MATHEMATICS OF COMPUTATION
Volume 69, Number 230, Pages 827–838
S 0025-5718(99)01099-6
Article electronically published on March 10, 1999

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 *Salem number* is an algebraic integer $\tau > 1$, of degree $\geqslant 4$, all of whose conjugates, apart from τ and τ^{-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 $\mathcal{S}_d$ of Salem numbers of degree $2d$ and trace -1. This set is tabulated in Table 1 for $2d \leqslant 14$. It is easy to see that $\mathcal{S}_d$ is finite for all d. In order to state our main result, we define the subset $\mathcal{S}_d^{'}$ of $\mathcal{S}_d$ to be those Salem numbers $\tau_{d,m}$ with minimal polynomial

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

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

Theorem 1.1. *For every $d \geqslant 4$, $\mathcal{S}_d$ is non-empty. Further, for $d \geqslant 5$, $\mathcal{S}_d^{'}$ is non-empty, and, for d sufficiently large,*

$$(2)\qquad |\mathcal{S}_d| \geqslant |\mathcal{S}_d^{'}| > \frac{0.1387d}{(\log\log d)^2},$$

so that certainly $|\mathcal{S}_d| \to \infty$ as $d \to \infty$.

In fact, it is likely that $|\mathcal{S}_d|$ 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 $\mathcal{A}_d$ of totally positive (i.e. all conjugates positive) algebraic integers of degree d and trace $2d-1$. We define the subset $\mathcal{A}_d^{'}$ of $\mathcal{A}_d$ to be those $\alpha_{d,m}$ in $\mathcal{A}_d$ with minimal

Received by the editor April 28, 1998.
1991 *Mathematics Subject Classification.* Primary 11R06.

polynomial

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

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

Corollary 1.2. *For every $d \geqslant 1$, $\mathcal{A}_d$ is non-empty. Also $\mathcal{A}'_d$ is non-empty for $d \geqslant 5$ and, for d sufficiently large,*

$$|\mathcal{A}_d| \geqslant |\mathcal{A}'_d| > \frac{0.1387d}{(\log\log d)^2}, \tag{4}$$

so that certainly $|\mathcal{A}_d| \to \infty$ 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 $d \geqslant 5$ and $1 \leqslant m \leqslant \lfloor \frac{d-1}{2} \rfloor$, $P_{d,m}(z)$ factors as the product of the minimal polynomial of a Salem number $\tau_{d,m}$ and a (possibly trivial) cyclotomic polynomial, which is*

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

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

$$C(z) = \left(\frac{z^{g_1}-1}{z-1}\right) \cdot \left(\frac{z^{g_2}-1}{z-1}\right) \cdot \left(\frac{z^{g_3}-1}{z^{g_4}-1}\right),$$

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 $d \equiv 4 \bmod 15$ and $m \equiv 1$ or $2 \bmod 15$, 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 $d \geqslant 5$, $1 \leqslant m \leqslant \lfloor \frac{d-1}{2} \rfloor$, $P_{d,m}$ has the nth cyclotomic polynomial C_n as a factor iff*

(i) n odd $\geqslant 3$, $d \equiv 0 \bmod n$, $m \equiv \frac{n-1}{2} \bmod n$

or

(ii) n odd $\geqslant 3$, $d \equiv \frac{n-1}{2} \bmod n$, $m \equiv 0$ or $\frac{n-3}{2} \bmod n$

or

(iii) $n = 12$, $d \equiv 3 \bmod 6$, $m \equiv 1 \bmod 6$

or

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

and in no other case. In particular, putting

$$\mathcal{M}_d = \quad \{m : 1 \leqslant m \leqslant \lfloor (d-1)/2 \rfloor, m \not\equiv \frac{p-1}{2} \bmod p \textit{ for all odd primes } p|d,$$
$$m \not\equiv 0 \textit{ or } \frac{q-3}{2} \bmod q \textit{ for all odd primes } q|2d+1\},$$

$P_{d,m}$ *is irreducible iff*

$$\begin{cases} m \in \mathcal{M}_d \textit{ if } d \not\equiv 4 \bmod 15, \\ m \in \mathcal{M}_d \cap \{m \not\equiv 1 \textit{ or } 2 \bmod 15\} \textit{ if } d \equiv 4 \bmod 15. \end{cases}$$

