SQUAREFREE VALUES OF POLYNOMIALS

Michael Filaseta*

1. Introduction.

The purpose of this paper is to present some results related to squarefree values of polynomials. For $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$, we define $N_f = \gcd(f(m), m \in \mathbb{Z})$. For computational reasons it is worth noting that

$$N_f = \gcd(f(m), m \in \{0, 1, ..., n\})$$

where n denotes the degree of $f(x)$. This observation is due to Hensel (cf. [1, p. 334]) and follows in a fairly direct manner after using Lagrange's interpolation formula to deduce that

$$f(m) = \sum_{j=0}^{n} (-1)^{n-j} \binom{m}{j} \binom{m-j-1}{n-j} f(j),$$

where m is any integer $> n$. We will be interested in estimating the number of polynomials $f(x)$ for which there exists an integer m such that $f(m)$ is squarefree. This property should hold for all polynomials $f(x)$ for which N_f is squarefree. However, this seems to be very difficult to establish. Nagel [8] showed that if $f(x) \in \mathbb{Z}[x]$ is an irreducible quadratic and N_f is squarefree, then $f(m)$ is squarefree for infinitely many integers m. Erdős [2]

*Research was supported in part by the NSF under grant number DMS-8903123.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

proved the analogous result for irreducible cubics. Nair [9] has shown that in the case of an irreducible polynomial $f(x)$ of degree n, one may obtain a similar theorem for k-free values of $f(x)$ provided that $k \geq (\sqrt{2} - \frac{1}{2})n$. Of related interest are the papers of Hooley [5], Nair [10], and Huxley and Nair [6]. The problem of determining whether there exists a polynomial $f(x) \in \mathbb{Z}[x]$ of degree ≥ 4 for which there are infinitely many integers m such that $f(m)$ is squarefree is open.

Our interest is in the simpler problem of showing that many polynomials take on at least one squarefree value. If one can show that (i) every polynomial $f(x) \in \mathbb{Z}[x]$ with N_f squarefree is such that $f(m)$ is squarefree for *at least one* integer m, then it will follow that (ii) every polynomial $f(x) \in \mathbb{Z}[x]$ with N_f squarefree is such that $f(m)$ is squarefree for *infinitely many* integers m (cf. the proof of Theorem 2 in [3]). In fact, (i) implies that (iii) every polynomial $f(x) \in \mathbb{Z}[x]$ is such that $f(m)/N_f$ is squarefree for infinitely many integers m. Our goal is to show the weaker result that almost all polynomials $f(x)$ with N_f squarefree take on at least one squarefree value.

To clarify our results, we define

$$S_n(N) = \{f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x] : |a_j| \leq N \text{ for } j = 0, 1, \ldots, n\}.$$

Thus, $|S_n(N)| = (2[N] + 1)^{n+1}$. We say that almost all polynomials $f(x)$ have a certain property P if for every non-negative integer n,

$$\lim_{N \to \infty} \frac{|\{f(x) \in S_n(N) : f(x) \text{ satisfies } P\}|}{|S_n(N)|} = 1. \tag{1}$$

Results associated with almost all polynomials go back to van der Waerden [12]. He showed that for almost all polynomials $f(x)$ the associated Galois group is the symmetric group on n letters where $n = \deg f(x)$. In particular, this implies that almost all polynomials are irreducible. A proof of this latter fact can be found in Pólya and Szegő [11, p. 156]. Other related results can be found in Gallagher [4] and the author's [3].

We make a brief historic remark on the phrase "almost all" in this context. Van der Waerden's *Algebra I* includes a comment on his result above [13, p. 204]. The German edition states that the Galois group is the symmetric group for asymptotically "100%" of the polynomials rather than using a German equivalent for "almost all." This led to a mistranslation in the English edition [14, p. 200] where a statement is made asserting that the Galois group is the symmetric group for "all" polynomials. The earliest editions of van der Waerden's *Algebra I* do not refer to his result above.

At times we will restrict our attention to polynomials $f(x)$ for which N_f is squarefree. An almost all result for such $f(x)$ will mean that (1) holds with $S_n(N)$ replaced by $\{f(x) \in S_n(N) : N_f \text{ squarefree}\}$. We will prove

Theorem 1. *Almost all polynomials $f(x)$ with N_f squarefree are such that $f(m)$ is squarefree for some integer m.*

Theorem 2. *Almost all polynomials $f(x)$ are such that there is an integer m for which $f(m)/N_f$ is squarefree.*

We will actually prove stronger results (see section 3). As a consequence of the stronger results, we note that almost all polynomials $f(x) = \sum_{j=0}^{n} a_j x^j$ are such that $f(m)/N_f$ is squarefree for some positive integer $m \le \psi\left(\max_{0 \le j \le n}\{|a_j|\}\right)$, where $\psi(x)$ is any function which tends to infinity with x.

We end this section by asking whether analogous results hold when one considers values

$f(m)$ with large prime factors rather than squarefree numbers. In particular, is there an absolute constant $c > 1$ (or even a $c > 1$ which depends on $\deg f(x)$) such that almost all polynomials $f(x)$ are such that there is a positive integer m and a prime p for which $p|f(m)$ and $p > m^c$?

2. Preliminaries

Throughout this section and the next we make use of the notation established in the introduction. We view n as being a fixed nonnegative integer so that, in particular, other quantities such as ϵ may depend on n. We will, however, stress when such a dependence is necessary. We reserve p for denoting primes.

Lemma 1. *Let $\epsilon > 0$, and let $B = B(N)$ be a function which increases to infinity with N. Suppose further that $B(N) = o(N)$. Then there exists $N_0 = N_0(n, \epsilon, B)$ such that if $N \geq N_0$, then the number of pairs $(f(x), m)$ with $f(x) \in S_n(N)$, $m \in \mathbb{Z} \cap [1, B]$, and $f(m)$ squarefree is in the interval*

$$\left[(1-\epsilon)\frac{6}{\pi^2}(2N)^{n+1}B, (1+\epsilon)\frac{6}{\pi^2}(2N)^{n+1}B\right].$$

Proof. Let $\epsilon' > 0$. Fix m_0 to be a positive integer satisfying $m_0 \geq (1/\epsilon') + 1$ so that if $m \geq m_0$, then

$$m^{n-1} + \cdots + m + 1 = \frac{m^n - 1}{m - 1} < \epsilon' m^n.$$

For the moment fix m to be an integer in $[m_0, B]$, and consider an integer d such that

$$|d| \leq (1-\epsilon')Nm^n. \tag{2}$$

If $a_0, a_1, \dots, a_{n-1}$ are arbitrary integers in $[-N, N]$ and N is sufficiently large, depending only on ϵ', we get that

$$\left| d - \left(a_{n-1} m^{n-1} + \cdots + a_1 m + a_0 \right) \right| \le N m^n. \tag{3}$$

We successively choose $a_0, a_1, \dots, a_{n-1}$ as above with $a_0 \equiv d \pmod{m}$ and for $j \in \{1, 2, \dots, n-1\}$,

$$a_j \equiv \left(d - a_0 - \cdots - a_{j-1} m^{j-1} \right) / m^j \pmod{m}.$$

Thus, the total number of choices for $(a_0, a_1, \dots, a_{n-1})$ is

$$\left(\frac{2[N]+1}{m} + O(1) \right)^n = \left(\frac{2N}{m} \right)^n + O_n \left(\frac{N^{n-1}}{m^{n-1}} \right).$$

By (3), we can now find a unique $a_n \in [-N, N]$ such that

$$d = a_n m^n + \cdots + a_1 m + a_0.$$

The above steps may be reversed. More specifically, given m and d as above, we must have that $a_0, \dots, a_{n-1}$ satisfy the congruences above, and this uniquely determines a_n as above. Thus, for m fixed in $[m_0, B]$, each integer d satisfying (2) has $(2N/m)^n + O_n\left(N^{n-1}/m^{n-1}\right)$ representations of the form $f(m)$ where $f(x) \in S_n(N)$.

