2) = p(p+1)/2$.

Proof. Write $m = a \cdot p_1^{b_1} \cdots p_r^{b_r}$ with $a \in \mathcal{P}(k(k+1))$ and $p_1, \ldots, p_r \nmid k(k+1)$ distinct primes. Note that the p_i are odd primes. We have either $z(a) = a$ or $z(a) = a/3$. In the latter case $z(m) \leq m/3$, and so $z(a) = a$ and hence $r \geq 1$. Assume first that $r \geq 2$. By Lemma 5 we have $z(m) \leq z(a)z(p_1^{b_1}) \cdots z(p_r^{b_r})$, and so on invoking Lemma 6 we obtain the inequality

$$\frac{z(m)}{m} \leq \left(\frac{p_1+1}{2p_1}\right) \cdots \left(\frac{p_r+1}{2p_r}\right) \leq \frac{2}{3} \cdot \frac{3}{5} < \frac{1}{2}. \tag{11}$$

It follows that $m = a \cdot p^b$ with $a \in \mathcal{P}(k(k+1))$, $p \nmid k(k+1)$ a prime, and $b \geq 1$. This implies that $p \nmid a$. If $e_p(k) = 1$, then

$$z(m) = z(a \cdot p^b) \leq a \cdot p^{b-1}(p-1)/2 < m/2,$$

by Lemma 6, contradicting our assumption on $z(m)$. If $e_p(k) = -1$ and $z(p)$ is a proper divisor of $(p+1)/2$, then

$$z(m) \leq a \cdot p^{b-1} z(p) \leq a \cdot p^{b-1}(p+1)/4 \leq m/2,$$

again contradicting our assumption on $z(m)$, and hence $e_p(k) = -1$ and $z(p) = (p+1)/2$. We have $(a, (p+1)/2) = 1$, since otherwise

$$z(m) = \operatorname{lcm}(z(a), z(p^b)) = \operatorname{lcm}(a, z(p^b)) \leq p^{b-1} \operatorname{lcm}(a, (p+1)/2) \leq a \cdot p^{b-1}(p+1)/4 \leq m/2.$$

Finally, we either have $z(p^2) = p(p+1)/2$ or $z(p^2) = (p+1)/2$. For $b \geq 2$, the latter case cannot occur as then $z(m) \leq m/p < m/2$. □

Corollary 5. *If m is a discriminator value, then either $m \in \mathcal{P}(k(k+1))$, or $m = a \cdot p^b$ with $a \in \mathcal{P}(k(k+1))$ and $p \nmid k(k+1)$ a prime satisfying $e_k(p) = -1$. Furthermore, if m is even, then $p \equiv 1 \pmod 4$.*

Proof. This is an immediate consequence on recalling that if m is a discriminator value, then $z(m) > m/2$ by Lemma 2. □

Lemma 8. *Let $p \nmid k(k+1)$ be a prime.*
a) *If $z(p^2) = (p+1)/2$, then*

$$z(m) = \frac{(p+1)m}{2p} \iff m = p \cdot a, \ (a, p(p+1)/2) = 1, \ z(a) = a.$$

b) *If $z(p^2) = p(p+1)/2$, then*

$$z(m) = \frac{(p+1)m}{2p} \iff m = p^b \cdot a, \quad b \geq 1, \ (a, p(p+1)/2) = 1, \ z(a) = a.$$

c) *If $z(p) \neq (p+1)/2$, then it never happens that $z(m) = m(p+1)/(2p)$.*

Proof. Part c is a corollary of Lemma 7 and so are the $\Rightarrow$ directions of parts a and b. Now let us prove the $\Leftarrow$ direction for part b (the proof for part a being very similar and easier). By assumption a and p^b are coprime and so $z(m) = \operatorname{lcm}(z(a), z(p^b))$. The assumption on $z(p^2)$ ensures that $z(p^b) = p^{b-1}(p+1)/2$. Since by assumption $z(a) = a$ and $(a, (p+1)/2) = 1$, we conclude that $z(m) = \operatorname{lcm}(a, p^{b-1}(p+1)/2) = m(p+1)/(2p)$. □

Note that the value of $z_k(p^b)$ only depends on the congruence class of k modulo p^b. For a given odd prime p it is thus a finite computation to determine the corresponding congruence classes in each of the three cases (with the number of congruence classes already given in Proposition 1). The results are recorded for the first few primes in Tab. 3. Using this table, Lemma 13 and Lemma 8, we can then write down results similar to the lemma below (for $p = 5$).

Lemma 9. *Suppose that* $5 \nmid k(k+1)$.
a) *If* $k \equiv 6, 18 \pmod{25}$*, then*

$$z(m) = \frac{3m}{5} \quad \Longleftrightarrow \quad m = 5 \cdot a,\ \ (15, a) = 1,\ \ a \in \mathcal{P}(k(k+1)).$$

b) *If* $k \equiv 1, 3, 8, 11, 13, 16, 21, 23 \pmod{25}$*, then*

$$z(m) = \frac{3m}{5} \quad \Longleftrightarrow \quad m = 5^b \cdot a,\ \ b \geq 1,\ \ (15, a) = 1,\ \ a \in \mathcal{P}(k(k+1)).$$

c) *If* $k \equiv 2 \pmod 5$*, then it never happens that* $z(m) = 3m/5$*.*

Here, and in general if $p \equiv 5 \pmod 6$, we require that $3 \nmid a$ (as a and $(p+1)/2$ have to be coprime), and for such a we have $z(a) = a$ if and only if $a \in \mathcal{P}(k(k+1))$ by Lemma 13, and so a distinction of cases depending on whether 3 is a special prime or not is unnecessary.

2.5. **Integers for which the index of appearance is large.** In this section we consider how large $\frac{z(m)}{m}$ can be for m with $z(m) < m$, something quite relevant for us. The smaller $\frac{z(m)}{m}$ is, the less likely it is that m occurs as a discriminator value (if $\frac{z(m)}{m} \leq \frac{1}{2}$, then certainly m does not occur as a discriminator value). The following quantities (considered in detail in Sec. 2.5.1) will play a main role. Some sample values are given in Tab. 4.

Definition 4 (ρ_k, σ_k, τ_k)**.** The supremum

$$\sup_{p \text{ prime}} \Big\{ \frac{z_k(f(p))}{f(p)} : z_k(f(p)) < f(p) \Big\},$$

we denote by ρ_k if $f(p) = p$, by σ_k if $f(p) = p^2$, and by τ_k if $f(p) = 2p^2$.

If $z(f(p)) < f(p)$, then $z(f(p))/f(p) \leq (p+1)/2p$, where the upper bound is decreasing as a function of p. This implies that in order to verify that, say, $\rho_k = (q+1)/2q$, it suffices to show that $z(q) = (q+1)/2$ and that either $z(p) = p$ or $z(p) < (p+1)/2$ for every prime $3 \leq p < q$.

As $z(2^n) = 2^n$, it is enough to take the supremum over the odd primes only. Since $z(p)/p \geq z(p^2)/p^2 \geq z(2p^2)/2p^2$ we have

$$\rho_k \geq \sigma_k \geq \tau_k.$$

Using these quantities Theorem 2 can be improved. In part I it was already noted that the interval $[n, 3n/2)$ occurring there can be replaced by the potentially larger interval $[n, n/\rho_k)$. We will show that ρ_k can be replaced by σ_k. Since $\sigma_k < \rho_k$ for infinitely many k (see Sec. 2.5.1), this is an improvement.

Theorem 5. *Let* $k > 2$ *be fixed. We have*

$$\mathcal{D}_k(n) \leq \min\{m \geq n : m \in \mathcal{A}_k \cup \mathcal{B}_k\},$$

with equality if the interval $[n, n/\sigma_k)$ *contains an integer* $m \in \mathcal{A}_k \cup \mathcal{B}_k$*. We have* $\sigma_k = 2/3$ *if* $k \equiv 1, 7 \bmod 9$*, and* $\sigma_k \leq 3/5$ *otherwise.*

If $\mathcal{D}_k(n)$ *is even, then*

$$\mathcal{D}_k(n) \leq \min\{m \geq n : m \in \mathcal{B}_k\},$$

with equality if the interval $[n, n/\tau_k)$ *contains an integer* $m \in \mathcal{B}_k$*. If* $k \equiv 0, 2, 4 \pmod 5$*, then* $\tau_k \leq 7/13$*, and* $\tau_k \leq 3/5$ *for general* k*.*

If $z(p) = (p+1)/2$ for some prime p, then we can replace sup by max in Definition 4. If $z(p)$ is never equal to $(p+1)/2$, but infinitely often to $z(p) = (p-1)/2$, then $\rho_k = 1/2$. If $z(p)$ is never equal to $(p+1)/2$ and at most finitely often to $(p-1)/2$, then $\rho_k < 1/2$. The same remarks hold, mutatis mutandis, for σ_k and τ_k, cf. the next three lemmas.

k	ρ_k	σ_k	τ_k
1	2/3	2/3	3/5
2	4/7	7/13	7/13
3	3/5	3/5	3/5
4	2/3	4/7	7/13
6	3/5	12/23	19/37
23	3/5	3/5	3/5
24	7/13	7/13	7/13
31	2/3	6/11	9/17
93	3/5	4/7	7/13
3202	2/3	2/3	15/29

TABLE 4. Some sample values of ρ_k, σ_k and τ_k

Lemma 10 ([4]). *Let $k \geq 1$ be fixed.*
a) *Suppose that $z(q_1) = (q_1+1)/2$ for some prime q_1. Let q be the smallest prime such that $z(q) = (q+1)/2$. Then*

$$\rho_k = \max\left\{\frac{z(p)}{p} : z(p) < p\right\} = \frac{q+1}{2q}.$$

b) *If there is no prime q_1 such that $z(q_1) = (q_1+1)/2$, then $\rho_k \leq 1/2$.*
c) *We have $\rho_k = 2/3$ if $k \equiv 1 \pmod 3$ and $\rho_k \leq 3/5$ otherwise.*

Lemma 11. *Let $k \geq 1$ be fixed.*
a) *Suppose that $z(q_1^2) = q_1(q_1+1)/2$ for some prime q_1. Let q be the smallest prime such that $z(q^2) = q(q+1)/2$. Then*

$$\sigma_k = \max\left\{\frac{z(p^2)}{p^2} : z(p^2) < p^2\right\} = \frac{q+1}{2q}.$$

b) *If there is no prime q_1 such that $z(2q_1^2) = q_1(q_1+1)/2$, then $\tau_k \leq 1/2$.*
c) *We have $\sigma_k = 2/3$ if $k \equiv 1, 7 \bmod 9$, and $\sigma_k \leq 3/5$ otherwise.*

Proof. We leave this to the reader, cf. the very similar (but more complicated) proof of Lemma 12. Only part c needs special attention, here we use Proposition 1 and Tab. 3. □

