Can. J. Math., Vol. XL, No. 2, 1988, pp. 339-351

IRREDUCIBILITY CRITERIA FOR POLYNOMIALS WITH NON-NEGATIVE COEFFICIENTS

MICHAEL FILASETA

1. Introduction. In [**7**, b.2, VIII, 128] Pólya and Szegö state the following theorem of A. Cohn:

THEOREM 1. *Let* $d_n d_{n-1} \dots d_0$ *be the decimal representation of a prime. Then*

$$f(x) = \sum_{j=0}^{n} d_j x^j$$

is irreducible.

Thus, for example, since 1289 is prime, $x^3 + 2x^2 + 8x + 9$ is irreducible. Brillhart, Odlyzko, and the author generalized Cohn's Theorem in three different directions. As examples of these types of generalizations, we note the following results, the first two of which are special cases of a result in [**1**] and the third of a result in [**3**].

THEOREM 2. *Let* $d_n d_{n-1} \dots d_0$ *be the base b representation of a prime where b is an integer* $\geqq 2$. *Then*

$$f(x) = \sum_{j=0}^{n} d_j x^j$$

is irreducible.

THEOREM 3. *Let*

$$f(x) = \sum_{j=0}^{n} d_j x^j$$

be such that $f(10)$ *is prime and* $0 \leqq d_j \leqq 167$ *for* $j = 0, 1, \dots, n$. *Then* $f(x)$ *is irreducible.*

THEOREM 4. *Let* $d_n d_{n-1} \dots d_0$ *be the decimal representation of wp where* $w \in \{1, 2, \dots, 9\}$ *and p is a prime. Then*

Received May 1, 1984 and in revised form April 7, 1987. This is dedicated to the memory of Pólya and Szegö.

https://doi.org/10.4153/CJM-1988-013-6 Published online by Cambridge University Press

$$f(x) = \sum_{j=0}^{n} d_j x^j$$

is irreducible over the rationals.

The purpose of this paper is to demonstrate how Theorem 3 can be improved. After proving a general theorem in Section 2, we show in Section 3 that, rather curiously, the bound 167 on the coefficients of $f(x)$ may be replaced by 10^{30}. Furthermore, if the degree of $f(x)$ is $\leqq 31$, then no upper bound whatsoever is needed. We therefore conclude that essentially any polynomial one might encounter with non-negative coefficients which is prime at 10 is irreducible. However, in Section 4 we show that in general in order to conclude the irreducibility of $f(x)$ in Theorem 3, some upper bound on the coefficients of $f(x)$ is needed. In Section 5, using the methods of Section 4, we construct an explicit example of a reducible polynomial $f(x)$ of degree 32 with $f(10)$ prime and with $f(x)$ having non-negative integer coefficients $<6.2 \times 10^{31}$; thus, the bound 10^{30} cannot be replaced by 6.2×10^{31}. Section 5 also contains some further discussion of the case when the degree of $f(x)$ is 32. In Sections 4 and 5, analogous results are also discussed for prime values of $f(b)$ where b is any positive integer. Finally, we note here that the original results of Brillhart, Odlyzko, and the author in [**1**] and [**3**] apply more directly to polynomials with negative coefficients than the theorems which follow.

2. A general theorem.

We begin with

LEMMA 1. *Let k and b be integers with $1 \leqq k < b$ and let*

$$D = \{z : |b - z| \leqq \sqrt{k}\}.$$

Suppose

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbf{Z}[x]$$

has the properties

(i) $a_j \geqq 0$ *for* $j = 0, 1, \dots, n$,

(ii) $|f(b)| = kp$ *for some prime* p,

and

(iii) *if* $f(\alpha) = 0$, *then* $\alpha \notin D$.

Then $f(x)$ is irreducible over the rationals.

