SQUAREFREE VALUES OF POLYNOMIALS ALL OF WHOSE COEFFICIENTS ARE 0 AND 1

Michael Filaseta and Sergei Konyagin

1. Introduction

Let n be a non-negative integer and consider the set of polynomials

$$S_n = \{f(x) = \sum_{j=0}^{n} \varepsilon_j x^j : \varepsilon_j \in \{0,1\} \text{ for each } j \text{ and } \varepsilon_0 = 1\}.$$

The condition $\varepsilon_0 = 1$ ensures that the elements of S_n are not divisible by x. Let

$$S = \bigcup_{n=0}^{\infty} S_n.$$

There are interesting open problems concerning the polynomials in S. Using the main result in [1] (with base 2) or using the well-known explicit formula for the number of irreducible polynomials of degree $\le n$ modulo 2, one can easily show that there are at least on the order of $2^n/n$ irreducible polynomials in S_n. Odlyzko (private communication) has asked whether almost all polynomials in S are irreducible? In other words, does

$$\lim_{n\to\infty} \frac{|\{f(x) \in S_n : f(x) \text{ is irreducible}\}|}{2^n} = 1?$$

It is not even known how to establish that the limit (or the limit supremum) is positive. Another open problem, posed by Odlyzko and Poonen [2], is to determine whether it is true that if α is a root with multiplicity > 1 of some polynomial $f(x)$ in S, then α is a root of unity.

The purpose of this paper is to establish two results concerning the polynomials in S. First, we shall show

Typeset by $\mathcal{AMS}$-TEX

Theorem 1. *Let $b = 3$, 4, or 5. Then there are infinitely many polynomials $f(x) \in S$ for which $f(b)$ is squarefree. Moreover, for such b, the density of polynomials $f(x) \in S$ for which $f(b)$ is squarefree is*

$$\lim_{n\to\infty} \frac{|\{f(x) \in S_n : f(b) \text{ is squarefree}\}|}{2^n} = \frac{6}{\pi^2} \prod_{p|b} \left(1 - \frac{1}{p^2}\right)^{-1}. \tag{1}$$

There are other trivial values of b for which one can obtain similar results (when $|b| \le 2$), but we do not know how to establish the analogous results for $b \ge 6$. As an immediate consequence of Theorem 1, we deduce the

Corollary. *Let $b = 3$, 4, or 5. There are infinitely many squarefree numbers in base b consisting only of the digits 0 and 1.*

The arguments can be modified slightly to allow for the possibility that $\varepsilon_0 = 0$ in the definition of S_n. Thus, for $b = 3$, 4, or 5, we can obtain the density of squarefree numbers in base b among the positive integers consisting only of the digits 0 and 1 in base b. For $b = 4$, the density is $1/2$ times the expression on the right-hand side of (1); for $b = 3$ and 5, the density is $3/4$ times the expression on the right-hand side of (1).

It is of some interest to know a corresponding result for base 10. By applying an argument similar to what we will use for $b = 4$ in Theorem 1, it can be shown that there are infinitely many squarefree numbers which consist only of the digits 0, 1, and 2. In fact, if d_1, d_2, and d_3 are any three distinct digits not equal to 0, 4, and 8 in some order, then there are infinitely many squarefree numbers m in base 10 with each digit of m being either d_1, d_2, or d_3. We will not address this issue further here.

Our second theorem concerns squarefree polynomials in S (polynomials without any roots having multiplicity > 1). We shall see how to obtain the next result as a fairly direct consequence of our approach to establishing Theorem 1.

Theorem 2. *Almost all polynomials in S are squarefree. In other words,*

$$\lim_{n\to\infty} \frac{|\{f(x) \in S_n : f(x) \text{ is squarefree}\}|}{2^n} = 1.$$

In the next section, we give a proof of Theorem 1 for the case that $b = 3$. In the process, we will establish some preliminaries for the cases $b = 4$ and 5. The remainder of the proof of Theorem 1 is given in Section 3. In Section 4, we will establish Theorem 2 using a lemma (Lemma 9) which aided in the proof of Theorem 1.

2. Some Preliminaries and the Case $b = 3$

Let n be a positive integer. For integers b and m with $m \geq 2$, we define $t(n) = t(n, m, b)$ as the number of $f(x) \in S_n$ for which m divides $f(b)$. We begin with an estimate for $t(n)$. Suppose first that m and b are integers which are not relatively prime. Then there is a prime p which divides both m and b. Observe that for every $f(x) \in S_n$, we have $f(b) \equiv 1 \pmod{p}$. Hence, for every $f(x) \in S_n$, m does not divide $f(b)$, and we deduce that $t(n) = 0$. The next lemma deals with the remaining situation where m and b are relatively prime integers.

Lemma 1. *Let m and b be relatively prime integers with $m \geq 2$. Then*

$$t(n) = \frac{2^n}{m}\,(1 + o(1))$$

as n approaches infinity.

Proof. Since

$$\sum_{j=0}^{m-1} e^{2\pi i a j/m} = \begin{cases} m & \text{if } m|a \\ 0 & \text{otherwise,} \end{cases}$$

we obtain

$$t(n) = \frac{1}{m} \sum_{f(x)\in S_n} \sum_{j=0}^{m-1} e^{2\pi i f(b) j/m} = \frac{1}{m} \sum_{j=0}^{m-1} \sum_{f(x)\in S_n} e^{2\pi i f(b) j/m}.$$

On the other hand, from the definition of S_n, we have

$$\sum_{f(x)\in S_n} e^{2\pi i f(b)j/m} = e^{2\pi i j/m} \prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right).$$

Observe that when $j = 0$, the right-hand side is 2^n. Hence,

$$t(n) = \frac{2^n}{m} + E,$$

where

$$E = \frac{1}{m} \sum_{j=1}^{m-1} e^{2\pi i j/m} \prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right).$$

It remains to show that $E = o(2^n)$.