We now let m vary over all the positive integers $m \le B$. We divide the pairs $(f(x), m)$, where $f(x) \in S_n(N)$ and $1 \le m \le B$, into 3 sets S_1, S_2, and S_3. The set S_1 consists of those $(f(x), m)$ for which $d = f(m)$ is squarefree, $m \in [m_0, B]$, and (2) holds. The set S_2 consists of those $(f(x), m)$ for which $d = f(m)$ is nonsquarefree, $m \in [m_0, B]$, and (2) holds. The set S_3 consists of the remaining pairs $(f(x), m)$. Then since for any $t > 0$ the number of squarefree numbers $\le t$ is $(6/\pi^2)t + O(\sqrt{t})$, we get that

$$\begin{aligned}|S_1| &= \sum_{m_0 \le m \le B} \left(\left(\frac{2N}{m}\right)^n (6/\pi^2)(1-\epsilon')(2N)m^n + O_n\left(N^n m\right) + O\left(N^{n+\frac{1}{2}}\right)\right) \\ &= (6/\pi^2)(1-\epsilon')(2N)^{n+1}B + O_n\left(N^{n+1}m_0\right) + O_n\left(N^n B^2\right) + O\left(N^{n+\frac{1}{2}}B\right),\end{aligned}$$

$$|S_2| = \left(1 - \frac{6}{\pi^2}\right)(1-\epsilon')(2N)^{n+1}B + O_n\left(N^{n+1}m_0\right) + O_n\left(N^n B^2\right) + O\left(N^{n+\frac{1}{2}}B\right),$$

and

$$\begin{aligned}|S_3| &= (2[N]+1)^{n+1}[B] - |S_1| - |S_2| \\ &= \epsilon'(2N)^{n+1}B + O_n\left(N^{n+1}m_0\right) + O_n\left(N^n B^2\right) + O\left(N^{n+\frac{1}{2}}B\right).\end{aligned}$$

Now, $|S_1|$ gives us a lower bound on the number of pairs $(f(x), m)$ with $f(m)$ squarefree and $m \in [1, B]$. An upper is

$$|S_1| + |S_3| < (6/\pi^2)(1+\epsilon')(2N)^{n+1}B + O_n\left(N^{n+1}m_0\right) + O_n\left(N^n B^2\right) + O\left(N^{n+\frac{1}{2}}B\right).$$

Thus, taking $\epsilon' = \epsilon/2$ and N sufficiently large, the result follows.

The proof of Lemma 1 given above is similar to the proof of Lemma 1 in [3]. Lemma 1 asserts that the $f(x) \in S_n(N)$ on average take on $\sim \dfrac{6}{\pi^2}B$ squarefree values as x ranges over the positive integers $\le B$. We note that this is true despite the fact that a positive proportion of the $f(x) \in S_n(N)$ take on *no* squarefree values. More specifically, observe that N_f is divisible by p^2 if and only if

$$f(x) \equiv x^2(x-1)^2 \cdots (x-(p-1))^2 g(x) + px(x-1)\cdots(x-(p-1))h(x) \pmod{p^2},$$

for some polynomials $g(x)$ and $h(x) \in \mathbb{Z}[x]$. Thus, if $p \geq n+1$, then $f(x) \equiv 0$ is the only such $f(x)$ modulo p^2; if $(n+1)/2 \leq p \leq n$, then there are exactly p^{n-p+1} incongruent such $f(x)$ modulo p^2; and if $p \leq n/2$, then there are exactly $p^{2n-3p+2}$ incongruent such $f(x)$ modulo p^2. A simple application of the sieve of Eratosthenes implies that for N sufficiently large, the proportion of $f(x) \in S_n(N)$ for which N_f is nonsquarefree is asymptotic to

$$1 - \prod_{p \leq n/2} \left(1 - \frac{1}{p^{3p}}\right) \prod_{(n+1)/2 \leq p \leq n} \left(1 - \frac{1}{p^{n+1+p}}\right) \prod_{p \geq n+1} \left(1 - \frac{1}{p^{2n+2}}\right)$$

$$\geq 1 - \prod_{p} \left(1 - \frac{1}{p^{3p}}\right) = 0.015675\ldots.$$

Thus, the polynomials $f(x) \in S_n(N)$ which take on at least one squarefree value as x ranges over the positive integers $\leq B$ on average take on $\geq (6/\pi^2)B(1.0159\ldots)$ squarefree values. This curiosity is due to the size of the coefficients of the polynomials under consideration in comparison to B.

For $f(x) \in \mathbb{Z}[x]$ and $\ell \in \mathbb{Z}$, we define $\rho(\ell) = \rho_f(\ell)$ to be the number of incongruent solutions to $f(x) \equiv 0 \pmod{\ell}$. The next lemma gives some basic properties of $\rho(\ell)$.

Lemma 2. *Let $f(x) \in \mathbb{Z}[x]$ of degree n. Then $\rho(\ell)$ has the following properties:*

(i) $\rho(\ell)$ is multiplicative (i.e., if ℓ_1 and ℓ_2 are relatively prime integers, then $\rho(\ell_1\ell_2) = \rho(\ell_1)\rho(\ell_2)$),

(ii) if $\rho(p) = p$, then either $p \leq n$ or $f(x) \equiv 0 \pmod{p}$,

(iii) if $\rho(p) < p$, then $\rho(p) \leq n$,

(iv) if $\rho(p^2) > \rho(p)$, then $f(x)$ has a multiple root modulo p (i.e., there exist an integer a and a polynomial $g(x)$ such that $f(x) \equiv (x-a)^2 g(x) \pmod{p}$),

(v) if $\rho(p^2) < p^2$, then $\rho(p^2) \leq pn$,

(vi) if $p > n$ and $\rho(p^r) = p^r$ for some positive integer r, then $f(x) \equiv 0 \pmod{p^r}$.