Proof. Assume $f(x)$ satisfies (i), (ii), and (iii) and $f(x) = g(x)h(x)$ with

$$\deg(g(x)) = r \geqq 1 \quad \text{and} \quad \deg(h(x)) = s \geqq 1.$$

We may also assume the leading coefficients of $g(x)$ and $h(x)$ are positive. Since

$$kp = |f(b)| = |g(b)|\,|h(b)|,$$

one of $|g(b)|$ or $|h(b)|$ is $\leqq k$. Say $|g(b)| \leqq k$. Write

$$g(x) = b_r \prod_{j=1}^{r} (x - \beta_j).$$

Since each root β_j of $g(x)$ is a root of $f(x)$, we have by (iii) that

$$|b - \beta_j| > \sqrt{k} \quad \text{for } j = 1, 2 \ldots, r.$$

Hence,

$$k \geqq |g(b)| = |b_r| \prod_{j=1}^{r} |b - \beta_j| > k^{r/2}$$

so that $r = 1$. Therefore, $g(x) = b_1 x + b_0$ with $b_1 > 0$. If $b_0 < 0$, then $g(x)$ and therefore $f(x)$ would have a positive real root, giving a contradiction to (i). Hence, $b_0 \geqq 0$, and

$$b > k \geqq |g(b)| = |b_1 b + b_0| \geqq b_1 b,$$

a contradiction, completing the proof.

Comment. A result similar to Lemma 1 (where the coefficients of $f(x)$ are allowed to be negative) can be found in [**6**].

We are now ready to prove

THEOREM 5. *Let*

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbf{Z}[x]$$

such that $a_j \geqq 0$ *for* $j = 0, 1, \ldots, n$, *and let* k *and* b *be positive integers with* $b \geqq 2$ *and* $k \leqq b - 1$. *Let*

$$m = [\pi/\sin^{-1}(\sqrt{k}/b)] - 1$$

where [ ] *denotes the greatest integer function, and fix*

$$B \leqq \gamma(b - \sqrt{k})^m (b - \sqrt{k} - 1)$$

where

$$\gamma = a_n \sqrt{k}/\{(b^2 - k)^{1/2} + \sqrt{k}\}.$$

Suppose that $a_j \leqq B$ *for* $j = 0, 1, \ldots, n - m - 1$ *and that* $f(b) = wp$ *for some positive integer* $w \leqq k$ *and some prime* p. *Then* $f(x)$ *is irreducible over the rationals.*

Proof. Let

$$S = \{\alpha = re^{i\theta}: r \geqq b - \sqrt{k} \quad \text{and}$$
$$|\theta| \leqq \sin^{-1}(\sqrt{k}/b)\}.$$

We show that if $\alpha \in S$, then $f(\alpha) \neq 0$. Lemma 1 will then imply Theorem 5 since S contains

$$D = \{z: |b - z| \leqq \sqrt{k}\}.$$

Fix $\alpha = re^{i\theta} \in S$ and assume $f(\alpha) = 0$. Since the coefficients of $f(x)$ are non-negative, $\theta \neq 0$. Therefore, α is not real and its conjugate is also an element of S and a root of $f(x)$. We may therefore assume that $\theta > 0$. Set

$$m' = [\pi/(2\theta)].$$

Define

$$\theta_0 = \sin^{-1}(\sqrt{k}/b) \quad \text{and} \quad \theta_1 = \pi - m\theta_0.$$

Consider the first case that $m \geqq m'$. Then

$$j\theta \in (0, \pi/2] \quad \text{for } j = 1, 2, \dots, m'$$

and

$$j\theta \in (\pi/2, \pi) \quad \text{for } j = m' + 1, \dots, m.$$

Indeed, $m\theta \leqq \{(\pi/\theta_0) - 1\}\theta \leqq \pi - \theta_0$ since $\theta \leqq \theta_0$. Hence, using

$$\alpha^{-j} = r^{-j}(\cos(-j\theta) + i\sin(-j\theta)),$$

we get

(1) $\operatorname{Re}(\alpha^{-j}) \geqq 0 \quad \text{for } j = 1, 2, \dots, m',$

