ACTA ARITHMETICA
L (1988)

Prime values of irreducible polynomials

by

MICHAEL FILASETA (Columbia, S.C.)

1. Introduction. Let $f(x)$ be a polynomial with integer coefficients and set $N = N_f = \text{g.c.d.}(f(n),\ n \in Z)$. For computational reasons, we note that (cf. [4])

$$N = \text{g.c.d.}(f(n),\ n \in \{1, 2, \ldots, g+1\}) \tag{1}$$

where g denotes the degree of the polynomial $f(x)$. A long standing conjecture of Bouniakowski [3] is the following:

CONJECTURE 1. *A necessary and sufficient condition for a polynomial $f(x) \in Z[x]$ to be irreducible is that there exist infinitely many integers m such that $f(m)/N$ is prime.*

Here and throughout this paper, "prime" values of polynomials necessarily refer to both positive and negative primes; however, the letter "p" will always denote a positive prime. Also, every polynomial $f(x)$ will have integer coefficients, and when we speak of $f(x)$ as being irreducible, we shall mean that $f(x)$ is irreducible over the rationals.

Perhaps the most definitive result in the direction of resolving the above conjecture is due to Richert [10] who showed that if $f(x)$ is irreducible, then there exist infinitely many integers m such that $f(m)/N$ is the product of at most $g+1$ primes. There are also stronger conjectures of Schinzel and Sierpiński [11] and heuristic arguments for related density results given by Bateman and Horn ([1], [2]).

On the other hand, the situation for reducible polynomials is much simpler. It is a trivial matter to show that if $f(x)$ is a reducible polynomial of degree g, then there are at most $2g$ integers m such that $f(m)$ is prime. More precise results can also be obtained (cf. [8]); in particular, with $f(x)$ a reducible polynomial as above, there are at most $g+4$ integers m such that $f(m)$ is prime. With this in mind, we consider the following finite version of Bouniakowski's conjecture.

CONJECTURE 2. *A necessary and sufficient condition for a polynomial*

$f(x) \in Z[x]$ of degree g to be irreducible is that there exist $g+5$ integers m such that $f(m)/N$ is prime.

As we shall see in Section 2, it is a fairly straightforward matter to show that Conjecture 1 and Conjecture 2 are actually equivalent. The proof will be similar to what one might use to show that if every arithmetic progression $an+b$ with $(a, b) = 1$ contains at least one prime, then every such arithmetic progression contains infinitely many primes. However, despite the equivalence of these conjectures, partial results about one of them may be far from being applicable to the other. For example, it is easy to verify Conjecture 2 for "many" irreducible polynomials, but to the best of my knowledge, no one has even established the mere existence of an irreducible polynomial $f(x)$ of degree >1 such that for infinitely many integers m, $f(m)/N$ is prime.

We direct our attention to Conjecture 2. Our main goal is to prove that Conjecture 2 is true for a positive proportion of the polynomials. To be more specific, we introduce the following notation. For any positive integer g, set

$$S(B) = S_g(B) = \{f(x) = \sum_{j=0}^{g} a_j x^j\colon |a_j| \leqslant B \text{ for } j = 0, 1, \ldots, g\}.$$

In other words, $S_g(B)$ is the set of all polynomials of degree $\leqslant g$ with integer coefficients bounded in absolute value by B. In particular, we note that $|S_g(B)| = (2[B]+1)^{g+1}$ where [ ] denotes the greatest integer function. It can be shown that (cf. [9]) the number of reducible polynomials in $S_g(B)$ is bounded by $O_g(B^g \log^2 B)$ so that (in some sense) almost all polynomials are irreducible. For related density results concerning irreducibility modulo primes and algebraic number fields with Galois group the symmetric group see [5] and [12].

We will prove the following:

THEOREM 1. *Let g be any positive integer, and let B be any positive number sufficiently large (depending on g). Then the number of irreducible polynomials $f(x) \in S_g(B)$ such that there exist at least $g+5$ integers m for which $f(m)$ is prime is*

$$\geqslant C(2B+1)^{g+1},$$

where $C > 0$ is a computable constant. In particular, one may choose $C = 1/1800$.