Proof. Property (i) is an immediate consequence of the Chinese Remainder Theorem. A theorem of Lagrange states that either the number of solutions to the congruence $f(x) \equiv 0 \pmod{p}$ is $\leq n$ or $f(x)$ is identically 0 as a polynomial modulo p. This easily implies (ii) and (iii). Each root m of $f(x)$ modulo p extends to at most p roots $m + kp$, where $k \in \{0, 1, \ldots, p-1\}$, modulo p^2. Furthermore, m will extend to exactly 1 root of $f(x)$ modulo p^2 unless m is a multiple root of $f(x)$ modulo p (cf. [7, pp. 63-69]). Thus, (iv) follows. From the above, if $\rho(p) < p$, then (v) is a consequence of (iii). Also, if $p \leq n$, then (v) is immediate since then $\rho(p^2) \leq p^2 \leq pn$. Now, suppose that $p > n$ and $\rho(p) = p$. Then $\rho(p^2) < p^2$ implies that $f(x) = pg(x)$ where $g(x)$ is a polynomial in $\mathbb{Z}[x]$ which is not identically 0 modulo p. By Lagrange's Theorem, we get that $g(x)$ has $\leq \deg g(x) = n$ roots modulo p. Each such root m of $g(x)$ modulo p corresponds to exactly p incongruent roots of $f(x)$ modulo p^2 since $f(m+kp) \equiv pg(m+kp) \equiv 0 \pmod{p^2}$ for each $k \in \{0, 1, \ldots, p-1\}$. Thus, (v) follows. Finally, we just note that the proof of (vi) is similar to the proof of (v).

Lemma 3. *For $B \geq e^e, f(x) \in \mathbb{Z}[x]$, and $z \leq \log\log B$, the number of positive integers $m \leq B$ for which $f(m)$ is not divisible by p^2 for each $p \leq z$ is equal to*

$$\prod_{p \leq z} \left(1 - \frac{\rho(p^2)}{p^2}\right) (B + O(\log B)).$$

In particular, there exists an absolute constant $C_1 > 0$ such that the number of positive integers $m \leq B$ for which $f(m)$ is squarefree is

$$\leq \prod_{p \leq z} \left(1 - \frac{\rho(p^2)}{p^2}\right) (B + C_1 \log B).$$

The proof of Lemma 3 is omitted. It is a direct application of the sieve of Eratosthenes. The main idea in the paper is to show that for most $f(x) \in S_n(N)$ the upper bound given above is very close to the actual number of integers $m \leq B$ for which $f(m)$ is squarefree. This is what is to be expected since the product above converges as z tends to infinity.

Lemma 4. *Let $x_j \in (0,1)$ for $j \in \{1, 2, \ldots, r\}$. Then*

$$\prod_{j=1}^{r} (1 - x_j) \geq 1 - \sum_{j=1}^{r} x_j.$$

The proof of Lemma 4 is easily done by induction since by the conditions on x_j,

$$\left(1 - \sum_{j=1}^{r-1} x_j\right) (1 - x_r) \geq 1 - \sum_{j=1}^{r} x_j.$$

Lemma 5. *As $f(x)$ ranges over all the incongruent polynomials of degree $\leq n$ modulo p^2, the average value of $\rho_f(p^2)$ is 1.*

We omit the proof of Lemma 5 as it follows in a fairly straight forward manner by using translation considerations to establish that each of $0, 1, \ldots, p^2 - 1$ have an equal probability of being attained as a value of $f(m) \pmod{p^2}$.

Our next goal is to show that for most $f(x) \in S_n(N)$, if

$$\prod_{p \leq z} \left(1 - \frac{\rho(p^2)}{p^2}\right) > 0,$$

then it is not too small. We formulate this in the following manner.

Lemma 6. *Let $\epsilon > 0$, and let N be sufficiently large (depending on n and ϵ). Let $z \leq \log\log N$. Then there exist positive numbers $n_0 = n_0(\epsilon)$ and $\epsilon' = \epsilon'(\epsilon, n)$ such that the* *number of* $f(x) \in S_n(N)$ *satisfying*

$$(i) \quad \prod_{p \le n^2+n_0} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) > 0 \quad \textit{and} \quad (ii) \quad \prod_{p \le z} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) < \epsilon'$$

is $\le \epsilon(2N)^{n+1}$.

Proof. Consider the $f(x) \in S_n(N)$ for which (i) holds (where n_0 as well as ϵ' are for the moment unspecified). Thus, $\rho(p^2) < p^2$ for each such $f(x)$ and each prime $p \le n^2 + n_0$. Hence,

$$\prod_{p \le n^2+n_0} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) \ge \prod_{p \le n^2+n_0} \left(1 - \frac{p^2-1}{p^2}\right) = \prod_{p \le n^2+n_0} \left(p^{-2}\right).$$

Now, consider any $f(x) \in S_n(N)$. We get from Lemma 2 (ii), (iii), and (iv) that for $n^2 + n_0 < p \le z$, either $\rho_f(p^2) \le n$ or $f(x)$ has a multiple root modulo p. Letting

$$c(n,z) = \prod_{n^2+n_0 < p \le z} \left(1 - \frac{n}{p^2}\right),$$

we see that $c(n,z)$ is greater than the product

$$c(n) = \prod_{p > n^2+n_0} \left(1 - \frac{n}{p^2}\right),$$

which is easily seen to converge to a positive quantity. Hence, for each $f(x) \in S_n(N)$,

$$\begin{aligned} \prod_{n^2+n_0 < p \le z} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) &\ge \prod_{n^2+n_0 < p \le z} \left(1 - \frac{n}{p^2}\right) \prod^*_{n^2+n_0 < p \le z} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) \\ &\ge c(n) \prod^*_{n^2+n_0 < p \le z} \left(1 - \frac{\rho_f(p^2)}{p^2}\right), \end{aligned}$$

where $\prod^*$ indicates that the product is over those primes p for which $f(x)$ has a multiple root modulo p. We now show that this latter product is not small for most polynomials $f(x) \in S_n(N)$.

Let $k = k(\epsilon)$ be a positive integer such that

$$\sum_{j=0}^{\infty} \left(\frac{7}{10}\right)^{2^j k} < \frac{\epsilon}{2e}.$$

Such a k exists since

$$\sum_{j=0}^{\infty} \left(\frac{7}{10}\right)^{2^j k} \leq \sum_{j=k}^{\infty} \left(\frac{7}{10}\right)^{j} = \frac{10}{3}\left(\frac{7}{10}\right)^{k}.$$

Define

$$t(j) = \left(n^2 + n_0\right)^{2^j} \quad \text{for} \quad j \in \{0, 1, \dots, s+1\},$$

where s is chosen so that $(n^2+n_0)^{2^s} < z \leq (n^2+n_0)^{2^{s+1}}$. Thus,

$$\prod_{n^2+n_0<p\leq z}^{*} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) \geq \prod_{j=0}^{s} \left(\prod_{t(j)<p\leq t(j+1)}^{*} \left(1 - \frac{\rho(p^2)}{p^2}\right)\right).$$

Let $T = T(n, N)$ be the set of $f(x) \in S_n(N)$ for which there is a $j \in \{0, 1, \dots, s\}$ such that $f(x)$ has a multiple root modulo p for $\geq 2^j k$ primes $p \in (t(j), t(j+1)]$. Also, we define $T' = T'(n, N)$ to be the set of $f(x) \in S_n(N)$ for which $\rho_f(p^2) = p^2$ for some prime $p \in (n^2 + n_0, z]$. We show that

$$|T \cup T'| \leq \epsilon\,(2N)^{n+1} \tag{4}$$

and then establish that $\prod_{p\leq z}\left(1 - \dfrac{\rho_f(p^2)}{p^2}\right) \geq \epsilon'$ for the remaining $f(x) \in S_n(N)$.