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

$$\begin{aligned} &z^{2d} + z^{2d-1} - z^{2d-3} - 2z^{2d-4} - \cdots - (2m-2)\, z^{2d-2m} \\ &- (2m-1)\left(z^{2d-(2m+1)} + z^{2d-(2m+2)} + \cdots + z^{2m+2} + z^{2m+1}\right) \\ &- (2m-2)\, z^{2m} - \cdots - 2z^4 - z^3 + z + 1. \end{aligned}$$

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 $\rho = \frac{1}{2}\left(1+\sqrt{5}\right)$, which is a limit of Pisot numbers $\vartheta_m < \rho$ with minimal polynomial

$$\left(z^{2m}\left(z^2 - z - 1\right) + 1\right) / (z-1) \quad (m \geqslant 1).$$

Then the standard construction ([Sa], [BDGPS]) proving that every Pisot number is a limit from below of Salem numbers shows that ϑ_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 $d \leqslant 40$ 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 ω_n iff n is a multiple of 4;

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

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

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

Lemma 2.2. *For $n \geqslant 3$*

$$\prod_{\substack{p|n \\ p \textit{ prime}}} \left(1 - \frac{1}{p}\right) > \frac{1}{e^\gamma \log\log n + 2.50637/\log\log n} =: f(n),$$

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* γ *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* $\bmod p$. *Then the number* N *of positive integers* $m \leqslant M$ *which are* $\not\equiv x_p \bmod p$ *for any* x_p *in* $\mathcal{R}_p$ *and any* $p \in \mathcal{D}$ *satisfies*

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

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* $d \geqslant 5$ *and* $1 \leqslant m \leqslant \lfloor (d-1)/2 \rfloor$ *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* $d \geqslant 5$ *the* $\tau_{d,m}$ $(1 \leqslant m \leqslant \lfloor (d-1)/2 \rfloor)$ *are all distinct. For* d, m *in this range,* $P_{d,m}(1) \neq 0$.

Proof. Consider

$$\begin{aligned} R_{d,m}(z) &:= (z-1)^2 P_{d,m}(z) \\ &= z^{2d}\left(z^2 - z - 1\right) + z^{2(d-m)} + z^{2(m+1)} - z^2 - z + 1. \end{aligned}$$

Then by a standard Rouché'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

$$R''_{d,m}(1) = 2\left(4m(m+1) + 1 - 2(2m-1)d\right) < 0$$

if

$$d \geqslant \left\lceil \frac{4m(m+1)+1}{2(2m-1)} \right\rceil = \begin{cases} 5 \text{ for } m = 1, 2, 3 \\ m+2 \text{ for } m \geqslant 4 \end{cases}$$

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

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

$$\begin{aligned} R_{d,m'}(\tau) = R_{d,m'}(\tau) - R_{d,m}(\tau) &= \tau^{2(d-m')} + \tau^{2(m'+1)} - \tau^{2(d-m)} - \tau^{2(m+1)} \\ &= (\tau^{2(m-m')} - 1)(-\tau^{2(m'+1)} + \tau^{2(d-m)}) \\ &> 0. \end{aligned}$$

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

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

$$-z^{2d} = \frac{u - z - 1 + \dfrac{1}{z}}{\dfrac{1}{u} - \dfrac{1}{z} - 1 + z}, \tag{5}$$

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

$$-z^{2d} = \frac{u - z - 1 + \dfrac{1}{z}}{\dfrac{1}{u} - \dfrac{1}{z} - 1 + z} = \frac{-u + z - 1 - \dfrac{1}{z}}{-\dfrac{1}{u} + \dfrac{1}{z} - 1 - z} \tag{6}$$

which gives

$$2\left(z - \frac{1}{z}\right) = u - \frac{1}{u}. \tag{7}$$

To solve (7), put $z = e^{2\pi i/4k}$ 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

$$2\left(z^r - z^{-r}\right) = \left(u^r - u^{-r}\right),$$

so that

$$2\left|\sin\frac{\pi r}{2k}\right| = \left|\sin\frac{\pi r\,(2m+1)}{2k}\right| \leqslant 1. \tag{8}$$

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

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

$$\left(-z^{2d}\right)^2 = \left(\frac{u - z - 1 + \dfrac{1}{z}}{\dfrac{1}{u} - \dfrac{1}{z} - 1 + z}\right)^2 = \left(-z^2\right)^{2d} = -\left(\frac{-u^2 - \left(-z^2\right) - 1 + \dfrac{1}{-z^2}}{\dfrac{1}{-u^2} - \dfrac{1}{-z^2} - 1 - z^2}\right). \tag{9}$$