Lemma 12. *Let $k \geq 1$ be fixed.*
a) *Suppose that $z(2q_1^2) = q_1(q_1+1)$ for some prime q_1. Let q be the smallest prime such that $z(2q^2) = q(q+1)$. Then $q \equiv 1 \pmod 4$ and*

$$\tau_k = \max\left\{\frac{z(2p^2)}{2p^2} : z(2p^2) < 2p^2\right\} = \frac{q+1}{2q}.$$

b) *If there is no prime q_1 such that $z(2q_1^2) = q_1(q_1+1)$, then $\tau_k \leq 1/2$.*
c) *We have $\tau_k \leq 3/5$. If $k \equiv 0, 2, 4 \pmod 5$, then $\tau_k \leq 7/13$.*

Proof. Put $\rho(p) = z(2p^2)/(2p^2)$. If $p > q$ and $\rho(p) < 1$, then

$$\rho(p) \leq \frac{p+1}{2p} < \frac{q+1}{2q} = \rho(q),$$

If $p < q$ and $\rho(p) < 1$, then $z(2p^2) \mid p(p-1)$, $z(2p^2) \mid p(p+1)/2$ or $z(2p^2) \mid p+1$. Since, respectively,

$$\rho(p) \leq \frac{p-1}{2p} < \frac{1}{2}, \quad \rho(p) \leq \frac{p+1}{4p} < \frac{1}{2} \quad \text{or} \quad \rho(p) \leq \frac{p+1}{2p^2} < \frac{1}{2} \tag{12}$$

and $(q+1)/(2q) > 1/2$, we have established that $\tau_k = (q+1)/(2q)$. In case $q \equiv 3 \pmod 4$, then $z(2)$ and $z(q^2)$ are both even and so $\rho(q) < 1/2$. Thus $q \equiv 1 \pmod 4$.
b) In this case, cf. (12), we have $\rho(p) < \frac{1}{2}$ for every prime p and so the supremum is $\leq \frac{1}{2}$.
c) We apply parts a and b together with the observation that $\rho(50) \in \{\frac{1}{5}, 1\}$ if $k \equiv 0, 4 \bmod 5$ (by Lemma 5) and $\rho(50) \leq \frac{2}{5}$ if $k \equiv 2 \bmod 5$ (by Lemma 6). □

The following extends [4, Lemma 14] with some extra statements involving the set $\mathcal{M}$.

Lemma 13. *Let $k \ge 1$. We have $z(m) = m$ if and only if*

$$\begin{cases} m \in \mathcal{P}(k(k+1)), \ 9 \nmid m; \\ m \in \mathcal{P}(k(k+1)), \ 9 \mid m, \ \text{and } 3 \text{ is not special.} \end{cases}$$

The remaining integers m satisfy $z(m) \le \rho_k m$, with $\rho_k = 2/3$ if $k \equiv 1 \pmod 3$ and $\rho_k \le 3/5$ otherwise. Let $\mathcal{M}$ be the set of integers that are divisible by some prime square p^2 with $p \nmid k(k+1)$ a prime. The integers m in $\mathcal{M}$ satisfy $z(m) \le \sigma_k m$, with $\sigma_k = 2/3$ if $k \equiv 1, 7 \bmod 9$, and $\sigma_k \le 3/5$ otherwise. The even integers m in $\mathcal{M}$ satisfy $z(m) \le \tau_k m \le 3m/5$. If $k \equiv 0, 2, 4 \pmod 5$, then $\tau_k \le 7/13$.

Corollary 6. *Suppose that $k \equiv 1 \pmod 3$. Then $z(m) = m$ if and only if $m \in \mathcal{P}(k(k+1))$.*

Proof of Lemma 13. Only the statements involving $\mathcal{M}$ need to be proved. Let $b \in \mathcal{M}$. We have

$$\frac{z(b)}{b} \le \sup_{m \in \mathcal{M}} \left\{ \frac{z(m)}{m} \right\} = \sup_{m \in \mathcal{M}_1} \left\{ \frac{z(m)}{m} \right\},$$

where $\mathcal{M}_1$ is the set of integers divisible by at most one prime square p^2 with $p \nmid k(k+1)$ (cf. the beginning of the proof of Lemma 7). Thus every $m \in \mathcal{M}_1$ is of the form $m = p^e \cdot m_1$, with $p \nmid k(k+1)$ some prime, $e \ge 2$ and $z(m_1) = m_1$. Since

$$\frac{z(m)}{m} \le \frac{z(p^2)}{p^2} \frac{p^{e-2}}{p^{e-2}} \frac{z(m_1)}{m_1} \le \frac{z(p^2)}{p^2},$$

we obtain that $z(b)/b \le \sigma_k$. If m is even, then $m = p^e \cdot 2^f \cdot m_1$, with $p \nmid k(k+1)$, $e \ge 2$, $f \ge 1$ and $z(m_1) = m_1$, and we have

$$\frac{z(m)}{m} \le \frac{z(2p^2)}{2p^2} \frac{p^{e-2}}{p^{e-2}} \frac{2^{f-1}}{2^{f-1}} \frac{z(m_1)}{m_1} \le \frac{z(2p^2)}{2p^2},$$

and hence $z(b)/b \le \tau_k$. The proof is concluded on invoking Lemmas 10c, 11c and 12c. □

2.5.1. *The numbers ρ_k, σ_k and τ_k: a close-up.* We investigate when there exists an integer k such that

$$(\rho_k, \sigma_k, \tau_k) = \Big(\frac{p_1+1}{2p_1}, \frac{p_2+1}{2p_2}, \frac{p_3+1}{2p_3} \Big), \quad \text{with } p_1, p_2, p_3 \text{ prescribed primes.} \tag{13}$$

The primes p_1, p_2 and p_3 are not required to be distinct. Our main tool is Corollary 4, which we will take for granted in the remainder of this section.

Lemma 14. *The equation (13) has a solution k if and only if $3 \le p_1 \le p_2 \le p_3$ and $p_3 \equiv 1 \bmod 4$. If $p_2 \equiv 1 \bmod 4$, then we require in addition that $p_3 = p_2$. If (13) is satisfied for some k, then it is satisfied for a positive density of integers k.*

Proof. Since $z(2^n) = 2^n$ the supremum is assumed in an odd prime and so p_1, p_2 and p_3 are odd. Since $\rho_k \ge \sigma_k \ge \tau_k$ we have $p_1 \le p_2 \le p_3$.

The density assertion follows on noting that if $k_1 \equiv k \bmod p^2$ for every odd prime $p \le p_3$, then $(\rho_{k_1}, \sigma_{k_1}, \tau_{k_1}) = (\rho_k, \sigma_k, \tau_k)$ (observe that $z_k(p^2)$ only depends on the residue class of k modulo p^2).

Note that (13) entails that $z(p_1) = (p_1+1)/2$, $z(p_2^2) = p_2(p_2+1)/2$ and $z(2p_3^2) = p_3(p_3+1)$. The latter identity forces p_3 to be congruent to $1 \bmod 4$ by Lemma 12a. If $p_2 \equiv 1 \bmod 4$, then $z(2p_2^2) = p_2(p_2+1)$. We have $z(2p^2)/2p^2 \le z(p^2)/p^2 < z(p_2^2)/p_2^2$ for $3 \le p < p_2$. We conclude that $\tau_k = (p_2+1)/2p_2$ and hence $p_3 = p_2$.

It remains to prove that if the conditions on the primes p_1, p_2 and p_3 are satisfied, there exists a k solving (13). We take $k \equiv 0 \bmod p$ for the odd primes $p < p_1$. If $p_2 = p_1$ we choose k to be in a residue class modulo p_1^2 such that $z(p_1^2) = p_1(p_1+1)/2$. If $p_2 > p_1$, we choose k to be in a residue class modulo p_1^2 such that $z(p_1^2) = (p_1+1)/2$, $k \equiv 0 \bmod p$ for the primes $p_1 < p < p_2$ and k in a residue class modulo p_2^2 such that $z(p_2^2) = p_2(p_2+1)/2$. If $p_2 \equiv 1 \bmod 4$, then $p_3 = p_2$ and we are done. Otherwise we take $k \equiv 0 \bmod p$ for the primes $p_2 < p < p_3$ with $p \equiv 1 \bmod 4$ and take k in a residue class modulo p_3^2 for which $z(p_3^2) = p_3(p_3+1)/2$. □

Example 1. By Lemma 14 there exists a solution to (13) with $(p_1, p_2, p_3) = (3, 7, 13)$. We will now find such a solution. We take $k \equiv 0 \bmod 3$ and $k \equiv 18 \bmod 25$. This ensures that $\rho_k = \frac{3}{5}$ and $\sigma_k \ge \frac{4}{7}$. On requiring that $k \equiv 44 \bmod 49$, it follows that $\sigma_k = \frac{4}{7}$. As $\tau_k \ne \frac{4}{7}$ and $\tau_k \ne \frac{6}{11}$, we have $\tau_k \ge \frac{7}{13}$. We choose $k \equiv 2 \bmod 13$ and $k \not\equiv 119 \bmod 169$ to ensure that $\tau_k = \frac{7}{13}$. Finally, one checks that $k = 93$ satisfies all the requirements, and we conclude that $(\rho_k, \sigma_k, \tau_k) = (\frac{3}{5}, \frac{4}{7}, \frac{7}{13})$. By computer calcuation one can verify that $368, 431, 543$ and 606 are the only other $k < 1000$ having this property.

2.6. **The incongruence index.** Apart from z_k we will also make use of the *incongruence index* ι_k, which was introduced in Moree and Zumalacárregui [11]. It will allow us to rule out many odd values of m with $z(m) = m$ as discriminator values (cf. Lemma 20).

Definition 5 (incongruence index)**.** Given an integer $m \geq 1$, the incongruence index $\iota_k(m)$ is the largest integer j such that $U_0(k), \ldots, U_{j-1}(k)$ are pairwise distinct modulo m.

Note that $\iota_k(m) \leq z_k(m)$. In practice frequently $\iota_k(m) < z_k(m)$, which shows that the following, easy to prove, variant of Lemma 2 is often stronger.

Lemma 15. *If $m = \mathcal{D}_k(n)$, then $\iota_k(m) \geq n$ and $\iota_k(m) > m/2$.*

The general idea is to use $z(m)$ whenever possible and if it proves itself too weak a tool, then try to work with $\iota(m)$.

Lemma 16. *Let $b \geq 1$ be an integer. Then*

$$\iota_k(5^b) = \begin{cases} (3 \cdot 5^{b-1} + 1)/2 & \text{if } k \equiv 1 \pmod 5 \text{ and } k \not\equiv 6 \pmod{25}; \\ 3 \cdot 5^{b-1} & \text{if } k \equiv 3 \pmod 5 \text{ and } k \not\equiv 18 \pmod{25}. \end{cases}$$

Proof. If $k \equiv 1, 3 \pmod 5$, then $e_5(k) = -1$ and so $z(5) = 3$. A trivial computation gives $U_3(k) = 16k^2 + 16k + 3$. This is a multiple of 5 for $k \equiv 1, 3 \pmod 5$, but not of 25 since the classes $k \equiv 6, 18 \pmod{25}$ are excluded. So, $5 \mid U_3(k)$, but $25 \nmid U_3(k)$ and by Lemma 10b it follows that $z(5^b) = 3 \cdot 5^{b-1}$, cf. Table 3.