For each $j \in \{1, 2, \ldots, m-1\}$, we rewrite the absolute value of the product above as

$$\begin{aligned}\left|\prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right)\right| &= \left|\prod_{k=1}^{n} e^{\pi i b^k j/m}\right| \left|\prod_{k=1}^{n} \left(e^{\pi i b^k j/m} + e^{-\pi i b^k j/m}\right)\right| \\ &= 2^n \prod_{k=1}^{n} \left|\cos(\pi b^k j/m)\right|.\end{aligned}$$

Since m and b are relatively prime and $1 \le j \le m-1$, the expression $b^k j/m$ is a rational number which differs from an integer by at least $1/m$. Therefore,

$$\left|\cos(\pi b^k j/m)\right| \le \left|\cos(\pi/m)\right|.$$

Since $m \ge 2$, this last expression is < 1. We obtain

$$\begin{aligned}|E| &\le \frac{1}{m} \sum_{j=1}^{m-1} \left|\prod_{k=1}^{n} \left(1 + e^{2\pi i b^k j/m}\right)\right| \\ &= \frac{2^n}{m} \sum_{j=1}^{m-1} \prod_{k=1}^{n} \left|\cos(\pi b^k j/m)\right| \le 2^n \left|\cos(\pi/m)\right|^n,\end{aligned}$$

and the lemma easily follows. ■

Lemma 2. *Let b be a positive integer, and let B be a real number > 0. Denote by $S(B,n)$ the number of $f(x) \in S_n$ such that $f(b)$ is not divisible by p^2 for every prime $p \leq B$. Then*

$$S(B,n) = 2^n \prod_{p \leq B,\ p \nmid b} \left(1 - \frac{1}{p^2}\right) + o\left(2^n\right).$$

Lemma 2 follows from Lemma 1 by an easy sieve argument and we omit the details. Observe that

$$\prod_{p \leq B,\ p \nmid b} \left(1 - \frac{1}{p^2}\right) = \prod_{p \nmid b} \left(1 - \frac{1}{p^2}\right) (1 + O(1/B)) = \frac{6}{\pi^2} \prod_{p \mid b} \left(1 - \frac{1}{p^2}\right)^{-1} (1 + O(1/B)).$$

Fix $\varepsilon > 0$. By choosing B sufficiently large and then choosing n sufficiently large, we deduce from Lemma 2 that $S(B,n)$ differs from

$$\frac{6 \times 2^n}{\pi^2} \prod_{p \mid b} \left(1 - \frac{1}{p^2}\right)^{-1}$$

by $\leq \varepsilon 2^n$. Thus, to prove Theorem 1, it suffices to show that the number of $f(x) \in S_n$ such that $f(b)$ is divisible by p^2 for some prime $p > B$ is $\leq \varepsilon 2^n$. For such an estimate we may suppose that B is arbitrarily large; more specifically, we can take $B \geq B_0$ where B_0 is an arbitrary constant depending only on ε. The proof of Theorem 1 for the case $b = 3$ therefore follows from the following lemma.

Lemma 3. *Let $\varepsilon > 0$, and let B be sufficiently large. Then there are $\leq \varepsilon 2^n$ polynomials $f(x) \in S_n$ for which there exists an integer $d > B$ such that $d^2 | f(3)$.*

Proof. Let d be an integer $> B$. Let r be the positive integer satisfying

$$3^{r/2} < d \leq 3^{(r+1)/2}.$$

We fix $\varepsilon_r, \varepsilon_{r+1}, \ldots, \varepsilon_n \in \{0,1\}$ arbitrarily and consider $f(x) = \sum_{j=0}^{n} \varepsilon_j x^j \in S_n$. Observe that for any choice of $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-1} \in \{0,1\}$, we have

$$0 \leq \sum_{j=0}^{r-1} \varepsilon_j 3^j < d^2.$$

Also, for distinct choices of the $r-$tuple $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{r-1})$ with each $\varepsilon_j \in \{0,1\}$, the numbers $\sum_{j=0}^{r-1} \varepsilon_j 3^j$ are distinct; hence, they are distinct modulo d^2. We deduce that with $\varepsilon_r, \varepsilon_{r+1}, \dots, \varepsilon_n \in \{0,1\}$ fixed, there is at most one choice of $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{r-1})$ such that $f(3)$ is divisible by d^2. It follows that there are at most 2^{n-r+1} choices for $f(x) \in S_n$ such that $f(3)$ is divisible by d^2. The inequality $3^{(r+1)/2} \geq d > B$ implies that r is large. Hence,

$$2^{n-r+1} = 2^{n+1}2^{-r} = 2^{n+1}(3^{r/2})^{-2\log 2/\log 3} \leq 2^{n+1}(3^{(r+1)/2})^{-5/4} \leq 2^{n+1}d^{-5/4}.$$

We deduce that the number of $f(x) \in S_n$ such that $f(3)$ is divisible by d^2 for some integer $d > B$ is

$$\leq 2^{n+1} \sum_{d>B} d^{-5/4}.$$

Since B is sufficiently large and $\sum_{d=1}^{\infty} d^{-5/4}$ converges, we deduce that this last expression is $\leq \varepsilon 2^n$, completing the proof of the lemma. ■

3. The Cases $b = 4$ and $b = 5$

In this section, we complete the proof of Theorem 1. We will improve on the argument given for Lemma 3 to obtain the desired result. We note that the work in this section allows us also to handle the case $b = 3$ here, but we have chosen to indicate the proof of the case $b = 3$ separately in the previous section partially because of its simplicity and partially because the case $b = 3$ of Theorem 1 by itself can be used to obtain Theorem 2 (see Section 4).