(2) $\operatorname{Re}(\alpha^{-j}) < 0 \quad \text{for } j = m' + 1, \dots, m,$

and

(3) $\operatorname{Im}(\alpha^{-j}) < 0 \quad \text{for } j = 1, \dots, m.$

Since $\theta_1 \geqq \theta_0$,

$$\tan(\pi - j\theta) \geqq \tan\theta_1 \geqq \tan\theta_0 = \{k/(b^2 - k)\}^{1/2}$$
$$\text{for } j = m' + 1, \dots, m.$$

Hence,

(4) $$|\operatorname{Im}(\alpha^{-j})| = r^{-j}\sin(\pi - j\theta)$$
$$\geqq r^{-j}\tan(\sin^{-1}(\sqrt{k}/b))\cos(\pi - j\theta)$$
$$= \{k/(b^2 - k)\}^{1/2}|\operatorname{Re}(\alpha^{-j})| \text{ for } j = m' + 1, \dots, m.$$

We consider

$$(5)\quad |f(\alpha)/\alpha^n| = \left|a_n + a_{n-1}\alpha^{-1} + \dots + a_{n-m}\alpha^{-m} + \sum_{j=m+1}^{n} a_{n-j}\alpha^{-j}\right|$$

where (in the case that $n < m$) we interpret a_{n-j} as zero for $j > n$ and the sum is zero if it is empty. Now if

$$|\mathrm{Re}(a_{n-m'-1}\alpha^{-m'-1} + \dots + a_{n-m}\alpha^{-m})| \leqq a_n - \gamma,$$

then we have by (1) and (5),

$$\begin{aligned}(6)\quad & |f(\alpha)/\alpha^n| \\ & \geqq |a_n + a_{n-1}\alpha^{-1} + \dots + a_{n-m}\alpha^{-m}| - \sum_{j=m+1}^{n} |a_{n-j}|\,|\alpha|^{-j} \\ & \geqq \mathrm{Re}(a_n + a_{n-1}\alpha^{-1} + \dots + a_{n-m}\alpha^{-m}) - \sum_{j=m+1}^{n} Br^{-j} \\ & > \mathrm{Re}(a_n + a_{n-1}\alpha^{-1} + \dots + a_{n-m'}\alpha^{-m'}) \\ & - |\mathrm{Re}(a_{n-m'-1}\alpha^{-m'-1} + \dots + a_{n-m}\alpha^{-m})| - \sum_{j=m+1}^{\infty} Br^{-j} \\ & \geqq \gamma - \{B/(r^m(r-1))\}.\end{aligned}$$

One easily checks that

$$\{k/(b^2 - k)\}^{1/2}(a_n - \gamma) = \gamma$$

so that, on the other hand, if

$$|\mathrm{Re}(a_{n-m'-1}\alpha^{-m'-1} + \dots + a_{n-m}\alpha^{-m})| > a_n - \gamma,$$

then we have by (2), (3), (4), and (5),

$$\begin{aligned}(7)\quad & |f(\alpha)/\alpha^n| \\ & > |a_n + a_{n-1}\alpha^{-1} + \dots + a_{n-m}\alpha^{-m}| - \sum_{j=m+1}^{\infty} Br^{-j} \\ & \geqq |\mathrm{Im}(a_{n-m'-1}\alpha^{-m'-1} + \dots + a_{n-m}\alpha^{-m})| - \sum_{j=m+1}^{\infty} Br^{-j} \\ & > \{k/(b^2 - k)\}^{1/2}(a_n - \gamma) - \sum_{j=m+1}^{\infty} Br^{-j} \\ & = \gamma - \{B/(r^m(r-1))\}.\end{aligned}$$

https://doi.org/10.4153/CJM-1988-013-6 Published online by Cambridge University Press

Thus, we see that in any case

$$|f(\alpha)/\alpha^n| > \gamma - \{B/(r^m(r - 1))\}.$$

Since

$$r \geqq b - \sqrt{k} \text{ and } B \leqq \gamma(b - \sqrt{k})^m(b - \sqrt{k} - 1),$$

we now get $|f(\alpha)| > 0$, a contradiction.

