SALEM NUMBERS OF NEGATIVE TRACE

C. J. SMYTH

Abstract. We prove that, for all \( d \geq 4 \), there are Salem numbers of degree \( 2d \) and trace \( -1 \), and that the number of such Salem numbers is \( \gg d / (\log \log d)^2 \). As a consequence, it follows that the number of totally positive algebraic integers of degree \( d \) and trace \( 2d - 1 \) is also \( \gg d / (\log \log d)^2 \).

1. Introduction

Recall that a \textit{Salem number} is an algebraic integer \( \tau > 1 \), of degree \( \geq 4 \), all of whose conjugates, apart from \( \tau \) and \( \tau^{-1} \), have modulus 1. How small can the trace of a Salem number be? It is known that all Salem numbers of degree up to 18 have trace at least \( -1 \) (Proposition 6.1).

The aim of this paper is to study the set \( S_d \) of Salem numbers of degree \( 2d \) and trace \( -1 \). This set is tabulated in Table 1 for \( 2d \leq 14 \). It is easy to see that \( S_d \) is finite for all \( d \). In order to state our main result, we define the subset \( S'_d \) of \( S_d \) to be those Salem numbers \( \tau_{d,m} \) with minimal polynomial

\[
P_{d,m}(z) = \left( z^2 (z^2 - z - 1) + z^{2(d-m)} + z^{2(m+1)} - z^2 - z + 1 \right) / (z - 1)^2.
\]

Here \( m \) must be in the range \( 1 \leq m \leq [(d-1)/2] \), and be such that \( P_{d,m} \) is irreducible. Then we have

\textbf{Theorem 1.1.} For every \( d \geq 4 \), \( S_d \) is non-empty. Further, for \( d \geq 5 \), \( S'_d \) is non-empty, and, for \( d \) sufficiently large,

\[
|S_d| \gg |S'_d| > \frac{0.1387d}{(\log \log d)^2},
\]

so that certainly \( |S_d| \to \infty \) as \( d \to \infty \).

In fact, it is likely that \( |S_d| \) grows at least exponentially with \( d \).

The Salem number \( \tau_{d,m} \) can in fact be associated with a particular tree, the three-armed star-like tree with \( 1, 2m \) and \( 2(d - m - 1) \) edges on its arms, in a manner described in [MRS].

As a consequence of the theorem, we obtain a similar result for the set \( A_d \) of totally positive (i.e. all conjugates positive) algebraic integers of degree \( d \) and trace \( 2d - 1 \). We define the subset \( A'_d \) of \( A_d \) to be those \( \alpha_{d,m} \) in \( A_d \) with minimal
Polynomial

$$Q_{d,m}(y) = y^d - (2d - 1) y^{d-1}$$

+ \sum_{k=2}^{d-1} (-1)^k y^{d-k} \left\{ \binom{2d-k}{k} - \sum_{i=\max(0,k-m-1)}^{\min(d-m-2,k-2)} \binom{2d-2m-3-i}{k-2-i} \binom{2m-k+1+i}{k-2-i} \right\} + (-1)^d.$$

Again, \( m \) must satisfy \( 1 \leq m \leq \lfloor (d-1)/2 \rfloor \) and be such that \( Q_{d,m} \) is irreducible. Then

**Corollary 1.2.** For every \( d \geq 1 \), \( A_d \) is non-empty. Also \( A'_d \) is non-empty for \( d \geq 5 \) and, for \( d \) sufficiently large,

$$|A_d| > |A'_d| > \frac{0.1387d}{(\log \log d)^2},$$

so that certainly \( |A_d| \to \infty \) as \( d \to \infty \).

The proofs of Theorem 1.1 and Corollary 1.2 are based on the following factorization of \( P_{d,m} \).

**Theorem 1.3.** For \( d \geq 5 \) and \( 1 \leq m \leq \lfloor (d-1)/2 \rfloor \), \( P_{d,m}(z) \) factors as the product of the minimal polynomial of a Salem number \( \tau_{d,m} \) and a (possibly trivial) cyclotomic polynomial, which is

$$C(z) = \begin{cases} C(z) C_{12}(z) & \text{if } d \equiv 3 \mod 6 \text{ and } m \equiv 1 \mod 6, \\
C(z) C_{30}(z) & \text{if } d \equiv 4 \mod 15 \text{ and } m \equiv 1 \text{ or } 2 \mod 15, \\
C(z) & \text{otherwise.} \end{cases}$$

Here \( C_{12}(z) = z^4 - z^2 + 1 \), \( C_{30}(z) = P_{4,1}(z) = z^8 + z^7 - z^5 - z^4 - z^3 - z + 1 \) and

$$C(z) = \frac{z^{g_1} - 1}{z - 1} \cdot \frac{z^{g_2} - 1}{z - 1} \cdot \frac{z^{g_3} - 1}{z - 1},$$

where \( g_1 = \gcd(d,2m+1), \ g_2 = \gcd(2d+1,2m+3), \ g_3 = \gcd(2d+1,m) \) and \( g_4 = \gcd(g_2,g_3) \) (\( = 1 \) or \( 3 \)).