Let $P(B, g)$ denote those polynomials in $S_g(B)$ which assume prime values at least $g+5$ times. Then this theorem establishes the existence of a positive computable constant C such that

$$\inf_g \left(\liminf_{B\to\infty} \frac{|P(B, g)|}{(2B+1)^{g+1}}\right) > C.$$

The value of $g+5$ here plays a minor role in what follows; we use it only to emphasize the connections to our work with the very plausible necessary and sufficient condition for a polynomial to be irreducible given by Conjecture 2. In the results above, one may replace $g+5$ with any function of g without affecting the constant C. We shall give two different proofs that such a constant exists. The second proof will not give as good an estimate on the value of C; on the other hand, it will provide us some additional information (see the comments following (6) in Section 4). No attempt here will be made to get a sharp estimate on C; the value of C given above is only to emphasize that C is computable.

The next two sections are devoted to preliminary results and the two proofs of Theorem 1. In Section 4, we will discuss further consequences of the methods of this paper and different ways of improving on the value of C given in Theorem 1. In particular, we will show that the first proof may be modified to permit the choice $C = 1/193$.

2. Preliminary remarks. We begin by establishing the equivalence of Conjectures 1 and 2. From the comments in the introduction, it is clear that this equivalence can be established from the following:

THEOREM 2. *Let g be a positive integer and let N_f be as defined by (1). If*

(i) *every irreducible polynomial $f(x)$ of degree g is such that there exists at least one integer m for which $f(m)/N_f$ is prime,*

then

(ii) *every irreducible polynomial $f(x)$ of degree g is such that there exist infinitely many integers m for which $f(m)/N_f$ is prime.*

Proof. Suppose (i) holds. Assume there is an irreducible polynomial, say $f(x) \in Z[x]$, of degree g such that

$$m^* = \max\{|m|\colon m \in Z, f(m)/N_f \text{ is prime}\}$$

exists. Let p be a prime satisfying

$$p > \max\{|f(m^*+1)|, 2(m^*+1)\}.$$

Define

$$g(x) = f(px+(m^*+1)).$$

Clearly, $g(x)$ is of degree g and is irreducible. Thus, to complete the proof, we will obtain a contradiction to (i) by showing that there is no integer m for which $g(m)/N_g$ is prime.

We first establish that $N_g = N_f$. Clearly, $N_f | N_g$ since each value of $g(x)$ at an integral argument corresponds to a value of $f(x)$ at an integral argument. Suppose q is a prime and r is a positive integer such that $q^r \| N_g$. Since $p > |f(m^*+1)| = |g(0)|$, $p \nmid N_g$. Hence, $q \neq p$. Now, since $q^r | N_g$, we know that

$$q^r \mid g(m) \quad \text{for} \quad m \in \{0, 1, \ldots, q^r-1\}.$$

But $g(m) = f(pm+(m^*+1))$ so that

$$f(pm+(m^*+1)) \equiv 0 \pmod{q^r} \quad \text{for} \quad m \in \{0, 1, \ldots, q^r-1\}.$$

Let n be any integer. Since $q \neq p$, there exist an $m \in \{0, 1, \ldots, q^r-1\}$ such that

$$pm+(m^*+1) \equiv n \pmod{q^r}.$$

Hence,

$$f(n) \equiv f(pm+(m^*+1)) \equiv 0 \pmod{q^r}.$$

Since n was an arbitrary integer, we now get that $q^r \mid N_f$ so that $N_g \mid N_f$ and finally

$$N_g = N_f.$$

To finish the proof, it remains to show that $g(m)/N_g = g(m)/N_f$ is composite for any integer m. Fix an integer m. Since $p > 2(m^*+1)$,

$$|pm+(m^*+1)| \geqslant m^*+1.$$

Thus, by our definition of m^*, we now get that

$$g(m)/N_g = f(pm+(m^*+1))/N_f$$

is composite, completing the proof.

We are now ready to consider 3 lemmas. Both proofs of Theorem 1 will rely on the use of all three lemmas. We note, however, that the second proof uses only the lower bound of Lemma 1 whereas the first proof uses both the lower and the upper bounds. In both cases, Lemma 2 will clearly play the major role.