Now let us investigate when $U_i(k) \equiv U_j(k) \pmod{5^b}$. Writing α, α^{-1} for the roots of the characteristic equation $x^2 - (4k+2)x + 1$, by (6) we need $\alpha^i - \alpha^{-i} \equiv \alpha^j - \alpha^{-j} \pmod{5^b}$, which on multiplication by α^{i+j} yields $(\alpha^i - \alpha^j)(\alpha^{i+j} + 1) \equiv 0 \pmod{5^b}$. So, 5 divides either $\alpha^i - \alpha^j$ or $\alpha^{i+j} + 1$ (5 is inert in $\mathbb{Z}[\alpha]$ as $e_5(k) = -1$). When $k \equiv 3 \pmod 5$ the second case doesn't happen. That is, for $k \equiv 3 \pmod 5$ we have that α is one of $2 \pm \sqrt{3} \pmod 5$ (the characteristic equation only depends on k modulo 5). Then $\alpha^2 = 2 \pm \sqrt{3}$ and $\alpha^3 \equiv 1 \pmod 5$. So, we see that $-1 \pmod 5$ is not in the multiplicative group generated by $\alpha \pmod 5$ when $\alpha = 3 \pmod 5$. Thus, $U_i(k) \equiv U_j(k) \pmod{5^b}$ forces $\alpha^i \equiv \alpha^j \pmod{5^b}$, so $\alpha^{i-j} \equiv 1 \pmod{5^b}$, so $U_{i-j} \equiv 0 \pmod{5^b}$ (assuming say $i > j$), so $z(5^b) = 3 \cdot 5^{b-1}$ divides $i - j$. This takes care of $\iota_k(5^b)$ in case $k \equiv 3 \pmod 5$.

In case $k \equiv 1 \pmod 5$, there is no i, j such that both $\alpha^i - \alpha^j \equiv 0 \pmod 5$ and $\alpha^{i+j} + 1 \equiv 0 \pmod 5$. To see why, assume there are such. Then $\alpha^{i+j} \equiv -1 \pmod 5$ and $\alpha^{i-j} \equiv 1 \pmod 5$. But when $k \equiv 1 \pmod 5$, then $\alpha = 3 \pm 2\sqrt{2}$. Now $\alpha^2 \equiv 2 \pm 2\sqrt{2} \pmod 5$ and $\alpha^3 \equiv -1 \pmod 5$. So, the order of α modulo 5 is exactly 6 so asking of i, j such that $\alpha^{i-j} \equiv 1 \pmod 5$ and $\alpha^{i+j} \equiv -1 \pmod 5$ gives $i - j \equiv 0 \pmod 6$ and $i + j \equiv 3 \pmod 6$. Summing them we get $2i \equiv 3 \pmod 6$, which is false (there is no such i with $2i \equiv 3 \pmod 6$).

So, when $k \equiv 1 \pmod 5$ and $k \not\equiv 6 \pmod{25}$, either 5^b divides $\alpha^{i-j} - 1$ or 5^b divides $\alpha^{i+j} + 1$. In the first case $i - j$ is a multiple of $z(5^b)$, so at least $3 \cdot 5^{b-1}$. The second case gives $\alpha^{i+j} \equiv -1 \pmod{5^b}$ so $i + j$ is an odd multiple of $3 \cdot 5^{b-1}$. The extreme case is $i + j = 3 \cdot 5^{b-1}$ and we see that if $i > j$, then $i \geq 3 \cdot 5^{b-1}/2$, so $i \geq (3 \cdot 5^{b-1} + 1)/2$. □

The next lemma studies to what extent a relatively small incongruence index remains relatively small after lifting to a larger modulus. Recall the definition (7) of $e_p(k)$.

Lemma 17. *Suppose that $p \nmid k(k+1)$ and $\left(\frac{k+1}{p}\right) = -1$. If $\iota_k(p^a) < p^a/2$ for some $a \geq 1$, then $\iota_k(p^b) < p^b/2$ for all $b \geq a$. Furthermore, if m is odd and $z_k(m) = m$, then $\iota_k(p^a \cdot m) < p^a \cdot m/2$.*

Proof. If $e_p(k) = 1$, then $z(p^a) \leq p^{a-1}(p-1)/2 < p^a/2$ for all $a \geq 1$ by Lemma 6. So

$$\left(\frac{k}{p}\right) = 1, \quad \left(\frac{k+1}{p}\right) = -1. \tag{14}$$

We show that $z_k(p^a) \leq \lfloor p^{a-1}(p+1)/4 \rfloor < p^a/2$ for all $a \geq 2$. Indeed, write $U_i \equiv U_j \pmod m$ with m coprime to $k(k+1)$ as

$$\alpha^i - \alpha^{-i} \equiv \alpha^j - \alpha^{-j} \pmod m,$$

which is equivalent to

$$(\alpha^i - \alpha^j)(\alpha^{-(i+j)} + 1) \equiv 0 \pmod m.$$

It suffices that $\alpha^{i+j} \equiv -1 \pmod{m}$. Using (14) we note that

$$\begin{aligned} \alpha^{(p+1)/2} &= \left((\sqrt{k+1}+\sqrt{k})^2\right)^{(p+1)/2} = (\sqrt{k+1}+\sqrt{k})^{p+1} \\ &= (\sqrt{k+1}+\sqrt{k})^p(\sqrt{k+1}+\sqrt{k}) \equiv (\sqrt{k+1}^p+\sqrt{k}^p)(\sqrt{k+1}+\sqrt{k}) \pmod{p} \\ &\equiv (-\sqrt{k+1}+\sqrt{k})(\sqrt{k+1}+\sqrt{k}) \equiv k-(k+1) \equiv -1 \pmod{p}. \end{aligned}$$

So, if we choose $m = p$ and $i + j = (p + 1)/2$, then we have that $U_i \equiv U_j \pmod{p}$. More generally, we can choose $m = p^a$. Since

$$\alpha^{(p+1)/2} \equiv -1 \pmod{p},$$

we get that

$$\alpha^{p^{a-1}(p+1)/2} \equiv -1 \pmod{p^a},$$

and we can see that $i_k(p^a) \le p^{a-1}(p+1)/4$. Indeed, if $p^{a-1}(p+1)/2 = 2\ell+1$, then $U_\ell \equiv U_{\ell+1} \pmod{p^a}$, so $i_k(p^a) \le \ell = \lfloor p^{a-1}(p+1)/4 \rfloor$. If $p^{a-1}(p+1)/2 = 2\ell$, then we have $U_{\ell-1} \equiv U_{\ell+1} \pmod{p^a}$, so $i_k(p^a) \le \ell = \lfloor p^{a-1}(p+1)/4 \rfloor$. So, at any rate in this case $i_k(p^a) < p^a/2$ for all $a \ge 1$.

We now turn our attention to the final assertion. Let i, j be such that $i < j < p^{\alpha-1}(p+1)/4+1$ and $U_i \equiv U_j \pmod{p^\alpha}$. Then $U_{mi} \equiv U_{mj} \pmod{p^\alpha m}$. To see this, note that both sides are 0 modulo m since m divides $U_{z(m)} = U_m$ and U_m divides $\gcd(U_{mi}, U_{mj})$. As for the divisibility by p^α, the congruence

$$U_{mi} \equiv U_{mj} \pmod{p^\alpha}$$

is implied by

$$(\alpha^{mi} - \alpha^{mj})(\alpha^{-m(i+j)} + 1) \equiv 0 \pmod{p^\alpha}$$

which holds because

$$\alpha^i - \alpha^j \mid \alpha^{mi} - \alpha^{mj}, \qquad \alpha^{-(i+j)} + 1 \mid \alpha^{-m(i+j)} + 1$$

(m is odd) and

$$(\alpha^i - \alpha^j)(\alpha^{-(i+j)} + 1) \equiv 0 \pmod{p^\alpha}.$$

Since certainly $im < jm \le \lfloor p^{\alpha-1}(p+1)/4 \rfloor + 1\rfloor m < p^\alpha m/2$, the proof is finished. □

Corollary 7. *Suppose that $p \nmid k(k+1)$ and $p \equiv 3 \pmod{4}$. If $\iota_k(p^a) < p^a/2$ for some $a \ge 1$, then $\iota_k(p^b) < p^b/2$ for all $b \ge a$. Furthermore, if m is odd and $z_k(m) = m$, then $\iota_k(p^a \cdot m) < p^a \cdot m/2$.*

Proof. If $\left(\frac{k+1}{p}\right) = 1$, then $\left(\frac{k}{p}\right) = -1$ (as $e_p(k) = -1$). Then by Lemma 6 we have $\iota_k(p^a) \le z_k(p^a) \le p^{a-1}(p+1)/4 < p^a/2$ for every $a \ge 1$. □

We expect that this corollary also holds for the primes $p \equiv 1 \pmod{4}$, but is more difficult to prove. As we do not need this generalization, we leave it to a possible sequel to this paper.

2.7. **The discriminatory properties of m with large $z(m)$.** The goal of this section is to prove Lemma 20. To this end we need the next fundamental lemma and Lemma 19

Lemma 18 (Lemmas 15 and 16 of [4])**.** *Let p be an odd prime and $b \ge 1$ be arbitrary.*
If p divides k, then $U_i(k) \equiv U_j(k) \pmod{p^b}$ if and only if $i \equiv j \pmod{z_k(p^b)}$.
If p divides $k+1$, then $U_i(k) \equiv U_j(k) \pmod{p^b}$ is equivalent to one of the following:

- *If $i \equiv j \pmod{2}$, then $i \equiv j \pmod{z_k(p^b)}$;*
- *If $i \not\equiv j \pmod{2}$, then $i \equiv -j \pmod{z_k(p^b)}$.*

Lemma 19. *Assume that $m = 2^a p^e$ with $a, e \ge 1$ is such that $e_p(k) = -1$, $p \equiv 1 \pmod{4}$ and $z(p) = (p+1)/2$. Then $U_i \equiv U_j \pmod{m}$ holds if and only if $i \equiv j \pmod{z(m)}$.*

Proof. A minor variation of the proof of [4, Lemma 9]. It rests only on [4, Lemma 4] and [4, Lemma 5], where now we should take Lemmas 4 and 6 from this paper. In addition a minor correction in the argument has to be made, as sketched in Sec. 3. □

Lemma 20. *Assume that $k \equiv 1 \pmod{3}$ and $z_k(25) = 15$. Suppose that $m = 5^e \cdot m_1$ with $e \ge 1$ and $z(m_1) = m_1$. Then $\iota(m) = z(m) = 3m/5$ if*

- *$m_1 \in \mathcal{B}_k$; or*
- *$m_1 \in \mathcal{A}_k$ and $k \equiv 3 \pmod{5}$,*

and otherwise m is not a discriminator value assumed by $\mathcal{D}_k$.