From the theorem one can readily read off the trace of \( \tau_{d,m} \). It is equal to \(-1 + n_1 + n_2 + n_3 + n_4\), where \( n_1 = 1 \) if \( g_1 > 1 \), and 0 otherwise, \( n_2 = 1 \) if \( g_2 > 1 \), and 0 otherwise, \( n_3 = 1 \) if \( g_3 > g_4 \), and 0 otherwise, and \( n_4 = 1 \) if \( d \equiv 4 \mod 15 \) and \( m \equiv 1 \) or 2 mod 15, and 0 otherwise. In particular, \( \tau_{d,m} \) has trace \(-1\) iff it has degree \( 2d \), i.e. iff \( P_{d,m} \) is irreducible.

Of course, we are particularly interested in the pairs \( d,m \) for which \( P_{d,m} \) is irreducible:

**Corollary 1.4.** For \( d \geq 5 \), \( 1 \leq m \leq \lfloor (d-1)/2 \rfloor \), \( P_{d,m} \) has the \( n \)th cyclotomic polynomial \( C_n \) as a factor if

(i) \( n \) odd \( \geq 3 \), \( d \equiv 0 \mod n \), \( m \equiv \frac{n-1}{2} \mod n \)

or

(ii) \( n \) odd \( \geq 3 \), \( d \equiv \frac{n-1}{2} \mod n \), \( m \equiv 0 \) or \( \frac{n-3}{2} \mod n \).
(iii) \( n = 12, d \equiv 3 \mod 6, m \equiv 1 \mod 6 \)

or

(iv) \( n = 30, d \equiv 4 \mod 15, m \equiv 1 \) or \( 2 \mod 15, \)

and in no other case. In particular, putting

\[
\mathcal{M}_d = \{ m : 1 \leq m \leq [(d - 1)/2], m \neq \frac{p - 1}{2} \mod p \text{ for all odd primes } p | d, \\
m \neq 0 \text{ or } q \equiv \frac{-3}{2} \mod q \text{ for all odd primes } q | 2d + 1 \},
\]

\( P_{d,m} \) is irreducible iff

\[
\begin{aligned}
m &\in \mathcal{M}_d \text{ if } d \not\equiv 4 \mod 15, \\
m &\in \mathcal{M}_d \cap \{ m \neq 1 \text{ or } 2 \mod 15 \} \text{ if } d \equiv 4 \mod 15.
\end{aligned}
\]

The polynomial \( Q_{d,m} \) is defined by \( Q_{d,m}(z + 1/z + 2) = z^{-d}P_{d,m}(z) \). Its factorization can thus be written down from the factorization of \( P_{d,m} \). In particular, \( Q_{d,m} \) is irreducible iff \( P_{d,m} \) is irreducible.

The polynomial \( P_{d,m}(z) \) can also be written

\[
\begin{aligned}
z^{2d} + z^{2d-1} - z^{2d-3} - 2z^{2d-4} - \ldots - (2m - 2)z^{2d-2m} \\
- (2m - 1)\left( z^{2d-(2m+1)} + z^{2d-(2m+2)} + \ldots + z^{2m+2} + z^{2m+1} \right) \\
- (2m - 2)z^{2m} - \ldots - 2z^4 - z^3 + z + 1.
\end{aligned}
\]

One way in which \( P_{d,m} \) (or, equivalently, \( \tau_{d,m} \)) arises naturally is the following: the smallest limit point in the set of Pisot numbers is \( \rho = \frac{1}{2} (1 + \sqrt{5}) \), which is a limit of Pisot numbers \( \vartheta_m < \rho \) with minimal polynomial

\[
(z^{2m} (z^2 - z - 1) + 1) / (z - 1) \quad (m \geq 1).
\]

Then the standard construction ([Sa], [BDGPS]) proving that every Pisot number is a limit from below of Salem numbers shows that \( \vartheta_m \) is a limit from below of the \( \tau_{d,m} \), as \( d \to \infty \).

The factorization of \( P_{d,m} \) described here was first conjectured on the basis of computational evidence obtained for \( d \leq 40 \) using Maple.

2. Standard Lemmas

Let \( \omega_n = e^{2\pi i/n} \). Then we need

Lemma 2.1. For all natural numbers \( n \),

(a) \(-\omega_n\) is a conjugate of \( \omega_n \) iff \( n \) is a multiple of 4;

(b) \(-\omega_n^2\) is a conjugate of \( \omega_n \) iff \( n \) is divisible by 2 but not by 4;

(c) \( \omega_n^2 \) is a conjugate of \( \omega_n \) iff \( n \) is odd.