We deal with T' first. By Lemma 2 (vi), each $f(x) \in T'$ is such that $f(x) \equiv 0 \pmod{p^2}$ for some prime $p \in (n^2 + n_0, z]$. Note that the number of $f(x) \in S_n(N)$ such that $f(x) \equiv 0 \pmod{p^2}$ for a given prime p is

$$\left(\frac{2N}{p^2} + O(1)\right)^{n+1} = \left(\frac{2N}{p^2}\right)^{n+1} + O_n\left(N^n\right).$$

The choice of $z \le \log\log N$ easily implies that the total number of such $f(x) \in T'$ is

$$\begin{aligned}
&\le \sum_{n^2+n_0<p\le z} \left(\left(\frac{2N}{p^2}\right)^{n+1} + O_n\left(N^n\right) \right) \\
&\le \left(\sum_{p>n^2+n_0} \left(\frac{2N}{p^2}\right)^{n+1} \right) + O_n\left(N^n \log\log N\right) \\
&\le (2N)^{n+1} \left(\sum_{p>n_0} \frac{1}{p^2} \right) + O_n\left(N^n \log\log N\right).
\end{aligned}$$

For n_0 chosen sufficiently large (depending only on ϵ) we get that $|T'| \le (\epsilon/2)(2N)^{n+1}$.

We now turn to considering T. We begin by dividing up T into subsets T_j which are not necessarily disjoint. For each $j \in \{0, 1, \ldots, s\}$, we define T_j as the set of $f(x) \in S_n(N)$ such that $f(x)$ has a multiple root modulo p for $\ge 2^j k$ primes $p \in (t(j), t(j+1)]$. Fix j, and set $w = 2^j k$. Let $p_1, \ldots, p_w$ be w distinct primes in $(t(j), t(j+1)]$. Define $T_j\left(p_1, \ldots, p_w\right)$ to be the set of $f(x) \in T_j$ such that $f(x)$ has a multiple root modulo p_j for each $j \in \{1, \ldots, w\}$. Note that each $f(x) \in T_j$ belongs to some set $T_j\left(p_1, \ldots, p_w\right)$. The number of incongruent polynomials modulo a prime p of degree $\le n$ which have a multiple root modulo p is equal to the number of incongruent polynomials of the form $(x-a)^2 g(x)$ where $a \in \{0, 1, \ldots, p-1\}$ and $\deg g(x) \le n-2$. Thus, the number of such polynomials is $\le p^n$. Thus, the Chinese Remainder Theorem easily gives that the number of incongruent polynomials $f(x)$ modulo $p_1 \cdots p_w$ of degree $\le n$ such that $f(x)$ has a multiple root modulo p_j for each $j \in \{1, \ldots, w\}$ is $\le p_1^n \cdots p_w^n$. By dividing $T_j\left(p_1, \ldots, p_w\right)$ into these $\le p_1^n \cdots p_w^n$ congruence classes, we get that

$$\left|T_j\left(p_1, \ldots, p_w\right)\right| \le \left(\frac{2N+1}{p_1 \cdots p_w} + 1 \right)^{n+1} p_1^n \cdots p_w^n.$$

By the definition of s, we have that $\left(n^2+n_0\right)^{2^s} < z$, so that for n_0 sufficiently large, $w \le 2^s k < z$. Also, each $p_j \le t(s+1) = t(s)^2 \le z^2$ so that $p_1 \cdots p_w \le z^{2z}$. The choice

$z \le \log\log N$ gives that

$$p_1 \cdots p_w \le \frac{2N}{n+1} - 1,$$

for N sufficiently large (depending on n). Hence,

$$\begin{aligned} |T_j\left(p_1, \ldots, p_w\right)| &\le \left(\frac{2N+1}{p_1 \cdots p_w} + \frac{\frac{2N}{n+1} - 1}{p_1 \cdots p_w} \right)^{n+1} p_1^n \cdots p_w^n \\ &= \left(1 + \frac{1}{n+1}\right)^{n+1} \frac{(2N)^{n+1}}{p_1 \cdots p_w} < e \frac{(2N)^{n+1}}{p_1 \cdots p_w}. \end{aligned}$$

Since each polynomial in T_j belongs to some $T_j\left(p_1, \ldots, p_w\right)$ described above, we now get that

$$|T_j| \le e(2N)^{n+1} \left(\sum_{t(j) < p \le t(j+1)} \frac{1}{p} \right)^w \le e(2N)^{n+1} c^w,$$

where we can take c to be any constant $> \log 2$ provided n_0 is sufficiently large. Here, we have used that

$$\sum_{p \le y} \frac{1}{p} = \log\log y + A + o(1),$$

for some absolute constant A. We take $c = 7/10$.

We are now ready to complete our estimate for $|T|$. We get that

$$|T| \le \sum_{j=0}^{s} |T_j| \le e(2N)^{n+1} \sum_{j=0}^{\infty} \left(\frac{7}{10}\right)^{2^j k} < \frac{\epsilon}{2} \left(2N\right)^{n+1},$$

by our choice of k. The above estimates on $|T'|$ and $|T|$ easily imply (4).

We now consider $\prod^*_{n^2+n_0<p\le z} \left(1 - \frac{\rho_f(p^2)}{p^2}\right)$ where $f(x) \in S_n(N) - T - T'$. By Lemma 2 (v), we get that for each prime p in the range of the product above, $\rho(p^2) \le np$. Also, for each $j \in \{0, 1, \ldots, s\}$, there are fewer than $2^j k$ primes $p \in (t(j), t(j+1)]$ for which $f(x)$ has a multiple root modulo p. Hence,

$$\prod^*_{t(j)<p\le t(j+1)} \left(1 - \frac{\rho_f(p^2)}{p^2}\right) \ge \prod^*_{t(j)<p\le t(j+1)} \left(1 - \frac{n}{p}\right) \ge \left(1 - \frac{n}{t(j)}\right)^{2^j k}.$$

Thus, using Lemma 4,

$$\prod_{n^2+n_0<p\le z}^{*} \left(1-\frac{\rho_f(p^2)}{p^2}\right) \ge \prod_{j=0}^{s}\left(1-\frac{n}{t(j)}\right)^{2^j k}$$
$$\ge 1-\sum_{j=0}^{s}\frac{2^j kn}{t(j)} = 1-\sum_{j=0}^{s}\frac{2^j kn}{(n^2+n_0)^{2^j}} > \frac{1}{2},$$

provided n_0 is sufficiently large. We note that we can choose n_0 so that everything above holds and so that n_0 only depends on ϵ (and not on n unless, of course, ϵ depends on n). For example, by checking the cases $n \le \sqrt{n_0}$ and $n > \sqrt{n_0}$ separately, the last inequality above is easily seen to hold provided that

$$\sum_{j=0}^{\infty}\frac{2^j k}{n_0^{2^j-(1/2)}} < \frac{1}{2},$$

which, since k only depended on ϵ, gives a lower bound on n_0 depending only on ϵ.