As in the previous section, we fix $\varepsilon > 0$ and consider B to be sufficiently large. Analogous to Lemma 3, we want to show for $b = 4$ and $b = 5$ that the number of $f(x) \in S_n$ such that $f(b)$ is divisible by d^2 for some $d > B$ is $\leq \varepsilon 2^n$.

For $b \geq 3$, we define

$$S(b) = \left\{ \sum_{j=0}^{\infty} \varepsilon_j b^j : \varepsilon_j \in \{0,1\}, \text{ all but finitely many } \varepsilon_j \text{ are } 0 \right\}$$

and

$$\begin{aligned} S' = S'(b) &= \{m_1 - m_2 : m_1, m_2 \in S(b), m_1 > m_2\} \\ &= \left\{ \sum_{j=0}^{\infty} \varepsilon_j b^j \in \mathbb{Z}^+ : \varepsilon_j \in \{-1,0,1\}, \text{ all but finitely many } \varepsilon_j \text{ are } 0 \right\}. \end{aligned}$$

For r and t positive integers, we consider the set

$$X(r,t) = X(r,t;b) = \{u \in \mathbb{Z} \cap [b^{r-1}, b^r) : \gcd(b,u) = 1 \text{ and } tu^2 \in S'\}.$$

The next several lemmas serve to estimate the size of $X(r,t)$. In the end, we will need a more intricate estimate for the case $b = 5$ than for the case $b = 4$; in particular, for the case $b = 5$, we will need to strengthen our next lemma which is a preliminary bound on $|X(r,t)|$.

Lemma 4. *Let $b \geq 3$, $r \geq 2$, and $t \geq 1$ be integers. Then*

$$|X(r,t)| \leq 3^{r+1} b^2.$$

Proof. For any positive integers m and s, m is in S' if and only if $b^s m$ is in S'. Thus, we may suppose that $b \nmid t$, and we do so. We may also suppose that $|X(r,t)| \neq 0$. Let u be in $X(r,t)$. Then tu^2 is in S'. By the definition of S', an element of S' is either relatively prime to b or it is divisible by b. Thus, the conditions $\gcd(b,u) = 1$ and $tu^2 \in S'$ imply $\gcd(b,t) = 1$.

We write

$$tu^2 = \sum_{k=0}^{\infty} \alpha_k b^k,$$

where each $\alpha_k = \alpha_k(u)$ is in $\{-1,0,1\}$. There are $3^{r+1}b^2$ different values for the $(r+2)-$tuple $(u', \alpha'_0, \alpha'_1, \dots, \alpha'_r)$ where u' is a non-negative integer $< b^2$ and $\alpha'_k \in \{-1,0,1\}$ for $k \in \{0,1,\dots,r\}$. Consider a fixed such $(r+2)-$tuple. The lemma will follow if we can show that there is at most one $u \in X(r,t)$ for which $u \equiv u' \pmod{b^2}$ and $\alpha_k(u) = \alpha'_k$ for every $k \in \{0,1,\dots,r\}$.

Let u and v be in $X(r,t)$ with $u \equiv v \pmod{b^2}$ and $\alpha_k(u) = \alpha_k(v)$ for every $k \in \{0,1,\dots,r\}$. We want to show that $u = v$. Let p be a prime divisor of b. Then $\gcd(b,u) = 1$ implies $p \nmid u$. Since $\gcd(u-v, u+v) = \gcd(u-v, 2u)$, we deduce that if p divides both $u-v$ and $u+v$, then $p = 2$. Also, $u \equiv v \pmod{b^2}$ implies $p^2|(u-v)$ so that in the case $p=2$, we have $4 \nmid (u+v)$. Since $\gcd(b,t) = 1$, it follows that $\gcd(b^{r+1}, t(u+v))$ is either 1 or 2 and, hence, divides b. The condition $\alpha_k(u) = \alpha_k(v)$ for every $k \in \{0,1,\dots,r\}$ implies $b^{r+1}|\left(tu^2 - tv^2\right)$. We deduce $b^r|(u-v)$. The conclusion $u = v$ now follows since u and v are positive integers $< b^r$. ■

Lemma 5. *Let j and s be positive integers. Let K be a set of $s-$tuples $(\kappa_1, \dots, \kappa_s)$ satisfying the two conditions:*

(i) For each $i \in \{1,2,\dots,s\}$, $\kappa_i \in \{1,2,3\}$.

(ii) For each $i \in \{j+1, j+2, \dots, s\}$, if $\kappa_{i-j} \in \{2,3\}$, then $\kappa_i \in \{1,2\}$.

Then

$$|K| \le \left(\frac{3}{1+\sqrt{2}}\right)^j \left(1+\sqrt{2}\right)^s.$$

Proof. For each $t \in \{1,2,\dots,j\}$, consider the elements $(\kappa_1,\dots,\kappa_s)$ of K and define K_t as the set of $[(s-t+j)/j]-$tuples $(\kappa_t, \kappa_{j+t}, \dots, \kappa_{[(s-t)/j]j+t})$. Thus, $|K| \le \prod_{t=1}^{j} |K_t|$. Also, observe that the number of components in each element of K is the sum over t of the number of components in each element of K_t. In other words,