The proof is an easy exercise. We also need the standard estimates

Lemma 2.2. For \( n \geq 3 \)

\[
\prod_{p | n \text{ prime}} \left( 1 - \frac{1}{p} \right) > \frac{1}{e\gamma \log \log n + 2.50637/\log \log n} =: f(n),
\]

say, and for \( n > 26 \)

\[
\omega(n) < \frac{\log n}{\log \log n - 1.1714} =: h(n),
\]
say. Here $\omega(n)$ is the number of distinct prime factors of $n$, and $\gamma$ is Euler’s constant 0.577\ldots.

For the proofs, see [RS], p.72, and [Robin], respectively, or [MSC].

We also need a (presumably well-known) crude sieving estimate:

**Lemma 2.3.** Let $\mathcal{D}$ be a finite set of pairwise relatively prime integers, all at least 2, and for each $p$ in $\mathcal{D}$ let $\mathcal{R}_p$ be a set of $r_p < p$ residue classes mod $p$. Then the number $N$ of positive integers $m \leq M$ which are not $x_p \mod p$ for any $x_p$ in $\mathcal{R}_p$ and any $p$ in $\mathcal{D}$ satisfies

$$|N - M \prod_{p \in \mathcal{D}} \left(1 - \frac{r_p}{p}\right)| \leq \prod_{p \in \mathcal{D}} (1 + r_p).$$

The proof is an easy application of the Principle of Inclusion and Exclusion and the Chinese Remainder Theorem. Alternatively, it is slight extension of the results of [HR], pp. 30-31.

3. **Proof of Theorem 1.3**

We first need

**Lemma 3.1.** For $d \geq 5$ and $1 \leq m \leq \lfloor (d-1)/2 \rfloor$ the polynomial $P_{d,m}$ has a real root $\tau_{d,m} > 1$. All other roots are on $|z| = 1$ except for $\tau_{d,m}^{-1}$. For fixed $d \geq 5$ the $\tau_{d,m} (1 \leq m \leq \lfloor (d-1)/2 \rfloor)$ are all distinct. For $d, m$ in this range, $P_{d,m}(1) \neq 0$.

**Proof.** Consider

$$R_{d,m}(z) := (z - 1)^2 P_{d,m}(z) = z^{2d}(z^2 - 1) + z^{2(d-m)} + z^{2(m+1)} - z^2 - z + 1.$$

Then by a standard Rouche’s Theorem argument to be found in [Sa], $R_{d,m}$ has at most one zero in $|z| > 1$. Further, if $R_{d,m}(1) < 0$ then $R_{d,m}$ will have exactly one zero in $|z| > 1$. Now

$$R_{d,m}(1) = 2(4m(m+1) + 1 - 2(2m-1)d) < 0$$

if

$$d \geq \left\lfloor \frac{4m(m+1)+1}{2(2m-1)} \right\rfloor = \begin{cases} 5 & \text{for } m = 1, 2, 3 \\ m + 2 & \text{for } m \geq 4 \end{cases}$$

This shows that $R_{d,m}$ has one root in $|z| > 1$ for $1 \leq m \leq d - 2 (d \geq 5)$.

Now $P_{d, d - m - 1} = P_{d, m}$, so that the $\tau_{d,m}$ can, for fixed $d$, be distinct only for $m \leq d - m - 1$, i.e. $m \leq \lfloor (d-1)/2 \rfloor$. Indeed, for $1 \leq m' < m \leq \lfloor (d-1)/2 \rfloor$ and $\tau := \tau_{d,m}$,

$$R_{d, m'}(\tau) = R_{d,m'}(\tau) - R_{d,m}(\tau) = \tau^{2(d-m')} + \tau^{2(m'+1)} - \tau^{2(d-m)} - \tau^{2(m+1)} = \left(\tau^{2(m'-m')} - 1\right)(-\tau^{2(m'+1)} + \tau^{2(d-m)}) > 0.$$

Thus the $\tau_{d,m}$ are distinct for $d$ fixed and $1 \leq m \leq \lfloor (d-1)/2 \rfloor$.

We now prove the theorem, or rather, Corollary 1.4 which is really an alternative formulation of Theorem 1.3.
We first write $R_{d,m}(z)/z = 0$ in the form

\begin{equation}
-z^{2d} = \frac{u - z - 1 + \frac{1}{z}}{\frac{1}{u} - \frac{1}{z} - 1 + z},
\end{equation}

where $u = z^{2m+1}$. We assume that $z = \omega_n$ is a zero of $P_{d,m}$ and so of (5), and, in order to use Lemma 2.1, separate three cases:

(a) The case $4|n$. Here $z = -\omega_n$ is also a root of (5), so that

\begin{equation}
-z^{2d} = \frac{u - z - 1 + \frac{1}{z}}{\frac{1}{u} - \frac{1}{z} - 1 + z} = -u + z - 1 - \frac{1}{z}
\end{equation}

which gives

\begin{equation}
2 \left( z - \frac{1}{z} \right) = u - \frac{1}{u}.
\end{equation}

To solve (7), put $z = e^{2\pi i/4}k$ say, with conjugates $z^{-r} = e^{2\pi i r/4k}$, where $(r, 4k) = 1$. Hence, applying the Galois element $z \mapsto z^r$, we get

\begin{equation}
2 \left( z^r - z^{-r} \right) = (u^r - u^{-r}),
\end{equation}

so that

\begin{equation}
2 \left| \sin \frac{\pi r}{2k} \right| = \left| \sin \frac{\pi r(2m + 1)}{2k} \right| \leq 1.
\end{equation}

Thus there can be no $r$ with $(r, 2k) = 1$ and $\frac{k}{3} < r \leq k$. However, the examples $(r,k) = (1,1), (2t - 1, 2t)$ and $(2t - 1, 2t + 1)$ for $t \geq 2$ show that every value of $k$ except $k = 3$ is impossible. For $k = 3$, $z = e^{2\pi i/12}$ and $2 \left( z - \frac{1}{z} \right) = 2i$. (7) has the unique solution $u = i = e^{2\pi i(2m+1)/12}$, giving $2m + 1 \equiv 3 \mod 12$, $m \equiv 1 \mod 6$. Then (5) gives $-z^{2d} \equiv 1$, $2d \equiv 6 \mod 12$, $d \equiv 3 \mod 6$.

(b) The case $2|n, 4 \n| n$. Starting with (5), use Lemma 2.1(b) to replace $z$ by $-z^2$, $u$ by $-u^2$ and eliminate $z^{2d}$ to obtain

\begin{equation}
(-z^{2d})^2 = \left( \frac{u - z - 1 + \frac{1}{z}}{\frac{1}{u} - \frac{1}{z} - 1 + z} \right)^2 = \left( -z^2 \right)^{2d} = -\left( \frac{-u^2 - (z^2) - 1 + \frac{1}{z^2}}{\frac{1}{-u^2} - \frac{1}{z^2} - 1 - z^2} \right).
\end{equation}

Clearing the denominators gives a plane algebraic curve $f(u, z) = 0$, independent of $d$. Since then also $f(-u^2, -z^2) = 0$, the pairs $(u, z)$ of interest lie on both curves. To find all possible $(u, z)$ pairs, we use a Maple program

\begin{itemize}
\item[(Sin)] which uses a version of the Euclidean algorithm to find all such intersection points, with multiplicities.
\end{itemize}

The program tells us that the only such intersection points with $z$ and $u$ nth roots of unity with $2|n, 4 \n| n$ are the pairs $(u, z) = (\alpha^3, \alpha)$ and $(\alpha^5, \alpha)$, where $\alpha$ is a primitive 30th root of unity. Both points have multiplicity one. Hence $2m + 1 = 3$ or $5$, $m = 1$ or $2$. [Alternatively, one can of course use the classical resultant method to find $z$, say, and then back-substitute to find the corresponding values of $u$. Doing this, one finds that the cyclotomic factors of this resultant are $C_{30}^2, (z - 1)^8, (z + 1)^8$.]
and \((z^2 + 1)^8\), from which the pairs \((z, u)\) can again be found. Then, using (5), we find that, when \(m = 1\), \(u = z^3\),

\[-z^{2d} = \frac{z^3 - z - 1 + \frac{1}{z}}{z^3 - z^{-1} - 1 + \frac{1}{z}} = -z^8\]
on routine simplification, using \(C_{30}(z) = 0\). Again, for \(m = 2\), \(u = z^5\), (3) gives \(-z^{2d} = -z^8\) again. Hence \(2d = 8 \mod 30, d = 4 \mod 15\), for \(m = 1\) or 2.

(c) The case \(n\) odd. In a way similar to the previous case, apply Lemma 2.1(c) to (5), and also replace \(z\) by \(z^2\), to obtain

\[-(-z^{2d})^2 = -\left(\frac{u - z - 1 + \frac{1}{z}}{u - \frac{1}{z} - 1 + z}\right)^2 = -(z^{2d})^2 = \frac{u^2 - 2z^2 - 1 + \frac{1}{z^2}}{1 - \frac{1}{u^2} - \frac{1}{z^2} - 1 + \frac{z^2}{u^2}}.

Clearing denominators this time gives

\[(u - 1)^2 (uz^2 - 1) (z - u) (z + 1) (z - 1) = 0.

Since neither \(\pm 1\) is a zero of \(P_{d,m}\), we need consider only the subcases where one of the first three factors is 0:

(i) \(u = 1\). Here \(u = z^{2m+1} = 1, m \equiv \frac{n - 1}{2} \mod n\). Then, from (5), \(z^{2d} = 1, z^d = 1\), i.e. \(d \equiv 0 \mod n\).