Proof. Note that $z(m) = 3m/5$. We first consider the case where m_1 is even. Note that this is equivalent with $m_1 \in \mathcal{B}_k$, as $\mathcal{B}_k = \{m_1 \text{ even} : z(m_1) = m_1\}$ by (8). Write $m_1 = 2^a \cdot m_2$ with m_2 odd. Since $z(2^a \cdot 5^e) = 2^a \cdot 3 \cdot 5^{e-1}$, we have $U_i(k) \equiv U_j(k) \pmod{2^a \cdot 5^e}$ if and only if $i \equiv j \pmod{2^a \cdot 3 \cdot 5^{e-1}}$ by Lemma 19. As $m_2 \in \mathcal{P}(k(k+1))$, it follows by Lemma 18 that $U_i(k) \equiv U_j(k) \pmod{m_1}$ if and only if $i \equiv j \pmod{m_1}$. Taken together these two equivalences show that $U_i(k) \equiv U_j(k) \pmod{m}$ if and only if $i \equiv j \pmod{3m/5}$. Thus in case m_1 is even, we conclude that $\iota(m) = 3m/5$.

It remains to deal with the case where m_1 is odd. Since by assumption $z(25) = 15$, we have $k \equiv 1, 3 \bmod 5$ (see Table 2).

First case: $k \equiv 1 \pmod 5$. The assumption $z(25) = 15$ ensures that $k \not\equiv 6 \pmod{25}$. By Lemma 16 and Lemma 17 (with $p = 5$) it then follows that $\iota(m) \le m/2$ and so m is not a discriminator value.

Second case: $k \equiv 3 \pmod 5$. Suppose that m_1 has an odd prime divisor that also divides $k+1$. Now write $m_1 = p^a \cdot m_2$ with $p \nmid m_2$. Clearly $z(p^a) = p^a$. Set $i = (p^a - 1) \cdot m_2 \cdot 3 \cdot 5^{e-1}/2$ and $j = (p^a + 1) \cdot m_2 \cdot 3 \cdot 5^{e-1}/2$. Then $i \not\equiv j \pmod 2$ and $p^a \mid (i + j)$. Thus, $U_i(k) \equiv U_j(k) \pmod{p^a}$ by Lemma 18. This lemma also implies that $U_i(k) \equiv U_j(k) \equiv U_0(k) \equiv 0 \pmod{m_2}$ as $i \equiv j \equiv 0 \pmod{m_2}$ and $m_2 \in \mathcal{P}(k(k+1))$. The proof of Lemma 16 shows that if $i \equiv j \pmod{3 \cdot 5^{e-1}}$, then $U_i(k) \equiv U_j(k) \pmod{5^e}$. We infer that $U_i(k) \equiv U_j(k) \pmod{p^a \cdot m_2 \cdot 5^e}$, and hence if m discriminates the numbers $U_0(k), \ldots, U_{n-1}(k)$, then $n \le (p^a+1)m_2 \cdot 3 \cdot 5^{e-1}/2$. The interval $[(p^a+1)/2, p^a)$ contains a power of 2, say 2^b. Then $2^b \cdot m_2 \cdot 5^e$ is a better discriminator than $p^a \cdot m_2 \cdot 5^e = m$. We conclude that if $m_1 \notin \mathcal{A}_k$, then m is not a discriminator value.

It remains to deal with the case where $m_1 \in \mathcal{A}_k$. The proof of Lemma 16 shows that $U_i(k) \equiv U_j(k) \pmod{5^e}$ if and only if $i \equiv j \pmod{3 \cdot 5^{e-1}}$. This in combination with Lemma 18 shows that $U_i(k) \equiv U_j(k) \pmod{m}$ if and only if $i \equiv j \pmod{3m/5}$. Hence $\iota(m) = 3m/5$. □

2.8. **Intervals containing special integers.** We will first discuss how to compute $n_p(\alpha)$ (cf. Def. 1). From basic Diophantine approximation we know there exist e, f, g and h such that

$$1 < \frac{p^f}{2^e} < \alpha \text{ and } 1 < \frac{2^h}{p^g} < \alpha.$$

We claim that $n_p(\alpha) \le 2^{e+1}p^g$. In order to see this observe that any integer $n := 2^k p^\ell \ge 2^{e+1}p^g$ satisfies either $k \ge e+1$, or $\ell \ge g$. In case $k \ge e+1$, we note that the number $2^{k-e}p^{\ell+f}$ is even and lies in $[n, n\alpha)$. In case $\ell \ge g$, we have $2^{k+h}p^{\ell-g} \in [n, n\alpha)$. Next one tries to to find an even integer $n_{\text{new}} := 2^k p^\ell \in [[2^{e+1}p^g/\alpha], 2^{e+1}p^g)$, where $[x]$ denotes the entier of x. If successful, we continue until we fail, each time considering the interval $[[n_{\text{new}}/\alpha], n_{\text{new}})$.

Example 2. We determine $n_7(5/3)$. Starting from $64 \cdot 7 = 448$ we can make either the substitution $32 \to 49$ or $7 \to 8$ with ratio $< 5/3$. Going down from 448 via $392, 256, 196, 128, 98, 64, 56$, we obtain $n_7(5/3) = 34$. From 32 we can go down in several steps to 2. Thus the integers $n \ge 1$ for which $[n, 5n/3)$ does not contain an even number of the form $2^a \cdot 7^b$, are precisely $n = 1$ and $n = 33$.

For some further examples see Tab. 2 and 5. The very large values appearing there were determined using more sophisticated techniques involving continued fractions, see Languasco et al. [8].

p	$n_p(3/2)$	$n_p(5/3)$
3	2	2
5	22	2
7	262	34
11	11	10
13	139	10
17	1398102	78644
19	342	308
23	22	20
137	45812984491	2516583
149	21846	19661
271	375299968947542	5153960756

TABLE 5. Some values of $n_p(3/2)$ and $n_p(5/3)$

Lemma 21.

a) *For* $n \geq 2^7 \cdot 5^6\,(= 2 \cdot 10^6)$ *the interval* $[\frac{380}{453}n, n]$ *contains an even integer of the form* $2^a \cdot 5^b$.
b) *For* $n \geq 2^7 \cdot 5^{15}\,(= 3.90625 \cdot 10^{13})$ *the interval* $[\frac{35}{39}n, n]$ *contains an even integer of the form* $2^a \cdot 5^b$.

Proof. a) Put $\alpha = \frac{453}{380}$. We start by noticing that $1 < \frac{2^7}{5^3} < \frac{5^7}{2^{16}} < \alpha$. This shows that by making either the substitution $2^{16} \to 5^7$ or $5^3 \to 2^7$, we can increase the even number $n = 2 \cdot 2^{16} \cdot 5^2$ in such a way to a further number of the same format with ratio in $(1, \alpha)$. The so produced sequence of integers is unbounded. The string of consecutive integers $2m$ with $m = 2^6 \cdot 5^6, 2^{20}, 2^4 \cdot 5^7, 2^{18} \cdot 5, 2^2 \cdot 5^8, 2^{16} \cdot 5^2$ also have the property that the ratio of consecutive terms is in $(1, \alpha)$.
b) Put $\beta = \frac{39}{35}$. We start by noticing that $1 < \frac{2^7}{5^3} < \frac{5^{16}}{2^{37}} < \beta$. This shows that by making either the substitution $2^{37} \to 5^{16}$ or $5^3 \to 2^7$, we can increase the even number $n = 2 \cdot 2^{37} \cdot 5^2$ in such a way to a further number of the same format with ratio in $(1, \beta)$. As in the proof of part a we can lower n to obtain the indicated starting value. □

Proposition 2. *Let* $p \geq 13$ *be a prime. If* p^e *be a potential wild prime power, then there exist integers* $a \geq 1$ *and* $b \geq 0$ *such that*

$$\frac{5(p+1)}{6p}p^e < 2^a \cdot 5^b < p^e. \tag{15}$$

Proof. For the purposes of this proof we say that p^e is *approachable* if there are integers $a \geq 1$ and $b \geq 0$ for which (15) holds. We put $\alpha_p = 5(p+1)/(6p)$. Note that $\alpha_{13} = \frac{35}{39}$ and $\alpha_p < \alpha_{151} = \frac{380}{453}$ for $p > 151$.

We first suppose that $p \geq 151$. We have $(\frac{380}{435}p^e, p^e) \subseteq (\alpha_p p^e, p^e)$ and hence p^e is approachable by Lemma 21a if $p^e > 2^7 \cdot 5^6$. If $p^e < 2^7 \cdot 5^6$, we conclude that $151 \leq p \leq 1409$ as $e \geq 2$ by Lemma 22. This leaves only one potential wild prime power, namely 181^2, which turns out to be approachable by $\{2 \cdot 5^6,\ 2^8 \cdot 5^3\}$.

It remains to deal with the primes $13 \leq p \leq 151$. We have $(\frac{35}{39}p^e, p^e) \subseteq (\alpha_p p^e, p^e)$ and hence p^e is approachable by Lemma 21b if $p^e > 2^7 \cdot 5^{15}$. This leaves the five potential wild prime powers $\{13^7, 19^4, 19^8, 43^7, 97^5\}$. These are approachable by $2^5 \cdot 5^9$, $2^3 \cdot 5^6$, $2^6 \cdot 5^{12}$, $2^3 \cdot 5^{15}$, $\{2^5 \cdot 5^{12}, 2^{12} \cdot 5^9, 2^{19} \cdot 5^6, 2^{26} \cdot 5^3\}$, respectively. □

3. Corrections to part I

In part I the conditions on k involving 6 (mod 9) in the definition of $\mathcal{B}_k$ were erroneously omitted. However, the proofs are only based on the definition $\mathcal{B}_k = \{m \text{ even} : z(m) = m\}$. Using Lemma 14 (Lemma 13 above), $\mathcal{B}_k$ was not quite correctly made explicit. The upshot is that if one replaces the definition of $\mathcal{B}_k$ in part I by the one used here, as far as we are aware only one further mathematical correction to part I is needed[2].

In the proof of Lemma 9 around line 12 at p. 61 it is implicitly assumed that $z(p_1^{b_1}) = p_1^{b_1-1}(p_1+1)/2$, which is not always guaranteed by our assumption that $z(p_1) = (p_1+1)/2$. However, by replacing the two lines there by the following ones, the proof is effortlessly fixed. "As for the divisibility by $p_1^{b_1}$, note that since $z(p_1^{b_1}) \mid (i-j)$ and $i-j$ is even, it follows that

$$i - j = 2z(p_1^{b_1})\ell,$$

for some positive integer ℓ. Since $\alpha^{z(p_1^{b_1})} \equiv -1 \pmod{p_1^{b_1}}$, it follows that $\alpha^{i-j} \equiv 1 \pmod{p_1^{b_1}}$."

We finish this section by pointing out some typos in part I:
p. 56, l. 3. For "$b \geq 1$" read "$b = 1$".
p. 56, l. -10. For "$\Delta(1) = 8$" read "$\Delta(1) = 32$".
p. 62, l. 2. Replace by "$19m/37 \geq z(m) = 2^a \cdot p^{b-1}(p+1)/(2k) \geq n$."
p. 63, l. -9. For "$5/6 < 2^{a-\alpha-1} < 1$" read "$5/6 < 2^{a-\alpha-1} \cdot 5^b < 1$".
p. 65, l. 10. The number field $\mathbb{K}$ is not defined. It is $\mathbb{Q}(\sqrt{k(k+1)})$.
p. 65. Lemma 14. One should read "sup" instead of "lim sup".
p. 70, l. 6. For "$p^a m_1 = m1$" read "$p^a m_1 = m$".