Clearing the denominators gives a plane algebraic curve $f(u,z) = 0$, independent of d. Since then also $f\left(-u^2, -z^2\right) = 0$, the pairs (u,z) of interest lie on both curves. To find all possible (u,z) pairs, we use a Maple program [Sm3] which uses a version of the Euclidean algorithm to find all such intersection points, with multiplicities. The program tells us that the only such intersection points with z and u nth roots of unity with $2|n$, $4 \nmid n$ are the pairs $(u,z) = \left(\alpha^3, \alpha\right)$ and $\left(\alpha^5, \alpha\right)$, where α 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 $m=1$, $u=z^3$,

$$-z^{2d}=\frac{z^3-z-1+1/z}{z^{-3}-z^{-1}-1+z}=-z^8$$

on routine simplification, using $C_{30}(z)=0$. Again, for $m=2$, $u=z^5$, (4) gives $-z^{2d}=-z^8$ again. Hence $2d=8 \bmod 30$, $d=4 \bmod 15$, 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

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

Clearing denominators this time gives

$$(u-1)^2\left(uz^2-1\right)(z-u)(z+1)(z-1)=0.$$

Since neither ±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 $u=z^{2m+1}=1$, $m\equiv\frac{n-1}{2} \bmod n$. Then, from (5), $z^{2d}=1$, $z^d=1$, i.e. $d\equiv 0 \bmod n$.

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

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

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 $|\mathcal{S}_d'|$. First we show that

Lemma 4.1. *The set $\mathcal{S}_d'$ is non-empty for $5\le d\le B:=7.98\times10^{12}$.*

Proof. First, direct Maple computation of the set $\mathcal{M}_d$ shows that $\mathcal{M}_d$, and hence $\mathcal{S}_d'$ is non-empty for $5\le d\le 2998$. The set $\mathcal{M}_d$ is shown for $d\le 60$ 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 $d\ge 2999$. Then, by Lemma 3.1, the polynomials $P_{d,m}$ for fixed d and $1\le m\le 1499=(2999-1)/2\le\lfloor(d-1)/2\rfloor$ 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, $m'\in\mathcal{M}_d$, so that $\mathcal{M}_d$ and hence $\mathcal{S}_d'$ is non-empty. For, if not, then, from the definition of $\mathcal{M}_d$, either $m'|2d+1$ or $(2m'+3)|2d+1$ or

$(2m'+1)|d$, implying that $m'' := m'$ or $2m'+1$ or $2m'+3$ divides $d(2d+1)$. But 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 $|\mathcal{S}_d'|$ for large d, i.e. for $d > B$. To do this, we apply Lemma 2.3, using the description of the integers m in $\mathcal{S}_d'$ given by Corollary 1.4.

First consider the case $d \not\equiv 4 \bmod 15$. Take $\mathcal{D}$ to be the set of odd primes dividing $d(2d+1)$, and $\mathcal{R}_p = \left\{\frac{1}{2}(p-1)\right\}$ if p is an odd prime dividing d, and $\mathcal{R}_q = \left\{0, \frac{1}{2}(q-3)\right\}$ if q is a prime dividing $2d+1$. Put $r_p = |\mathcal{R}_p|$. 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 $M = \lfloor (d-1)/2 \rfloor$, we obtain

$$|\mathcal{S}_d'| \geqslant M \prod_{p|d_3} \left(1 - \frac{1}{p}\right) \prod_{\substack{q|2d+1 \\ q\neq 3}} \left(1 - \frac{2}{q}\right) - 2^{\omega(d)} 3^{\omega(2d+1)}. \tag{10}$$

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 $d \equiv 4 \bmod 15$ we have $2d+1 \equiv 9 \bmod 15$, so $3|2d+1$, but $3 \nmid d$, $5 \nmid d$, $5 \nmid 2d+1$. Thus there are seven excluded residue classes mod 15 : $m \not\equiv 0, 1, 2, 3, 6, 9, 12 \bmod 15$, and the lemma gives

$$|\mathcal{S}_d'| \geqslant M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{\substack{q|2d+1 \\ q\neq 3}} \left(1 - \frac{2}{q}\right)\left(1 - \frac{7}{15}\right) - 2^{\omega(d)} 3^{\omega(2d+1)-1}(1+7). \tag{11}$$

