ACTA ARITHMETICA
LX.3 (1992)

# Squarefree values of polynomials

by

Michael Filaseta* (Columbia, S.C.)

**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

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

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] 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 $k \ge (\sqrt{2} - \frac{1}{2})n$. 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 $\ge 4$ 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

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

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

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

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 nonnegative 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

$m \le \psi(\max_{0\le j\le n}\{|a_j|\})$, where $\psi(x)$ is any function which tends to infinity with $x$.

**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 $\varepsilon$ may depend on $n$. We will, however, stress when such a dependence is necessary. We reserve $p$ for denoting primes.

LEMMA 1. *Let $\varepsilon > 0$, and let $B = B(N)$ be a function which increases to infinity with $N$. Suppose further that $B(N) = o(N)$. Then there exists $N_0 = N_0(n, \varepsilon, B)$ such that if $N \ge N_0$, 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*

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

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

$$m^{n-1} + \ldots + m + 1 = \frac{m^n - 1}{m-1} < \varepsilon' m^n .$$

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

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

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

$$|d - (a_{n-1}m^{n-1} + \ldots + a_1 m + a_0)| \le Nm^n . \tag{3}$$

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

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

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

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

The above steps may be reversed. More specifically, given $m$ and $d$ as above, we must have that $a_0, \ldots, a_{n-1}$ 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 $(2N/m)^n + O_n(N^{n-1}/m^{n-1})$ 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

$$\begin{aligned}
|S_1| &= \sum_{m_0 \le m \le B} \left( \left( \frac{2N}{m} \right)^n \frac{6}{\pi^2} (1-\varepsilon')(2N) m^n + O_n(N^n m) + O(N^{n+1/2}) \right) \\
&= (6/\pi^2)(1-\varepsilon')(2N)^{n+1} B + O_n(N^{n+1} m_0) \\
&\quad + O_n(N^n B^2) + O(N^{n+1/2} B)\,, \\
|S_2| &= \left( 1 - \frac{6}{\pi^2} \right) (1-\varepsilon')(2N)^{n+1} B + O_n(N^{n+1} m_0) \\
&\quad + O_n(N^n B^2) + O(N^{n+1/2} B)\,,
\end{aligned}$$

and

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

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 one is

$$\begin{aligned}
|S_1| + |S_3| < (6/\pi^2)(1+\varepsilon')(2N)^{n+1} B + O_n(N^{n+1} m_0) \\
+ O_n(N^n B^2) + O(N^{n+1/2} B)\,.
\end{aligned}$$

Thus, taking $\varepsilon' = \varepsilon/2$ 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 $\sim (6/\pi^2)B$ 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

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

for some polynomials $g(x)$ and $h(x) \in \mathbb{Z}[x]$. Thus, if $p \ge n+1$, then $f(x) \equiv 0$ is the only such $f(x)$ modulo $p^2$; if $(n+1)/2 \le p \le n$, then there are exactly $p^{n-p+1}$ incongruent such $f(x)$ modulo $p^2$; and if $p \le n/2$, 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

$$1-\prod_{p\le n/2}\left(1-\frac{1}{p^{3p}}\right)\prod_{(n+1)/2\le p\le n}\left(1-\frac{1}{p^{n+1+p}}\right)\prod_{p\ge n+1}\left(1-\frac{1}{p^{2n+2}}\right)$$
$$\ge 1-\prod_{p}\left(1-\frac{1}{p^{3p}}\right)=0.015675\ldots$$

Thus, the polynomials $f(x)\in S_n(N)$ which take on at least one squarefree value as $x$ ranges over the positive integers $\le B$ on average take on $\ge (6/\pi^2)B$ $(1.0159\ldots)$ 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 $l\in\mathbb{Z}$, we define $\varrho(l)=\varrho_f(l)$ to be the number of incongruent solutions to $f(x)\equiv 0\ (\mathrm{mod}\, l)$. The next lemma gives some basic properties of $\varrho(l)$.

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

(i) *$\varrho(l)$ is multiplicative (i.e., if $l_1$ and $l_2$ are relatively prime integers, then $\varrho(l_1l_2)=\varrho(l_1)\varrho(l_2)$),*

(ii) *if $\varrho(p)=p$, then either $p\le n$ or $f(x)\equiv 0\ (\mathrm{mod}\, p)$,*