For every positive integer g and every positive real numbers B, M_1, and M_2, define

$$T(B, M_1, M_2) := T_g(B, M_1, M_2) := \Big|\{(a_g, \ldots, a_1, a_0, m):$$

$$f(x) = \sum_{j=0}^{g} a_j x^j \in S(B),\ m \in (M_1, M_2] \cap Z, \text{ and } f(m) \text{ is prime}\}\Big|.$$

We now get the following:

Lemma 1. *Let g be a positive integer and let M_1 and M_2 be any positive real numbers satisfying*

$$3 \leqslant M_1+1 \leqslant M_2.$$

Then there exist $B_0 = B_0(g, M_2)$ and an absolute constant B_1 such that if $B > B_0$, then

$$T(B, M_1, M_2) > (1/3)(2B+1)^{g+1}(M_2-M_1)/(\log B);$$

and if $B > B_1$, then

$$T(B, M_1, M_2) < 3(2B+1)^{g+1}(M_2-M_1)/(\log B).$$

Proof. We first establish the lower bound for $T_g(B, M_1, M_2)$. Fix an integer $m \in (M_1, M_2]$ and consider any integer d with $|d| \leqslant (B/2)m^g$. We note that if $m > 2$, then one easily gets that for any choice of integers a_0, $a_1, \ldots, a_{g-1} \in [-B, B]$,

$$|d-(a_{g-1}m^{g-1}+\ldots+a_1 m+a_0)| < Bm^g. \tag{2}$$

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

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

Thus, the total number of choices for $(a_0, a_1, \ldots, a_{g-1})$ is at least $2^g[B/m]^g$. We now choose a_g so that

$$d = a_g m^g+\ldots+a_1 m+a_0.$$

By (2), it follows that a_g is an integer in the interval $[-B, B]$. Hence, there are at least $2^g[B/m]^g$ different choices for

$$f(x) = \sum_{j=0}^{g} a_j x^j \in S(B)$$

such that $f(m) = d$. Since m can be any integer in the interval $(M_1, M_2]$ and d can be any integer (and, in particular, any prime) in the interval $[-(B/2)m^g, (B/2)m^g]$, we now get

$$T(B, M_1, M_2) \geqslant \sum_{m \in (M_1, M_2]} 2^g[B/m]^g(2\pi(Bm^g/2)).$$

For B sufficiently large (depending on both g and M_2), we now get that

$$T(B, M_1, M_2) > (1/3)(2B+1)^{g+1}(M_2-M_1)/(\log B).$$

To prove the upper bound in Lemma 1, choose any integers $a_g, \ldots, a_2$, $a_1 \in [-B, B]$ and any integer $m \in (M_1, M_2]$ and consider the number of choices of an integer $a_0 \in [-B, B]$ such that $(a_g m^g+\ldots+a_1 m)+a_0$ is prime. By an application of Selberg's sieve (cf. [6], p. 124), for B sufficiently large (independent of g, M_1, and M_2) there are less than $3(2B+1)/(\log B)$ choices of a_0 as above. Thus, for B sufficiently large, we get

$$T(B, M_1, M_2) < 3(2B+1)^{g+1}(M_2-M_1)/(\log B),$$

completing the proof.

Before proceeding to Lemma 2, we note here that when using Lemma 1, we will need a specific estimate on $B_0(g, M_2)$. More precisely, we will want

$$B_0(g, M_2) > e^{\tau M_2}$$

where τ is any positive constant. For fixed g and $B_0(g, M_2)$ as above, the proof of Lemma 1 is easily seen to carry over. We are now ready to proceed to our main lemma.

LEMMA 2. *Let g and B be positive integers and let m_1 and m_2 be any two distinct integers $< B$. Then for B sufficiently large (independent of m_1 and m_2), the number of polynomials $f(x) \in S_g(B)$ such that $f(m_1)$ and $f(m_2)$ are both prime is*

$$< 32\Big\{\prod_{p|(m_2-m_1)} \big(1-(1/p)\big)^{-1}\Big\}\frac{(2B+1)^{g+1}}{\log^2 B}.$$

Proof. We give here only a sketch of the proof; the details are well known in the theory of Brun's sieve. We present our proof in a form which can easily be followed through with the aid of the excellent book of Halberstam and Richert [6]. We first note that the rank of the $2\times(g+1)$ matrix over Z_p

$$\begin{bmatrix} m_1^g & m_1^{g-1} & \dots & m_1 & 1 \\ m_2^g & m_2^{g-1} & \dots & m_2 & 1 \end{bmatrix}$$

is 2 if $p \not| (m_2-m_1)$ and is 1 if $p|(m_2-m_1)$. Thus, if $p \not| (m_2-m_1)$, then the number of $(g+1)$-tuples $(a_g, \dots, a_1, a_0) \in Z_p^{g+1}$ such that

$$a_g m_1^g + \dots + a_1 m_1 + a_0 \equiv 0 \pmod p$$

or

$$a_g m_2^g + \dots + a_1 m_2 + a_0 \equiv 0 \pmod p$$

is $p^{g-1}(2p-1)$. If $p|(m_2-m_1)$, then the number of solutions as above is p^g.