Combining the above, we get that for $f(x) \in S_n(N) - T - T'$ and $f(x)$ satisfying (i),

$$\prod_{p\le z}\left(1-\frac{\rho(p^2)}{p^2}\right) \ge \frac{c(n)}{2}\left(\prod_{p\le n^2+n_0} p^{-2}\right).$$

Thus, the lemma follows by letting ϵ' be the right-hand side above.

Lemma 7. *Let $\epsilon > 0$, and let N be sufficiently large (depending on n and ϵ). Let $z \in [2, \log\log N]$. Then*

$$\sum_{f(x)\in S_n(N)}\left(\prod_{p\le z}\left(1-\frac{\rho_f(p^2)}{p^2}\right)\right) = \left(\prod_{p\le z}\left(1-\frac{1}{p^2}\right)\right)(2N)^{n+1} + O_n\left(N^{n+\epsilon}\right). \tag{5}$$

Proof. For each $p \le z$, consider the p^{2n+2} incongruent polynomials modulo p^2 of degree $\le n$, and let $w_1(p), \dots, w_r(p)$, where $r = r(p) = p^{2n+2}$, denote some ordering of the values of $\rho_f(p^2)$ as $f(x)$ ranges over these polynomials. Let $p_1, \dots, p_t$ represent the $t = \pi(z)$

primes $\leq z$, and let $f_1(x), \ldots, f_t(x)$ denote arbitrary polynomials with integral coefficients. Then the Chinese Remainder Theorem implies that the number of $f(x) \in S_n(N)$ such that $f(x) \equiv f_j(x) \pmod{p_j^2}$ for every $j \in \{1, \ldots, t\}$ is

$$\left(\frac{2[N]+1}{p_1^2 \cdots p_t^2} + O(1)\right)^{n+1} = \left(\frac{2N}{p_1^2 \cdots p_t^2}\right)^{n+1} + O_n\left(\left(\frac{2N}{p_1^2 \cdots p_t^2}\right)^n\right),$$

where we have used that since $z \leq \log\log N$,

$$p_1^2 \cdots p_t^2 \leq (\log\log N)^{2\log\log N} < N^{\epsilon'}, \tag{6}$$

where $\epsilon' \in (0,1)$ and N is sufficiently large (depending on ϵ'). For later purposes, we fix $\epsilon' = \min\{1/2, \epsilon\}$. If w_j' denotes the number of incongruent roots of $f_j(x)$ modulo p_j^2, then the contribution of the $f(x) \equiv f_j(x) \pmod{p_j^2}$ (for all $j \in \{1, \ldots, t\}$) on the left-hand side of (5) is

$$\prod_{j=1}^{t}\left(1 - \frac{w_j'}{p_j^2}\right)\left(\left(\frac{2N}{p_1^2 \cdots p_t^2}\right)^{n+1} + O_n\left(\left(\frac{2N}{p_1^2 \cdots p_t^2}\right)^n\right)\right).$$

Hence, summing over all $f(x) \in S_n(N)$, we get that

$$\sum_{f(x)\in S_n(N)} \prod_{p\leq z}\left(1 - \frac{\rho_f(p^2)}{p^2}\right)$$

$$= \prod_{p\leq z}\left(\left(1 - \frac{w_1(p)}{p^2}\right) + \cdots + \left(1 - \frac{w_r(p)}{p^2}\right)\right)\left(\left(\frac{2N}{p_1^2 \cdots p_t^2}\right)^{n+1} + O_n\left(\left(\frac{2N}{p_1^2 \cdots p_t^2}\right)^n\right)\right).$$

Recalling the definition of $w_j(p)$ and Lemma 5, we get that

$$\prod_{p\leq z}\left(\sum_{j=1}^{r(p)}\left(1 - \frac{w_j(p)}{p^2}\right)\right) = \prod_{p\leq z}\left(r(p) - \frac{r(p)}{p^2}\right) = \left(\prod_{p\leq z} p^{2n+2}\right)\prod_{p\leq z}\left(1 - \frac{1}{p^2}\right).$$

Thus,

$$\sum_{f(x)\in S_n(N)} \prod_{p\leq z}\left(1 - \frac{\rho_f(p^2)}{p^2}\right) = \prod_{p\leq z}\left(1 - \frac{1}{p^2}\right)\left((2N)^{n+1} + O_n\left((2N)^n \prod_{p\leq z} p^2\right)\right).$$

Recalling our choice of $\epsilon' = \min\{1/2, \epsilon\}$ in (6), we get the desired result.

3. The Main Theorems

We are now ready to prove Theorems 1 and 2 of the introduction. As mentioned there, we will actually be able to prove slightly stronger results.

Theorem 3. *Let $n \in \mathbb{Z}^+ \cup \{0\}$, and let $B(N)$ be a function which increases to infinity with N. Then the proportion of polynomials $f(x) \in S_n(N)$ with N_f squarefree which satisfy that $f(m)$ is squarefree for some integer $m \in [1, B]$ tends to 1 as N tends to infinity.*

Theorem 4. *Let $n \in \mathbb{Z}^+ \cup \{0\}$, and let $B(N)$ be a function which increases to infinity with N. Then the proportion of polynomials $f(x) \in S_n(N)$ which satisfy that $f(m)/N_f$ is squarefree for some integer $m \in [1, B]$ tends to 1 as N tends to infinity.*

Proof of Theorem 3. We suppose, as we may, that $B(N) = o(N)$ and that N is sufficiently large (depending on ϵ given below and n). Recall the discussion after Lemma 1 and, in particular, that there is a positive proportion of $f(x) \in S_n(N)$ for which N_f is squarefree. Alternatively, one may deduce that N_f is squarefree for a positive proportion of the $f(x) \in S_n(N)$ as a consequence of Theorem 1 in [3], which stated that for a positive proportion of the $f(x) \in S_n(N)$, there is an integer m for which $f(m)$ is prime. Let $\epsilon > 0$. To obtain Theorem 3, we need only prove that if N is sufficiently large, there are $\leq \epsilon(2N)^{n+1}$ polynomials $f(x) \in S_n(N)$ with N_f squarefree and such that $f(m)$ is nonsquarefree for all integers $m \in [1, B]$. In fact, for later purposes, we prove something stronger. Using the notation of Lemma 6 with $n_0 = n_0(\epsilon/2)$, we prove that the set T of $f(x) \in S_n(N)$ such that (i) $\gcd\left(N_f, \prod_{p \leq n^2+n_0} p^2\right)$ is squarefree and (ii) $f(m)$ is nonsquarefree for every integer $m \in [1, B]$ satisfies $|T| \leq \epsilon(2N)^{n+1}$ (provided N is sufficiently large). Assume that