[2]We use the amended definition for results quoted from part I involving $\mathcal{B}_k$.

4. Wild prime powers

Motivated by Corollary 5 we make the following definition.

Definition 6 (wild prime power)**.** A prime power p^e with $p \nmid k(k+1)$ such that p^e exactly divides $\mathcal{D}_k(n)$ for some integer n, we call a wild prime power for k.

Obviously any wild prime power is odd. By Corollary 5 any discriminator value is divisible by at most one wild prime power.

Lemma 22. *A prime number is never wild.*

Proof. Suppose that p is a wild prime. Then $p > 2$ and $\mathcal{D}_k(n) = ap$ for some k, n and an integer a coprime to p satisfying $z(a) = a$. In addition, we have $z(p) = (p+1)/2$. It follows that $n \le z(ap) \le z(a)z(p) \le a(p+1)/2$. Clearly there is a power 2^b in the interval $[(p+1)/2, p)$. As $a2^b \ge a(p+1)/2$ is even and satisfies $z(a2^b) = a2^b$, it discriminates $U_0(k), \ldots, U_{n-1}(k)$. Since $a2^b < ap$, this contradicts the minimality of $\mathcal{D}_k(n)$. ☐

Next we study when p^e with $e > 1$ is wild. This involves the exponent set $\mathcal{M}_p$.

Definition 7 (Exponent set)**.** Given any odd prime p, the exponent set is defined as

$$\mathcal{M}_p := \left\{ e \ge 1 : \left\{ e\frac{\log p}{\log 2} \right\} > 1 - \frac{\log(1+1/p)}{\log 2} \right\}.$$

A simple application of Weyl's criterion (cf. the proof of [11, Proposition 1] or [1, Proposition 1]) gives

$$\lim_{x\to\infty} \frac{\#\{m \in \mathcal{M}_p : m \le x\}}{x} = \frac{\log(1+1/p)}{\log 2}.$$

In particular, $\mathcal{M}_p$ is an infinite set.

Proposition 3. *Let $p \ge 3$ be a prime. The set of integers $e \ge 1$ for which there is no integer a such that*

$$p^e \frac{(p+1)}{2p} \le 2^a < p^e \tag{16}$$

equals $\mathcal{M}_p$.

Proof. Put $\rho = (p+1)/(2p)$ and assume (16) does hold for some integers a and e. By taking logarithms and after some easy manipulations (16) is seen to be equivalent with

$$\frac{\log \rho}{\log 2} \le a - e\frac{\log p}{\log 2} < 0.$$

It follows that $a = \lfloor e \log p / \log 2 \rfloor$, and we are left with

$$\left\{ e\frac{\log p}{\log 2} \right\} \le -\frac{\log \rho}{\log 2} = 1 - \frac{\log(1+1/p)}{\log 2}.$$

Hence $\mathcal{M}_p$ is precisely the set of e for which (16) has no solution. ☐

Note that the lower bound in (16) is assumed if and only if $e = 1$ and p is a Mersenne prime.

Definition 8 (potentially wild prime power)**.** A prime power p^e with $e \in \mathcal{M}_p$ is said to be *potentially wild.*

Tables 6 and 7 list smallest potentially wild prime powers.

Lemma 23. *If p^e is a wild prime power, then it is also potentially wild.*

Proof. Suppose that p^e is a wild prime power for k. Then $\mathcal{D}_k(n) = p^e m$, with $p \nmid k(k+1)$ and m composed of only prime factors dividing $k(k+1)$. We assume that $e \notin \mathcal{M}_p$ and derive a contradiction. We must have $z(p^e) = p^{e-1}(p+1)/2$ and $z(m) = m$. It follows that $n \le z(p^e m) \le p^{e-1}(p+1)m/2$. Since by assumption $e \notin \mathcal{M}_p$, there exists an integer a such that (16) is satisfied. The number $2^a m$ is even, and by Lemma 18 we have $\iota_k(2^a m) = 2^a m$. Since $2^a m \ge p^{e-1}(p+1)/2m \ge n$ we conclude that the numbers $U_0(k), \ldots, U_{n-1}(k)$ are pairwise distinct modulo $2^a m$. Now since $2^a m < p^e m$, it follows that $p^e m$ cannot be a discriminator value, a contradiction showing that $e \in \mathcal{M}_p$ and hence the potential wildness of p^e. ☐

p	exponent
13	$7, 17, 27, 37$
17	$11, 22, 34$
37	19
73	21
97	$5, 10, 15, 20, 25$
181	$2, 4, \dots, 20, 22$
1933	12
2389	9
4993	7
10321	3
11290229	7

TABLE 6. Potential wild prime powers $p^e \le 10^{50}$ with $5 < p \le 10^{10}$ and $p \equiv 1 \pmod 4$

p	exponent
3	$3, 5, 8, 10, 13, 15, 17, 20, 22, 25, \dots, 97, 99, 102, 104$
7	$6, 11, 16, 21, 26, 32, 37, 42, 47, 52, 58$
11	$2, 13, 15, 26, 37, 39$
19	$4, 8, 12, 16, 20, 24, 28, 32$
23	$19, 21$
31	22
43	$7, 9, 14, 18, 27$
67	15
71	20
79	23
49667	$5, 10$

TABLE 7. Potential wild prime powers $p^e \le 10^{50}$ with $p \le 10^7$ and $p \equiv 3 \pmod 4$

Remark 4. An alternative proof of Lemma 22 is obtained on noting that $1 \notin \mathcal{M}_p$. Thus p is not potentially wild and so not wild.

The following result represents an important milepost on our way towards a proof of Theorem 3.

Theorem 6. *Suppose that $k \equiv 1 \bmod 3$. If $z_k(25) = 15$ and p^e is a wild prime power for k, then $p = 5$ and e is in $\mathcal{M}_5$.*

Proof. The conditions on k ensure that $(k(k+1), 15) = 1$. Let $m = \mathcal{D}_k(n)$ be a discriminator value. Suppose that a wild prime power p^e with $p \nmid k(k+1)$ occurs in m. Then $m = p^e \cdot m_1$ with $z(m_1) = m_1$. Since we must have $z(m) > m/2$, it follows that $z(p^e) = p^{e-1}(p+1)/2$. The number m discriminates the numbers n up to at most $(p+1)p^{e-1}m_1/2$.

We want to show that $p = 5$, and will assume that $p \ne 5$. Recall that $e \ge 2$. We first consider the case where $p^e \in \{3^2, 7^2, 11^2\}$. Since $\iota_k(m)$ only depends on the congruence class of k modulo m, it is a finite computation to verify that $\iota_k(3^2) \le 4$, $\iota_k(7^2) \le 7 \cdot 3 < 7^2/2$ if $7 \nmid k(k+1)$ and $\iota_k(11^2) \le 11 \cdot 5 < 11^2/2$ if $11 \nmid k(k+1)$. By Corollary 7 we infer from this that, under the above assumptions on k, $\iota_k(p^e) < p^e/2$ for $p \in \{3, 7, 11\}$. We note that m_1 is odd in this three cases as $p \equiv 3 \pmod 4$ and hence $z(m) = \operatorname{lcm}(z(p^e), z(m_1)) \le m/2$ otherwise. We can thus apply the final assertion of Corollary 7 to conclude that $\iota_k(m) < m/2$, which shows that our assumption that m is a discriminator value was wrong to begin with. Thus $p \ge 13$ and so by Proposition 2 there exist integers $a \ge 1$ and $b \ge 0$ such that

$$\frac{5(p+1)}{6p}p^e < 2^a \cdot 5^b < p^e. \tag{17}$$

We write $m_1 = 2^c \cdot m_2$, with m_2 odd. We now infer that

$$z(2^a \cdot 5^b \cdot m_1) = \operatorname{lcm}(z(2^{a+c}), z(5^b), z(m_2)) = \operatorname{lcm}(2^{a+c}, 3 \cdot 5^{b-1}, m_2) = 3m/5,$$

where we used that $(30, m_2) = 1$ and $z(5^b) = 5^{b-1} \cdot 3$, which is a consequence of $z_k(25) = 15$. Then $2^a \cdot 5^b \cdot m_1 < p^e \cdot m_1$ discriminates the integers up to $3 \cdot 2^a \cdot 5^{b-1} \cdot m_1$. The lower bound part of inequality (17) now guarantees that $2^a \cdot 5^{b-1} \cdot m_1 > (p+1)p^{e-1}m_1/2$, showing that $2^a \cdot 5^b \cdot m_1$ is a better discriminator than m. We conclude that $p = 5$. By Lemma 23 it follows that 5^e is potentially wild and hence $e \in \mathcal{M}_5$ by Definition 8. □

Corollary 8. *Suppose that 5^e is a wild prime power for an integer k satisfying $k \equiv 1 \pmod 3$. Then*

$$e \in \mathcal{M}_5 = \{3, 6, 9, 12, 15, 18, 21, \ldots\} \quad \textit{and} \quad k \equiv 1, 3, 8, 11, 13, 16, 21, 23 \pmod{25}.$$

Remark 5. If we would restrict to wild prime powers of *even* discriminator values, then necessarily $p \equiv 1 \pmod 4$ and there is no need to consider the primes $3, 7$ and 11 separately. In this case Corollary 7 is not needed.

Remark 6. Our proof of Theorem 6 eventually depends on quite a number of numerical coincidences and we are doubtful whether there exists a more conceptual proof.

4.1. **Some specific cases.** In this section we will demonstrate Corollary 8. If m has an odd prime divisor, we denote the smallest such by $P_{\text{odd}}(m)$, otherwise we put $P_{\text{odd}}(m) = 1$.

Proposition 4.
a) *Suppose that $k \equiv 3 \pmod 5$ and $k \not\equiv 18 \pmod{25}$. Then $\mathcal{D}_k(3 \cdot 5^{e-1}) = 5^e$ for every e in $\mathcal{M}_5$ with $5^e < P_{odd}(k(k+1))$.*
b) *Suppose that $k \equiv 1, 3 \pmod 5$ and $k \not\equiv 6, 18 \pmod{25}$. Then $\mathcal{D}_k(6 \cdot 5^{e-1}) = 2 \cdot 5^e$ for every e in $\mathcal{M}_5$ with $2 \cdot 5^e < P_{odd}(k(k+1))$.*

Proof. We only prove part a, the proof of b being similar. By Lemma 16 we have $\mathcal{D}_k(3 \cdot 5^{e-1}) \le 5^e$. The assumption on P_{odd} ensures that up to 5^e only powers of two occur in $\mathcal{A}_k \cup \mathcal{B}_k$. It then follows by Theorem 3 that $\mathcal{D}_k(3 \cdot 5^{e-1}) = 2^a \cdot 5^b$, with $a, b \ge 0$ and $2^a \cdot 5^b \le 5^e$. If $b = 0$, then we must have $3 \cdot 5^{e-1} \le 2^a < 5^e$, contradicting our assumption that $e \in \mathcal{M}_5$. We have $\iota_k(2^a \cdot 5^b) \le 3 \cdot 2^a \cdot 5^{b-1} \le z_k(2^a \cdot 5^b)$. We require that $3 \cdot 2^a \cdot 5^{b-1} \ge 3 \cdot 5^{e-1}$. In combination with $2^a \cdot 5^b \le 5^e$, this gives $2^a \cdot 5^b = 5^e$, completing the proof. □

Two simple ways to obtain a k with $P_{\text{odd}}(k(k+1))$ large are to take k to be a power of two such that $k+1$ is a prime, or to take k a prime such that $k+1$ is a power of two. This then leads to the *Fermat*, respectively *Mersenne primes*. Conjecturally there are only finitely many Fermat primes, but infinitely many Mersenne primes. The largest known Fermat primes is 65537, in contrast huge Mersenne primes are known. We will thus restrict to the case where k is a Mersenne prime. Proposition 4 then has the following corollary.