In the case that $m < m'$, (1) holds for $j \leqq m$, and hence, as in (6),

$$|f(\alpha)/\alpha^n| > a_n - \{B/(r^m(r - 1))\}$$
$$\geqq \gamma - \{B/(r^m(r - 1))\} > 0.$$

This completes the proof.

Comments. (1) For $k = 1$ in Theorem 5, one may replace the conclusion that $f(x)$ is irreducible over the rationals with the statement that $f(x)$ is irreducible over the integers.

(2) Theorem 5 can be used to test the irreducibility of an arbitrary polynomial if b is chosen sufficiently large and a translation is made so that the coefficients of the polynomial are non-negative.

(3) Note that in Theorem 5, γ is chosen so that

$$\gamma = a_n/(1 + \cot(\theta_1)).$$

A similar choice for γ will be made in the proof of our next theorem.

(4) Theorem 5 can be improved slightly by either of the following means:

(i) For $w \leqq \sqrt{k}$, $a_0, a_1, \ldots, a_{n-m-1}$ may be allowed to be negative but must in absolute value be $\leqq B$.

(ii) We may use instead of S the region D of Lemma 1 and take into account the fact that if

$$\alpha = re^{i\theta} \quad \text{with } \theta \simeq \sin^{-1}(\sqrt{k}/b),$$

then $|\alpha| > b - \sqrt{k} + C$ where C is small but possible to calculate via the law of cosines.

3. The case $b = 10$. In comment (4) (ii) of Section 2, we suggested a way of improving Theorem 5. We illustrate this by the following theorem.

THEOREM 6. *Let*

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbf{Z}[x]$$

be such that $f(10)$ *is a prime. If* $0 \leqq a_j \leqq a_n 10^{30}$ *for each* $j = 0, 1, \ldots, n - 1$, *then* $f(x)$ *is irreducible.*

https://doi.org/10.4153/CJM-1988-013-6 Published online by Cambridge University Press

Proof. We use ideas from the proof of Theorem 5. Here $b = 10$ and $k = 1$. Write $T = S_1 \cup S_2 \cup S_3$ where

$$S_1 = \{\alpha = re^{i\theta}: r \geqq 9.75,\ \pi/32 < |\theta| \leqq \sin^{-1}(1/10)\},$$

$$S_2 = \{\alpha = re^{i\theta}: r \geqq 9.64,\ \pi/33 < |\theta| \leqq \pi/32\},$$

and

$$S_3 = \{\alpha = re^{i\theta}: r \geqq 9,\ 0 \leqq |\theta| \leqq \pi/33\}.$$

Then $D = \{z: |10 - z| < 1\} \subset T$ so that we need only show for all $\alpha \in T$ we have $f(\alpha) \neq 0$. Assume for some $\alpha = re^{i\theta} \in T$ we have $f(\alpha) = 0$. We may take $\theta > 0$. As in (6) and (7), we can arrive at

$$(8) \quad |f(\alpha)/\alpha^n| > \gamma - \{B/(r^m(r - 1))\}.$$

Here the choice of m and γ depends on which set S_j, $j = 1, 2$, or 3, to which α belongs. For S_1 we may take $\gamma = a_n(0.035)$ and $m = 31$. For S_2 we may take $\gamma = a_n(0.089)$ and $m = 31$. For S_3 we may take $\gamma = a_n(0.087)$ and $m = 32$. In each case we may use (8) in conjunction with the inequalities on r in the definitions of S_j for $j = 1, 2$, and 3 to get with $B \leqq a_n 10^{30}$

$$|f(\alpha)| > 0,$$

giving a contradiction which completes the proof.

Comment. Theorem 5 also suggests generalizations of Theorem 4. Thus, for example, if $f(x)$ is a polynomial with non-negative coefficients which are $\leqq 5.79 \times 10^7$ and if $f(10) = wp$ for some $w \in \{1, 2, \dots, 9\}$ and p a prime, then $f(x)$ is irreducible over the rationals. As with the above theorem, improvements on this upper bound on the coefficients can be made.