(ii) \(u = z^{-2}, z^{2m+3} = 1, m \equiv \frac{n - 3}{2} \mod n\), and, from (5), \(z^{2d+1} = 1, d \equiv \frac{n - 1}{2} \mod n\).

(iii) \(u = z, z^{2m} = 1, z^m = 1, m \equiv 0 \mod n\), and, from (5), \(z^{2d+1} = 1, d \equiv \frac{n - 1}{2} \mod n\).

This completes the proof of Corollary 1.4. Theorem 1.3 now follows readily by collecting together all the cyclotomic factors \(C_n(z)\) of \(P_{d,m}\) for \(n\) odd, and noting that \(\gcd(g_1, g_2) = \gcd(g_1, g_3) = 1\), and \(g_4 = \gcd(g_2, g_3) = 1\) or 3.

4. PROOF OF THEOREM 1.1

For the proof, we need to find a positive lower bound for \(|S'_d|\). First we show that

**Lemma 4.1.** The set \(S'_d\) is non-empty for \(5 \leq d \leq B := 7.98 \times 10^{12}\).

**Proof.** First, direct Maple computation of the set \(M_d\) shows that \(M_d\), and hence \(S'_d\) is non-empty for \(5 \leq d \leq 2998\). The set \(M_d\) is shown for \(d \leq 60\) in Table 2 (at the end of this paper). Next, we find, again using Maple, that the primes \(m' \in \{5, 29, 53, 89, 113, 173, 509, 659, 743, 809, 1013, 1499\}\) have the property that, for each of these primes \(m'\), the numbers \(2m' + 1\) and \(2m' + 3\) are also both prime. Further, there is no repeated prime in the multiset of all such \(m', 2m' + 1, 2m' + 3\) for \(m'\) in the above set of primes.

Now suppose that \(d \geq 2999\). Then, by Lemma 3.1, the polynomials \(P_{d,m}\) for fixed \(d\) and \(1 \leq m \leq 1499 = (2999 - 1)/2 \leq [(d - 1)/2]\) all are divisible by the minimal polynomials of distinct Salem numbers. I claim that for \(m\) equal to at least one \(m'\) on the above list, \(m' \in M_d\), so that \(M_d\) and hence \(S'_d\) is non-empty. For, if not, then, from the definition of \(M_d\), either \(m'|2d + 1\) or \((2m' + 3)|2d + 1\) or
we get 
\[ d \] 
now 
\[ \prod m'' \geq \prod m' = 4.08 \times 10^{27} > 1.27 \times 10^{26} = B(2B + 1) \geq d(2d + 1) \]
gives a contradiction.

We next find a lower bound for \(|S_d'\)| for large \(d\), i.e. for \(d > B\). To do this, we apply Lemma 2.3 using the description of the integers \(m\) in \(S_d'\) given by Corollary 1.2.

First consider the case \(d \not\equiv 4 \mod 15\). Take \(D\) to be the set of odd primes dividing \(d(2d + 1)\), and \(R_p = \{\frac{1}{2}(p - 1)\}\) if \(p\) is an odd prime dividing \(d\), and \(R_q = \{0, \frac{1}{2}(q - 3)\}\) if \(q\) is a prime dividing \(2d + 1\). Put \(r_p = |R_p|\). Then \(r_p = 1\) for \(p|d\), \(r_3 = 1\) if \(3|2d + 1\); otherwise \(r_q = 2\) if \(q|2d + 1\), \(q \neq 3\). Hence, applying Lemma 2.3 with \(M = [(d - 1)/2]\), we obtain

\[
|S_d'| \geq M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1, q \neq 3} \left(1 - \frac{2}{q}\right) - 2^{\omega(d)}3^{\omega(2d+1)}.
\]

Here \(\omega(r)\) is the number of prime factors of \(r\), and \(d_3 = 3d\) if \(3|2d + 1\), while \(d_3 = d\), otherwise.

Similarly, for the case \(d \equiv 4 \mod 15\) we have \(2d + 1 \equiv 9 \mod 15\), so \(3|2d + 1\), but \(3 \nmid d\). Thus there are seven excluded residue classes mod 15: \(m \not\equiv 0, 1, 2, 3, 6, 9, 12 \mod 15\), and the lemma gives

\[
|S_d'| \geq M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{2}{q}\right) \left(1 - \frac{7}{15}\right) - 2^{\omega(d)}3^{\omega(2d+1)-1}(1 + 7).
\]