We are now ready to set up the Brun sieve. Let

$$A = \{f(m_1)f(m_2)\colon f(x) \in S_g(B)\}.$$

For square-free integers d, we define $w(d)$ as a multiplicative function such that for a prime p

$$w(p) = \begin{cases} 2-(1/p) & \text{if} \quad p \not| (m_2-m_1), \\ 1 & \text{if} \quad p|(m_2-m_1). \end{cases}$$

Set $\chi(d) = \chi_1(d)$ as defined in [6], p. 58, and

$$R_d = \sum_{\substack{a\in A\\ d|a}} 1 - \{(2B+1)^{g+1} w(d)/d\}.$$

By our previous comments, we know that

$$R_d \ll_g \{((2B+1)/d)+2\}^g d^g w(d) \ll_g (B^g+d^g)\, w(d).$$

Let $z = B^u$ where u is a positive real number to be chosen shortly. Let S denote the number of elements of A which are divisible by no prime $p \leqslant z$. The Brun sieve now gives that for any real number λ with

$$0 < \lambda e^{1+\lambda} < 1,$$

one has

$$\begin{aligned} S \leqslant (2B+1)^{g+1} &\prod_{p\leqslant z} \big(1-(w(p)/p)\big) \\ &\times \{1+\big(2\lambda^3 e^{2\lambda}/(1-\lambda^2 e^{2+2\lambda})\big)\exp\big(c_1/\lambda(\log z)\big)\} \\ &+O_g\big(B^g z^{\{2+(2.01/(e^{\lambda}-1))\}}\big) \\ &+O_g\big(z^{(g+1)\{2+(2.01/(e^{\lambda}-1))\}}\big) \end{aligned} \tag{3}$$

where c_1 is some fixed constant. We take $\lambda = 1/4$ and $u = 1/(9.1)$. We also rewrite the above product by noting that if $p \not| (m_2-m_1)$, then

$$1-\big(w(p)/p\big) = \big(1-(1/p)\big)^2, .$$

and if $p|(m_2-m_1)$, then

$$1-\big(w(p)/p\big) = 1-(1/p).$$

Using that

$$\prod_{p\leqslant z} \big(1-(1/p)\big) \sim e^{-\gamma}/(\log z)$$

where $\gamma = 0.57721\ldots$ is Euler's constant, together with (3), we now get that for B sufficiently large

$$S \leqslant 31.75\Big(\prod_{p|(m_2-m_1)} \big(1-(1/p)\big)^{-1}\Big)(2B+1)^{g+1}/\log^2 B.$$

To finish the proof, we note that as in the first part of the proof of Lemma 1, one can show that the total number of polynomials $f(x) \in S_g(B)$, with $|f(m_1)|$ or $|f(m_2)|$ a prime $\leqslant z$, is $< 4(2B+1)^g \pi(z)$. Thus, for B sufficiently large, the number of polynomials $f(x) \in S_g(B)$ such that $f(m_1)$ and $f(m_2)$ are both prime is

$$< S + 40(2B+1)^g \big(B^{1/(9.1)}/(\log B)\big),$$

whence the lemma now follows.

The following lemma has a simple proof which we leave to the reader.

LEMMA 3. *Let U be a set of N elements, and let θ, α, and β be positive* *real numbers with*

$$\alpha+\beta=\theta<1.$$

Let K be a positive integer and $V_1, V_2, \ldots, V_K$ be subsets of U such that

$$|V_j|\geqslant \theta N \quad \textit{for} \quad j=1,2,\ldots,K.$$

Then for any positive integer r and for $K\geqslant(1-\alpha)(r-1)/\beta$, there exist at least αN elements of U each of which is a member of at least r of the subsets V_j.