4. Results depending on the degree of $f(x)$. We begin with the following:

LEMMA 2. *If $f(x) \in \mathbf{Z}[x]$ is of degree $n \geqq 1$ and has non-negative coefficients, then it has no zero in the sector*

$$S = \{z = \rho e^{i\phi}: \rho > 0,\ |\phi| < \pi/n\}.$$

Proof. Let $z = \rho e^{i\phi} \in S$. If z is real, then since $f(x)$ has non-negative coefficients, $f(z) \neq 0$. Suppose z is not real. Then either $\mathrm{Im}(z^j) > 0$ for all $j = 1, 2, \dots, n$ or $\mathrm{Im}(z^j) < 0$ for all $j = 1, 2, \dots, n$. In either case, we get that

$$|\mathrm{Im}(f(z))| > 0.$$

Thus, $f(z) \neq 0$, completing the proof.

We now show that if the degree of $f(x)$ is small enough in the results of the previous section, then no upper bound whatsoever is needed on the coefficients of $f(x)$ to deduce its irreducibility. More precisely, we show

THEOREM 7. *Let $b > 1$ be an integer, and let*

$$N_1 = \pi/\sin^{-1}(1/b).$$

If $f(x) \in \mathbf{Z}[x]$ is of degree $n < N_1$ and has non-negative coefficients and if $f(b)$ is prime, then $f(x)$ is irreducible.

Proof. Take $k = 1$ in Lemma 1. Note that

$$\{z:|b - z| \leqq 1\} \subset \{z = \rho e^{i\phi}:\rho > 0, |\phi| \leqq \sin^{-1}(1/b)\}$$
$$\subset \{z = \rho e^{i\phi}:\rho > 0, |\phi| < \pi/n\}.$$

By Lemma 2, $f(z)$ has no zeroes in $\{z:|b - z| \leqq 1\}$ so that by Lemma 1, $f(z)$ is irreducible.

Theorem 7 implies in the case that $b = 10$ that any polynomial $f(x) \in \mathbf{Z}[x]$ of degree $\leqq 31$ which has non-negative coefficients is irreducible if $f(10)$ is prime. We now prove a general result which shows that this is best possible. More precisely, when the choice $b = 10$ is taken in the following results, we can deduce that there is a polynomial $f(x) \in \mathbf{Z}[x]$ of degree 32 which has non-negative coefficients, is reducible, and is such that $f(10)$ is prime. Using methods related to this section, an explicit example of such an $f(x)$ is given in Section 5. This also establishes that the upper bound 167 in Theorem 3 (or 10^{30} in Theorem 6) cannot be omitted.

LEMMA 3. *If $g(x) \in \mathbf{Z}[x]$ has no non-negative real roots, then there is an $h(x) \in \mathbf{Z}[x]$ such that $g(x)h(x)$ has all positive coefficients.*

Proof. Suppose $g(x) \in \mathbf{Z}[x]$ has no non-negative real roots. Then the constant term of $g(x)$ is non-zero. Since $g(x)h(x)$ is to have positive coefficients, we consider only $h(x) \in \mathbf{Z}[x]$ with non-zero constant terms. Note that if

$$g(x)h(x) = \sum_{j=0}^{n} a_j x^j \in \mathbf{Z}[x]$$

has non-negative coefficients, then for a suitable positive integer d, we get that

$$g(x)h(x)(x^d + x^{d-1} + \ldots + 1)$$

has all positive coefficients. Thus, it suffices to show that for a given $g(x)$ as in the lemma, there is an $h(x) \in \mathbf{Z}[x]$ such that $g(x)h(x)$ has non-negative coefficients.