Corollary 9. *Suppose that $p \equiv 1 \pmod 4$ is a prime > 5 such that $q := 2^p - 1$ is also a prime. Then $\mathcal{D}_q(6 \cdot 5^{e-1}) = 2 \cdot 5^e$, for all those e in $\mathcal{M}_5$ for which $2 \cdot 5^e < q$.*

Proof. This follows from part b, on noting that if $p \equiv 1 \pmod 4$ and $p > 5$, then $2^p - 1 \equiv 1 \pmod 5$ and $2^p - 1 \not\equiv 6 \pmod{25}$. □

We note that $2^{82589933} - 1$, the largest known prime number as of Oct. 2022, satisfies the conditions of the corollary. A similar corollary of part a is not possible as any Mersenne prime > 3 is $\not\equiv 3 \pmod 5$.

For n large enough the behavior of $\mathcal{D}_q(n)$ with q a Mersenne prime is particularly easy as the following corollary of Theorems 2 and 3 shows.

Corollary 10. *Let $q = 2^p - 1 > 3$ be a Mersenne prime. Then for $n \ge n_q^o(3/2)$ we have*

$$\mathcal{D}_q(n) = \min\{m \ge n : m = 2^a \cdot q^b \ \textit{and}\ a, b \ge 0\}.$$

Equality already holds for $n \ge n_q^o(5/3)$ if $p \equiv 1 \pmod 4$ and $p > 5$.

One finds that $n_7^o(3/2) = 131$ and some computation leads, for every $n \ge 1$, to

$$\mathcal{D}_7(n) = \min\{m \ge n : m = 2^a \cdot 7^b \text{ and } a, b \ge 0\}.$$

For Mersenne primes $q > 7$ the numbers $n_q^o(3/2)$ and $n_q^o(5/3)$ seem to be huge [8], and hence a complete characterization infeasible. For example, $n_{131071}^o(5/3) = \lceil 2^{16} \cdot 131071^{23897} \cdot 3/5 \rceil$, a number having 122 298 digits!!

5. Proofs of Theorems 3 and 5

We first prove Theorem 5, since it will be used in our proof of Theorem 3.

Proof of Theorem 5. Recall that $\mathcal{S}_{k,n} := \{m \in \mathcal{A}_k \cup \mathcal{B}_k : m \geq n\}$. Let $m = \mathcal{D}_k(n)$ be a discriminator value with $m \notin \mathcal{S}_{k,n}$. If $z(m) = m$, then $m \in \mathcal{S}_{k,n}$ by (1)and so we may assume that $z(m) < m$.

By Lemma 22 it follows that $m \in \mathcal{M}$, with $\mathcal{M}$ as in Lemma 13. This entails by Lemma 13 that $n \leq z(m) \leq \sigma_k m$ and hence $m \geq n/\sigma_k$. By assumption there is an integer $m_1 \in \mathcal{S}_{k,n}$ with $m < n/\sigma_k$, showing that m_1 is a better discriminator than m. We conclude that $m \in \mathcal{S}_{k,n}$. In case m is even, we repeat this proof, but this time using the inequality $z(m) \leq \tau_k m$. □

Proof of Theorem 3. By Theorem 1 we may assume that $k > 1$. Suppose that $k \not\equiv 1 \pmod 3$. Thus $6 \mid k(k+1)$, and so all integers of the form $2^a \cdot 3^b$ with $a \geq 1$ and $b \in \{0, 1\}$ belong to $\mathcal{B}_k$. We have $\sigma_k \leq 3/5$. Now by Theorem 5 it suffices to check that for every $n \geq 2$ there is an integer m_1 of the form $2^a \cdot 3^b$ with $a \geq 1$ and $b \in \{0, 1\}$ in the interval $[n, 5n/3) \subseteq [n, n/\sigma_k)$. This can be done with help of the substitutions $3 \to 2^2$ and $2 \to 3$, which can be applied starting from $n = 2$.

Next suppose that $k \equiv 1 \pmod 3$ and $k \equiv 0, 4 \pmod 5$. Now $10 \mid k(k+1)$, and so all integers of the form $2^a \cdot 5^b$ with $a \geq 1$ and $b \geq 0$ belong to $\mathcal{B}_k$. We apply Theorem 2. It is easy to see that for every $n \geq 22$ the interval $[n, 2n/3)$ contains an integer of the form $2^a \cdot 5^b$ with $a \geq 1$ and $b \geq 0$. Thus if $m \notin \mathcal{S}_{k,n}$, then $n \leq 21$. The odd primes ≤ 21 are not wild by Lemma 23. This leaves us only with 9. However, 9 is not potentially wild (see Tab. 7) and so certainly not wild.

Put $m = \mathcal{D}_k(n)$. Either $z(m) = m$ or $z(m) < m$, in which case we have $m = p^e \cdot m_1$ with $z(m_1) = m_1$ and p^e a wild prime power. By Theorem 6 we conclude that $p = 5$. It follows that either $z(m) = m$ or $m = 5^b m_1$ with $z(m) = 3m/5$ and $z(m_1) = m_1$. In part I we established that the only discriminator values m with $z(m) = m$ satisfy $m \in \mathcal{A}_k \cup \mathcal{B}_k$. These discriminate $U_0(k), \ldots, U_{m-1}(k)$ and hence $\mathcal{D}_k(n) \leq \min\{\mathcal{S}_{k,n}\}$. It remains to deal with the case where $m = 5^b \cdot m_1$ with $b \geq 1$, $z(m) = 3m/5$ and $z(m_1) = m_1$. On invoking Lemma 20 the proof of (4) is now completed.

Let $p > 2$ be a prime divisor of $k(k+1)$. If $n \geq n_p(5/3)$, then the interval $[n, 5n/3)$ contains an even integer of the form $2^a \cdot p^b$. This number is in $\mathcal{B}_k$ and $\geq n$ and so in $\mathcal{S}_{k,n}$. As it is less than $5n/3$, it follows by (4) that $\mathcal{D}_k(n) = \min \mathcal{S}_{k,n}$.

By assumption k has an odd prime divisor p. If $n \geq n_p^o(5/3)$, then the interval $[n, 5n/3)$ contains an integer of the form $2^a \cdot p^b$. This number is in $\mathcal{A}_k \cup \mathcal{B}_k$ and $\geq n$ and so in $\mathcal{S}_{k,n}$. As it is less than $5n/3$, it follows by (4) that $\mathcal{D}_k(n) = \min \mathcal{S}_{k,n}$. □

6. Effective bounds for wild prime powers and elements in $\mathcal{F}_k$

It was proved in part I that the set $\mathcal{F}_k$ is finite for $k > 1$. Here, we precise our proof by showing that this set can be effectively determined and establish Theorem 4.

Definition 9 (prime types). We say that a prime p is of

- type I if $p \mid k$;
- type II if $p \mid k+1$;
- type III if $p \nmid k(k+1)$, $e_p(k) = 1$;
- type IV if $p \nmid k(k+1)$, $e_p(k) = -1$,

with $e_p(k)$ as defined in (7).

Lemma 24. *Let $k \geq 2$. There are only finitely many odd discriminators which are not made up of primes p dividing k.*

Proof. Let m be an odd discriminator value not made up only of primes of type I. Then by Corollary 5 we can write $m = p_1^{a_1} \cdot m_1$, where p_1 is of type IV and unique, and m_1 is only made up of primes of type I or II. We will show that both $p_1^{a_1}$ and m_1 are bounded. Note that

$$z(m) = \operatorname{lcm}[z(p_1^{a_1}), z(m_1)].$$

We may assume that $z(p_1^{a_1}) = p_1^{a_1-1}(p_1+1)/2$, for otherwise $z(m) < m/2$, contradicting our assumption that m is a discriminator value. If there is a power of 2, say 2^b, in the the interval $[p_1^{a_1-1}(p_1+1)/2, p_1^{a_1}]$, then $2^b \cdot m_1 < m$ is a better discriminator than m. We thus may assume there is no power of 2 in this interval, which guarantees the existence of an integer a such that

$$p_1^{a_1} < 2^{a+1} < p_1^{a_1}\left(1 + 1/p_1\right).$$

Thus, $p_1^{a_1} > (p_1/(p_1+1))2^{a+1}$. Since $p_1 \geq 3$, it follows that $p_1^{a_1} > (3/4)2^{a+1}$. Further,

$$z(p_1^{a_1}) = p_1^{a_1}\left(\frac{p_1+1}{2p_1}\right) \leq \frac{2p_1^{a_1}}{3} < \frac{2^{a+2}}{3}.$$

Now let p be any odd prime factor dividing $k(k+1)$. Since $k(k+1)$ cannot be a power of 2 for $k > 1$ such a prime p exists. We search for a pair of positive integers (u, v) such that

$$\frac{2}{3} \cdot 2^{u+1} < p^v < \frac{3}{4} \cdot 2^{u+1}.$$

This we find quickly, since the above condition is equivalent to

$$\left\{(u+1)\frac{\log 2}{\log p}\right\} \in \left(\frac{\log(4/3)}{\log p}, \frac{\log(3/2)}{\log p}\right), \tag{18}$$

and the sequence of fractional parts $\{nx\}$ is dense (even uniformly distributed) for irrational x. Let u be the minimal positive integer with this property. Note that the corresponding v is uniquely determined. By contradiction we will now show that $a \leq u$, leading to the bound

$$\ell := p_1^{a_1} < 2^{u+1}. \tag{19}$$

Assume that $a > u$ is any integer. We note that

$$p_1^{a_1-1}(p_1+1)/2 < (2/3)2^{a+1} < 2^{a-u} \cdot p^v < (3/4)2^{a+1} < p_1^{a_1}.$$

Thus,

$$2^a < \frac{p_1^{a_1-1}(p_1+1)}{2} < 2^{a-u} \cdot p^v < p_1^{a_1} < 2^{a+1},$$

and we conclude that $m_2 := m_1 2^{a-u} p^v$ has the property that $z(m_2) = m_2$. If n satisfies $\mathcal{D}_k(n) = m$, then $n \leq m_1 \cdot z(p_1^{a_1})$. The even integer m_2 satisfies $m_1 \cdot z(p_1^{a_1}) < m_2 < m = m_1 \cdot p_1^{a_1}$ and discriminates the integers $U_0(k), \ldots, U_{m_1 z(p_1^{a_1})-1}(k)$, contradicting the (discriminatory) minimality of m. This shows that, if $p_1^{a_1}$ is such that $p_1^{a_1} < 2^{a+1} < p_1^{a_1} + p_1^{a_1-1}$ and m is actually a discriminator, then $a \leq u$ and (19) is satisfied.

