Salajan's conjecture on discriminating terms in an exponential sequence

Pieter Moree and Ana Zumalacárregui

Abstract

Given a sequence of distinct positive integers $v_1, v_2, \ldots$ and any positive integer n, the discriminator $D_v(n)$ is defined as the smallest positive integer m such $v_1, \ldots, v_n$ are pairwise incongruent modulo m. We consider the discriminator for the sequence $u_1, u_2, \ldots$, where u_j equals the absolute value of $((-3)^j - 5)/4$, that is $u_j = (3^j - 5(-1)^j)/4$. We prove a 2012 conjecture of Sabin Salajan characterizing the discriminator of the sequence $u_1, u_2, \ldots$.

1 Introduction

Given a sequence of distinct positive integers $v_1, v_2, \ldots$ and any positive integer n, the discriminator $D_v(n)$ is defined as the smallest positive integer m such $v_1, \ldots, v_n$ are pairwise incongruent modulo m. Browkin and Cao [5] relate it to cancellations algorithms similar to the sieve of Eratosthenes.

The main problem is to give an easy description or characterization of $D_v(n)$ (in many cases such a characterization does not seem to exist). Arnold, Benkoski and McCabe [2] might have been the first to consider this type of problem (they introduced also the name). They considered the case where $v_j = j^2$. Subsequently various authors, see e.g. [4, 11, 16, 17], studied the discriminator for polynomial sequences.

It is a natural problem to study the discriminator for non-polynomial sequences. Very little work has been done in this direction. E.g. there are some conjectures due to Sun [16] in case $v_j = j!$, $v_j = \binom{2j}{j}$ and $v_j = a^j$.

In this paper we study the discriminator for a closely related sequence $u_1, u_2, \ldots$ with $u_j = |(-3)^j - 5|/4 = (3^j - 5(-1)^j)/4$. This sequence satisfies the binary recurrence $u_n = 2u_{n-1} + 3u_{n-2}$, for every $n \geq 3$. with starting values $u_1 = 2$ and $u_2 = 1$. The first few terms are

$$2, 1, 8, 19, 62, 181, 548, 1639, 4922, \ldots$$

Note that for $j \geq 2$ we have $u_{j+1} > u_j$ and that all u_j are distinct. It is almost immediate that the terms are of alternating parity. Since all u_j are distinct the number

$$D_S(n) = \min\{m \geq 1 : u_1, \ldots, u_n \text{ are pairwise distinct modulo } m\}$$

Mathematics Subject Classification (2000). 11T22, 11B83

is well-defined. Note that $D_S(n) \geq n$. In Table 1 we give the values of $D_S(n)$ for $1 \leq n \leq 32768$ (with the powers of 5 underlined).

TABLE 1

range	value	range	value
1	1	129 – 256	256
2	2	257 – 512	512
3 – 4	4	513 – 1024	1024
5 – 8	8	1025 – 2048	2048
9 – 16	16	2049 – 2500	$\underline{3125}$
17 – 20	$\underline{25}$	2501 – 4096	4096
21 – 32	32	4097 – 8192	8192
33 – 64	64	8193 – 12500	$\underline{15625}$
65 – 100	$\underline{125}$	12501 – 16384	16384
101 – 128	128	16385 – 32768	32768

Based on this table Sabin Salajan, who at the time was an intern with the first author, proposed a conjecture that we will prove in this paper to be true. The first author had asked Sabin to find second order linear recurrences for which the discriminator values have a nice structure. After an extensive search Sabin came up with the sequence $u_1, u_2, \ldots$. For convenience we call this sequence the *Salajan sequence* S and its associated discriminator D_S the *Salajan discriminator*. If $m = D_S(n)$ for some $n \geq 1$, then we say that m is a *Salajan value*, otherwise it is a *Salajan non-value*.

Theorem 1 *Let $n \geq 1$. Put $e = \lceil \log_2(n) \rceil$ and $f = \lceil \log_5(5n/4) \rceil$. Then*

$$D_S(n) = \min\{2^e, 5^f\}.$$

Corollary 1 *If the interval $[n, 5n/4)$ contains a power of 2, say 2^a, then we have $D_S(n) = 2^a$.*

Note that 2^e is the smallest power of 2 which is $\geq n$ and that 5^f is the smallest power of 5 which is $\geq 5n/4$.

From Table 1 one sees that not all powers of 5 are Salajan values. Let $\mathcal{F}$ be the set of integers $b \geq 1$ such that the interval $[4 \cdot 5^{b-1}, 5^b]$ does not contain a power of 2. Then it is not difficult to show that the image of D_S is given by $\{2^a : a \geq 0\} \cup \{5^b : b \in \mathcal{F}\}$. Using Weyl's criterion one can easily establish (see Section 7.2) the following proposition.

Proposition 1 *As x tends to infinity we have $\#\{b \in \mathcal{F} : b \leq x\} \sim \beta x$, with $\beta = 3 - \log 5/\log 2 = 0.678\ldots$.*

2 Strategy of the proof of Theorem 1

For the benefit of the reader we describe the strategy of the (somewhat lengthy) proof of Theorem 1.

We first show that if $2^e \geq n$ and $5^f \geq 5n/4$, then $D_S(n) \leq \min\{2^e, 5^f\}$. This gives us the absolutely crucial upper bound $D_S(n) < 2n$.

Next we study the periodicity of the sequence modulo d and determine its period $\rho(d)$. The idea is to use the information so obtained to show that many d are Salajan non-values. In case $3 \nmid d$ the sequence turns out to be purely periodic with even period that can be given precisely. This is enough for our purposes as we can show that $3|D_S(n)$ does not occur.

Now we restrict to the d with $3 \nmid d$. Using that $D_S(n) < 2n$ one easily sees that if $\rho(d) \le d/2$, then d is a Salajan non-value. The basic property (3) of the period together with the evenness of the period now excludes composite values of d. Thus we have $d = p^m$, with p a prime.

In order for $\rho(p^m) > p^m/2$ to hold we find that we must have $\mathrm{ord}_9(p) = (p-1)/2$, that is 9 must have maximal possible order modulo p. Moreover, 9 must have maximal possible order modulo p^m, that is $\mathrm{ord}_9(p) = \varphi(p^m)/2$. (A square cannot have a multiplicative order larger than $\varphi(p^m)/2$ modulo p^m.) This is about as far as the study of the periodicity will get us. To get further we will use a more refined tool, the *incongruence index*. Given an integer m, this is the maximum k such that $u_1, \ldots, u_k$ are pairwise distinct modulo m. We write $\iota(m) = k$. For $3 \nmid m$, $\iota(m) \le \rho(m)$. Using that $D_S(n) < 2n$ one notes that if $\iota(d) \le d/2$, then d is a Salajan non-value.

For the primes $p > 3$ we show by a lifting argument that if $\iota(p) < \rho(p)$, then $p^2, p^3, \ldots$ are Salajan non-values. Likewise, we prove that if $\iota(p) \le p/2$, then $p, p^2, p^3, \ldots$ are Salajan non-values. We then show that except for $p = 5$, all primes with $\mathrm{ord}_9(p) = (p-1)/2$ satisfy $\iota(p) < \rho(p)$. At this point we are left with the primes $p > 5$ satisfying $\mathrm{ord}_9(p) = (p-1)/2$ as only possible Salajan values. Then using classical exponential sums techniques, and some combinatorial arguments, we infer that $\iota(p) < 4p^{3/4}$. Using this bound, after some computational work, we then conclude that $\iota(p) \le p/2$ for every $p > 5$.