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

$$\begin{aligned}
|\mathcal{S}_d'| &\geqslant M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{2}{q}\right) - 2^{\omega(d)} 3^{\omega(2d+1)} \\
&> M \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{1}{q}\right)^2 \prod_{\substack{q \geqslant 5 \\ q \text{prime}}} \left(1 - \frac{1}{(q-1)^2}\right) - 2^{h(d)} 3^{h(2d+1)} \\
&> Mf(d(2d+1)) f(2d+1) \left(1 - \frac{1}{2^2}\right)^{-1} \times 0.66 - 2^{h(d)} 3^{h(2d+1)} \qquad (12)
\end{aligned}$$

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

$$\begin{aligned}
|\mathcal{S}_d'| &\geqslant M\left(1 - \frac{1}{3}\right)\left(1 - \frac{2}{3}\right)^{-1} \prod_{p|d} \left(1 - \frac{1}{p}\right) \prod_{q|2d+1} \left(1 - \frac{2}{q}\right) - 2^{h(d)} 3^{h(2d+1)} \\
&= 2Mf(d(2d+1)) f(2d+1) \times 0.66 - 2^{h(d)} 3^{h(2d+1)},
\end{aligned}$$

which is stronger than (12). Hence (12) certainly holds for $d \not\equiv 4 \bmod 15$.

For $d \equiv 4 \bmod 15$, we obtain, from (11), using $3|2d+1$ and $5 \nmid 2d+1$, that

$$
\begin{aligned}
|\mathcal{S}_d'| &\geqslant M \cdot \frac{8}{15}\left(1-\frac{2}{3}\right)^{-1} \prod_{p|d}\left(1-\frac{1}{p}\right) \prod_{q|2d+1}\left(1-\frac{1}{q}\right)^2 \\
&\quad \times \prod_{\substack{q \geqslant 3 \\ q \text{ prime}}}\left(1-\frac{1}{(q-1)^2}\right)\left(1-\frac{1}{4^2}\right)^{-1} - \frac{8}{3} 2^{h(d)} 3^{h(2d+1)} \\
&> \frac{384}{225} \times 0.66 M f\left(d(2d+1)\right) f\left(2d+1\right) - \frac{8}{3} 2^{h(d)} 3^{h(2d+1)}. \qquad (13)
\end{aligned}
$$

Hence, from (12) and (13), we have

$$
|\mathcal{S}_d'| > c_1 M f\left(d(2d+1)\right) f\left(2d+1\right)\left(1-\frac{2^{h(d)} 3^{h(2d+1)}}{c_2 M f\left(d(2d+1)\right) f\left(2d+1\right)}\right), \qquad (14)
$$

where $c_1 = 1.1264, c_2 = 0.4224$ for $d \equiv 4 \bmod 15$, and $c_1 = c_2 = 0.88$ otherwise. Thus we see that for

$$
\frac{2^{h(d)} 3^{h(2d+1)}}{\lfloor (d-1)/2 \rfloor f\left(d(2d+1)\right) f\left(2d+1\right)} < 0.4224
$$

we have $|\mathcal{S}_d'| > 0$. 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,

$$
\begin{aligned}
|\mathcal{S}_d'| &> \left(0.88 \times \frac{1}{2} \times e^{-2\gamma} - o(1)\right) d/\left(\log\log d\right)^2 \\
&> 0.1387 d/\left(\log\log d\right)^2.
\end{aligned}
$$

5. Proof of Corollary 1.2

First, note that, from my tables [Sm1], $|\mathcal{A}_d| > 0$ for $1 \leqslant d \leqslant 7$. For larger values of d, we use the correspondence $\tau + \tau^{-1} + 2 = \alpha$. This shows that $\mathcal{A}_d' > 0$ for all d, and gives the asymptotic lower bound (4).

It remains only to show that if τ 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 (1), we can write

$$
R_{d,m}(z) = P_{d,m}(z)(z-1)^2 = \left(z^{2d+1}-1\right)(z-1) - z^2\left(z^{2(d-m-1)}-1\right)\left(z^{2m}-1\right),
$$

so that

$$
\begin{aligned}
\frac{P_{d,m}(z)}{z^d} &= \frac{z^{d+1/2} - z^{-(d+1/2)}}{z^{1/2} - z^{-1/2}} - \frac{z^{d-m-1} - z^{-(d-m-1)}}{z^{1/2} - z^{-1/2}} \cdot \frac{z^m - z^{-m}}{z^{1/2} - z^{-1/2}} \\
&= U_{2d}(x) - U_{2(d-m)-3}(x) \cdot U_{2m-1}(x),
\end{aligned}
$$