Fix $p_1^{a_1} = \ell$ and let $t = z(\ell) < \ell$. Now we look at the numbers $m_1 \cdot t < m_1 \cdot \ell$ with $m_1 > 1$. Let q be any odd prime dividing m_1. Let (e_q, f_q) be the first pair of indices such that $q^{e_q} \cdot t < 2^{f_q} < q^{e_q} \cdot \ell$ (it exists because of an argument with fractional parts as above). Then, if q^e divides m_1 with $e \geq e_q$, we can replace q^e by $q^{e-e_q} \cdot 2^{f_q}$. This has the effect of replacing m_1 by $m_1 \cdot 2^{f_q} \cdot q^{-e_q}$, which is a better discriminator for the numbers $n \leq m_1 \cdot t$ than the number $m_1 \cdot \ell$ is. This can be done for each q dividing m_1. Since there are only finitely many q (namely, odd primes of type I and II), we see that m is bounded. □

To make the argument effective we need to find N so that the containment condition (18) holds for some positive integer $u \leq N$ and bound ℓ in (19).

Let $\theta = \log 2/\log p$. Note that $\theta \notin \mathbb{Q}$. Recall now that the *discrepancy* D_N of a sequence $\{a_m\}_{m=1}^N$ of real numbers (not necessarily distinct) is defined as

$$D_N = \sup_{0 \leq \gamma \leq 1}\left|\frac{\#\{m \leq N\ :\ \{a_m\} < \gamma\}}{N} - \gamma\right|.$$

From the above definition we see that the inequality

$$\#\{m \leq N\ :\ \alpha \leq \{a_m\} < \beta\} \geq (\beta - \alpha)N - 2D_N N$$

holds for all $0 \leq \alpha \leq \beta \leq 1$. Thus, setting $a_m = m\theta$ for all $m = 1, \ldots, N$, and letting

$$I = \left(\frac{\log(4/3)}{\log p}, \frac{\log(3/2)}{\log p}\right),$$

which is an interval of length $\log(9/8)/\log p$, we have

$$\#\{m \leq N : \{a_m\} \in I\} \geq |I|N - 2D_N N = \left(\frac{\log(9/8)}{\log p}\right)N - 2D_N N. \tag{20}$$

In particular, if the right-hand side is positive, then there is $u \le N$ with $\{a_u\} \in I$. We now upper bound D_N. The Koksma-Erdős-Turán inequality (see Lemma 3.2 in [6]) bounds the discrepancy D_N by

$$D_N \le \frac{3}{H} + \frac{3}{N} \sum_{m=1}^{H} \frac{1}{m\|a_m\|}, \tag{21}$$

where $\|x\|$ is the distance from x to the nearest integer and $H \le N$ is an arbitrary positive integer.

To bound $\|a_m\|$, note that

$$\|a_m\| = \left| m\frac{\log 2}{\log p} - t \right| = \frac{1}{\log p} |m \log 2 - t \log p|,$$

where t is an integer such that $t \le m(\log 2)/(\log p) + 1 < 2m$. Note that $\|a_m\| \ne 0$, since $\theta \in \mathbb{R} \setminus \mathbb{Q}$. Thus, $|m \log 2 - t \log p| \ne 0$ and a lower bound for it can be obtained by using the theory of linear forms in logarithms.

Let us recall Matveev's main theorem [9]. It applies to algebraic numbers, but we recall it here only for rational numbers. For a rational number $\gamma = r/s$ with coprime integers r and $s > 0$, let $h(\gamma) := \max\{\log |r|, \log s\}$.

Theorem 7 (Matveev [9])**.** *Let $\gamma_1, \ldots, \gamma_k$ be positive rational numbers, let $b_1, \ldots, b_k$ be non-zero integers, and assume that*

$$\Lambda := \gamma_1^{b_1} \cdots \gamma_k^{b_k} - 1, \tag{22}$$

is non-zero. Then for every

$$B \ge \max\{|b_1|, \ldots, |b_k|\}$$

we have

$$\log |\Lambda| > -1.4 \cdot 30^{k+3} \cdot k^{4.5} \, (1 + \log B) \, h(\gamma_1) \cdots h(\gamma_k).$$

In our case, we take

$$\Lambda = 2^m \cdot p^{-t} - 1,$$

which is non-zero, since p is an odd prime. Note that $\Lambda = e^{\Gamma} - 1$, where $\Gamma = m \log 2 - t \log p$. So, either $|\Gamma| \ge 1/2$, or $|\Gamma| < 1/2$. If $|\Gamma| < 1/2$, then

$$2|\Gamma| > |e^{\Gamma} - 1| = |\Lambda|,$$

and we can apply Matveev's theorem to get a lower bound on $|\Lambda|$ and hence on $|\Gamma|$. Either way, we take in Matveev's theorem

$$k = 2, \quad \gamma_1 = 2, \quad \gamma_2 = p, \quad b_1 = m, \quad b_2 = -t,$$

and, noting that we can set $B := 2m$, we get

$$2|m \log 2 - t \log p| > \exp\left(-C_1 (\log 2)(1 + \log(2m)) \log p\right), \tag{23}$$

where $C_1 = 1.4 \cdot 30^5 \cdot 2^{4.5}$. Since $1.4 \cdot 30^5 \cdot 2^{4.5} \cdot \log 2 < 6 \cdot 10^8 - \log 2$, we get

$$|m \log 2 - t \log p| > \exp(-6 \cdot 10^8 (1 + \log(2m)) \log p) = p^{-6 \cdot 10^8 (1+\log(2m))} \quad \text{for} \quad m \ge 1.$$

We thus obtain that, if $H \ge 15$ and $2m \le H$, then

$$1 + \log(2m) \le 1 + \log H \le 1.63 \log H \qquad (H \ge 15),$$

and so the inequality (23) leads to

$$\frac{1}{\|a_m\|} \le (\log p) \, p^{(6 \cdot 1.63) \cdot 10^8 \log H} < p^{(10^9 - 2) \log H} = H^{(10^9 - 2) \log p} < H^{10^9 \log p - 2}.$$

Thus,

$$D_N \le 3 \left(\frac{1}{H} + \frac{H^{10^9 \log p - 2}}{N} \sum_{m=1}^{H} \frac{1}{m} \right) < 3 \left(\frac{1}{H} + \frac{H^{10^9 \log p - 1}}{N} \right).$$

where we trivially bounded the sum by H. Choosing $H := \left\lfloor N^{10^{-9}/\log p} \right\rfloor$ we get, assuming still that $H \ge 15$ and therefore that

$$N^{10^{-9}/\log p} \ge 15, \quad \text{which is equivalent to} \quad N \ge 15^{10^9 \log p}, \tag{24}$$

that

$$D_N \le 3\Big(\frac{1}{H}+\frac{H^{10^9\log p-1}}{N}\Big)\le 3\left(\left\lfloor N^{10^{-9}/\log p}\right\rfloor^{-1}+N^{-10^{-9}/\log p}\right)\le 7N^{-10^{-9}/\log p},$$

where we use the trivial observation that if $x\ge 15$, then

$$\frac{1}{\lfloor x\rfloor}+\frac{1}{x}\le\frac{1}{x}\Big(\frac{1}{1-\frac{1}{x}}+1\Big)\le\frac{29}{14}\cdot\frac{1}{x}<\frac{7}{3}\cdot\frac{1}{x}.$$

Turning now our attention to the inequality (19), we see that

$$N\left(\frac{\log(9/8)}{\log p}-2D_N\right)>N\left(\frac{\log(9/8)}{\log p}-14N^{-10^{-9}/\log p}\right). \tag{25}$$

Thus, if $N\ge N_0$ with

$$N_0:=\left(\frac{15\log p}{\log(9/8)}\right)^{10^9\log p}, \tag{26}$$

the right–hand side of (25) is at least

$$\frac{N}{15}\frac{\log(9/8)}{\log p} \tag{27}$$

and hence positive. Note that the inequality $N\ge N_0$, with N_0 as in (26), ensures that the inequality (24) is satisfied. Hence, we have established the following result.

Lemma 25. *Let p be an odd prime factor of $k(k+1)$. There is a positive integer u such that*

$$\left\{(u+1)\frac{\log 2}{\log p}\right\}\in\left(\frac{\log(4/3)}{\log p},\frac{\log(3/2)}{\log p}\right) \tag{28}$$

and

$$u+1<\left(\frac{15\log p}{\log(9/8)}\right)^{10^9\log p}.$$

The argument can be iterated to give an upper bound on the largest element of $\mathcal{F}_k$.

Lemma 26. *If m is an odd discriminator not entirely made up of primes dividing k, then*

$$m<2^{(k+1)^{10^{10}\log\log(k+1)}}.$$

Proof. We keep the notation from the proof of Lemma 24. As such, we write $m=p_1^{a_1}\cdot m_1$, where m_1 is made up of primes p dividing $k(k+1)$. By the argument from that proof, we conclude that

$$p_1^{a_1}<2^{a+1}\le 2^{u+1},$$

with u the smallest integer satisfying (18). By Lemma 25 and since $15/\log(9/8)<130$, it follows that

$$u+1\le(130\log p)^{10^9\log p}=p^{10^9\log(130\log p)}.$$

Therefore, with the notation of Lemma 24, we have

$$\ell=p_1^{a_1}<2^{u+1}\le 2^{p^{10^9\log(130\log p)}}. \tag{29}$$

Now let $q\mid m_1$, which implies $q\mid k(k+1)$. We need to estimate the smallest pair of positive integers (e_q,f_q) such that, if we put

$$t:=z(\ell)=p_1^{a_1-1}(p_1+1)/2,$$

then

$$q^{e_q}\cdot t<2^{f_q}<q^{e_q}\cdot\ell. \tag{30}$$

Taking logarithms, we have

$$e_q+\frac{\log\ell}{\log q}-\frac{\log(\ell/t)}{\log q}<f_q\frac{\log 2}{\log q}<e_q+\frac{\log\ell}{\log q}.$$

Since $\ell/t=2p_1/(p_1+1)\ge 3/2$, the above condition places $\{f_q(\log 2)/(\log q)\}$ in one (or two) intervals of total length $\log(\ell/t)/(\log q)\ge\log(3/2)/(\log q)$. More precisely, if $\{\log\ell/\log q\}>\log(3/2)/(\log q)$, it then follows that it suffices that

$$\left\{f_q\frac{\log 2}{\log q}\right\}\in\left(\left\{\frac{\log\ell}{\log q}\right\}-\frac{\log(3/2)}{\log q},\left\{\frac{\log\ell}{\log q}\right\}\right),$$

whereas if $\{\log \ell/\log q\} < \log(3/2)/\log q$, it suffices that

$$\left\{f_q \frac{\log 2}{\log q}\right\} \in \left(1 + \left\{\frac{\log \ell}{\log q}\right\} - \frac{\log(3/2)}{\log q}, 1\right) \cup \left(0, \left\{\frac{\log \ell}{\log q}\right\}\right).$$