Thus we are left with $D_S(n) = 2^a$ for some a or $D_S(n) = 5^b$ for some b. By Lemma 2 and Lemma 3 it now follows that $2^a \ge n$ and $5^b \ge 5n/4$. This then completes the proof.

3 Preparations for the proof

We will show that 2^e with $2^e \ge n$ and 5^f with $5^f \ge 5n/4$ are admissible discriminators. That is, we will show that the sequence $u_1, \ldots, u_n$ lie in distinct residue classes modulo 2^e and in distinct residue classes modulo 5^f.

Let p be a prime. If $p^a|n$ and $p^{a+1} \nmid n$, then we put $\nu_p(n) = a$. The following result is well-known, for a proof see, e.g., Beyl [3].

Lemma 1 *Let p be a prime, $r \ne -1$ an integer satisfying $r \equiv 1 \pmod{p}$ and n a natural number. Then*

$$\nu_p(r^n - 1) = \begin{cases} \nu_2(n) + \nu_2(r^2 - 1) - 1 & \text{if } p = 2 \text{ and } n \text{ is even;} \\ \nu_p(n) + \nu_p(r - 1) & \text{otherwise.} \end{cases}$$

Corollary 2 *Let $f \ge 2$ and p be an odd prime. If g is a primitive root modulo p, then g is a primitive root modulo p^f if and only if $g^{p-1} \not\equiv 1 \pmod{p^2}$.*

Corollary 2 is a classical result from elementary number theory. For an alternative proof see, e.g., Apostol [1, Theorem 10.6].

Proposition 2 *Let $n \geq 1$ be an integer, p a prime and put $e_p = \lfloor \log_p(n-1) \rfloor$. Let $r \equiv 1 (\text{mod } p)$ be an integer $\neq -1$. Put $r_p = \nu_p(r-1)$. If $p = 2$, we assume in addition that r is a square. The integers $r, \ldots, r^n$ are pairwise distinct modulo $p^{e_p + r_p + 1}$.*

Proof. Write $m = p^{e_p+r_p+1}$. Let $1 \leq i < j \leq n$ and suppose that $r^i \equiv r^j (\text{mod } m)$, thus $r^{j-i} \equiv 1 (\text{mod } m)$ and hence $\nu_p(r^{j-i} - 1) \geq e_p + r_p + 1$. Note that $\nu_p(k) \leq e_p$ for $1 \leq k \leq n-1$. Thus $\nu_p(j-i) \leq e_p$ and, by Lemma 1, we deduce that $\nu_p(r^{j-i} - 1) \leq e_p + r_p$. Contradiction. □

Corollary 3
The integers $9, \ldots, 9^n$ are pairwise distinct modulo 2^{e_2+4}.
The integers $81, \ldots, 81^n$ are pairwise distinct modulo 5^{e_5+2}.

Lemma 2 *Let $n \geq 2$ be an integer with $n \leq 2^m$. Then, we have that $u_1, \ldots, u_n$ are pairwise distinct modulo 2^m.*

Proof. For $n = 2$ the result is obvious. So assume that $n \geq 3$. Since the terms of the sequence alternate between even and odd, it suffices to compare the remainders (mod 2^m) of the terms having an index with the same parity. Thus assume that we have

$$u_{2j+\alpha} \equiv u_{2k+\alpha} (\text{mod } 2^m) \text{ with } 1 \leq 2j + \alpha < 2k + \alpha \leq n, \ \alpha \in \{1, 2\}.$$

It follows from this that $9^{k-j} \equiv 1 (\text{mod } 2^{m+2})$. We have $\nu_2(9^{k-j} - 1) = \nu_2(k-j) + 3$ by Lemma 1. Further, $2k - 2j \leq n - 1 < 2^m$, so $\nu_2(k-j) \leq m-2$ (here we used that $n \geq 3$). Therefore $\nu_2(9^{k-j} - 1) = \nu_2(k-j) + 3 \leq (m-2) + 3 = m+1$, which implies that $9^{k-j} - 1$ cannot be divisible by 2^{m+2}. Contradiction. □

Remark. The incongruence of u_i and u_j (mod 2^m) with i and j of the same parity and $1 \leq i < j \leq n$ is equivalent with $9, 9^2, \ldots, 9^{\lfloor (n-1)/2 \rfloor}$ being pairwise incongruent mod 2^m. Using this observation and Corollary 3 we obtain an alternative proof of Lemma 2.

On noting that trivially $D_S(n) \geq n$ and that for $n \geq 2$ the interval $[n, 2n-1]$ always contains some power of 2, we obtain the following corollary to Lemma 2.

Corollary 4 *We have $n \leq D_S(n) \leq 2n - 1$.*

Lemma 3 *The integers $u_1, \ldots, u_n$ are pairwise distinct modulo 5^m iff*

$$5^m \geq 5n/4.$$

Proof. If $5^m < 5n/4$, then $1 + 4 \cdot 5^{m-1} \leq n$. By Lemma 1 we have

$$81^{5^{m-1}} \equiv 1 (\text{mod } 5^m),$$

which ensures that $u_1 \equiv u_{1+4\cdot 5^{m-1}} (\mathrm{mod}\ 5^m)$. Next let us assume that $5^m \geq 5n/4$. This ensures that $m \geq 1$. The remainders of the sequence modulo 5 are $2, 1, 4, 3, 2, 1, \ldots$ and so the sequence has period 4 modulo 5. Thus we may assume that $m \geq 2$. It suffices to show that $u_{j_1} \not\equiv u_{k_1} (\mathrm{mod}\ 5^m)$ with $1 \leq j_1 < k_1 \leq n$ in the same congruence class modulo 4. We will argue by contradiction. Thus we assume that

$$u_{4j+\alpha} \equiv u_{4k+\alpha} (\mathrm{mod}\ 5^m) \text{ with } 1 \leq 4j + \alpha < 4k + \alpha \leq n,\ \alpha \in \{1, 2, 3, 4\}.$$

From this it follows that $81^{k-j} \equiv 1 (\mathrm{mod}\ 5^m)$, where $k - j \leq (n - \alpha)/4 < n/4 \leq 5^{m-1}$ by hypothesis and hence $\nu_5(k - j) \leq m - 2$. On invoking Lemma 1 we now infer that $\nu_5(81^{k-j} - 1) = \nu_5(k - j) + 1 \leq m - 2 + 1 = m - 1$. Contradiction. □

`Remark`. The incongruence of u_i and u_j (mod 5^m) with i and j in the same residue class modulo 4 and $1 \leq i < j \leq n$ is equivalent with $81, 81^2, \ldots, 81^{\lfloor (n-1)/4 \rfloor}$ being pairwise incongruent mod 5^m. Using this observation and Corollary 3 we obtain an alternative proof of Lemma 3.

In order to determine whether a given m discriminates $u_1, \ldots, u_n$ modulo m, we can separately consider whether $u_i \not\equiv u_j (\mathrm{mod}\ m)$ with $1 \leq i < j \leq n$ of the same parity (case 1) and with distinct parity (case 2). The first case is easy and covered by Lemma 4, the second case is trivial in case m is a power of 2 or 5, but in general much harder than the first case.