where $x = \sqrt{z} + 1/\sqrt{z}$ and [Robins]

$$
U_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} x^{n-2k} \qquad (15)
$$

is the nth 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 1 shows that, for $2d = 8, 10, 12, 14$, there are respectively $1, 3, 9, 39$ elements of $\mathcal{S}_d$. It was obtained from the tables in [Sm1], using the transformation $\tau + \tau^{-1} + 2 = \alpha$, where α 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 $\mathcal{S}_7$ mentioned above. The exception is the number α having minimal polynomial $z^7 - 13z^6 + 62z^5 - 135z^4 + 140z^3 - 67z^2 + 14z - 1$, which has two such conjugates. For this α, the τ 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 $2d \leqslant 18$, 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 2 shows, for $d \leqslant 60$, the set $\mathcal{M}_d$ 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.

#	2d	Coefficients of $z^{2d},\dots,z^d$							
1	8	1	1	−1	−4	−5			
2	10	1	1	−1	−5	−9	−11		
3	10	1	1	0	−1	−1	−1		
4	10	1	1	0	−2	−4	−5		
5	12	1	1	−2	−6	−6	−3	−1	
6	12	1	1	−2	−7	−11	−14	−15	
7	12	1	1	−2	−7	−10	−11	−11	
8	12	1	1	−1	−3	−3	−3	−3	
9	12	1	1	−1	−3	−2	0	1	
10	12	1	1	−1	−4	−6	−8	−9	
11	12	1	1	−1	−5	−10	−14	−15	
12	12	1	1	0	−1	−2	−3	−3	
13	12	1	1	0	−2	−4	−5	−5	
14	14	1	1	−4	−15	−26	−31	−29	−27
15	14	1	1	−4	−16	−32	−48	−59	−63
16	14	1	1	−4	−17	−36	−56	−70	−75
17	14	1	1	−3	−10	−15	−17	−17	−17
18	14	1	1	−3	−10	−13	−8	2	7
19	14	1	1	−3	−11	−19	−25	−28	−29
20	14	1	1	−3	−11	−18	−20	−17	−15
21	14	1	1	−3	−11	−17	−16	−9	−5
22	14	1	1	−3	−12	−24	−37	−47	−51
23	14	1	1	−3	−12	−23	−33	−39	−41
24	14	1	1	−3	−12	−22	−29	−31	−31
25	14	1	1	−3	−13	−28	−45	−58	−63
26	14	1	1	−3	−13	−27	−41	−50	−53
27	14	1	1	−2	−6	−7	−6	−5	−5
28	14	1	1	−2	−6	−6	−2	3	5
29	14	1	1	−2	−7	−11	−13	−12	−11
30	14	1	1	−2	−7	−11	−14	−16	−17
31	14	1	1	−2	−7	−10	−9	−5	−3
32	14	1	1	−2	−7	−10	−10	−8	−7
33	14	1	1	−2	−7	−9	−5	3	7
34	14	1	1	−2	−7	−9	−6	0	3
35	14	1	1	−2	−8	−16	−25	−31	−33
36	14	1	1	−2	−8	−15	−22	−27	−29
37	14	1	1	−2	−8	−14	−18	−19	−19
38	14	1	1	−2	−8	−13	−14	−11	−9
39	14	1	1	−2	−9	−19	−30	−38	−41
40	14	1	1	−2	−9	−18	−27	−33	−35
41	14	1	1	−1	−3	−3	−3	−4	−5
42	14	1	1	−1	−4	−7	−10	−11	−11
43	14	1	1	−1	−4	−6	−6	−4	−3
44	14	1	1	−1	−4	−6	−7	−7	−7
45	14	1	1	−1	−4	−5	−3	1	3
46	14	1	1	−1	−4	−5	−4	−2	−1
47	14	1	1	−1	−5	−11	−18	−23	−25
48	14	1	1	−1	−5	−10	−15	−18	−19
49	14	1	1	−1	−5	−9	−12	−13	−13
50	14	1	1	−1	−6	−13	−21	−27	−29
51	14	1	1	0	−1	−2	−3	−3	−3
52	14	1	1	0	−2	−4	−6	−7	−7

TABLE 2. Values of m for which the polynomial $P_{d,m}$ is irreducible, for $d \leq 60$.