$$s = \sum_{t=1}^{j} \left[\frac{s-t+j}{j}\right]. \tag{2}$$

Fixing $t \in \{1, 2, \ldots, j\}$, we consider the elements $(\psi_1, \psi_2, \ldots, \psi_{[(s-t+j)/j]})$ of K_t. For each $i \in \{1, 2, \ldots, [(s-t+j)/j]\}$, we define N_i as the number of different choices for $\psi_1, \psi_2, \ldots, \psi_i$ which arise. In other words, N_i is the number of $i-$tuples $(\psi_1, \psi_2, \ldots, \psi_i)$ obtained from the first i components of the elements of K_t. Thus, $|K_t| = N_{[(s-t+j)/j]}$. By condition (i), $N_1 \leq 3$. By conditions (i) and (ii), $N_2 \leq 7$ (there are ≤ 3 choices for (ψ_1, ψ_2) with $\psi_1 = 1$ and ≤ 4 choices for (ψ_1, ψ_2) with $\psi_1 \in \{2, 3\}$). Fix $i \in \{3, 4, \ldots, [(s-t+j)/j]\}$. Let M be the number of $(i-1)-$tuples $(\psi_1, \psi_2, \ldots, \psi_{i-1})$ with $\psi_{i-1} = 1$. Observe that $M \leq N_{i-2}$. By condition (i), there are $\leq 3M$ possible $i-$tuples $(\psi_1, \psi_2, \ldots, \psi_i)$ with $\psi_{i-1} = 1$. On the other hand, by condition (ii), there are $\leq 2(N_{i-1} - M)$ possible $i-$tuples $(\psi_1, \psi_2, \ldots, \psi_i)$ with $\psi_{i-1} \in \{2, 3\}$. Therefore,

$$N_i \leq 3M + 2(N_{i-1} - M) = 2N_{i-1} + M \leq 2N_{i-1} + N_{i-2}.$$

Recall that $N_1 \leq 3$ and $N_2 \leq 7$. An easy induction argument now gives $N_i \leq 3(1+\sqrt{2})^{i-1}$. Thus,

$$|K_t| = N_{[(s-t+j)/j]} \leq 3(1+\sqrt{2})^{[(s-t)/j]} = \left(\frac{3}{1+\sqrt{2}}\right)\left(1+\sqrt{2}\right)^{[(s-t+j)/j]}.$$

The lemma now follows from $|K| \leq \prod_{t=1}^{j} |K_t|$ and (2). ■

Lemma 6. *Let b be an odd integer ≥ 5, and let r and j be positive integers with $j \leq r$. Let a and t be positive integers and suppose that $b^j || a$. Then the number of positive integers $u < b^r$ with $\gcd(b, u) = 1$ and such that both tu^2 and $t(u+a)^2$ are in S' is $\leq (b-1)3^j(1+\sqrt{2})^{r-j}$.*

Proof. As in the proof of Lemma 4, we may suppose that $\gcd(b, t) = 1$ and do so. Let u be as in the statement of the lemma. Let

$$D(u) = t(u+a)^2 - tu^2 = ta(2u+a).$$

Since tu^2 and $t(u+a)^2$ are in S', we have

$$(3) \qquad tu^2 = \sum_{k=0}^{\infty} \alpha_k b^k \quad \text{and} \quad t(u+a)^2 = \sum_{k=0}^{\infty} \beta_k b^k$$

for some integers α_k and β_k in $\{-1, 0, 1\}$. We write

$$(4) \qquad u = \sum_{k=0}^{r-1} u_k b^k \quad \text{and} \quad D(u) = \sum_{k=0}^{\infty} d_k b^k$$

where, for each non-negative integer k, $u_k \in [0, b-1]$ and

$$(5) \qquad d_k = \beta_k - \alpha_k \in [-2, 2].$$

Note that since $b \geq 5$, $D(u)$ has a unique representation as in (4) with $d_k \in [-2, 2]$. Suppose now that v is a positive integer $< b^r$ with $v \neq u$ and $\gcd(b, v) = 1$ and such that both tv^2 and $t(v+a)^2$ are in S'. Let ℓ be the non-negative integer satisfying $b^\ell || (v-u)$. Then $D(v) - D(u) = 2ta(v-u)$ so that

$$b^{\ell+j} || \left(D(v) - D(u)\right).$$

Viewing the numbers $u_0, u_1, \dots, u_{\ell-1}$ in (4) as fixed, we deduce that the numbers $d_0, d_1, \dots,$ $d_{\ell+j-1}$ are uniquely determined. Furthermore, the number u_ℓ uniquely determines the value of $d_{\ell+j}$ and different values of u_ℓ lead to different values of $d_{\ell+j}$. In particular, there is at most one choice of u_ℓ which leads to $d_{\ell+j} = 0$. We refer to such a choice of u_ℓ as "nice."

We keep the notation above and still view $u_0, u_1, \dots, u_{\ell-1}$ as fixed. Suppose that $\ell \geq 1$. Since b is an odd integer relatively prime to tu, we obtain that $\gcd(b, t(u+v)) = 1$ so that $b^\ell || \left(tv^2 - tu^2\right)$. Hence, the numbers $\alpha_0, \alpha_1, \dots, \alpha_{\ell-1}$ in (3) are uniquely determined. Different values of u_ℓ lead to different values of α_ℓ. We are interested only in u for which $tu^2 \in S'$ so that $\alpha_\ell \in \{-1, 0, 1\}$. Therefore, there are at most 3 different values of u_ℓ such that $tu^2 \in S'$.

Since α_ℓ and β_ℓ are in $\{-1,0,1\}$, for each $d_\ell \in \{-2,-1,0,1,2\}$, there are at most $3-|d_\ell|$ values of α_ℓ such that (5) holds. In particular, we deduce that if $\ell \ge j$ and $u_{\ell-j}$ is not nice (so that $d_\ell \ne 0$), then there are at most two values of α_ℓ, and hence at most two values of u_ℓ, for which tu^2 and $t(u+a)^2$ are both in S'.