Lemma 4 *Suppose that $3 \nmid m$ and $1 \leq \alpha \leq n$. We have $u_i \not\equiv u_j (\mathrm{mod}\ m)$ for every pair (i, j) satisfying $\alpha \leq i < j \leq n$ with $i \equiv j (\mathrm{mod}\ 2)$ iff $ord_9(4m) > (n - \alpha)/2$.*

Proof. We have $u_i \not\equiv u_{i+2k} (\mathrm{mod}\ m)$ iff $9^k \not\equiv 1 (\mathrm{mod}\ 4m)$. Thus $u_i \not\equiv u_j (\mathrm{mod}\ m)$ for every pair (i, j) with $\alpha \leq i < j \leq n$ and $i \equiv j (\mathrm{mod}\ 2)$ iff $9^k \not\equiv 1 (\mathrm{mod}\ 4m)$ for $1 \leq k \leq (n - \alpha)/2$. □

Alternative proof of Lemma 2. If i and j are of different parity, then $u_i \not\equiv u_j (\mathrm{mod}\ 2)$. Hence we may assume that i and j are of the same parity. On invoking Lemma 4 we then obtain that $u_1, \ldots, u_n$ are distinct modulo 2^m iff $\mathrm{ord}_9(2^{m+2}) > (n - 1)/2$. By Lemma 1 we have $\mathrm{ord}_9(2^{m+2}) = 2^{m-1}$, concluding the proof. □

Alternative proof of Lemma 3. The remainders of the sequence modulo 5 are $2, 1, 4, 3, 2, 1, \ldots$ and so terms u_i and u_j with i and j of different parity are incongruent. Now by Lemma 4 the integers $u_1, \ldots, u_n$ are pairwise distinct modulo 5^f iff $\mathrm{ord}_9(4 \cdot 5^f) > (n - 1)/2$. Since 3 is a primitive root modulo 5 and $3^4 \not\equiv 1 (\mathrm{mod}\ 5^2)$, we have by Corollary 2 that 3 is a primitive root modulo 5^f and hence $\mathrm{ord}_3(5^f) = 4 \cdot 5^{f-1} = \varphi(5^f)$, with φ Euler's totient function. On making use of the trivial observation that, for integers m coprime to 3,

$$2\mathrm{ord}_9(4m) = \mathrm{lcm}(2, \mathrm{ord}_3(4m)), \tag{1}$$

we infer that $\mathrm{ord}_9(4 \cdot 5^f) = \mathrm{ord}_9(5^f) = \mathrm{ord}_3(5^f)/2 = 2 \cdot 5^{f-1}$. The proof is now finished by noting that the condition $\mathrm{ord}_9(4 \cdot 5^f) > (n - 1)/2$ is equivalent to $5^f \geq 5n/4$. □

4 Periodicity and discriminators

4.1 Generalities

We say that a sequence of integers $\{v_j\}_{j=1}^{\infty}$ is *(eventually) periodic* modulo d if there exist integers $n_0 \geq 1$ and $k \geq 1$ such that

$$v_n \equiv v_{n+k} (\text{mod } d) \tag{2}$$

for every $n \geq n_0$. The minimal choice for n_0 is called the *pre-period.* The smallest $k \geq 1$ for which (2) holds for every $n \geq n_0$ is said to be the *period* and denoted by $\rho_v(d)$. In case we can take $n_0 = 1$ we say that the sequence is *purely periodic* modulo d.

Let $\{v_j\}_{j=1}^{\infty}$ be a second order linear recurrence with the two starting values and the coefficients of the defining equation being integers. Note that, for a given d, there must be a pair (a, b) such hat $a \equiv v_n$ and $b \equiv v_{n+1}$ modulo d for infinitely many n. Since a pair of consecutive terms determines uniquely all subsequent ones, it follows that the sequence is periodic modulo d. If we consider n-tuples instead of pairs modulo d, we see that an nth order linear recurrence with the n starting values and the coefficients of the defining equation being integers, is always periodic modulo d.

If a sequence v is periodic modulo d_1 and modulo d_2 and $(d_1, d_2) = 1$, then we obviously have

$$\rho_v(d_1 d_2) = \text{lcm}(\rho_v(d_1), \rho_v(d_2)). \tag{3}$$

If the sequence is purely periodic modulo d_1 and modulo d_2 and $(d_1, d_2) = 1$, then it is also purely periodic modulo $d_1 d_2$. Another trivial property of ρ_v is that if the sequence v is periodic modulo d_2, then for every divisor d_1 of d_2 we have

$$\rho_v(d_1) | \rho_v(d_2). \tag{4}$$

The following result links the period with the discriminator. Its moral is that if $\rho_v(d)$ is small enough, we cannot expect d to occur as D_v-value, i.e. d does not belong to the image of D_v.

Lemma 5 *Assume that $D_v(n) \leq g(n)$ for every $n \geq 1$ with g non-decreasing. Assume that the sequence v is purely periodic modulo d with period $\rho_v(d)$. If $g(\rho_v(d)) < d$, then d is a D_v-non-value.*

Proof. Since $v_1 \equiv v_{1+\rho_v(d)} (\text{mod } d)$ we must have $\rho_v(d) \geq n$. Suppose that d is a D_v-value, that is for some n we have $D_v(n) = d$. Then $d = D_v(n) \leq g(n) \leq g(\rho_v(d))$. Contradiction. □

4.2 Periodicity of the Salajan sequence

The purpose of this section is to establish Theorem 2, which gives an explicit formula for the period $\rho(d)$ and the pre-period for the Salajan sequence. Since it is easy to show that $3 \nmid D_S(n)$, it would be actually enough to study those integers d with $3 \nmid d$ (in which case the Salajan sequence is purely periodic modulo d). However, for completeness we discuss the periodicity of the Salajan sequence for *every* d.

Theorem 2 *Suppose that $d > 1$. Write $d = 3^\alpha \cdot \delta$ with $(\delta, 3) = 1$. The period of the Salajan sequence modulo d, $\rho(d)$, exists and satisfies $\rho(d) = 2\mathrm{ord}_9(4\delta)$. The pre-period equals* $\max(1, \alpha)$.

Corollary 5 *The Salajan sequence is purely periodic iff $9 \nmid d$.*

Lemma 6 *Write $d = 3^\alpha \cdot \delta$ with $(\delta, 3) = 1$. The Salajan sequence is purely periodic iff $9 \nmid d$. Furthermore, if $9 \nmid d$, then $\rho(d) \,|\, 2\mathrm{ord}_9(\delta)$.*

Proof. Since $u = 2, \overline{1, 8} (\mathrm{mod}\ 9)$ the condition $9 \nmid d$ is necessary for the Salajan sequence to be purely periodic modulo d.

We will now show that it is also sufficient. Let us first consider the case where $\alpha = 0$. We note that $u_n \equiv u_{n+2k} (\mathrm{mod}\ d)$ iff $3^n \equiv 3^{n+2k} (\mathrm{mod}\ 4\delta)$. It follows that $\rho(d) \,|\, 2\mathrm{ord}_9(4\delta) \,|\, 2k$. If $\alpha = 1$, then we use (3) and the observation that $2 = \rho(3) \,|\, 2\mathrm{ord}_9(4\delta)$. □

`Remark`. The above proof shows that if $\rho(d)$ is even, then $\rho(d) = 2\mathrm{ord}_9(4\delta)$.