Furthermore, we need only show that there is an $h(x)$ with real coefficients such that $g(x)h(x)$ has non-negative coefficients; for suppose this has been shown. Then, as above, we may assume that all the coefficients of $g(x)h(x)$ are positive. Write

$$g(x) = \sum_{j=0}^{r} b_j x^j,$$

and let R be a positive integer such that $Rg(x)h(x)$ has all its coefficients greater than

$$\sum_{j=0}^{r} |b_j|.$$

Write

$$Rh(x) = \sum_{j=0}^{s} \gamma_j x^j,$$

and set $c_j = [\gamma_j]$ where [ ] denotes the greatest integer function. Let

$$H(x) = \sum_{j=0}^{s} c_j x^j \in \mathbf{Z}[x].$$

Then

$$g(x)H(x) = g(x)\left\{Rh(x) - \sum_{j=0}^{s} (\gamma_j - c_j)x^j\right\}$$

$$= Rg(x)h(x) - g(x)\left\{\sum_{j=0}^{s} (\gamma_j - c_j)x^j\right\}$$

which has all positive coefficients since each coefficient of

$$g(x)\left\{\sum_{j=0}^{s} (\gamma_j - c_j)x^j\right\}$$

is

$$\leqq \left(\sum_{j=0}^{r} |b_j|\right) \max_{0 \leqq j \leqq s} \{ |\gamma_j - c_j| \} < \sum_{j=0}^{r} |b_j|.$$

Thus, the lemma would be proven.

Write

$$g(x) = b_r \prod_{j=1}^{u} (x + \beta_j) \prod_{j=1}^{v} (x^2 - 2r_j(\cos \theta_j)x + r_j^2)$$

where b_r is an integer, $\beta_j > 0$ (for $j = 1, \ldots, u$), and $r_j > 0$ and $0 < \theta_j < \pi$ (for $j = 1, \ldots, v$). Let $\kappa = \rho e^{i\phi}$ and $\lambda = \rho e^{-i\phi}$ where $\rho > 0$ and $0 < \phi < \pi$. From the above, we need only show that for such κ and λ, there is an $h(x) \in \mathbf{R}[x]$ (depending on κ and λ) such that

$$(x - \kappa)(x - \lambda)h(x)$$

has all non-negative coefficients. Let s be the non-negative integer satisfying

$$(\pi/\phi) - 2 \leqq s < (\pi/\phi) - 1.$$

For $j = 0, 1, \ldots, s$, define

$$c_j = (\kappa^{s-j+1} - \lambda^{s-j+1})/(\kappa - \lambda).$$

Note that

$$c_j = \rho^{s-j} \sin(\,(s - j + 1)\phi)/\sin(\phi) > 0$$

for $j = 0, 1, \ldots, s$. Let

$$h(x) = \sum_{j=0}^{s} c_j x^j.$$

Then

$$\begin{aligned}(x - \kappa)(x - \lambda)h(x) &= (x^2 - (\kappa + \lambda)x + \kappa\lambda)h(x)\\ &= x^{s+2} - \frac{\kappa^{s+2} - \lambda^{s+2}}{\kappa - \lambda}x + \frac{\kappa^{s+1} - \lambda^{s+1}}{\kappa - \lambda}\kappa\lambda\\ &= x^{s+2} - \rho^{s+1}\frac{\sin(\,(s + 2)\phi)}{\sin \phi}x\\ &\quad + \rho^{s+2}\frac{\sin(\,(s + 1)\phi)}{\sin \phi}\end{aligned}$$

which, by our choice of s, has non-negative coefficients. This completes the proof.

Comments. (1) This Lemma follows from methods developed by Diamond and Essen [**2**] or from [**4**, Problem #A4]. Also, the corresponding result for real coefficients can be found in a paper by Meissner [**5**].

(2) The converse of the lemma clearly holds for a given $g(x) \in \mathbf{Z}[x]$.