$|T| > \epsilon(2N)^{n+1}$. Let $z = \log\log B$. For each $f(x) \in S_n(N)$, we denote $W(f(x))$ as the number of integers $m \in [1, B]$ such that $f(m)$ is squarefree. Then Lemma 3 implies that

$$W(f(x)) = \prod_{p \le z} \left(1 - \frac{\rho(p^2)}{p^2}\right) B + E(f(x)),$$

where

$$E(f(x)) \le C_1 \prod_{p \le z} \left(1 - \frac{\rho(p^2)}{p^2}\right) \log B.$$

Thus, using Lemma 7, we get that

$$\begin{aligned} \sum_{f(x) \in S_n(N)} W(f(x)) &= \sum_{f(x) \in S_n(N)} \left(\prod_{p \le z} \left(1 - \frac{\rho(p^2)}{p^2}\right) B + E(f(x)) \right) \\ &= \prod_{p \le z} \left(1 - \frac{1}{p^2}\right) (2N)^{n+1} B + E_1, \end{aligned} \tag{7}$$

with

$$E_1 = \sum_{f(x) \in S_n(N)} E(f(x)) + O_n\left(N^{n+\frac{1}{2}} B\right) \le C_2 \left(N^{n+1} \log B + N^{n+\frac{1}{2}} B\right),$$

where $C_2 = C_2(n)$ and we note that E_1 may be negative (so that, in particular, we claim no bound on $|E_1|$ at this point). Note that

$$\prod_{p \le z} \left(1 - \frac{1}{p^2}\right) > \prod_{p} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2}.$$

Recalling that $z = \log\log B(N)$, we get that since N and, hence, $B(N)$ are sufficiently large,

$$\frac{6}{\pi^2} < \prod_{p \le z} \left(1 - \frac{1}{p^2}\right) < \frac{6}{\pi^2} + \frac{\epsilon'}{2},$$

where $\epsilon' > 0$ is arbitrarily small and possibly depends on ϵ and n. Thus,

$$\sum_{f(x) \in S_n(N)} W(f(x)) = \frac{6}{\pi^2} (2N)^{n+1} B + E_2,$$

where

$$E_2 \le \epsilon'(2N)^{n+1}B.$$

On the other hand, Lemma 1 gives us that

$$\sum_{f(x)\in S_n(N)} W(f(x)) = \frac{6}{\pi^2}(2N)^{n+1}B + E_3,$$

where

$$|E_3| \le \epsilon'(2N)^{n+1}B.$$

Thus, in fact,

$$|E_2| = |E_3| \le \epsilon'(2N)^{n+1}B.$$

Recalling how E_2 was obtained, we now get that

$$|E_1| \le 2\epsilon'(2N)^{n+1}B.$$

The importance of this last inequality is that, unlike with the previous inequality on E_1, we now are supplied with a lower bound on E_1. More specifically, $E_1 \ge -2\epsilon'(2N)^{n+1}B$.

Recalling the definitions of T and $E(f(x))$, we get that

$$E(f(x)) = -\prod_{p\le z}\left(1 - \frac{\rho_f(p^2)}{p^2}\right) B \quad \text{for all } f(x) \in T.$$

Thus,

$$\sum_{f(x)\in T} E\left(f(x)\right) = -\sum_{f(x)\in T}\prod_{p\le z}\left(1 - \frac{\rho_f(p^2)}{p^2}\right) B.$$

The definition of T easily implies that for each prime $p \le n^2 + n_0$, $\rho_f(p^2) < p^2$ for all $f(x) \in T$. Thus, by Lemma 6, there exists an ϵ'' such that

$$\prod_{p\le z}\left(1 - \frac{\rho_f(p^2)}{p^2}\right) \ge \epsilon'' \tag{8}$$

for all but at most $(\epsilon/2)(2N)^{n+1}$ polynomials $f(x) \in T$. Since by assumption $|T| > \epsilon(2N)^{n+1}$, there are $\geq (\epsilon/2)(2N)^{n+1}$ polynomials $f(x) \in T$ for which (8) holds. Hence,

$$\sum_{f(x)\in T} E\left(f(x)\right) \leq -\frac{\epsilon}{2}\epsilon''\left(2N\right)^{n+1} B.$$

On the other hand,

$$\begin{aligned}\sum_{\substack{f(x)\in S_n(N)\\ E(f(x))>0}} E\left(f(x)\right) &\leq C_1 \sum_{\substack{f(x)\in S_n(N)\\ E(f(x))>0}} \prod_{p\leq z}\left(1-\frac{\rho_f(p^2)}{p^2}\right)\log B\\ &\leq C_1|S_n(N)|\log B \leq C_1(2N)^{n+1}\log B + O_n\left((2N)^n\log B\right).\end{aligned}$$

Thus, recalling the definition of E_1,

$$E_1 \leq -\frac{\epsilon}{2}\epsilon''\left(2N\right)^{n+1} B + O\left(\left(2N\right)^{n+1}\log B\right) + O_n\left(N^{n+\frac{1}{2}}B\right).$$

We are still free to choose $\epsilon' > 0$. We take $\epsilon' = (\epsilon\epsilon'')/5$. Then the above contradicts that

$$|E_1| \leq 2\epsilon'(2N)^{n+1}B = \frac{2}{5}\epsilon\epsilon''(2N)^{n+1}B,$$

completing the proof.

Proof of Theorem 4. For $n = 0$, the theorem is clear, so we only consider $n \geq 1$. Let $\epsilon \in (0,1)$, and let N be sufficiently large (depending on n and ϵ). Assume that there exists $\geq \epsilon(2N)^{n+1}$ polynomials $f(x) \in S_n(N)$ such that $f(m)/N_f$ is nonsquarefree for every $m \in [1,B]$. Let T_1 denote the set of such polynomials. By the proof of Theorem 3 and the notation of Lemma 6, the number $n_0 = n_0(\epsilon/6)$ is such that $|T_2| \leq (\epsilon/3)(2N)^{n+1}$ where T_2 denotes the set of $f(x) \in S_n(N)$ for which (i) $\gcd\left(N_f, \prod_{p\leq n^2+n_0} p^2\right)$ is squarefree and (ii) $f(m)$ is nonsquarefree for each integer $m \in [1,B]$. Since increasing the size of n_0 will only decrease the number of $f(x)$ for which (i) and (ii) hold, we may assume that $n_0 \geq 7$. We do this so that later we may use that

$$\sum_{j \geq n_0} \frac{1}{j^2} < \frac{4}{25}.$$

Let $T_3 = T_1 - T_2$ so that T_3 consists of $\geq (2\epsilon/3)(2N)^{n+1}$ polynomials $f(x) \in T_1$ for which N_f is divisible by p^2 for some $p \leq n^2 + n_0$. Define

$$M = M(n, \epsilon) = \left(\frac{4(n^2 + n_0)}{\epsilon} \right)^{2(n^2 + n_0)}$$

and

$$B' = B'(N) = \frac{1}{M} B \left(\frac{N}{(2M)^n} \right) - 1.$$

Using the notation of Lemma 6, define

$$n_1 = n_1(\epsilon) = n_0 \left(\frac{\epsilon}{4(2M)^{n^2+n+2}} \right).$$

The proof of Theorem 3 implies that there are

$$\leq \frac{\epsilon}{2(2M)^{n^2+n+2}} \left| S_n\left((2M)^n N\right) \right|$$

polynomials $g(x) \in S_n\left((2M)^n N\right)$ for which (i$'$) $\gcd\left(N_g, \prod_{p \leq n^2+n_1} p^2\right)$ is squarefree and (ii$'$) $g(m)$ is nonsquarefree for each integer $m \in [1, B'((2M)^n N)]$. We will obtain a contradiction by showing that there are more than $(\epsilon/(2(2M)^{n^2+n+2})) \left| S_n\left((2M)^n N\right) \right|$ such $g(x)$ (with even $\gcd\left(N_g, \prod_{p \leq n^2+n_1} p\right) = 1$).