Lemma 7 *Assume that $9 \nmid d$ and $d > 1$. The Salajan sequence is purely periodic with period $\rho(d) = 2\mathrm{ord}_9(4\delta)$, where $d = 3^\alpha \cdot \delta$ with $(\delta, 3) = 1$.*

Proof. By the previous remark it suffices to show that $\rho(d)$ is even. If $\alpha = 1$, then $2 = \rho(3) \,|\, \rho(d)$ (here we use (4)) and we are done, so we may assume that $\alpha = 0$. If $5 \,|\, d$, then $4 = \rho(5) \,|\, \rho(d)$ and so we may assume that $(5, d) = 1$. Suppose that $\rho(d)$ is odd. Then

$$u_n \equiv u_{n+\rho(d)} (\mathrm{mod}\ d) \tag{5}$$

iff $3^n - 5(-1)^n \equiv 3^{n+\rho(d)} + 5(-1)^n (\mathrm{mod}\ 4d)$ iff $5^*(1 - 3^{\rho(d)})/2 \equiv (-3)^{-n} (\mathrm{mod}\ 2d)$, where 5^* is the inverse of 5 modulo $2d$. Now if (5) is to hold for every $n \geq 1$, then $(-3)^n$ assumes only one value as n ranges over the positive integers. Since $(-3)^{\phi(2d)} \equiv 1 (\mathrm{mod}\ 2d)$ we must have $(-3)^n \equiv 1 (\mathrm{mod}\ 2d)$ for every $n \geq 1$. This implies that $d = 2$ or $d = 1$. Since $5^*(1 - 3^2)/2 \not\equiv 1 (\mathrm{mod}\ 4)$ it follows that $d = 1$. Contradiction. □

Proof of Theorem 2. It is an easy observation that modulo 3^α the Salajan sequence has pre-period $\max(\alpha, 1)$ and period two. This in combination with Lemma 7 and (3) then completes the proof. □

4.3 Comparison of $\rho(d)$ with d

Lemma 8 *Let $p > 3$. We have $\rho(p^m) \,|\, \rho(p)p^{m-1}$.*

Proof. Since $3^{\rho(p)} \equiv 1 (\mathrm{mod}\ p)$ we have $3^{\rho(p)p^{m-1}} \equiv 1 (\mathrm{mod}\ p^m)$ and, provided that $\rho(p)$ is even, this implies that $u_k \equiv u_{k+\rho(p)p^{m-1}} (\mathrm{mod}\ p^m)$ for every $k \geq 1$. □

Corollary 6 *Either $\rho(p^2) = \rho(p)$ or $\rho(p^2) = p\rho(p)$.*

Proof. We have $\rho(p)|\rho(p^2)|p\rho(p)$.

Lemma 9 *We have $\rho(2^e) = 2^e$ and $\rho(3^e) = 2$. If p is odd, then $\rho(p^e)|\varphi(p^e)$.*

Proof. From Lemma 1 and Lemma 7 we infer that $\mathrm{ord}_9(2^{e+2}) = 2^{e-1}$ and hence $\rho(2^e) = 2^e$. For n large enough modulo 3^e the sequence alternates between $-5/4$ and $5/4$ modulo 3^e. Since these are different residue classes, we have $\rho(3^e) = 2$.

It remains to prove the final claim. If $p = 3$ it is clearly true and thus we may assume that $p > 3$. Note that $\rho(p^e) = 2\mathrm{ord}_9(4p^e) = 2\mathrm{ord}_9(p^e)$ and that $2\mathrm{ord}_9(p^e) \,|\, 2(\varphi(p^e)/2) = \varphi(p^e)$. □

Corollary 7 *We have $\rho(d) \leq d$.*

Lemma 10 *Suppose that $d_1, d_2 > 1$ and $(d_1, d_2) = 1$. Then*

$$\rho(d_1 d_2) \leq \rho(d_1)\rho(d_2)/2 \leq d_1 d_2/2.$$

Proof. We have $\rho(d_1 d_2) = \mathrm{lcm}(\rho(d_1), \rho(d_2))$. By Lemma 7 both $\rho(d_1)$ and $\rho(d_2)$ are even. It thus follows that $\rho(d_1 d_2) \leq \rho(d_1)\rho(d_2)/2$. The final estimate follows by Corollary 7. □

5 Non-values of $D_S(n)$

Recall that if $m = D_S(n)$ for some $n \geq 1$ we call m a Salajan value and otherwise a Salajan non-value.

Most of the following proofs rely on the simple fact that for certain sets of integers we have that if $u_1, \ldots, u_n$ are in n distinct residue classes modulo m, then $m \geq 2n$ contradicting Corollary 4.

5.1 $D_S(n)$ is not a multiple of 3

Lemma 11 *We have $3 \nmid D_S(n)$.*

Proof. We argue by contradiction and so assume that $D_S(n) = 3^\alpha m$ with $(m, 3) = 1$ and $\alpha \geq 1$. Since by definition $u_\alpha \not\equiv u_{\alpha+2t} (\mathrm{mod}\ 3^\alpha m)$ for $t = 1, \ldots, \lfloor (n-\alpha)/2 \rfloor$ and $u_\alpha \equiv u_{\alpha+2t} (\mathrm{mod}\ 3^\alpha)$ for every $t \geq 1$, it follows that $u_i \not\equiv u_j (\mathrm{mod}\ m)$ with $\alpha \leq i < j \leq n$ and i and j of the same parity. By Lemma 4 it then follows that $\mathrm{ord}_9(4m) > (n - \alpha)/2$. By Lemma 7, Corollary 7 and Corollary 4 we then find that $n - \alpha + 1 \leq 2\mathrm{ord}_9(4m) = \rho(m) \leq m \leq 2n/3^\alpha$. This implies that $n \leq 3^\alpha(\alpha - 1)/(3^\alpha - 1)$. On the other hand, by Corollary 4 we have $3^\alpha m \leq 2n$ and hence $n \geq 3^\alpha/2$. Combining the upper and the lower bound for n yields $3^\alpha \leq 2\alpha - 1$, which has no solution with $\alpha \geq 1$. □

`Remark.` It is not difficult to show directly that if $3 \nmid m$, then $2\mathrm{ord}_9(4m) \leq m$ and thus a proof of Lemma 11 can be given that is free of periodicity considerations and only involves material from Section 3.

5.2 $D_S(n)$ is a prime-power

Assume $9 \nmid d$. By Corollary 5 and Corollary 4 we can take $g(n) = 2n - 1$ in Lemma 5. This yields Lemma 12. However, for the convenience of the reader we give a more direct proof.

Lemma 12 *Suppose that d with $9 \nmid d$ satisfies $\rho(d) \le d/2$, then d is a Salajan non-value.*

Proof. Suppose that $d = D_S(n)$ for some integer n. By Corollary 4 we have $d < 2n$. By Lemma 2 the condition $9 \nmid d$ guarantees that the Salajan sequence is purely periodic modulo d. Since $u_1 \equiv u_{1+\rho(d)} (\text{mod d})$ we must have $\rho(d) \ge n$. Now suppose that $d \ge 2\rho(d)$. It then follows that $d \ge 2n$, contradicting $d = D_S(n) < 2n$. □

We now have the necessary ingredients to establish the following result. Let p be odd. On noting that in $(\mathbb{Z}/p^m\mathbb{Z})^*$ a square has maximal order $\varphi(p^m)/2$, we see that the following result says that a Salajan value is either a power of two or prime power p^m with 9 having maximal multiplicative order in $(\mathbb{Z}/p^m\mathbb{Z})^*$.