(iii) *if $\varrho(p)<p$, then $\varrho(p)\le n$,*

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

(v) *if $\varrho(p^2)<p^2$, then $\varrho(p^2)\le pn$,*

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

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 $f(x)\equiv 0\ (\mathrm{mod}\, p)$ is $\le n$ 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 $\varrho(p)<p$, then (v) is a consequence of (iii). Also, if $p\le n$, then (v) is immediate since then $\varrho(p^2)\le p^2\le pn$. Now, suppose that $p>n$ and $\varrho(p)=p$. Then $\varrho(p^2)<p^2$ 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, $g(x)$ has $\le \deg g(x)=n$ 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 $f(m+kp)\equiv pg(m+kp)\equiv 0\ (\mathrm{mod}\, p^2)$ 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 $B \ge e^e, f(x) \in \mathbb{Z}[x]$, and $z \le \log\log B$, the number of positive integers $m \le B$ for which $f(m)$ is not divisible by $p^2$ for each $p \le z$ is equal to*

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

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

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

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 $m \le B$ 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*

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

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

$$\Big(1 - \sum_{j=1}^{r-1} x_j\Big)(1 - x_r) \ge 1 - \sum_{j=1}^{r} x_j.$$

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

We omit the proof of Lemma 5 as it follows in a fairly straightforward 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

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

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

Lemma 6. *Let $\varepsilon > 0$, and let $N$ be sufficiently large (depending on $n$ and $\varepsilon$). Let $z \le \log\log N$. Then there exist positive numbers $n_0 = n_0(\varepsilon)$ and*

$\varepsilon' = \varepsilon'(\varepsilon, n)$ *such that the number of* $f(x) \in S_n(N)$ *satisfying*

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

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

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

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

Now, consider any $f(x) \in S_n(N)$. We find from Lemma 2(ii), (iii), and (iv) that for $n^2 + n_0 < p \le z$, either $\varrho_f(p^2) \le n$ 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 $f(x) \in S_n(N)$,

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

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

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

Such a $k$ exists since

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

Define

$$t(j)=(n^2+n_0)^{2^j} \qquad \text{for } j\in\{0,1,\ldots,s+1\}\,,$$

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

$$\prod_{n^2+n_0<p\le z}^{*}\left(1-\frac{\varrho_f(p^2)}{p^2}\right) \ge \prod_{j=0}^{s}\left(\prod_{t(j)<p\le t(j+1)}^{*}\left(1-\frac{\varrho(p^2)}{p^2}\right)\right).$$

Let $T=T(n,N)$ be the set of $f(x)\in S_n(N)$ for which there is a $j\in\{0,1,\ldots,s\}$ such that $f(x)$ has a multiple root modulo $p$ for $\ge 2^j k$ 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 $\varrho_f(p^2)=p^2$ for some prime $p\in(n^2+n_0,z]$. We show that

$$|T\cup T'| \le \varepsilon(2N)^{n+1} \tag{4}$$

and then establish that $\prod_{p\le z}(1-\varrho_f(p^2)/p^2)\ge \varepsilon'$ 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

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

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

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

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

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 $T_j(p_1,\ldots,p_w)$ 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 $T_j(p_1,\ldots,p_w)$. 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 $\le p^n$. Therefore, the Chinese Remainder Theorem easily yields that the number of incongruent polynomials $f(x)$ modulo $p_1 \ldots p_w$ of degree $\le n$ such that $f(x)$ has a multiple root modulo $p_j$ for each $j \in \{1,\ldots,w\}$ is $\le p_1^n \ldots p_w^n$. By dividing $T_j(p_1,\ldots,p_w)$ into these $\le p_1^n \ldots p_w^n$ congruence classes, we get

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

By the definition of $s$ we have $(n^2+n_0)^{2^s} < z$, 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 $p_1 \ldots p_w \le z^{2z}$. The choice $z \le \log\log N$ gives

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

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

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

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

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

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

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

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

We now consider $\prod^{*}_{n^2+n_0<p\le z} (1-\varrho_f(p^2)/p^2)$ where $f(x) \in S_n(N) - T - T'$. By Lemma 2(v), for each prime $p$ in the range of the product above, $\varrho(p^2) \le np$. 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,

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

Thus, using Lemma 4,

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

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 $\varepsilon$ (and not on $n$ unless, of course, $\varepsilon$ 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 $\varepsilon$, gives a lower bound on $n_0$ depending only on $\varepsilon$.

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

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

Thus, the lemma follows by letting $\varepsilon'$ be the right-hand side above.

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

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

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

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

where we have used the fact that since $z \le \log\log N$,

$$p_1^2 \ldots p_t^2 \le (\log\log N)^{2\log\log N} < N^{\varepsilon'}, \tag{6}$$

where $\varepsilon' \in (0,1)$ and $N$ is sufficiently large (depending on $\varepsilon'$). For later purposes, we fix $\varepsilon' = \min\{1/2, \varepsilon\}$. 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