In any case, there is an interval J of length $0.5\log(3/2)/\log q$ such that, if $\{f_q \log 2/\log q\} \in J$, then the estimate (30) holds with some appropriate positive integer e_q. Note that $0.5\log(3/2) > \log(9/8)$, so by the arguments from the proof of Lemma 25, it follows that if $N \geq N_0$, where N_0 satisfies (26), then there are at least

$$\frac{N \log(9/8)}{15 \log p}$$

values of $f \leq N$ such that $\{f \log 2/\log q\} \in J$. This in turn implies the inequalities $q^e t < 2^f < q^e \ell$. The only situation in which we are in trouble is when $e = 0$, in which case $t < 2^f < \ell$. Assume this happens. By inequality (29), we get

$$f < p^{10^9 \log(130 \log p)}.$$

If this were so for all the acceptable values for f, we would get by (27) that

$$\frac{N \log(9/8)}{15 \log p} < p^{10^9 \log(130 \log p)},$$

and therefore

$$N < \left(\frac{15 \log p}{\log(9/8)}\right) p^{10^9 \log(130 \log p)} < p^{(10^9+1)\log(130 \log p)}. \tag{31}$$

To ensure that this doesn't happen we ask that $N \geq N_1$, where

$$N_1 = \left(\frac{15 \log p}{\log(9/8)}\right)^{1.1 \cdot 10^9 \log p}. \tag{32}$$

Indeed, since $15/\log(9/8) > 127$, the above inequality forces

$$N > p^{1.1 \cdot 10^9 \log(127 \log p)}.$$

To see that (31) fails for such N, assume it doesn't and we get

$$p^{1.1 \cdot 10^9 \log(127 \log p)} < N < p^{(10^9+1)\log(130 \log p)},$$

and so

$$\frac{\log(130 \log p)}{\log(127 \log p)} > \frac{1.1 \cdot 10^9}{10^9 + 1} > 1.09.$$

However, this is false since the function $(\log(130) + x)/(\log(127) + x)$ on the left with $x = \log\log p$ is decreasing for $x \geq 0$ with the maximum $\log(130)/\log(127) = 1.04\ldots$ at $x = 0$, which is not larger than 1.09. It then follows that by choosing N as in (32) then there is some f such that $q^e \cdot t < 2^f < q^e \cdot \ell$ and $e > 0$. Since $15/\log(9/8) < 130$, it follows that, in particular,

$$f_q \leq (130 \log p)^{1.1 \cdot 10^9 \log p},$$

and since $p \leq k + 1$, we get

$$q^{e_q} \leq 2^{f_q} \leq 2^{(k+1)^{1.1 \cdot 10^9 \log(130 \log(k+1))}}.$$

Thus,

$$m_1 \leq \prod_{\substack{q \mid k(k+1) \\ q \text{ odd}}} q^{e_q} \leq 2^{\omega(k(k+1))(k+1)^{1.1 \cdot 10^9 \log(130 \log(k+1))}} < 2^{(k+1)^{10^{10} \log\log(k+1)}}. \tag{33}$$

The right-most inequality follows because of the trivial estimate

$$\omega(k(k+1)) = \omega(k) + \omega(k+1) \leq \frac{2\log(k+1)}{\log 2} < 4\log(k+1) \leq (k+1)^3,$$

and, furthermore,

$$3 + 1.1 \cdot 10^9 \log(130 \log(k+1)) < 10^{10} \log\log(k+1),$$

which holds for $k \geq 6$. One may check by hand that this is also true for $k \in \{2, 3, 4, 5\}$. Indeed, in these cases $p \in \{3, 5\}$, and one checks that in each of the cases one may choose $u \leq 20$ satisfying the containment (28) of Lemma 25. □

Lemma 27. *Let $k \geq 2$. There are only finitely many discriminators which are even and not divisible only by primes p dividing $k(k+1)$.*

Proof. We write $m = 2^z \cdot m_1$ with $z \geq 1$ and m_1 odd. The previous arguments showed that m_1 has at most one prime factor not of type I or II. If it has one, it is of type IV. Assume $m_1 = p_1^{a_1} \cdot m_2$, where p_1 is of type IV. Then $z(p_1) \mid (p_1+1)/2$. If $z(p_1) \mid (p_1+1)/4$, then $z(m) \leq 2^a m_2 p_1^{a_1-1}(p_1+1)/4 < m/2$, and we get a contradiction. A similar contradiction is obtained if $z(p_1^2) \mid (p_1+1)/2$, so we may assume that $z(p_1^{a_1}) = p_1^{a_1-1}(p_1+1)/2$. As in previous occasions, there exists a with

$$p_1^{a_1} < 2^{a+1} < p_1^{a_1}(1+1/p_1).$$

Thus, $p_1^{a_1} > (3/4)2^{a+1}$. As in the previous application, we pick an odd prime q dividing $k(k+1)$ and let u be minimal such that

$$\frac{2}{3} \cdot 2^{u+1} < q^v < \frac{3}{4} \cdot 2^{u+1}$$

for some (unique) v. Then, if $a > u$, it follows that $2^{a-u} q^v m_2$ is a better discriminator than m_1. This shows that $p_1^{a_1} < 2^{a+1} \leq 2^{u+1}$ is bounded. The bound is the same as in Lemma 25. Next, for each odd prime $q \mid m_2$ (of type I or II) we find (e_q, f_q) such that $q^{e_q} \cdot t < 2^{f_q} < q^{e_q} \cdot \ell$, with $(t, \ell) = (z(p_1^{a_1}), p_1^{a_1})$, for all finitely many choices $p_1^{a_1}$. Then, if the exponent of q in m exceeds e_q, we can replace m by $m \cdot 2^{f_q} \cdot q^{-e_q}$, which yields a better discriminator. This holds for all prime factors q of m_2, so also m_2 is bounded. The bounds given in (33) apply to m_1.

It remains to bound the exponent z of 2 in the factorization of m. We know by now that $m = 2^z m_1$ and that m_1 is odd and bounded, cf. (33), as

$$m_1 < 2^{\omega(k(k+1))(k+1)^{1.1\cdot 10^9 \log(130 \log(k+1))}}.$$

Further, $z(m_1) < m_1$. Put $(t, \ell) = (z(m_1), m_1)$. Again, we pick some odd prime q dividing $k(k+1)$ and search for integers x, y such that the inequality $2^x \cdot t < q^y < 2^x \cdot \ell$ holds, where $\ell = m_1$ and $t = z(m_1)$. This is equivalent to

$$x + \frac{\log \ell}{\log 2} - \frac{\log(\ell/t)}{\log 2} < y \frac{\log q}{\log 2} < x + \frac{\log \ell}{\log 2}.$$

Note that this is again satisfied if $\{y \log q / \log 2\}$ is in one or two intervals of length $\log(\ell/t)/\log 2 > \log(3/2)/\log 2$. The argument with linear forms in logarithms works and gives a bound on y as in Lemma 25. This shows that

$$2^x < q^y < (k+1)^{(k+1)^{10^9 \log(130 \log(k+1)}} < 2^{(\log(k+1)/\log 2)(k+1)^{10^9 \log(130 \log(k+1))}}.$$

If $x > 0$, and $z > x$ then we replace $2^z m_1$ by $2^{z-x} m_1 q^y$, which is a better discriminator. This shows that $z \leq x$ when x is positive. To ensure that x is positive we argue as in the previous lemma to conclude that if we replace the exponent $10^9 \log(130 \log(k+1))$ by $1.1 \cdot 10^9 \log(130 \log(k+1))$, then there is a choice of (x, y) with $x > 0$. For such x we have $z \leq x$ is also bounded, so

$$m < 2^{(\omega(k(k+1)) + (\log(k+1)/\log 2))(k+1)^{1.1\cdot 10^9 \log(130 \log k)}} < 2^{(k+1)^{10^{10} \log\log(k+1)}},$$

which is what we wanted to show. Again the last inequality holds for $k \geq 6$ and for smaller values of k can be checked by hand. □

Acknowledgments

Work on this article was started during a February-June 2017 stay of the second author at the Max Planck Institute for Mathematics (MPIM) and continued during further stays in September 2019-February 2020, June 2021 and a few days in April and July 2023. (We stress that these stays were only very partially devoted to work on this paper.) The second and third author thank the MPIM for making these stays possible. Alessandro Languasco provided a lot of help with computing Table 5 and $n_p(\alpha)$ in general (see [8] for a description of his algorithm). This required a big investment of both his time and that of his CPU's. Thanks are also due to Alexandru Ciolan for his input in some early versions.

References

[1] A. Ciolan and P. Moree, Browkin's discriminator conjecture, *Colloq. Math.* **156** (2019), 25–56.

[2] A. de Clercq, F. Luca, L. Martirosyan, M. Matthis, P. Moree, M.A. Stoumen and M. Weiß, Binary recurrences for which powers of two are discriminating moduli, *J. Integer Sequences* **23** (2020), Article 20.11.3, pp. 10.

[3] K. Dilcher and K.B. Stolarsky, Resultants and discriminants of Chebyshev and related polynomials, *Trans. Amer. Math. Soc.* **357** (2005), 965–981.

[4] B. Faye, F. Luca and P. Moree, On the discriminator of Lucas sequences, *Ann. Math. Québec* **43** (2019), 51–71.

[5] M. Ferrari, Binary recurrences with prime powers as fixed points of their discriminator, *Integers* **21** (2021), Paper No. A116, 9 pp.

[6] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New-York, 1974.

[7] M. Langevin, Quelques applications de nouveaux rsultats de Van der Poorten, Séminaire Delange-Pisot-Poitou, 17e année: 1975/76, Théorie des nombres: Fasc. 2, Exp. No. G12, 11 pp. Secrétariat Math., Paris, 1977.

[8] A. Languasco, F. Luca, P. Moree and A. Togbé, Sequences of integers generated by two fixed primes, arXiv preprint.

[9] E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers II, *Izv. Ross. Akad. Nauk. Ser. Math.* **64** (2000), 125–180; English translation *Izv. Math.* **64** (2000), 1217–1269.

[10] P. Moree, Artin's primitive root conjecture – a survey, *Integers* **12A** (2012), No. 6, 1305–1416.

[11] P. Moree and A. Zumalacárregui, Salajan's conjecture on discriminating terms in an exponential sequence, *J. Number Theory* **160** (2016), 646–665.

[12] C. Sanna, On the divisibility of the rank of appearance of a Lucas sequence, *Int. J. Number Theory* **18** (2022), 2145–2156.

[13] R. Tijdeman, On the maximal distance between integers composed of small primes, *Compositio Math.* **28** (1974), 159–162.

Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129, Torino, Italy
E-mail address: matteo.ferrari@polito.it

School of Mathematics, University of the Witwatersrand
P. O. Box Wits 2050, South Africa
E-mail address: florian.luca@wits.ac.za

Max Planck Institute for Mathematics
Vivatsgasse 7, 53111 Bonn, Germany
E-mail address: moree@mpim-bonn.mpg.de