Lemma 13 *A Salajan value > 1 must be of the form p^m, with $p = 2$ or $p > 3$ and $m \ge 1$. Further, one must have $\text{ord}_9(p^m) = \varphi(p^m)/2$ and $\text{ord}_9(p) = (p-1)/2$. If $m \ge 2$ we must have $3^{p-1} \not\equiv 1 (\text{mod } p^2)$.*

Proof. Suppose that $d > 1$ is a Salajan value that is not a prime power. Thus we can write $d = d_1 d_2$ with $d_1, d_2 > 1$, $(d_1, d_2) = 1$. By Lemma 11 we have $3 \nmid d_1 d_2$. By Lemma 10 we have $\rho(d_1 d_2) \le d_1 d_2/2$, which by Lemma 12 implies that $d = d_1 d_2$ is a non-value. Thus d is a prime power p^m. By Lemma 11 we have $p = 2$ or $p > 3$. Now let us assume that $p > 3$. By Lemma 9 we have either $\rho(p^m) = \varphi(p^m)$ or $\rho(p^m) \le \varphi(p^m)/2$. The latter inequality leads to $\rho(p^m) \le p^m/2$ and hence to p^m being a non-value. Using Theorem 2 we infer that $\text{ord}_9(p^m) = \varphi(p^m)/2$. Now if $\text{ord}_9(p^m) < (p-1)/2$, this leads to $\text{ord}_9(p^m) < \varphi(p^m)$ and hence we must have $\text{ord}_9(p^m) = (p-1)/2$. Finally, suppose that $m \ge 2$ and $3^{p-1} \equiv 1 (\text{mod } p^2)$. Then $\text{ord}_9(p^m) < \varphi(p^m)/2$. This contradiction shows that if $m \ge 2$ we must have $3^{p-1} \not\equiv 1 (\text{mod } p^2)$. □

The possible Salajan values can be further limited by using some results on a quantity we will baptise as the *incongruence index*.

5.3 $D_S(n)$ is a prime or a small prime power

Put $\mathcal{P} = \{p : p > 3,\ \text{ord}_9(p) = (p-1)/2\}$. If a prime $p > 3$ is a Salajan value, then by Lemma 13 we must have $p \in \mathcal{P}$. If $p \in \mathcal{P}$, then by Theorem 2 we have $\rho(p) = p - 1$. This will be used a few times in the sequel. Let

$$\mathcal{P}_j = \{p : p > 3,\ p \equiv j (\text{mod } 4),\ \text{ord}_3(p) = p - 1\},\ j \in \{1, 3\}$$

and

$$\mathcal{P}_2 = \{p : p > 3,\ p \equiv 3 (\text{mod } 4),\ \text{ord}_3(p) = (p-1)/2\}.$$

By equation (1) we have $2\text{ord}_9(p) = \text{lcm}(2, \text{ord}_3(p))$. From this we infer that $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3$. We have

$$\mathcal{P}_1 = \{5, 17, 29, 53, 89, 101, 113, 137, 149, 173, 197, 233, 257, 269, 281, 293, \ldots\},$$

$$\mathcal{P}_2 = \{11, 23, 47, 59, 71, 83, 107, 131, 167, 179, 191, 227, 239, 251, 263, \ldots\},$$

$$\mathcal{P}_3 = \{7, 19, 31, 43, 79, 127, 139, 163, 199, 211, 223, 283, \ldots\}.$$

(The reader interested in knowing the natural densities of these sets, under GRH, is referred to the appendix.)

The aim of this section is to establish the following result, the proof of which makes use of properties of the incongruence index and is given in Section 5.4.1.

Proposition 3 *Let $d > 1$ be an integer coprime to 10. If d is a Salajan value, then $d \in \mathcal{P}_1 \cup \mathcal{P}_2$.*

5.3.1 The incongruence index

Definition 1 *Let $\{v_j\}_{j=1}^{\infty}$ be a sequence of integers and m an integer. Then the largest number k such that $v_1, \ldots, v_k$ are pairwise incongruent modulo m, we call the incongruence index, $\iota_v(m)$, of v modulo m.*

Note that $\iota_v(m) \leq m$. In case the sequence v is purely periodic modulo d, we have $\iota_v(d) \leq \rho_v(d)$. A minor change in the proof of Lemma 5 yields the following result.

Lemma 14 *Assume that $D_v(n) \leq g(n)$ for every $n \geq 1$ with g non-decreasing. If $d > g(\iota_v(d))$, then d is a D_v-non-value.*

Likewise a minor variation in the proof of Lemma 12 gives the following result, which will be of vital importance in order to discard possible Salajan values. (For the Salajan sequence u we write $\iota(d)$ instead of $\iota_u(d)$.)

Lemma 15 *If $\iota(d) \leq d/2$, then d is a Salajan non-value.*

5.3.2 Lifting from p^m to p^{m+1}

Lemma 16 *If $p > 3$ and $\iota(p^m) < \rho(p^m)$, then $\iota(p^{m+1}) < p^{m+1}/2$.*

Proof. Either $\rho(p^{m+1}) = \rho(p^m)$ or $\rho(p^{m+1}) = p\rho(p^m)$. In the first case

$$\iota(p^{m+1}) \leq \rho(p^{m+1}) = \rho(p^m) \leq p^m < p^{m+1}/2,$$

so we may assume that $\rho(p^{m+1}) = p\rho(p^m)$. This implies that

$$3^{\rho(p^m)} \equiv 1 + kp^m (\text{mod } p^{m+1}) \tag{6}$$

with $p \nmid k$. From this we infer that $u_{i+j\rho(p^m)}$ assumes p different values modulo p^{m+1} as j runs through $0, 1, \ldots, p-1$. Put $j_1 = \iota(p^m) + 1$. By assumption there exists $1 \leq i_1 < j_1$ such that $u_{i_1} \equiv u_{j_1} (\text{mod } p^m)$. Modulo p^{m+1} we have

$$\{u_{i_1+j\rho(p^m)} : 0 \leq j \leq p-1\} = \{u_{j_1+j\rho(p^m)} : 0 \leq j \leq p-1\}.$$

The cardinality of these sets is p. Now let us consider the subsets obtained from the above two sets if we restrict j to be $\leq p/2$. Each contains $(p+1)/2$ different elements. It follows that these sets must have an element in common. Say we have

$$u_{i_1+k_1\rho(p^m)} \equiv u_{j_1+k_2\rho(p^m)} (\text{mod } p^{m+1}),\ 0 \leq k_1, k_2 \leq p/2.$$

Since by assumption $i_1 \not\equiv j_1 (\text{mod } \rho(p^m))$, we have that

$$i_1 + k_1\rho(p^m) \neq j_1 + k_2\rho(p^m).$$

The proof is completed on noting that $i_1 + k_1\rho(p^m)$ and $j_1 + k_2\rho(p^m)$ are bounded above by

$$\iota(p^m)+1+(p-1)\frac{\rho(p^m)}{2} \le (p+1)\frac{\rho(p^m)}{2} \le (p+1)\frac{\varphi(p^m)}{2} = p^{m-1}\frac{(p^2-1)}{2} < \frac{p^{m+1}}{2},$$

where we used that by assumption $\iota(p^m) + 1 \le \rho(p^m)$ and Lemma 9. □

Lemma 17 *Suppose that $l \ge 1$. If $\iota(p^l) \le p^l/2$, then $\iota(p^m) \le p^m/2$ for every $m > l$.*

Proof. Note that $p > 5$. If $p \notin \mathcal{P}$, then $\rho(p^m) \le p^{m-1}\rho(p) \le p^{m-1}(p-1)/2 \le p^m/2$ and hence $\iota(p^m) \le \rho(p^m) \le p^m/2$, so we may assume that $p \in \mathcal{P}$. Now we proceed by induction. Suppose that we have established that $\iota(p^k) \le p^k/2$ for $l \le k \le m-1$. By Corollary 6 there are two cases to be considered.
Case 1. $\rho(p^2) = \rho(p) = p - 1$.
In this case $\rho(p^m) \le p^{m-2}\rho(p) = \varphi(p^{m-1}) \le p^{m-1} \le p^m/2$, and hence $\iota(p^m) \le p^m/2$.
Case 2. We have $\rho(p^2) = p\rho(p)$ and hence $\rho(p^m) = p^{m-1}\rho(p) = \varphi(p^m)$. By assumption we have $\iota(p^{m-1}) \le p^{m-1}/2 < p^{m-2}(1-1/p) = \rho(p^{m-1})$. By Lemma 16 it then follows that $\iota(p^m) \le p^m/2$. □

On combining the latter two lemmas with Lemma 15 we arrive at the following more appealing result.