We now apply Lemma 2.2 to (10) and (11). Thus for \(d \not\equiv 4 \mod 15\), and \(3 \nmid 2d + 1\) we get

\[
|S_d'| \geq M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{2}{q}\right) - 2^{\omega(d)}3^{\omega(2d+1)}
\]

\[
> M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{1}{q}\right)^2 \prod_{q \geq 5 \text{prime}} \left(1 - \frac{1}{(q - 1)^2}\right) - 2^{\omega(d)}3^{\omega(2d+1)}
\]

\[
(12) > M f(d(2d + 1)) f(2d + 1) \left(1 - \frac{1}{2^2}\right)^{-1} \times 0.66 - 2^{\omega(d)}3^{\omega(2d+1)}
\]

as \(\prod_{q \geq 3 \text{prime}} \left(1 - \frac{1}{(q - 1)^2}\right) > 0.66\). Now if \(3|2d + 1\) we obtain similarly

\[
|S_d'| \geq M \left(1 - \frac{1}{3}\right) \left(1 - \frac{2}{3}\right)^{-1} \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{2}{q}\right) - 2^{\omega(d)}3^{\omega(2d+1)}
\]

\[
= 2M f(d(2d + 1)) f(2d + 1) \times 0.66 - 2^{\omega(d)}3^{\omega(2d+1)},
\]

which is stronger than (12). Hence (12) certainly holds for \(d \not\equiv 4 \mod 15\).
For $d \equiv 4 \mod 15$, we obtain, from (11), using $3|2d+1$ and $5 \not| 2d+1$, that
\[
|S_d'| \geq M \cdot \frac{8}{15} \left(1 - \frac{2}{3}\right)^{-1} \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{1}{q}\right)^2
\times \prod_{q \geq 3 \text{ prime}} \left(1 - \frac{1}{(q-1)^2}\right)^{-1} - \frac{8}{3} 2^{h(d)} 3^{h(2d+1)} \cdot \frac{384}{225} 
\times 0.66 M f(d(2d+1)) f(2d+1) - \frac{8}{3} 2^{h(d)} 3^{h(2d+1)}.
\]
(13) 

Hence, from (12) and (13), we have
\[
|S_d'| > \frac{384}{225} \times 0.66 M f(d(2d+1)) f(2d+1) - \frac{8}{3} 2^{h(d)} 3^{h(2d+1)}.
\]
(14) 

where $c_1 = 1.1264, c_2 = 0.4224$ for $d \equiv 4 \mod 15$, and $c_1 = c_2 = 0.88$ otherwise. Thus we see that for
\[
\frac{2^{h(d)} 3^{h(2d+1)}}{[(d-1)/2] f(d(2d+1)) f(2d+1)} < 0.4224
\]
we have $|S_d'| > 0$. A straightforward Maple calculation shows that this happens for $d \geq B = 7.98 \times 10^{12}$.

Finally, from (13) and the definition of $f(d)$ we see that, for large $d$,
\[
|S_d'| > \left(0.88 \times \frac{1}{2} \times e^{-2\gamma} - o(1)\right) d/ (\log \log d)^2
\]
\[
> 0.1387d/ (\log \log d)^2.
\]

5. Proof of Corollary 1.2

First, note that, from my tables [Sm1], $|A_d| > 0$ for $1 \leq d \leq 7$. For larger values of $d$, we use the correspondence $\tau + \tau^{-1} + 2 = \alpha$. This shows that $A_d' > 0$ for all $d$, and gives the asymptotic lower bound (1).

It remains only to show that if $\tau$ has minimal polynomial $P_{d,m}(z)$, then $\alpha = \tau + \tau^{-1} + 2$ has minimal polynomial $Q_{d,m}(y)$ given by (3). Now, using (14), we can write
\[
R_{d,m}(z) = P_{d,m}(z)(z-1)^2 = (z^{2d+1} - 1)(z-1) - z^2 \left(z^{2(d-m-1)} - 1\right) (z^{2m-1}),
\]
so that
\[
\frac{P_{d,m}(z)}{z^d} = \frac{z^{d+1/2} - z^{-(d+1/2)}}{z^{1/2} - z^{-1/2}} - \frac{z^{d-m-1} - z^{-(d-m-1)}}{z^{1/2} - z^{-1/2}} + \frac{z^m - z^{-m}}{z^{1/2} - z^{-1/2}}
\]
\[
= U_{2d}(x) - U_{2(d-m)-3}(x) \cdot U_{2m-1}(x),
\]
where $x = \sqrt{z} + 1/\sqrt{z}$ and [Robins]
\[
U_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} x^{n-2k}
\]
(15) 

is the $n$th Chebyshev polynomial of the second kind, with defining property
\[
U_n(t+1/t) = \frac{t^{n+1} - t^{-(n+1)}}{t - t^{-1}}.
\]
Now, for \( \alpha = \tau + \tau^{-1} + 2 \) we have \( \sqrt{\alpha} = \sqrt{\tau} + 1/\sqrt{\tau} \), so that \( y = \alpha \) is a root of

\[
Q_{d,m}(y) = U_{2d}(\sqrt{y}) - U_{2(d-m)-3}(\sqrt{y}) \cdot U_{2m-1}(\sqrt{y})
\]

which, using (15), gives (3).