Since $b \nmid u$, there are at most $b-1$ choices for u_0 in (4). Fix u_0 and consider the choices for $u_1, \dots, u_{r-1}$ as in (4) with u as in the lemma. For $\ell \in \{1,2,\dots,r-1\}$ and for any given $u_1,\dots,u_{\ell-1}$, there are at most 3 different values of u_ℓ, say $\gamma_i = \gamma_i(u_0,u_1,\dots,u_{\ell-1})$ where i is a positive integer ≤ 3. At most one such u_ℓ is nice, and if such a choice of u_ℓ exists we can suppose that it is γ_1 and do so. We define $\phi_\ell(u_\ell) = i$ where $i \in \{1,2,3\}$ with $u_\ell = \gamma_i$. Observe that u in (4) is uniquely determined by the value of $(\phi_1(u_1), \phi_2(u_2), \dots, \phi_{r-1}(u_{r-1}))$ (where we are still viewing u_0 as fixed). Also, if $\ell \in \{j+1, j+2, \dots, r-1\}$ and $\phi_{\ell-j}(u_{\ell-j}) \in \{2,3\}$ (so that $u_{\ell-j}$ is not nice), then $\phi_\ell(u_\ell) \le 2$. Thus, the set of $(r-1)$–tuples $(\phi_1(u_1),\dots,\phi_{r-1}(u_{r-1}))$ satisfies the conditions of the set K in Lemma 5 with $s = r-1$. Recalling that there are $\le b-1$ choices for the value of u_0, we deduce that the number of $u < b^r$ with $\gcd(b,u) = 1$ and such that both tu^2 and $t(u+a)^2$ are in S' is

$$\le (b-1)\left(\frac{3}{1+\sqrt{2}}\right)^j \left(1+\sqrt{2}\right)^{r-1} < (b-1)3^j(1+\sqrt{2})^{r-j},$$

establishing the lemma. ■

Lemma 7. *Let b be a positive integer ≥ 3. Let r and ℓ be positive integers with $1 \le \ell \le r$. Let t be a positive integer. Then there exist $3^{r-\ell+2}$ intervals each of length $< 2b^\ell$ with the union of these intervals containing all numbers u for which $b^{r-1} \le u < b^r$ and $tu^2 \in S'$.*

Proof. Let s be the positive integer satisfying

$$\frac{b^{s-1}}{b-1} < t \le \frac{b^s}{b-1}.$$

For $u < b^r$ and $tu^2 \in S'$, we obtain

$$tu^2 = \sum_{k=0}^{2r+s-1} \alpha_k b^k \quad \text{for some } \alpha_k \in \{-1,0,1\}.$$

Fix α_k for $r+s+\ell-2 \le k \le 2r+s-1$. Let

$$\alpha = \sum_{k=r+s+\ell-2}^{2r+s-1} \alpha_k b^k - \sum_{k=0}^{r+s+\ell-3} b^k \quad \text{and} \quad \beta = \sum_{k=r+s+\ell-2}^{2r+s-1} \alpha_k b^k + \sum_{k=0}^{r+s+\ell-3} b^k.$$

For $b^{r-1} \le u < b^r$ and $tu^2 \in S'$, we deduce that tu^2 is in some such $[\alpha,\beta]$ so that $u \in [\gamma,\delta]$ where

$$[\gamma,\delta] = \left[\sqrt{\alpha/t}, \sqrt{\beta/t}\right] \cap \left[b^{r-1}, b^r\right].$$

Observe that

$$\beta - \alpha = 2 \sum_{k=0}^{r+s+\ell-3} b^k < \frac{2b^{r+s+\ell-2}}{b-1}.$$

Therefore,

$$\begin{aligned}\delta - \gamma \le \sqrt{\beta/t} - \sqrt{\alpha/t} &= \frac{\beta-\alpha}{t(\sqrt{\beta/t}+\sqrt{\alpha/t})} \\ &< \frac{\beta-\alpha}{t\gamma} \le \frac{\beta-\alpha}{tb^{r-1}} < \frac{2b^{r+s+\ell-2}/(b-1)}{b^{r+s-2}/(b-1)} = 2b^{\ell}.\end{aligned}$$

Hence, the $3^{r-\ell+2}$ choices for $\alpha_{r+s+\ell-2},\ldots,\alpha_{2r+s-1}$, each in $\{-1,0,1\}$, lead to $3^{r-\ell+2}$ intervals $[\gamma,\delta]$ of length $< 2b^{\ell}$ satisfying the conditions of the lemma. ■

Since $b \ge 3$, it is not difficult to check that the intervals in the proof of Lemma 7 above are disjoint. On the other hand, it is already clear in the statement of Lemma 7 that we may consider these intervals to be disjoint.

Lemma 8. *Let b be an odd integer ≥ 5. Let r and t be positive integers. Then*

$$|X(r,t)| \ll \exp\left(\frac{\log 3(\log b + \log(1+\sqrt{2}))\, r}{\log(3b)}\right),$$

where the implied constant depends on b but not on r or t.