3. Two proofs of Theorem 1.

Proof 1. We begin with the equation

$$\sum_{f(x)\in S(B)}\Big(\sum_{\substack{M_1<m\leqslant M_2\\ f(m)\text{prime}}}1\Big)^2=2\sum_{f(x)\in S(B)}\Big(\sum_{\substack{M_1<m_1<m_2\leqslant M_2\\ f(m_1)\text{and} f(m_2)\text{prime}}}1\Big)+\sum_{f(x)\in S(B)}\Big(\sum_{\substack{M_1<m\leqslant M_2\\ f(m)\text{prime}}}1\Big).$$

By Lemma 1 and Lemma 2, this is

$$<64(2B+1)^{g+1}/(\log^2 B)\Big\{\sum_{M_1<m_1<m_2\leqslant M_2}\prod_{p|(m_2-m_1)}(1+(2/p))\Big\}$$
$$+3(2B+1)^{g+1}(M_2-M_1)/(\log B).$$

Now,

$$(4)\qquad \sum_{M_1<m_1<m_2\leqslant M_2}\prod_{p|(m_2-m_1)}(1+(2/p))$$
$$\leqslant\sum_{M_1<m_1<m_2\leqslant M_2}\Big(\sum_{d|(m_2-m_1)}(2^{\nu(d)}/d)\Big)$$
$$=\sum_{d\leqslant M_2-M_1}(2^{\nu(d)}/d)\sum_{\substack{M_1<m_1<m_2\leqslant M_2\\ m_2\equiv m_1(\operatorname{mod} d)}}1$$
$$\leqslant(M_2-M_1+1)\sum_{d\leqslant M_2-M_1}(2^{\nu(d)}/d)\,\{((M_2-M_1+1)/d)+1\}$$
$$=(M_2-M_1+1)^2\sum_{d\leqslant M_2-M_1}(2^{\nu(d)}/d^2)+(M_2-M_1+1)\sum_{d\leqslant M_2-M_1}(2^{\nu(d)}/d)$$
$$<3(M_2-M_1)^2$$

where $\nu(d)$ denotes the number of distinct prime divisors of d and where $M=M_2-M_1$ is sufficiently large. Thus, we now get that

$$\sum_{f(x)\in S(B)}\Big(\sum_{\substack{M_1<m\leqslant M_2\\ f(m)\text{prime}}}1\Big)^2$$
$$<192\,\{(2B+1)^{g+1}/(\log^2 B)\}(M_2-M_1)^2+3\,\{(2B+1)^{g+1}/(\log B)\}(M_2-M_1).$$

We set

$$B=e^M.$$

Then, when M is sufficiently large and $M_1\geqslant 2$, we get by Lemma 1 and the Cauchy–Schwarz inequality,

$$(1/9)(2B+1)^{2g+2}(M_2-M_1)^2/\log^2 B$$
$$<\Big(\sum_{f(x)\in S(B)}\Big(\sum_{\substack{M_1<m\leqslant M_2\\ f(m)\text{ prime}}}1\Big)\Big)^2$$
$$\leqslant\Big(\sum_{\substack{f(x)\in S(B)\\ \text{There is an } m\in(M_1,M_2]\\ \text{such that } f(m) \text{ is prime}}}1\Big)\Big(\sum_{f(x)\in S(B)}\Big(\sum_{\substack{M_1<m\leqslant M_2\\ f(m)\text{prime}}}1\Big)^2\Big)$$
$$<195\Big(\sum_{\substack{f(x)\in S(B)\\ \text{There is an } m\in(M_1,M_2]\\ \text{such that } f(m) \text{ is prime}}}1\Big)\left(\frac{(2B+1)^{g+1}(M_2-M_1)^2}{\log^2 B}\right).$$

We now choose $M_1=kM$ and $M_2=(k+1)M$ where $k\in\{1,\ldots,K\}$ and K is a constant, possibly depending on g, which is to be chosen. The above inequality implies for each $k\in\{1,\ldots,K\}$ that

$$\sum_{\substack{f(x)\in S(B)\\ \text{There is an } m\in(kM,(k+1)M]\\ \text{such that } f(m) \text{ is prime}}}1>\frac{1}{1755}(2B+1)^{g+1}.$$

Theorem 1 now follows by taking $K=\varkappa(g+4)$ where $\varkappa$ is a sufficiently large constant and using the above range on k together with Lemma 3.