LEMMA 4. *Let $b > 1$ be an integer and $N_2 = \pi/\tan^{-1}(1/b)$. Let n be the positive integer such that $N_2 \leqq n < N_2 + 1$. Then there is a polynomial of degree n with non-negative integer coefficients and with the coefficient of x positive which is divisible by $(x - b)^2 + 1$.*

Proof. Let $\rho = (b^2 + 1)^{1/2}$ and $\phi = \tan^{-1}(1/b)$. Note that

$$(x - b)^2 + 1 = (x - \kappa)(x - \lambda)$$

where $\kappa = \rho e^{i\phi}$ and $\lambda = \rho e^{-i\theta}$. Taking $h(x)$ as in the above proof gives a polynomial

$$f(x) = ((x - b)^2 + 1)h(x)$$

with non-negative coefficients of degree n. The previous proof describes how to modify $f(x)$ so as to obtain a polynomial of degree n which has non-negative integer coefficients and which is divisible by $(x - b)^2 + 1$. In this case, however, $f(x)$ already has integer coefficients. Furthermore, the coefficient of x in $f(x)$ is

$$-\rho^{n-1} \sin(n\phi)/(\sin \phi).$$

For $b \geqq 2$, one can show that N_2 is not a integer. Thus $\pi = N_2\phi < n\phi < (N_2 + 1)\phi = \pi + \phi < 2\pi$ so that the coefficient of x in $f(x)$ is non-zero, completing the proof.

THEOREM 8. *Let $b > 1$ be an integer. Let*

$$N_1 = \pi/\sin^{-1}(1/b) \quad \text{and} \quad N_2 = \pi/\tan^{-1}(1/b).$$

For any integer $n < N_1$, there does not exist a reducible polynomial $f(x) \in \mathbf{Z}[x]$ of degree n having non-negative coefficients for which $f(b)$ is prime. On the other hand, for any integer $n \geqq N_2$, there exist infinitely many reducible $f(x) \in \mathbf{Z}[x]$ of degree n with non-negative coefficients for which $f(b)$ is prime.

Proof. The first part of Theorem 8 is an immediate consequence of Theorem 7. Now, suppose $n \geqq N_2$, and note that this implies $n \geqq 3$. Let $g(x) = (x - b)^2 + 1$. Let m be the integer satisfying $N_2 \leqq m < N_2 + 1$. By Lemma 4, there is a polynomial $u(x) \in \mathbf{Z}[x]$ such that $g(x)u(x)$ is of degree m, has non-negative coefficients, and has a non-zero coefficient of x. Clearly, $n \geqq m$. Let

$$h(x) = u(x)(x^{n-m} + \ldots + x + 1).$$

Then $g(x)h(x)$ is of degree n, has non-negative coefficients, and has non-zero constant term. Let

$$w(x) = 2bh(x) + 1.$$

Since the coefficients of $g(x)h(x)$ are non-negative and the coefficient for x is non-zero, the coefficient of x in $g(x)h(x)$ must be at least 1; hence, $g(x)w(x)$ has non-negative coefficients. Also,

$$h(b) = g(b)h(b) > 0 \text{ and } w(b) = 2bh(b) + 1 > 0.$$

Now, $h(b)$ and $w(b)$ are relatively prime, so every sufficiently large integer is of the form $ch(b) + dw(b)$ for some c and d positive integers. In particular, there is a prime p such that for some positive integers c and d, $ch(b) + dw(b) = p$. Set

$$f(x) = g(x)(ch(x) + dw(x)).$$

Here, $f(x)$ is reducible, has all non-negative coefficients, and is such that $f(b) = p$, a prime. Since there are infinitely many choices for the prime p, we get that there are infinitely many choices for $f(x)$, finishing the proof of the theorem.

5. Concluding remarks. In this section, several results are discussed without proof. The proofs depend on elementary results about uniform distribution, on results about simple continued fractions, on the results contained in the previous sections of this paper, and on more advanced results concerning gaps between consecutive primes.