Proof. Consider an arbitrary positive integer $\ell \le r$. By Lemma 7, $X(r,t)$ is contained in the union of $3^{r-\ell+2}$ disjoint intervals $[\gamma_i, \delta_i]$, with $1 \le i \le 3^{r-\ell+2}$, where each interval is of length $< 2b^\ell$. For each $i \in \{1, 2, \dots, 3^{r-\ell+2}\}$ and $k \in \{1, 2, \dots, b-1\}$, we set

$$X_{i,k}(r,t) = \{u \in X(r,t) : u \in [\gamma_i, \delta_i] \text{ and } u \equiv k \pmod b\}.$$

Let $n_{i,k} = |X_{i,k}(r,t)|$. Then

$$\begin{aligned}
\sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} \frac{n_{i,k}(n_{i,k}-1)}{2} &= \sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} |\{(u,v) : u \in X_{i,k}(r,t), v \in X_{i,k}(r,t), \text{ and } u < v\}| \\
&= \sum_{\substack{1 \le a < 2b^\ell \\ b|a}} \sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} |\{(u,v) : u \in X_{i,k}(r,t), v \in X_{i,k}(r,t), \text{ and } v-u = a\}| \\
&\le \sum_{\substack{1 \le a < 2b^\ell \\ b|a}} |\{(u,v) : u \in X(r,t), v \in X(r,t), \text{ and } v-u = a\}|.
\end{aligned}$$

From Lemma 6, we now deduce that

$$\begin{aligned}
\sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} \frac{n_{i,k}(n_{i,k}-1)}{2} &\le \sum_{j=1}^{\ell} \sum_{\substack{1 \le a < 2b^\ell \\ b^j || a}} (b-1)3^j(1+\sqrt{2})^{r-j} \\
&\le \sum_{j=1}^{\ell} 2b^{\ell-j}(b-1)3^j(1+\sqrt{2})^{r-j} \ll b^\ell(1+\sqrt{2})^r.
\end{aligned}$$

Therefore,

$$\begin{aligned}
|X(r,t)| &= \sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} n_{i,k} \le \sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} \left(1 + \frac{n_{i,k}(n_{i,k}-1)}{2}\right) \\
&= \sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} 1 \; + \; \sum_{i=1}^{3^{r-\ell+2}} \sum_{k=1}^{b-1} \frac{n_{i,k}(n_{i,k}-1)}{2} \ll 3^{r-\ell} + b^\ell(1+\sqrt{2})^r.
\end{aligned}$$

We choose

$$\ell = \left[\frac{(\log 3 - \log(1+\sqrt{2}))\, r}{\log(3b)}\right] + 1$$

to obtain the lemma. ■

Lemma 9. *Let $b = 4$ or 5. Let $\varepsilon > 0$, and let $B = B(\varepsilon)$ be sufficiently large. Then the number of $f(x) \in S_n$ such that $f(b)$ is divisible by d^2 for some integer $d > B$ is $\le \varepsilon 2^n$.*

Proof. Since B is sufficiently large, the number of $f(x) \in S_n$ as in the lemma is 0 unless n is also large. We therefore consider n large. Let r be a positive integer for which $b^r > B$. We consider the integers d such that $b^{r-1} \le d < b^r$. For $f(x) \in S_n$, we have $0 < f(b) \le b^{n+1}$ so that if $f(b)$ is divisible by d^2 (which is $\ge b^{2r-2}$), then $r \le (n+3)/2$. We therefore suppose, as we may, that $r \le (n+3)/2$.

Recall that each $f(x) \in S_n$ has constant term 1 so that if $f(b)$ is divisible by d^2, then $\gcd(b, d) = 1$. If $f(b) = td^2$, then we also have that $1 \le t = f(b)/d^2 \le b^{n-2r+3}$ so that $d \in X(r, t)$ for some positive integer $t \le b^{n-2r+3}$. We use Lemmas 4 and 8 to obtain that the number of $f(x) \in S_n$ for which there exists a $d \in [b^{r-1}, b^r)$ such that $d^2 | f(b)$ is

$$\le \sum_{t=1}^{b^{n-2r+3}} |X(r,t)| \ll \begin{cases} 4^{n-2r} 3^r & \text{for } b = 4 \\ 5^{n-2r} \exp\left(\dfrac{\log 3 (\log 5 + \log(1+\sqrt{2}))\, r}{\log 15} \right) & \text{for } b = 5. \end{cases}$$

In either case, if $r > n/(2.4)$, the above expression on the right is easily $\ll 2^n/(nB)$. We restrict our attention now to $r \le n/(2.4)$. We note that our method for obtaining this bound on r is not the best possible, and it would be easy to replace 2.4 with a larger number; however, 2.4 will be sufficient for what follows.

Let s denote a positive integer $\le n - 2r$. We consider $f(x) = \sum_{j=0}^{n} \varepsilon_j x^j \in S_n$ with $\varepsilon_{2r+s-2}, \varepsilon_{2r+s-1}, \dots, \varepsilon_n$ fixed elements from $\{0, 1\}$. Thus, we obtain 2^{2r+s-3} different values of $f(b)$. Let $N(d)$ denote the number of different $(2r+s-3)$-tuples $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{2r+s-3})$, with each $\varepsilon_j \in \{0, 1\}$, such that $d^2 | f(b)$. Suppose $N(d) \ge 1$. Consider the $f(x)$ counted by $N(d)$, and let $f_1(x)$ denote the $f(x)$ which minimizes the value of $f(b)$. Then there are $N(d) - 1$ other $f(x)$ counted by $N(d)$ each having the property that $d^2 | f(b)$. For each of these $N(d) - 1$ different $f(x)$, we obtain

$$0 < f(b) - f_1(b) \le b^{2r+s-2} \le d^2 b^s.$$

Thus, there are at least $N(d)-1$ different $f(x)\in S_n$ (with $\varepsilon_{2r+s-2},\varepsilon_{2r+s-1},\dots,\varepsilon_n$ fixed) such that $f(b)-f_1(b)=td^2$ for some positive integer $t\le b^s$. Different choices for $f(x)$ give different values for t. We deduce that there are at least $N(d)-1$ different $t\le b^s$ for which $d\in X(r,t)$.