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

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

$$\begin{aligned}\sum_{f(x)\in S_n(N)} \prod_{p\le z}\left(1 - \frac{\varrho_f(p^2)}{p^2}\right) &= \prod_{p\le z}\left(\left(1 - \frac{w_1(p)}{p^2}\right) + \ldots + \left(1 - \frac{w_r(p)}{p^2}\right)\right) \\ &\quad \times \left(\left(\frac{2N}{p_1^2 \ldots p_t^2}\right)^{n+1} + O_n\left(\left(\frac{2N}{p_1^2 \ldots p_t^2}\right)^{n}\right)\right).\end{aligned}$$

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

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

Thus,

$$\begin{aligned}\sum_{f(x)\in S_n(N)} \prod_{p\le z}\left(1 - \frac{\varrho_f(p^2)}{p^2}\right) &= \prod_{p\le z}\left(1 - \frac{1}{p^2}\right)\left((2N)^{n+1} + O_n\left((2N)^n \prod_{p\le z} p^2\right)\right).\end{aligned}$$

Recalling our choice of $\varepsilon' = \min\{1/2, \varepsilon\}$ 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 such 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 $f(x) \in S_n(N)$ such 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 $\varepsilon$ 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 $\varepsilon > 0$. To obtain Theorem 3, we need only prove that if $N$ is sufficiently large, there are $\le \varepsilon(2N)^{n+1}$ 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 $n_0 = n_0(\varepsilon/2)$, we prove that the set $T$ of $f(x) \in S_n(N)$ such that (i) $\gcd(N_f, \prod_{p \le n^2+n_0} p^2)$ is squarefree and (ii) $f(m)$ is nonsquarefree for every integer $m \in [1, B]$ satisfies $|T| \le \varepsilon(2N)^{n+1}$ (provided $N$ is sufficiently large). Assume that $|T| > \varepsilon(2N)^{n+1}$. Let $z = \log\log B$. For each $f(x) \in S_n(N)$, we denote by $W(f(x))$ the number of integers $m \in [1, B]$ such that $f(m)$ is squarefree. Then Lemma 3 implies that

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

where

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

Thus, using Lemma 7, we get

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

with

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

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

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

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

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

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

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

where

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

On the other hand, Lemma 1 gives us

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

where

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

Thus, in fact,

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

Recalling how $E_2$ was obtained, we now get

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

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

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

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

Thus,

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

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

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

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

$$\sum_{f(x) \in T} E(f(x)) \le -\frac{\varepsilon}{2}\varepsilon''(2N)^{n+1}B\,.$$

On the other hand,

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

Thus, recalling the definition of $E_1$,

$$E_1 \le -\frac{\varepsilon}{2}\varepsilon''(2N)^{n+1}B + O((2N)^{n+1}\log B) + O_n(N^{n+1/2}B)\,.$$

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

$$|E_1| \le 2\varepsilon'(2N)^{n+1}B = \tfrac{2}{5}\varepsilon\varepsilon''(2N)^{n+1}B\,,$$

completing the proof.

Proof of Theorem 4. For $n = 0$, the theorem is clear, so we only consider $n \ge 1$. Let $\varepsilon \in (0,1)$, and let $N$ be sufficiently large (depending on $n$ and $\varepsilon$). Assume that there exist $\ge \varepsilon(2N)^{n+1}$ 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 $n_0 = n_0(\varepsilon/6)$ is such that $|T_2| \le (\varepsilon/3)(2N)^{n+1}$ where $T_2$ denotes the set of $f(x) \in S_n(N)$ for which (i) $\gcd(N_f, \prod_{p \le n^2+n_0} p^2)$ 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 $n_0 \ge 7$. We do this so that later we may use the estimate

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

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

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

and

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

Using the notation of Lemma 6, define

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

The proof of Theorem 3 implies that there are

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

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

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

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

Note that $\varepsilon \in (0, 1)$ implies that the right-hand side above is $> n^2 + n_0$ so that $p^k < 4(n^2 + n_0)/\varepsilon$. 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 $p \leq n^2 + n_0$. 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 $p \leq n^2 + n_0$ is

$$\begin{aligned}&\leq (2N + 1)^n\left(\frac{2N + 1}{p^{k+1}} + 1\right) \leq \frac{\varepsilon}{4(n^2 + n_0)}(2N + 1)^{n+1} + (2N + 1)^n \\ &\leq \frac{\varepsilon}{3(n^2 + n_0)}(2N)^{n+1}\,.\end{aligned}$$

Hence,

$$|T_4| \leq \pi(n^2 + n_0)\frac{\varepsilon}{3(n^2 + n_0)}(2N)^{n+1} \leq \frac{\varepsilon}{3}(2N)^{n+1}\,.$$

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

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

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

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 see that $p^{k+1}$ does not divide $M_f$. This easily implies that each of $M_f$ and $P_f$ is $\le M(n,\varepsilon)$ for every $f(x) \in T_5$.