We begin by restricting our attention to $p \leq n^2 + n_0$. For each such p, let $k = k(p) = k(p, n, \epsilon)$ be the minimal positive integer such that

$$p^{k+1} \geq \frac{4(n^2 + n_0)}{\epsilon}.$$

Note that $\epsilon \in (0,1)$ implies that the right-hand side above is $> n^2 + n_0$ so that $p^k < 4(n^2+n_0)/\epsilon$. Let T_4 be the set of polynomials $f(x) \in T_3$ such that p^{k+1} divides N_f for at least one prime $p \le n^2 + n_0$. The constant term of each such $f(x)$, being $f(0)$, must be divisible by p^{k+1}. Thus, the number of $f(x) \in T_3$ for which p^{k+1} divides N_f for a given prime $p \le n^2 + n_0$ is

$$\le (2N+1)^n \left(\frac{2N+1}{p^{k+1}} + 1 \right) \le \frac{\epsilon}{4(n^2+n_0)} (2N+1)^{n+1} + (2N+1)^n \le \frac{\epsilon}{3(n^2+n_0)} (2N)^{n+1}.$$

Hence,

$$|T_4| \le \pi\left(n^2+n_0\right) \frac{\epsilon}{3(n^2+n_0)} (2N)^{n+1} \le \frac{\epsilon}{3} (2N)^{n+1}.$$

Define $T_5 = T_3 - T_4$. Thus, $|T_5| \ge (\epsilon/3)(2N)^{n+1}$.

For $f(x) \in T_5$, define

$$M_f = \prod_{r=1}^{\infty} \Big(\prod_{\substack{p \le n^2+n_0 \\ p^r | N_f}} p \Big) \quad \text{and} \quad P_f = M_f \prod_{p | M_f} p.$$

Note that $N_f = M_f Q_f$ where $\gcd(Q_f, \prod_{p \le n^2+n_0} p) = 1$ and that $P_f \le M_f^2$. By the definition of T_5, for each prime $p \le n^2 + n_0$ and each $f(x) \in T_5$, we have that p^{k+1} does not divide M_f. This easily implies that each of M_f and P_f is $\le M(n, \epsilon)$ for every $f(x) \in T_5$.

We now define a function $\alpha : T_5 \to S_n\left((2M)^n N\right)$ as follows. For each $f(x) \in T_5$ and each prime $p \le n^2 + n_0$, define $r = r(p, f(x))$ to be the nonnegative integer satisfying that p^r divides M_f and p^{r+1} does not divide M_f. In particular, p^{r+1} does not divide N_f so that there is an integer $a = a(p, f(x)) \in [1, p^{r+1}]$ such that $f(a) \not\equiv 0 \pmod{p^{r+1}}$. Necessarily, $f(a) \equiv 0 \pmod{p^r}$. By the Chinese Remainder Theorem, there is a minimal positive integer $b = b(f(x))$ such that $f(b)$ is divisible by M_f and, for each prime $p \le n^2 + n_0$, $f(b)$

is not divisible by pM_f. Furthermore, since $f(x) \in T_5$,

$$1 \leq b \leq \prod_{p \leq n^2+n_0} p^{r(p,f(x))+1} \leq \prod_{p \leq n^2+n_0} p^{k(p)+1} \leq \left(\prod_{p \leq n^2+n_0} p^{k(p)} \right)^2 \leq M(n,\epsilon).$$

Define

$$g(x) = f\left(P_f x + b\right)/M_f.$$

Each coefficient of $f(P_f x + b)$ is divisible by M_f, except possibly the constant term $f(b)$. But $f(b) \equiv 0 \pmod{M_f}$, and thus $g(x) \in \mathbb{Z}[x]$. Furthermore, it is easily verified that each coefficient of $g(x)$ has absolute value $\leq N(2M)^n$. We define $\alpha(f(x)) = g(x)$.

Note that M_f and P_f are uniquely determined by one another; in other words, given M_f, one can determine P_f, and given P_f, one can determine M_f. Since there exist $\leq M(n,\epsilon)$ possible values for P_f and $\leq M(n,\epsilon)$ possible values for b, it is easy to see that for each $g(x)$ in the image of α, there are at most M^2 possible $f(x) \in T_5$ such that $\alpha(f(x)) = g(x)$. In particular, since N is sufficiently large,

$$\begin{aligned} |\alpha(T_5)| &\geq \frac{1}{M^2}\,|T_5| \geq \frac{\epsilon}{3M^2}(2N)^{n+1} \\ &= \frac{\epsilon}{3(2^{n^2+n})(M^{n^2+n+2})}\left(2(2M)^n N\right)^{n+1} \geq \frac{\epsilon}{(2M)^{n^2+n+2}}\left|S_n\left((2M)^n N\right)\right|. \end{aligned}$$

On the other hand, one can check that the definitions of b and $g(x)$ above imply that for $g(x) \in \alpha(T_5)$,

$$\gcd\left(N_g, \prod_{p \leq n^2+n_0} p\right) = 1.$$

Recall that by assumption, each $f(x) \in T_5 \subseteq T_1$ is such that $f(m)/N_f$ is nonsquarefree for each integer $m \in [1,B]$. Note that $B'\left((2M)^n N\right) = (B(N)/M) - 1$. Now, if $m \in [1, (B(N)/M) - 1]$ and b is as in the definition of α, then $P_f m + b$ is a positive integer

$\leq B(N)$. Also, the definition of M_f implies that M_f divides N_f. We now get that if $f(x) \in T_5$ and $g(x) = \alpha(f(x))$, then $g(m) = f(P_f m + b)/M_f$ is nonsquarefree for each integer $m \in [1, B'((2M)^n N)]$.