Lemma 18
1) *If $p > 3$ and $\iota(p) < \rho(p)$, then $p^2, p^3, \ldots$ are all Salajan non-values.*
2) *If $\iota(p) \le p/2$, then $p, p^2, p^3, \ldots$ are all Salajan non-values.*

Proof. 1) If the conditions on p are satisfied, then by Lemma 16 it follows that $\iota(p^2) \le p^2/2$, which by Lemma 17 implies that $\iota(p^m) \le p^m/2$ for every $m \ge 2$. By Lemma 15 it then follows that p^m is a non-value.
2) If $\iota(p) \le p/2$, then $\iota(p^m) \le p^m/2$ for every $m \ge 1$ by Lemma 17 and by Lemma 15 it then follows that p^m is a non-value. □

We will see in Proposition 5 that actually $\iota(p) \le p/2$ for $p > 5$.

5.4 If $\mathbf{ord}_9(p) = (p-1)/2$, then $\iota(p) < \rho(p)$ unless $p = 5$

Lemma 15 in combination with the following lemma shows that every $p \in \mathcal{P}_3$ is a Salajan non-value. Recall that if $p \in \mathcal{P}$, then $\rho(p) = p - 1$.

Lemma 19 *Suppose that $p \in \mathcal{P}_3$. Then $\iota(p) \le p/2 < p - 1 = \rho(p)$.*

Proof. Since by assumption 3 is a primitive root modulo p, we have that $(\frac{3}{p}) = -1$. It follows that

$$1 = u_2 = \frac{(\frac{3}{p}) + 5}{4} \equiv \frac{3^{(p-1)/2} + 5}{4} = u_{\frac{p-1}{2}} (\text{mod } p).$$

We infer that $\iota(p) \leq (p-1)/2$. □

On using Lemma 16 the following result can be used to show that if $p \in \mathcal{P}_1$ and $m \geq 2$, then p^m is a Salajan non-value.

Lemma 20 *If $p > 5$ and $p \in \mathcal{P}_1 \cup \mathcal{P}_2$, then there exists $k \leq p-3$ such that $u_k \equiv u_{k+1} (\text{mod } p)$ and hence $\iota(p) < p - 1 = \rho(p)$.*

Proof. Note that

$$u_{2m-1} \equiv u_{2m} (\text{mod } p) \text{ iff } 3^{2m} \equiv 15 (\text{mod } p)$$

and

$$u_{2m} \equiv u_{2m+1} (\text{mod } p) \text{ iff } 3^{2m} \equiv -5 (\text{mod } p).$$

If $p \in \mathcal{P}_1$, then 3 is a primitive root modulo p, hence $(\frac{3}{p}) = -1$ and $(\frac{-3}{p}) = -1$ as $p \equiv 1 (\text{mod } 4)$. If $p \in \mathcal{P}_2$, then $(\frac{3}{p}) = 1$ and $(\frac{-3}{p}) = -1$ as $p \equiv 3 (\text{mod } 4)$. We see that $(\frac{15}{p}) = (\frac{-3}{p})(\frac{-5}{p}) = -(\frac{-5}{p})$ and hence either 15 or -5 is a square modulo p. Since by assumption $\text{ord}_9(p) = (p-1)/2$, every square $s \neq 0$ modulo p is of the form $s = 3^{2k}$ for some $1 \leq k \leq (p-1)/2$. It follows that either $3^{2k} \equiv -5 (\text{mod } p)$ or $3^{2k} \equiv 15 (\text{mod } p)$ for some $1 \leq k \leq (p-1)/2$. Since $3^{p-1} \equiv 1 (\text{mod } p)$ and, modulo p, -5 and 15 are not congruent to 1, it follows that $2k \leq p-3$ and so $\iota(p) \leq p - 3 + 1 = p - 2$. □

`Remark.` We have $(\frac{15}{p}) = (\frac{-5}{p})$ in case $p \in \mathcal{P}_3$ and $(\frac{-5}{p}) = -1$ iff $p \equiv \pm 1 (\text{mod } 5)$. We infer that if $p > 5$ and $p \in \mathcal{P}$, then there exists $k \leq p - 3$ such that $u_k \equiv u_{k+1} (\text{mod } p)$, except when $p \in \mathcal{P}_3$ and $p \equiv \pm 1 (\text{mod } 5)$.

`Remark.` It is not true in general that $\iota(p) < \rho(p)$, there are many counterexamples, e.g., $p = 193, 307, 1093, 1181, 1871$. It is an open problem whether there are infinitely many prime numbers p such that $\iota(p) = \rho(p)$.

5.4.1 Proof of Proposition 3

Suppose that $(d, 10) = 1$. By Lemma 13 it follows that $d = p^m$ with $p > 5$ and $p \in \mathcal{P}$. It follows from Lemmas 19 and 20 that $\iota(p) < \rho(p)$ for every $p \in \mathcal{P}$ with $p > 5$, which implies by Lemma 18 that $m = 1$ and $d = p$.

By Lemma 12 and Lemma 19 every prime $p \in \mathcal{P}_3$ is a Salajan non-value. On recalling that $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3$ the proof is then completed. □

5.5 $D_S(n)$ is not a 'big' prime

We will now use classical exponential sum techniques to show that, for sufficiently large primes, the condition given in Corollary 2 is not satisfied. Therefore, big primes are Salajan non-values.

Let us denote by ψ the additive characters of the group G and ψ_0 the trivial character. For any non-empty subset $A \subseteq G$, let us define the quantity

$$|\widehat{A}| = \max_{\psi \neq \psi_0} \left| \sum_{a \in A} \psi(a) \right|, \tag{7}$$

where the maximum is taken over all non-trivial characters in G.

Lemma 21 *Let G be a finite abelian group. For any given non-empty subsets $A, B \subseteq G$, whenever $A \cap (B+B) = \emptyset$ we have*

$$|B| \leq \frac{|\widehat{A}||G|}{|A| + |\widehat{A}|},$$

where $|\widehat{A}|$ is the quantity defined in (7).