Proof 2 (for $C=1/7000$). Consider a subinterval $I\subset\mathbf{R}\cap(1,\infty)$ of length $(1/1164)(\log B)$ in the interval $(0, M]$. Thus, if s denotes the number of integers in I, then

$$(1/1164)(\log B)-2\leqslant s\leqslant(1/1164)(\log B)+1.$$

By Lemma 2 we know that the total number of $(g+3)$-tuples $(a_g,\ldots,a_0,m_1,m_2)$ such that $f(x)=\sum_{j=0}^{g}a_jx^j\in S(B)$ and both $f(m_1)$ and $f(m_2)$ are prime is

$$<32\sum_{m_1,m_2\in I}\left(\prod_{p|(m_2-m_1)}(1-(1/p))^{-1}\frac{(2B+1)^{g+1}}{\log^2 B}\right).$$

This can be estimated as in (4) to obtain the following upper bound on the number of $(g+3)$-tuples as above:

$$(96)s^2(2B+1)^{g+1}/\log^2 B<(97)(1/1164)^2(2B+1)^{g+1}$$

for B sufficiently large. Denote this final upper bound by W. Let u_j denote the number of polynomials $f(x)\in S(B)$ such that there exist exactly j integers $m\in I$ such that $f(m)$ is prime. Then the above estimates imply that

$$\sum_{j=2}^{s} u_j\binom{j}{2}\leqslant W.$$

Now, let R denote the set of polynomials $f(x)\in S(B)$ such that there are at least 2 integers $m\in I$ for which $f(m)$ is prime. Then the total number of $(g+2)$-tuples $(a_g, \ldots, a_0, m)$ such that $f(x)\in R$, $m\in I$, and $f(m)$ is prime is

$$\sum_{j=2}^{s} u_j j\leqslant 2\sum_{j=2}^{s} u_j\binom{j}{2}\leqslant 2W.$$

On the other hand, by Lemma 1, we see that the total number of $(g+2)$-tuples $(a_g, \ldots, a_0, m)$ such that $f(x)\in S(B)$, $m\in I$, and $f(m)$ is prime is

$$\geqslant(1/3)(1/1164)(2B+1)^{g+1}.$$

Thus, the number of polynomials $f(x)\in S(B)$ such that there exists exactly one integer $m\in I$ such that $f(m)$ is prime is

$$\geqslant\{(1/3)(1/1164)-2(97)(1/1164)^2\}(2B+1)^{g+1}.$$

Theorem 1 now follows with the constant $C=1/7000$ by iterating the interval I and using Lemma 3 as in the previous proof.

4. Further comments. We begin by stating some consequences of the above methods.

COROLLARY 1. *Let g be a fixed positive integer. Then for B sufficiently large, there exist at least $(1/1800)(2B+1)^{g+1}$ polynomials $f(x)=\sum_{j=0}^{g} a_j x^j\in S(B)$ such that for some positive integer $m<\log\max_{0\leqslant j\leqslant g}\{|a_j|\}$, one has that $f(m)$ is prime.*

Furthermore, there are at least $(1/3600)(2B+1)^{g+1}$ polynomials $f(x)=\sum_{j=0}^{g} a_j x^j\in S(B)$ such that for $g+5$ integers $m<3600(g+4)\log\max_{0\leqslant j\leqslant g}\{|a_j|\}$, one has that $f(m)$ is prime.

COROLLARY 2. *Let ε be any positive real number and let B be sufficiently large (depending on ε). Then there exists a $\delta>0$, depending only on ε, such that there are at least $\delta(2B+1)^{g+1}$ polynomials $f(x)=\sum_{j=0}^{g} a_j x^j\in S(B)$ satisfying $f(m)$ is prime for some positive integer*

$$m<\varepsilon\log\max\{|a_0|, |a_1|, \ldots, |a_g|\}. \tag{5}$$

We discuss only briefly the above results. Corollary 1 follows from a combination of the first proof of Theorem 1 and Lemma 3. Corollary 2 follows from the first proof of Theorem 1 with the choice $B=e^{\tau M}$ for some τ sufficiently large. Note that Corollary 2 may be restated as: a positive proportion of the polynomials $f(x)=\sum_{j=0}^{g} a_j x^j\in Z[x]$ are such that $f(m)$ is prime for some positive integer m satisfying (5). Lemma 1 may be used to show that this result is best possible; more precisely, if $u(x)$ is any function for which $\lim_{x\to\infty}(u(x)/\log x)=0$, then almost all polynomials $f(x)=\sum_{j=0}^{g} a_j x^j\in Z[x]$ satisfy $f(m)$ is composite for all $m<u(\max\{|a_0|, \ldots, |a_g|\})$.