Thus far, we have shown that there are

$$\geq \frac{\epsilon}{(2M)^{n^2+n+2}} \left| S_n\left((2M)^n N\right) \right|$$

polynomials $g(x) \in S_n((2M)^n N)$ such that $\gcd(N_g, \prod_{p \leq n^2+n_0} p) = 1$ and (ii$'$) holds. Let T_1' denote the set of all such $g(x)$. Let T_2' denote the set of all $g(x) \in T_1'$ which also satisfy that $\gcd(N_g, \prod_{p \leq n^2+n_1} p) = 1$. It now suffices to prove that

$$|T_2'| > \frac{\epsilon}{2(2M)^{n^2+n+2}} \left| S_n\left((2M)^n N\right) \right|.$$

For $p \in (n^2 + n_0, n^2 + n_1]$, define $k' = k'(p) = k'(p, n, \epsilon)$ as the minimal positive integer such that

$$p^{k'+1} \geq \frac{4(n^2+n_1)(2M)^{n^2}+n+2}{\epsilon}.$$

Then following the argument which led to an estimate of $|T_5|$, we get that there are

$$\geq \frac{2\epsilon}{3(2M)^{n^2+n+2}} \left| S_n\left((2M)^n N\right) \right|$$

polynomials $g(x) \in T_1'$ such that if $p \in (n^2 + n_0, n^2 + n_1]$ and p^r divides N_g, then $r \leq k'(p)$. Let T_3' denote the set of all such $g(x)$. Note that $T_2' \subseteq T_3'$. In fact, our goal now is to show that most of the polynomials in T_3' are in T_2'.

For each $g(x) \in T_3'$, let

$$M_g' = \prod_{r=1}^{\infty} \Bigg(\prod_{\substack{n^2+n_0 < p \leq n^2+n_1 \\ p \mid N_g}} p \Bigg) = \prod_{r=1}^{\infty} \Bigg(\prod_{\substack{p \leq n^2+n_1 \\ p \mid N_g}} p \Bigg).$$

Note that with n and ϵ fixed, so are M and $k'(p)$ for each $p \in (n^2 + n_0, n^2 + n_1]$. Thus, M'_g takes on a finite number of distinct values. Let M' be one such value of M'_g. By the definition of n_1 and the proof of Theorem 3, we get that there are

$$\leq \frac{\epsilon}{2(2M)^{n^2+n+2}} \left| S_n\left(\frac{(2M)^n N}{M'}\right)\right| \leq \frac{\epsilon}{(2M)^{n^2+n+2}(M')^{n+1}} \left|S_n\left((2M)^n N\right)\right|$$

polynomials $h(x) \in S_n((2M)^n N/M')$ such that $\gcd\left(N_h, \prod_{p \leq n^2+n_1} p\right) = 1$ and $h(m)$ is nonsquarefree for each positive integer $m \leq B'((2M)^n N/M') \leq B'((2M)^n N)$. We note that we want the above to hold for every choice of M', and we can do this since N is sufficiently large and there are only finitely many values of M'. Since every prime factor of M' is $> n^2+n_0 > n$, we get by Lemma 2 (vi) that each $g(x)$ with $M'_g = M'$ satisfies $g(x) \equiv 0 \pmod{M'}$. But this means that $g(x) = M'h(x)$ for some $h(x) \in S_n((2M)^n N/M')$. The definition of $M' = M'_g$ implies that every such $h(x)$ satisfies $\gcd\left(N_h, \prod_{p \leq n^2+n_1} p\right) = 1$. Also, using that $\gcd\left(P_f, \prod_{n^2+n_0 < p \leq n^2+n_1} p\right) = 1$, one can show from the definition of M_f and M'_g that $M_f M'_g$ divides N_f where $\alpha(f(x)) = g(x)$. One gets that for $h(x)$ as above, $h(m) = f(P_f m + b)/(M_f M'_g)$ is nonsquarefree for each positive integer $m \leq B'((2M)^n N/M')$. We now get that

$$\begin{aligned} |T'_3 - T'_2| &\leq {\sum}^* \frac{\epsilon}{(2M)^{n^2+n+2}(M')^{n+1}} \left|S_n\left((2M)^n N\right)\right| \\ &= \frac{\epsilon}{(2M)^{n^2+n+2}} \left({\sum}^* (M')^{-n-1}\right) \left|S_n\left((2M)^n N\right)\right|, \end{aligned}$$

where ${\sum}^*$ denotes that the sum is over those values of M' which are strictly greater than 1. Since each such M' is divisible by some prime $p > n^2 + n_0$, we get that each such M' is $\geq n^2 + n_0 \geq n_0$. Thus, since $n \geq 1$,

$${\sum}^* (M')^{-n-1} \leq \sum_{j \geq n_0} \frac{1}{j^2},$$

which, by our choice of $n_0 \geq 7$, is $< 4/25$. Hence,

$$|T_3' - T_2'| \leq \frac{4\epsilon}{25(2M)^{n^2+n+2}} \left| S_n\left((2M)^n N\right)\right|,$$

so that

$$|T_2'| \geq |T_3'| - |T_3' - T_2'| \geq \frac{38\epsilon}{75(2M)^{n^2+n+2}} \left| S_n\left((2M)^n N\right)\right|,$$

which completes the proof.

Before concluding the paper, we note that Theorem 4 and, hence, Theorem 2 can be improved slightly. For $f(x) \in \mathbb{Z}[x]$, write $N_f = U_f V_f$, where V_f is the largest squarefree factor of N_f. Then one may replace the role of $f(m)/N_f$ in the statement of Theorem 4 with $f(m)/U_f$. The proof is essentially the same with the following minor changes. One defines $\alpha(f(x)) = g(x)$ where now $g(x) = f(P_f x + b)/\gcd(M_f, U_f)$. Then $g(x) \in \alpha(T_5)$ implies that $\gcd(N_g, \prod_{p \leq n^2+n_0} p^2)$ is squarefree. One considers, instead of T_2', the set T_2'' of $g(x) \in S_n((2M)^n N)$ such that (i$'$) and (ii$'$) hold. Since $T_2' \subseteq T_2''$, the lower bound for $|T_2'|$ obtained in the proof of Theorem 4 is a lower bound for $|T_2''|$, and the desired improvement follows.

References

1. L. E. Dickson, *History of the Theory of Numbers, Vol. I*, Chelsea, New York, 1971.

2. P. Erdős, *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416–425.

3. M. Filaseta, *Prime values of irreducible polynomials*, Acta Arith. **50** (1988), 133–145.

4. P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math., Vol. 24, Amer. Math. Soc. (1973), 91–101.

5. C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26.

6. M. Huxley and M. Nair, *Power free values of polynomials, III*, Proc. London Math. Soc. **41** (1980), 66–82.

7. W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, Reading, Massachusetts, 1977.

8. T. Nagel, *Zur Arithmetik der Polynome*, Abhandl. Math. Sem. Hamburg **1** (1922), 179–194.

9. M. Nair, *Power free values of polynomials*, Mathematika **23** (1976), 159–183.

10. M. Nair, *Power free values of polynomials, II*, Proc. London Math. Soc. **38** (1979), 353–368.

11. G. Pólya and G. Szegő, *Problems and Theorems in Analysis II*, Springer-Verlag, New York, 1976.

12. B. L. van der Waerden, *Die Seltenheit der Reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. **43** (1936), 133–147.

13. B. L. van der Waerden, *Algebra I*, Springer-Verlag, Berlin, 1971.

14. B. L. van der Waerden, *Algebra*, Vol. I, 7th edition, translated by F. Blum and J. R. Schulenberger, Frederick Ungar Publ. Co., New York, 1970.