2d	Values of m
10	1
12	2
14	2
16	1 2 3
18	2 3
20	1 4
22	1 2 3 4
24	2 3
26	1 2 4 5
28	1 2 4 5 6
30	3 5 6
32	1 2 5 7
34	3 4
36	2 3 5 6 8
38	4 7 8
40	1 3 4 5 6 8 9
42	2 5 6 8 9
44	2 4 7 8
46	1 2 3 4 5 6 7 8 9 10
48	3 5 6 8 11
50	1 4 5 8 10 11
52	1 2 3 4 5 7 8 9 10 11 12
54	2 3 8 9 12
56	1 2 4 5 7 11 13
58	1 2 3 4 5 6 7 8 9 10 11 12 13
60	3 5 6 8 9 11 14
62	1 4 5 8 10 11 13
64	2 3 4 7 8 9 12 14
66	2 3 6 8 9 11 12 14 15
68	4 5 7 11 13 14
70	1 4 5 6 8 9 11 13 14 15 16
72	2 3 5 6 8 9 11 12 14 15 17
74	2 4 7 8 13 14 17
76	1 3 5 6 8 10 12 13 17 18
78	2 3 5 8 9 11 12 14 15 17 18
80	1 4 5 8 10 11 13 14 16 19
82	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
84	2 8 9 12 14 18
86	1 2 4 5 7 8 10 11 14 16 17 19 20
88	1 2 3 4 6 7 8 9 10 11 12 13 14 15 17 18 19 20 21
90	3 6 8 11 15 20
92	1 2 4 5 7 8 10 13 16 17 19 20 22
94	2 3 4 7 9 12 13 14 17 18 22
96	2 3 5 6 8 9 11 12 14 15 17 18 20 21 23
98	5 7 8 13 14 19 20 23
100	1 3 4 5 6 8 9 10 11 13 14 15 16 18 19 20 21 23 24
102	2 3 5 6 9 11 12 14 15 17 18 20 21 23 24
104	4 8 13 17 22
106	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
108	2 3 5 6 8 9 11 12 14 15 17 18 20 21 23 24 26
110	1 4 8 10 11 13 14 19 20 23 25 26
112	1 2 4 5 6 7 8 9 11 12 13 14 15 16 18 19 20 21 22 23 25 26 27
114	2 3 8 12 14 17 18 24 27
116	1 2 4 7 8 10 11 16 17 19 20 22 23 25 28
118	1 3 4 5 6 8 10 11 12 13 15 18 19 20 22 25 26 27
120	3 5 6 8 9 14 18 20 21 23 24 29

Acknowledgments

I thank George Greaves, Sergei Konyagin, and James McKee for helpful remarks.

References

[BDGPS] M.J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.P. Schreiber, Pisot and Salem numbers, Birkhäuser Verlag, Basel, 1992. MR **93k:**11095

[B] D.W. Boyd, Small Salem numbers, Duke Math. J. **44**, (1977), 315-327. MR **56:**11952

[HR] H. Halberstam and H.-E. Richert, Sieve methods, Academic Press, London, 1974. MR **54:**12689

[MRS] J.F. McKee, P. Rowlinson and C.J. Smyth, Salem numbers and Pisot numbers from stars, in: Number Theory in Progress: Proceedings of the International Conference on Number Theory in Honor of Andrzej Schinzel, held in Zakopane, Poland, June 30–July 9, 1997 (K. Györy, Editor), de Gruyter, Berlin, 1999, Vol. 1, 309–319.

[MSC] D.S. Mitrinović, J. Sándor and B. Crstici, Handbook of Number Theory, Kluwer, Dordrecht, 1996. MR **97f:**11001

[Robin] G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n, Acta Arith. **42** (1983), 367-389. MR **85j:**11109

[Robins] R.M. Robinson, Intervals containing infinitely many conjugate sets of algebraic integers, Studies in Mathematical Analysis and Related Topics, Stanford University Press, 1962, 305-315. MR **26:**2433

[RS] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Ill. J. Math **6**, (1962), 64-94. MR **25:**1139

[Sa] R. Salem, Power series with integer coefficients, Duke Math J., **12** (1945), 153-172. MR **6:**206b

[Sm1] C.J. Smyth, Totally positive algebraic integers of small trace, Annales de l'Institute Fourier de l'Univ. de Grenoble, **34** (1984), 1-28. MR **86f:**11091

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

[Sm3] C.J. Smyth, A Euclidean algorithm for finding the intersection points of plane curves (in preparation).

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