We now turn to methods for improving on the constants contained in this paper. We begin by noting that the first half of the proof of Lemma 1 can be extended to improve on both the upper and lower bounds for $T(B, M_1, M_2)$. More precisely, we get

LEMMA 1*. *Let g be a positive integer and let ε, M_1, M_2, and B be positive real numbers. Then there exist $M_0^*=M_0^*(\varepsilon, g)$ and $B_0^*=B_0^*(\varepsilon, g, M_2)$ such that whenever*

$$M_2\geqslant M_1+1\geqslant M_0^* \quad \textit{and} \quad B\geqslant B_0^*,$$

we get

$$\begin{aligned}(1-\varepsilon)(2B+1)^{g+1}&(M_2-M_1)/(\log B)\\ &<T(B, M_1, M_2)<(1+\varepsilon)(2B+1)^{g+1}(M_2-M_1)/(\log B).\end{aligned}$$

A direct application of Lemma 1* will enable an immediate improvement on the admissible choice for C given by the first proof of Theorem 1; we may take

$$C=1/193. \tag{6}$$

Lemma 1* can also be used to improve on the constant C given by the second proof of Theorem 1. But the second proof can also be modified in an additional manner. In that proof, we estimated the number of polynomials $f(x)\in S(B)$ such that there exists exactly one integer m, from a certain fixed interval I, for which $f(m)$ is prime. This is a merit of the second proof of Theorem 1 which the first proof does not have, i.e., the second proof actually shows that in certain intervals I with length of order $\log B$ (and with B sufficiently large), a positive proportion of the polynomials $f(x)\in S(B)$ are such that there exists *exactly* one integer $m\in I$ for which $f(m)$ is prime. Hence, one may take into account the number of polynomials $f(x)\in S(B)$

such that more than one such integer m exists; such an estimate leads to obtaining the choice $C = 1/386$, a value which is less than the value given in (6).

We have only considered here some simple ideas for improving the value of C given in Theorem 1. This value can undoubtedly be improved further by using sieve techniques other than the Brun sieve for Lemma 2.

In conclusion, we note that Theorem 1 does not concern itself with polynomials $f(x) \in S(B)$ for which $N_f \neq 1$. Since a positive proportion of the polynomials $f(x) \in S(B)$ are such that $N_f \neq 1$, the value of C in Theorem 1 must be < 1. Indeed, one can only hope to achieve

$$C \overset{?}{\underset{?}{=}} \prod_p \left(1 - \frac{1}{p^p}\right) = 0.72199\ldots$$

We also note that we have only considered a particular type of density that can be associated with polynomials. For example, a variation on a problem posed by Odlyzko [7] is to determine whether for any choice of $B \geqslant 1$

$$\liminf_{g \to \infty} \frac{|\{f(x) \in S_g(B) \colon f(x) \text{ is irreducible}\}|}{(2B+1)^{g+1}}$$

is positive.

Acknowledgments. I thank Andrew Odlyzko, David Richman, and Jim Walker for some helpful conversations in connection with this paper.

References

[1] P. T. Bateman and R. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. 16 (1962), pp. 363–367.

[2] — — *Primes represented by irreducible polynomials in one variable*, Proc. Sympos. Pure Math., Vol. 8, Amer. Math. Soc., Providence, R. I., 1965, pp. 119–135.

[3] V. Bouniakowski, *Sur les diviseurs numériques invariables des fonctions rationelles entieres*, Mem. Acad. Sci. St. Petersburg 6 (1857), pp. 305–309.

[4] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York 1971, p. 334.

[5] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math., Vol. 24, Amer. Math. Soc., 1973, pp. 91–101.

[6] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London 1974.

[7] A. Odlyzko, private communication.

[8] O. Ore, *Einige Bemerkungen über Irreduzibilität*, Jahresbericht der Deutschen Math. – Ver. 44 (1934), pp. 146–151.

[9] G. Pólya and G. Szegő, *Problems and Theorems in Analysis II*, Springer-Verlag, New York 1976, p. 156.

[10] H.-E. Richert, *Selberg's sieve with weights*, Mathematika 16 (1969), pp. 1–22.

[11] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), pp. 185–208; *Corrigendum*: ibid. 5 (1959), p. 259.

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

Received on 4.10.1985
and in revised form on 26.6.1986 (1548)