6. Tables

Table II shows that, for \( 2d = 8, 10, 12, 14 \), there are respectively 1, 3, 9, 39 elements of \( S_d \). It was obtained from the tables in [Sm1], using the transformation \( \tau + \tau^{-1} + 2 = \alpha \), where \( \alpha \) is totally positive of degree \( d \) and trace \( 2d - 1 \). Several examples of Salem numbers of trace \( -1 \), including the unique degree 8 example, had been found earlier by Boyd (personal communication).

It is interesting to note [Sm1] that there are in fact 40 totally positive algebraic integers of degree 7 and trace 13. All but one of them has exactly one conjugate > 4, giving the 39 elements of \( S_7 \) mentioned above. The exception is the number \( \alpha \) having minimal polynomial \( z^7 - 13z^6 + 62z^5 - 135z^4 + 140z^3 - 67z^2 + 14z - 1 \), which has two such conjugates. For this \( \alpha \), the \( \tau \) defined by \( \tau + \tau^{-1} + 2 = \alpha \) has, of course, two conjugates in \( (1, \infty) \), so is not a Salem number.

The results of [Sm1], combined with further computation using the same method as in that paper, also show that

**Proposition 6.1.** For \( 2d \leq 18 \), all Salem numbers of degree \( 2d \) have trace at least \(-1\).

This further computation consisted of an unsuccessful search for totally positive algebraic integers of degree \( d = 8 \) or 9 and trace \( \leq 2d - 2 \). There are, however, examples of totally positive algebraic integers of large degree \( d \) and trace \( < 2d - 1 \) ([Sm3]). Thus there may well be Salem numbers of large degree and trace \( < -1 \).

Table II shows, for \( d \leq 60 \), the set \( M_d \) of those \( m \) for which \( P_{d,m} \) is irreducible.
Table 1. Minimal polynomials of all Salem numbers of trace \(-1\) and degree \(2d\) up to 14.

<table>
<thead>
<tr>
<th>#</th>
<th>2d</th>
<th>Coefficients of (z^{2d}, \ldots, z^d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>1 1  1</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>1 1  1</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>1 1  0</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>1 1  0</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>8</td>
<td>12</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>1 1  0</td>
</tr>
<tr>
<td>13</td>
<td>12</td>
<td>1 1  0</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>1 1  (-4)</td>
</tr>
<tr>
<td>15</td>
<td>14</td>
<td>1 1  (-4)</td>
</tr>
<tr>
<td>16</td>
<td>14</td>
<td>1 1  (-4)</td>
</tr>
<tr>
<td>17</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>18</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>19</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>20</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>21</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>22</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>23</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>24</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>25</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>26</td>
<td>14</td>
<td>1 1  (-3)</td>
</tr>
<tr>
<td>27</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>28</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>29</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>30</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>31</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>32</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>33</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>34</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>35</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>36</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>37</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>38</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>39</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>40</td>
<td>14</td>
<td>1 1  (-2)</td>
</tr>
<tr>
<td>41</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>42</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>43</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>44</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>45</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>46</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>47</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>48</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>49</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>50</td>
<td>14</td>
<td>1 1  (-1)</td>
</tr>
<tr>
<td>51</td>
<td>14</td>
<td>1 1  0</td>
</tr>
<tr>
<td>52</td>
<td>14</td>
<td>1 1  0</td>
</tr>
</tbody>
</table>
Table 2. Values of $m$ for which the polynomial $P_{d,m}$ is irreducible, for $d \leq 60$. 