With $\varepsilon_{2r+s-2},\varepsilon_{2r+s-1},\dots,\varepsilon_n$ still fixed, we bound the number of $f(x)\in S_n$ such that there is a $d\in[b^{r-1},b^r)$ for which $d^2|f(b)$. This number is

$$\le \sum_{b^{r-1}\le d<b^r} N(d) = \sum_{\substack{b^{r-1}\le d<b^r\\ N(d)\ge 1}} (N(d)-1) + \sum_{\substack{b^{r-1}\le d<b^r\\ N(d)\ge 1}} 1.$$

From our comments above and from Lemmas 4 and 8, we deduce that

$$\sum_{\substack{b^{r-1}\le d<b^r\\ N(d)\ge 1}} (N(d)-1) \le \sum_{b^{r-1}\le d<b^r} \sum_{\substack{1\le t\le b^s\\ d\in X(r,t)}} 1 = \sum_{1\le t\le b^s} \sum_{\substack{b^{r-1}\le d<b^r\\ d\in X(r,t)}} 1$$
$$= \sum_{1\le t\le b^s} |X(r,t)| \ll \begin{cases} 4^s 3^r & \text{for } b=4\\ 5^s \exp\left(\dfrac{\log 3(\log 5+\log(1+\sqrt{2}))\,r}{\log 15}\right) & \text{for } b=5.\end{cases}$$

Also,

$$\sum_{\substack{b^{r-1}\le d<b^r\\ N(d)\ge 1}} 1 \le b^r.$$

Letting $\varepsilon_{2r+s-2},\varepsilon_{2r+s-1},\dots,\varepsilon_n$ now vary, we deduce that the number of $f(x)\in S_n$ such that there exists a $d\in[b^{r-1},b^r)$ for which $d^2|f(b)$ is

$$\ll 2^{n-2r-s}4^s3^r + 2^{n-2r-s}4^r \qquad \text{for b} = 4$$

and

$$\ll 2^{n-2r-s}5^s \exp\left(\frac{\log 3(\log 5+\log(1+\sqrt{2}))\,r}{\log 15}\right) + 2^{n-2r-s}5^r \qquad \text{for b} = 5.$$

In the case $b=4$, we choose

$$s = \left[\frac{r\log(4/3)}{\log 4}\right] + 1;$$

and in the case $b = 5$, we choose

$$s = \left[\frac{r}{\log 5} \left(\log 5 - \frac{\log 5 + \log(1+\sqrt{2})}{\log 15} (\log 3) \right) \right] + 1.$$

It is easily checked that since $1 \le r \le n/(2.4)$, in either case the choice of s is a positive integer $\le n - 2r$. We obtain that the number of $f(x) \in S_n$ such that $f(b)$ is divisible by some d^2 with $b^{r-1} \le d < b^r$ is

$$\ll 2^{n-2r-s} b^r \ll \begin{cases} 2^n \exp(-0.14r) & \text{for } b = 4 \\ 2^n \exp(-0.034r) & \text{for } b = 5. \end{cases}$$

In either case, $b = 4$ or $b = 5$, since $e^2 > b$, the above bound is $\ll 2^n e^{-2r/100} \ll 2^n b^{-r/100}$.

Letting r vary over the positive integers for which $b^r > B$, we easily obtain now that the number of $f(x) \in S_n$ such that $f(b)$ is divisible by d^2 for some $d > B$ is $\ll 2^n B^{-1/100}$. Since B is sufficiently large, the proof of the lemma is complete. ■

4. The Proof of Theorem 2

Let R be a fixed real number ≥ 1. We begin by estimating the number of $f(x) \in S_n$ divisible by the square of a non-constant polynomial in $\mathbb{Z}[x]$ of degree $\le R$. We will show that there are $o(2^n)$ such $f(x)$.

Odlyzko and Poonen [2] have obtained extensive results about the roots of polynomials in S_n. For our purposes, it suffices to know that these roots are bounded in absolute value by 2 which is easily established as follows. Let $f(x) \in S_n$, and write $f(x) = \sum_{j=0}^{m} \varepsilon_j x^j$ where $m \le n$, $\varepsilon_j \in \{0, 1\}$ for each j, and $\varepsilon_0 = \varepsilon_m = 1$. If $\alpha \in \mathbb{C}$ and $|\alpha| \ge 2$, then

$$|f(\alpha)| \ge \left| \sum_{j=0}^{m} \varepsilon_j \alpha^j \right| \ge |\alpha|^m - \sum_{j=0}^{m-1} |\alpha|^j = |\alpha|^m - \frac{|\alpha|^m - 1}{|\alpha| - 1}$$

$$= \frac{|\alpha|^{m+1} - 2|\alpha|^m + 1}{|\alpha| - 1} = \frac{(|\alpha| - 2)|\alpha|^m + 1}{|\alpha| - 1} > 0.$$

Thus, $f(\alpha) \neq 0$, and we deduce that all roots of the polynomials in S_n necessarily have absolute value < 2.

Let $g(x) \in \mathbb{Z}[x]$ of degree $r \in [1, R]$, and suppose that $g(x)$ is a factor of some polynomial in S_n. It follows that the roots of $g(x)$ are < 2. Also, since polynomials in S_n are monic, the leading coefficient of $g(x)$ must be ± 1. Since the degree of $g(x)$ is $\leq R$, it follows that each coefficient of $g(x)$ has absolute value less than or equal to the product of 2^R (an upper bound on the absolute value of the product of the roots of $g(x)$) and 2^R (an upper bound on the number of combinations of $r \leq R$ roots taken k at a time where $k \in \{0, 1, \ldots, r\}$). Since the absolute value of the coefficients of $g(x)$ are bounded by 4^R and since $g(x)$ has degree $\leq R$, there are

$$\leq \left(2 \times 4^R + 1\right)^{R+1}$$

different possible values of $g(x)$. To establish what we first set out to show, it suffices then to obtain that for each such $g(x)$, there are $o(2^n)$ different possible $f(x) \in S_n$ divisible by $g(x)^2$.