Proof. The number N of pairs $(b, b') \in B \times B$ such that $b + b' \in A$ equals

$$N = \frac{1}{|G|} \sum_{\psi} \sum_{A} \sum_{B \times B} \psi(b + b' - a) = \frac{|B|^2|A|}{|G|} + R \tag{8}$$

where, by the orthogonality of the characters,

$$\begin{aligned} |R| &= \left| \frac{1}{|G|} \sum_{\psi \neq \psi_0} \sum_{A} \sum_{B \times B} \psi(b + b' - a) \right| \leq \frac{1}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{A} \psi(a) \right| \left| \sum_{B} \psi(b) \right|^2 \\ &\leq \frac{|\widehat{A}|}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{B} \psi(b) \right|^2 . \end{aligned}$$

Note that

$$\left| \sum_{B} \psi(b) \right|^2 = \sum_{b, b' \in B} \psi(b - b'),$$

since as complex numbers $\overline{\psi(b)} = \psi(-b)$, and that by orthogonality of the characters

$$\sum_{\psi} \sum_{b, b' \in B} \psi(b - b') = \begin{cases} 0 & \text{if } b \neq b', \\ |G| & \text{if } b = b'. \end{cases}$$

Thus

$$|R| \leq \frac{|\widehat{A}|}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{B} \psi(b) \right|^2 = \frac{|\widehat{A}|}{|G|} \left(|G||B| - |B|^2 \right). \tag{9}$$

Since by assumption $N = 0$, it follows from (8) and (9) that

$$\frac{|B|^2|A|}{|G|} \leq \frac{|\widehat{A}|}{|G|} (|G||B| - |B|^2),$$

which concludes the proof. □

We will need the following auxiliary result, which can be found in [7].

Lemma 22 *Let p be a prime and g be a primitive root modulo p. The set*

$$A = \{(x,y) : \, 3g^x - g^y \equiv 30 \pmod p\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$$

has $p-2$ elements and satisfies $|\widehat{A}| < p^{1/2}$.

Remark. It is easy to see that any subset of an abelian group satisfies that $|A|^{1/2} \le |\widehat{A}|$, so the bound in Lemma 22 is essentially best possible.

Remark. In fact this result is true in a more general context (see for example [7]): let g be a primitive root in a finite field $\mathbb{F}_q$ and a, b and c be non-zero elements in the field. Then, the set $A_g(a,b,c) = \{(x,y) : ag^x - bg^y = c\}$ in $\mathbb{F}_q$ has $q-2$ elements and satisfies $|\widehat{A}_g(a,b,c)| < q^{1/2}$.

Proposition 4 *Let $p > 3$ be a prime. Suppose that $u_1, \ldots, u_n$ are pairwise distinct modulo p. Then $p > \left\lfloor \frac{n}{4} \right\rfloor^{4/3}$.*

Proof. First observe that if two elements have the same parity index, then $u_i \not\equiv u_{i+2k} (\mathrm{mod}\ p)$ iff $9^k \not\equiv 1 (\mathrm{mod}\ p)$, thus $\mathrm{ord}_9(p) \ge n/2$. (Alternatively one might invoke Lemma 4 to obtain this conclusion.) By hypothesis, comparing elements with distinct parity index, it follows that

$$3 \cdot 9^k - 9^s \equiv 30 \pmod p, \ 1 \le k, s \le \left\lfloor \tfrac{n}{2} \right\rfloor \tag{10}$$

has no solution (otherwise $u_{2k} \equiv u_{2s-1} \pmod p$, with $1 \le 2k, 2s-1 \le n$).

We will now show that the non existence of solutions to equation (10) implies that $p > \lfloor \frac{n}{4} \rfloor^{4/3}$. Let g be a primitive root modulo p and let A be the set defined in Lemma 22. Let m be the smallest integer such that $g^m \equiv 9 \pmod p$ and

$$B = \{(mx, my) : 1 \le x, y \le \lfloor n/4 \rfloor\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}.$$

Note that, since $\mathrm{ord}_9(p) \ge n/2$, it follows that $|B| = \left\lfloor \frac{n}{4} \right\rfloor^2$ (since m generates a subgroup of order at least $n/2$ modulo $p-1$).

Observe that the non existence of solutions to equation (10) implies that

$$3 \cdot g^{mk} - g^{ms} \equiv 30 \pmod p, \ 1 \le k, s \le \left\lfloor \tfrac{n}{2} \right\rfloor$$

has no solutions and in particular $A \cap (B+B) = \emptyset$ (since clearly $B + B \subseteq \{(mx, my) : 1 \le x, y \le \lfloor n/2 \rfloor\}$). It follows from Lemma 21 and Lemma 22 that

$$|B| = \left\lfloor \frac{n}{4} \right\rfloor^2 \le \frac{|\widehat{A}||G|}{|A| + |\widehat{A}|} \le \frac{p^{1/2}(p-1)^2}{p-2+p^{1/2}} < p^{3/2}, \tag{11}$$

which concludes the proof. □

Corollary 8 *If $p > 5$ is a prime number, then p is a Salajan non-value.*

Proof. First observe that, if $n \ge 2060$ then it follows from Proposition 4 that if, for some prime $p \ge n$ the elements $u_1, \ldots, u_n$ are pairwise distinct modulo p then

$$p > \left\lfloor \frac{n}{4} \right\rfloor^{4/3} \ge 2n,$$

and by Corollary 2 it follows that p is a Salajan non-value. For primes $5 \le p \le 2060$, the result follows from the calculations included in Table 1. □

Taking $n = \iota(p)$ in Proposition 4 we obtain, after some numerical work, the following estimate. Since $\iota(29) = 14$ the bound is sharp.

Proposition 5 *Let $p > 5$ be a prime. Then $\iota(p) \le \min((p-1)/2, 4p^{3/4})$.*

Proof. By Proposition 4 we infer that $\iota(p) < 3 + 4p^{3/4}$. A tedious analysis using the one but last estimate for $|B|$ in (11) gives the more elegant bound $\iota(p) < 4p^{3/4}$. For $p < 4111$ one verifies the claimed bound by direct computation. Since $4p^{3/4} < (p-1)/2$ for $p \ge 4111$, we are done. □

6 The proof of Salajan's conjecture

In Section 3, we established that powers of 2 and powers of 5 were candidates for Salajan values. Finally, after studying the characteristics of the period and the incongruence index of the Salajan sequence, we discard in Section 5 any other possible candidates.

Proof of Theorem 1. It follows from Proposition 3 that if $d > 1$ is a Salajan value, then either $(10, d) > 1$ or $d \in \mathcal{P}_1 \cup \mathcal{P}_2$. It follows from Corollary 8 that no prime greater than 5 can be a Salajan value and hence $(10, d) > 1$. By Lemma 12 it follows that d has to be a prime power. Therefore, since $(10, d) > 1$, the discriminator must be a power of 2 or a power of 5.

First suppose that $D_S(n) = 2^e$. On invoking Lemma 2 it then follows that $e = \min\{a : 2^a \ge n\}$. Next suppose that $D_S(n) = 5^f$. By Lemma 3 it then follows that $f = \min\{a : 2^a \ge 5n/4\}$. So we have $D_S(n) = 2^e$ or $D_S(n) = 5^f$. By the definition of the discriminator we now infer that $D_S(n) = \min\{2^e, 5^f\}$. □

7 Appendix

7.1 The natural density of the sets $\mathcal{P}_i$

Standard methods allow one to determine, assuming the Generalized Riemann Hypothesis, the densities of the sets $\mathcal{P}_i$ defined in Section 5.3. (For a survey of related material see Moree [13].)

Proposition 6 *Assume GRH. We have*

$$\#\{p \le x : p \in \mathcal{P}_i\} = \delta(\mathcal{P}_i)\frac{x}{\log x} + O\Big(\frac{x \log\log x}{\log^2 x}\Big),$$

with $\delta(\mathcal{P}_1) = \delta(\mathcal{P}_2) = 3A/5 = 0.224373488\ldots$ and $\delta(\mathcal{P}_3) = 2A/5 = 0.149582325\ldots$ and

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots,$$

the Artin constant.