We now define a function $\alpha : T_5 \to S_n((2M)^n N)$ 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 such 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 $f(x) \in T_5$,

$$1 \le b \le \prod_{p \le n^2+n_0} p^{r(p,f(x))+1} \le \prod_{p \le n^2+n_0} p^{k(p)+1} \le \Big( \prod_{p \le n^2+n_0} p^{k(p)} \Big)^2 \le M(n,\varepsilon)\,.$$

Define

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

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 $\le N(2M)^n$. 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 $\le M(n,\varepsilon)$ possible values for $P_f$ and $\le M(n,\varepsilon)$ possible values for $b$, it is easy to see that for each $g(x)$ in the image of $\alpha$, 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,

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

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

$$\gcd\Big(N_g, \prod_{p \le n^2+n_0} p\Big) = 1 .$$

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 $B'((2M)^n N) = (B(N)/M) - 1$. Now, if $m \in [1, (B(N)/M) - 1]$ and $b$ is as in the definition of $\alpha$, then $P_f m + b$ is a positive integer $\le B(N)$. Also, the definition of $M_f$ implies that $M_f$ divides $N_f$. We now conclude 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

$$\ge \frac{\varepsilon}{(2M)^{n^2+n+2}} |S_n((2M)^n N)|$$

polynomials $g(x) \in S_n((2M)^n N)$ such that $\gcd(N_g, \prod_{p \le n^2+n_0} p) = 1$ and (ii′) holds. Let $T_1'$ denote the set of all such $g(x)$. Let $T_2'$ denote the set of all $g(x) \in T_1'$ such that also $\gcd(N_g, \prod_{p \le n^2+n_{L_1}} p) = 1$. It now suffices to prove that

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

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

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

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

$$\ge \frac{2\varepsilon}{3(2M)^{n^2+n+2}} |S_n((2M)^n N)|$$

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 $r \le k'(p)$. 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

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

Note that with $n$ and $\varepsilon$ 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 find that there are

$$\le \frac{\varepsilon}{2(2M)^{n^2+n+2}}\left|S_n\left(\frac{(2M)^nN}{M'}\right)\right| \le \frac{\varepsilon}{(2M)^{n^2+n+2}(M')^{n+1}}|S_n((2M)^nN)|$$

polynomials $h(x) \in S_n((2M)^nN/M')$ such that $\gcd(N_h, \prod_{p\le n^2+n_1} p) = 1$ and $h(m)$ is nonsquarefree for each positive integer $m \le B'((2M)^nN/M') \le B'((2M)^nN)$. 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 see 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 $h(x) \in S_n((2M)^nN/M')$. The definition of $M' = M'_g$ implies that every such $h(x)$ satisfies $\gcd(N_h, \prod_{p\le n^2+n_1} p) = 1$. Also, using the fact that $\gcd(P_f, \prod_{n^2+n_0<p\le n^2+n_1} p) = 1$, one can show from the definition of $M_f$ and $M'_g$ that $M_fM'_g$ divides $N_f$ where $\alpha(f(x)) = g(x)$. One finds that for $h(x)$ as above, $h(m) = f(P_fm + b)/(M_fM'_g)$ is nonsquarefree for each positive integer $m \le B'((2M)^nN/M')$. Therefore,

$$\begin{aligned}|T'_3 - T'_2| &\le \sum\nolimits^* \frac{\varepsilon}{(2M)^{n^2+n+2}(M')^{n+1}}|S_n((2M)^nN)| \\ &= \frac{\varepsilon}{(2M)^{n^2+n+2}}\Big(\sum\nolimits^* (M')^{-n-1}\Big)|S_n((2M)^nN)|,\end{aligned}$$

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 deduce that each such $M'$ is $\ge n^2 + n_0 \ge n_0$. Thus, since $n \ge 1$,

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

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

$$|T'_3 - T'_2| \le \frac{4\varepsilon}{25(2M)^{n^2+n+2}}|S_n((2M)^nN)|,$$

so that

$$|T'_2| \ge |T'_3| - |T'_3 - T'_2| \ge \frac{38\varepsilon}{75(2M)^{n^2+n+2}}|S_n((2M)^nN)|,$$

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 $N_f = U_fV_f$, 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 $\gcd(N_g, \prod_{p \le n^2+n_0} p^2)$ 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*, in: Proc. Sympos. Pure Math. 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*, Abh. Math. Sem. Hamburg. Univ. 1 (1922), 179–194.

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

[10] —, *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, 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] —, *Algebra I*, Springer, Berlin 1966.

[14] —, *Algebra*, Vol. I, 7th edition, translated by F. Blum and J. R. Schulenberger, Frederick Ungar Publ. Co., New York 1970.



MATHEMATICS DEPARTMENT
UNIVERSITY OF SOUTH CAROLINA
COLUMBIA, SOUTH CAROLINA 29208
U.S.A.



*Received on 2.7.1990*
*and in revised form on 19.3.1991* (2058)