<table>
<thead>
<tr>
<th>$d$</th>
<th>Values of $m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>1 2 3</td>
</tr>
<tr>
<td>18</td>
<td>2 3</td>
</tr>
<tr>
<td>20</td>
<td>1 4</td>
</tr>
<tr>
<td>22</td>
<td>1 2 3 4</td>
</tr>
<tr>
<td>24</td>
<td>2 3</td>
</tr>
<tr>
<td>26</td>
<td>1 2 4 5</td>
</tr>
<tr>
<td>28</td>
<td>1 2 4 5 6</td>
</tr>
<tr>
<td>30</td>
<td>3 5</td>
</tr>
<tr>
<td>32</td>
<td>1 2 5 7</td>
</tr>
<tr>
<td>34</td>
<td>3 4</td>
</tr>
<tr>
<td>36</td>
<td>2 3 5 6 8</td>
</tr>
<tr>
<td>38</td>
<td>4 7 8</td>
</tr>
<tr>
<td>40</td>
<td>1 3 4 5 6 8 9</td>
</tr>
<tr>
<td>42</td>
<td>2 5 6 8 9</td>
</tr>
<tr>
<td>44</td>
<td>2 4 7 8</td>
</tr>
<tr>
<td>46</td>
<td>1 2 3 4 5 6 7 8 9 10</td>
</tr>
<tr>
<td>48</td>
<td>3 5 6 8 11</td>
</tr>
<tr>
<td>50</td>
<td>1 4 5 8 10 11</td>
</tr>
<tr>
<td>52</td>
<td>1 2 3 4 5 7 8 9 10 11 12</td>
</tr>
<tr>
<td>54</td>
<td>2 3 8 9 12</td>
</tr>
<tr>
<td>56</td>
<td>1 2 4 5 7 11 13</td>
</tr>
<tr>
<td>58</td>
<td>1 2 3 4 5 6 7 8 9 10 11 12 13</td>
</tr>
<tr>
<td>60</td>
<td>3 5 6 8 9 11 14</td>
</tr>
<tr>
<td>62</td>
<td>1 4 5 8 10 11 13</td>
</tr>
<tr>
<td>64</td>
<td>2 3 4 7 8 9 12 14</td>
</tr>
<tr>
<td>66</td>
<td>2 3 6 8 9 11 12 14 15</td>
</tr>
<tr>
<td>68</td>
<td>4 5 7 11 13 14</td>
</tr>
<tr>
<td>70</td>
<td>1 4 5 6 8 9 11 13 14 15 16</td>
</tr>
<tr>
<td>72</td>
<td>2 3 5 6 8 9 11 12 14 15 17</td>
</tr>
<tr>
<td>74</td>
<td>2 4 7 8 13 14 17</td>
</tr>
<tr>
<td>76</td>
<td>1 3 5 6 8 10 12 13 17 18</td>
</tr>
<tr>
<td>78</td>
<td>2 3 5 8 9 11 12 14 15 17 18</td>
</tr>
<tr>
<td>80</td>
<td>1 4 5 8 10 11 13 14 16 19</td>
</tr>
<tr>
<td>82</td>
<td>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21</td>
</tr>
<tr>
<td>84</td>
<td>2 8 9 12 14 18</td>
</tr>
<tr>
<td>86</td>
<td>1 2 4 5 7 8 10 11 14 16 17 19 20</td>
</tr>
<tr>
<td>88</td>
<td>1 2 3 4 6 7 8 9 10 11 12 13 14 15 17 18 19 20 21 22</td>
</tr>
<tr>
<td>90</td>
<td>3 6 8 11 15 20</td>
</tr>
<tr>
<td>92</td>
<td>1 2 4 5 7 8 10 13 16 17 19 20 22</td>
</tr>
<tr>
<td>94</td>
<td>2 3 4 7 9 12 13 14 17 18 22</td>
</tr>
<tr>
<td>96</td>
<td>2 3 5 6 8 9 11 12 14 15 17 18 20 21 23</td>
</tr>
<tr>
<td>98</td>
<td>5 7 8 13 14 19 20 23</td>
</tr>
<tr>
<td>100</td>
<td>1 3 4 5 6 8 9 10 11 13 14 15 16 18 19 20 21 23 24</td>
</tr>
<tr>
<td>102</td>
<td>2 3 5 6 9 11 12 14 15 17 18 20 21 23 24</td>
</tr>
<tr>
<td>104</td>
<td>4 8 13 17 22</td>
</tr>
<tr>
<td>106</td>
<td>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25</td>
</tr>
<tr>
<td>108</td>
<td>2 3 5 6 8 9 11 12 14 15 17 18 20 21 23 24 26</td>
</tr>
<tr>
<td>110</td>
<td>1 4 8 10 11 13 14 19 20 23 25 26</td>
</tr>
<tr>
<td>112</td>
<td>1 2 4 5 6 7 8 9 11 12 13 14 15 16 18 19 20 21 22 23 25 26 27</td>
</tr>
<tr>
<td>114</td>
<td>2 3 8 12 14 17 18 24 27</td>
</tr>
<tr>
<td>116</td>
<td>1 2 4 7 8 10 11 16 17 19 20 22 23 25 28</td>
</tr>
<tr>
<td>118</td>
<td>1 3 4 5 6 8 10 11 12 13 15 18 19 20 22 25 26 27</td>
</tr>
<tr>
<td>120</td>
<td>3 5 6 8 9 14 18 20 21 23 24 29</td>
</tr>
</tbody>
</table>
I thank George Greaves, Sergei Konyagin, and James McKee for helpful remarks.

**References**


[Sm2] C.J. Smyth, Cyclotomic factors of reciprocal polynomials and totally positive algebraic integers of small trace, University of Edinburgh preprint, MS96-024, 1996.


Department of Mathematics and Statistics, James Clerk Maxwell Building, King’s Buildings, University of Edinburgh, Mayfield Road, Edinburgh, EH9 3JZ, Scotland, UK.

E-mail address: chris@maths.ed.ac.uk

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use