Corollary 9 *The result also holds for the set $\mathcal{P}$, where we find $\delta(\mathcal{P}) = \delta(\mathcal{P}_1) + \delta(\mathcal{P}_2) + \delta(\mathcal{P}_3) = 8A/5 = 0.598329301\ldots$.*

Proof. These three results can be obtained by a variation of the classical result of Hooley [8] and this yields the estimate with $\delta(\mathcal{P}_i)$ yet to be determined. We note that the sets $\mathcal{P}_i$ are mutually disjunct. By [12, Theorem 4] we have $\delta(\mathcal{P}_1) = 3A/5$ and $\delta(\mathcal{P}_1 \cup \mathcal{P}_3) = A$. This gives $\delta(\mathcal{P}_3) = 2A/5$. By [14, Theorem 3] we have $\delta(\mathcal{P}) = 8A/5$ and hence $\delta(\mathcal{P}_2) = \delta(\mathcal{P}) - \delta(\mathcal{P}_1 \cup \mathcal{P}_3) = 3A/5$. □

For the benefit of the reader we give a perhaps more insightful argument why $\delta(\mathcal{P}_2) = 3A/5$.

Assuming GRH we have, cf. Moree [14],

$$\delta(\mathcal{P}_2) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_{2n}, 3^{1/2n}) : \mathbb{Q}]} - \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(i, \zeta_{2n}, 3^{1/2n}) : \mathbb{Q}]},$$

where the first sum gives the density of the primes p such that $\mathrm{ord}_3(p) = (p-1)/2$ and the second sum the density of the primes p such that $p \equiv 1(\mathrm{mod}\ 4)$ and $\mathrm{ord}_3(p) = (p-1)/2$. Since for n even, $i \in \mathbb{Q}(\zeta_{2n})$, we find that

$$\delta(\mathcal{P}_2) = \sum_{(n,2)=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_{2n}, 3^{1/2n}) : \mathbb{Q}]} - \sum_{(n,2)=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(i, \zeta_{2n}, 3^{1/2n}) : \mathbb{Q}]}.$$

Now suppose that n is odd. If $3|n$, then $\sqrt{-3} \in \mathbb{Q}(\zeta_{2n})$. Since $\sqrt{3} \in \mathbb{Q}(\zeta_{2n}, 3^{1/2n})$, it follows that $\mathbb{Q}(i, \zeta_{2n}, 3^{1/2n}) = \mathbb{Q}(\zeta_{2n}, 3^{1/2n})$. On the other hand, if $(n,3) = 1$ one infers that $[\mathbb{Q}(i, \zeta_{2n}, 3^{1/2n}) : \mathbb{Q}] = 2[\mathbb{Q}(\zeta_{2n}, 3^{1/2n}) : \mathbb{Q}]$. This leads to

$$\delta(\mathcal{P}_2) = \frac{1}{2} \sum_{(n,6)=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_{2n}, 3^{1/2n}) : \mathbb{Q}]} = \frac{1}{4} \sum_{(n,6)=1} \frac{\mu(n)}{n\varphi(n)} = \frac{3}{5}A,$$

where we used that $[\mathbb{Q}(\zeta_{2n}, 3^{1/2n}) : \mathbb{Q}] = \varphi(2n)2n = 2\varphi(n)n$ if $(n,6) = 1$ and the identity

$$\sum_{(n,6)=1} \frac{\mu(n)}{n\varphi(n)} = \prod_{p>3} \left(1 - \frac{1}{p(p-1)}\right) = \frac{12}{5}A.$$

7.2 Counting the elements $\leq x$ in $\mathcal{F}$

In this section, written jointly with Izabela Petrykiewicz, we will establish Proposition 1 from the introduction.

Recall that $\mathcal{F} = \{f\ :\ [4 \cdot 5^{f-1}, 5^f]$ contains no power of $2\}$. Consider $\mathcal{G} = \mathbb{N} \backslash \mathcal{F}$. We have that g is in $\mathcal{G}$ iff $4 \cdot 5^{g-1} \leq 2^k \leq 5^g$ for some $k \in \mathbb{N}$. Thus we have g is in $\mathcal{G}$ iff $2\log 2 + (g-1)\log 5 \leq k \log 2 \leq g \log 5$, that is iff $2 + (g-1)\alpha \leq k \leq g\alpha$, where $\alpha = \log 5/\log 2$. Since k is an integer, we may replace $g\alpha$ by $[g\alpha]$ and the condition becomes $k \in [[g\alpha] + \{g\alpha\} + 2 - \alpha, [g\alpha]]$. Note that there can be only an integer in this interval iff $\{g\alpha\} \leq \alpha - 2$. Note that α is irrational. Now it is a consequence of Weyl's criterion, see, e.g., [6, 9], that for a fixed $0 < \beta < 1$ we have

$$\#\{g \leq x : \{g\alpha\} \leq \beta\} \sim \beta x,\ \ x \to \infty.$$

On applying this with $\beta = \alpha - 2$ the proof of Proposition 1 is easily completed. □

Acknowledgement. This project was started in the context of an internship of Sabin Salajan at MPIM in 2012 and a visit of the first author to the second author to ICMAT in Madrid. The project was taken up again during a two week visit of Bernadette Faye (Senegal) at MPIM. The first author thanks Bernadette for discussions and her help with some computer experiments. Further he thanks David Brink, Igor Shparlinski and Arne Winterhof for helpful e-mail correspondence and Paul Tegelaar for comments on an earlier version. The idea of the proof of Proposition 1 is due to Izabela Petrykiewicz.

References

[1] T. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[2] L.K. Arnold, S.J. Benkoski and B.J. McCabe, The discriminator (a simple application of Bertrand's postulate), *Amer. Math. Monthly* **92** (1985), 275-277.

[3] R.F. Beyl, Cyclic subgroups of the prime residue group, *Amer. Math. Monthly* **84** (1977), 46-48.

[4] P.S. Bremser, P.D. Schumer and L.C. Washington, A note on the incongruence of consecutive integers to a fixed power, *J. Number Theory* **35** (1990), 105-108.

[5] J. Browkin and H.-Q. Cao, Modifications of the Eratosthenes sieve, *Colloq. Math.* **135** (2014), 127–138.

[6] Y. Bugeaud, *Distribution modulo one and Diophantine approximation*, Cambridge Tracts in Mathematics **193**, Cambridge University Press, Cambridge, 2012.

[7] J. Cilleruelo and A. Zumalacárregui, An additive problem in finite fields with powers of elements of large multiplicative order, *Rev. Mat. Complut.* **27** (2014), 501–508.

[8] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.

[9] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Pure and Applied Mathematics, Wiley-Interscience, New York-London-Sydney, 1974

[10] H.B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience Publishers John Wiley and Sons, New York-London-Sydney, 1965.

[11] P. Moree, The incongruence of consecutive values of polynomials, *Finite Fields Appl.* **2** (1996), 321-335.

[12] P. Moree, Uniform distribution of primes having a prescribed primitive root, *Acta Arith.* **89** (1999), 9–21.

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

[14] P. Moree, Near-primitive roots, *Funct. Approx. Comment. Math.* **48.1** (2013), 133–145.

[15] P. Moree and G. L. Mullen, Dickson polynomial discriminators, *J. Number Theory* **59** (1996), 88–105.

[16] Zhi-Wei Sun, On functions taking only prime values, *J. Number Theory* **133** (2013), 2794–2812.

[17] M. Zieve, A note on the discriminator, *J. Number Theory* **73** (1998), 122-138.