Fix $g(x)$ as above. Suppose that $f(x) = \sum_{j=0}^{n} \varepsilon_j x^j \in S_n$ is divisible by $g(x)^2$. We consider the set $T_n(f(x))$ consisting of the polynomials $w(x) = \sum_{j=0}^{n} \varepsilon'_j x^j \in S_n$ where there is exactly one $k \in \{1, 2, \ldots, n\}$ for which $\varepsilon'_k \neq \varepsilon_k$. In other words, $w(x) = \sum_{j=0}^{n} \varepsilon'_j x^j \in T_n(f(x))$ if and only if there is a $k \in \{1, 2, \ldots, n\}$ such that $\varepsilon'_\ell = \varepsilon_\ell$ for every $\ell \in \{0, 1, \ldots, n\}$ with $\ell \neq k$ and $\varepsilon'_k = 1 - \varepsilon_k$. Thus, $|T_n(f(x))| = n$. Since $f(x)$ is divisible by $g(x)^2$ and $f(x)$ has constant term 1, it must be the case that $g(x)$ is not divisible by x. If $w(x) = \sum_{j=0}^{n} \varepsilon'_j x^j \in T_n(f(x))$ and $k \in \{1, 2, \ldots, n\}$ with $\varepsilon'_k \neq \varepsilon_k$, then $f(x) - w(x) = \pm x^k$ is not divisible by $g(x)^2$. We deduce that the elements of $T_n(f(x))$ are not divisible by $g(x)^2$.

Now, suppose that $f_1(x)$ and $f_2(x)$ are distinct polynomials in S_n with each divisible by $g(x)^2$. We show that $T_n(f_1(x))$ and $T_n(f_2(x))$ are disjoint. If the sets were not disjoint, then there would be some $w(x)$ which differs from each of $f_1(x)$ and $f_2(x)$ by a power of x. By considering $f_1(x) - f_2(x)$, it follows that for some k and ℓ in $\{1, 2, \dots, n\}$ with $k > \ell$, $x^k \pm x^\ell = x^\ell(x^{k-\ell} \pm 1)$ is divisible by $g(x)^2$. Since the roots of $x^{k-\ell} \pm 1$ are distinct and since $g(x)$ is not divisible by x, we deduce that $g(x)^2$ cannot divide $x^\ell(x^{k-\ell} \pm 1)$. Hence, $T_n(f_1(x))$ and $T_n(f_2(x))$ are disjoint.

For each $f(x) \in S_n$ divisible by $g(x)^2$, there correspond n polynomials, namely the elements of $T_n(f(x))$, which are not divisible by $g(x)^2$, and these n polynomials are different for different $f(x)$. Thus, there are $\le 2^n/(n+1)$ polynomials in S_n divisible by $g(x)^2$. Hence, there are $o(2^n)$ polynomials in S_n divisible by $g(x)^2$ and thus $o(2^n)$ polynomials $f(x) \in S_n$ which are divisible by the square of a polynomial of degree $\le R$.

Fix $\varepsilon > 0$. It suffices to show that if R is sufficiently large, then there are $\le \varepsilon 2^n$ polynomials $f(x) \in S_n$ which are divisible by the square of a polynomial in $\mathbb{Z}[x]$ of degree $> R$. We will use Theorem 1 with $b = 4$ and the fact already established that the roots of the polynomials in S_n have absolute value < 2. We note, however, the case $b = 3$ of Theorem 1 could be used instead of the case $b = 4$ if we use that the roots of the polynomials in S_n have real parts < 1.5 (cf. [1] or [2]).

Let $f(x) \in S_n$ with $f(x)$ divisible by the square of a polynomial $g(x) \in \mathbb{Z}[x]$ of degree $r > R$. We may suppose that $g(x)$ is monic (otherwise, replace $g(x)$ with $-g(x)$). Then the roots of $f(x)$ and hence $g(x)$ have absolute value < 2. If $\beta_1, \dots, \beta_r$ denote the roots of $g(x)$, then $g(x) = \prod_{j=1}^r (x - \beta_j)$ and

$$|g(4)| = \prod_{j=1}^{r} |4 - \beta_j| \ge 2^r > 2^R.$$

Since $f(x)$ is divisible by $g(x)^2$, we deduce that $f(4)$ is divisible by d^2 for some integer $d > 2^R$. On the other hand, from Lemma 9 with $b = 4$, we obtain that for R sufficiently large, there are $\le \varepsilon 2^n$ such polynomials $f(x) \in S_n$. Hence, Theorem 2 follows.

Acknowledgments: Research of the first author was supported by NSA Grant MDA904-92-H-3011 and NSF Grant DMS-9400937. Research of the second author was supported by a grant from the Cultural Initiative Fund and the Russian Academy for Natural Sciences and by Grant MC5000 from the International Science Foundation. The authors also gratefully acknowledge NSF EPSCoR Grant EHR 9108772 and ONR Contract N0014-91-51343 which provided support for the second author while he visited the University of South Carolina where this research took place.

References

1. J. Brillhart, M. Filaseta, and A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Can. J. Math. **33** (1981), 1055–1059.
2. A. M. Odlyzko and B. Poonen, *Zeros of polynomials with* 0, 1 *coefficients*, L'Enseignement Mathématique **39** (1993), 317–348.

Michael Filaseta
Mathematics Department
University of South Carolina
Columbia, SC 29208
U.S.A.
filaseta@math.sc.edu

Sergei Konyagin
Department of Mechanics and Mathematics
State University
Moscow 119899
Russia
kon@sci.math.msu.su