For almost all positive integers b, one can show that there are no integers between

$$N_1 = \pi/\sin^{-1}(1/b) \text{ and } N_2 = \pi/\tan^{-1}(1/b).$$

In such cases, we will say that Theorem 8 is sharp. For example, Theorem 8 is sharp when $b = 10$. In this case, Theorem 8 implies that if $f(x) \in \mathbf{Z}[x]$ has non-negative coefficients, is of degree $\leqq 31$, and is such that $f(10)$ is prime, then $f(x)$ is irreducible; on the other hand, there exist reducible polynomials $f(x) \in \mathbf{Z}[x]$ with non-negative coefficients of degree 32 such that $f(10)$ is prime. There are, however, infinitely many choices for a positive integer b for which Theorem 8 is not sharp. For example, one can show that Theorem 8 is not sharp whenever $b > 1$ is chosen to be the denominator of an odd convergent to the simple continued fraction for π. The $b \leqq 10000$ for which Theorem 8 is not sharp are 6, 7, 14, 21, 28, and $113k$ where $k \in \{1, 2, \dots, 17\}$.

Let b be a positive integer, and suppose Theorem 8 is sharp for b; thus, there is no integer between N_1 and N_2. Let $n = [N_1] + 1$. Let $f(x) \in \mathbf{Z}[x]$ be a reducible polynomial of degree n given by Theorem 8. Then for b sufficiently large, it is possible to show that

$$f(x) = (x^2 - 2bx + (b^2 + 1))h(x)$$

where $h(x) \in \mathbf{Z}[x]$ is irreducible and has all positive coefficients. In particular, for $b = 10$, this result is true.

An explicit example of a reducible polynomial $f(x) \in \mathbf{Z}[x]$ of degree 32 for which $f(10)$ is prime is given by

$$f(x) = x^{32} + 130x^2 + 5603286754010141567161572637720x$$
$$+ 61091041047613095559860106059529.$$

Thus, the upper bound 10^{30} on the coefficients in Theorem 6 cannot be replaced by 6.2×10^{31}. The above example was arrived at in the following manner. Let $g(x) = x^2 - 20x + 101$, and let $h(x)$ be the polynomial given in the proof of Lemma 4. The coefficient of x in $g(x)h(x)$ is, in this case, large enough so that $f_k(x) = g(x)h(x) + kg(x)$ has non-negative coefficients for every non-negative integer $k \leqq 2.8 \times 10^{29}$. On the other hand, $f_k(x)$ is reducible and is such that $f_k(10) = h(10) + k$. A search for a prime of the form $h(10) + k$ was made. Such a prime was found when $k = 130$ giving the above example. In general, let

$$g(x) = x^2 - 2bx + (b^2 + 1).$$

The polynomial $f(x) = g(x)h(x)$ constructed in Lemma 4 may have a small coefficient for x, so a different choice for $f_k(x)$ is necessary in the above idea. For example, one could set

$$f_k(x) = kg(x) + g(x)h(x)(x + 1)$$

and proceed as above. Let $\epsilon > 0$, and let b be sufficiently large (depending on ϵ). Let n be as in Lemma 4. Then the above choice for $f_k(x)$ gives an example of a reducible polynomial $f(x) \in \mathbf{Z}[x]$ with non-negative coefficients bounded by $(1 + \epsilon)b^n$ such that $f(b)$ is prime. The success of this method depends on results about gaps between primes. One can thus show that for b sufficiently large, the upper bound for the coefficients in Theorem 5 cannot be replaced by $(1 + \epsilon)b^n$.

In conclusion, the author would like to thank Professor David Boyd and Professor Harold Diamond for some helpful suggestions throughout the paper.

References

1. J. Brillhart, M. Filaseta and A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Can. J. Math. *33* (1981), 1055-1059.
2. H. Diamond and M. Essen, *Functions with non-negative convolutions*, J. Math. Anal. and Appl. *63* (1978), 463-489.
3. M. Filaseta, *A further generalization of an irreducibility theorem of A. Cohn*, Can. J. Math. *34* (1982), 1390-1395.
4. J. McKay, *The William Lowel Putnam mathematical competition*, Amer. Math. Monthly *80* (1973), 170-178.
5. E. Meissner, *Über positive Darstellungen von Polynomen*, Math. Ann. *70* (1911), 223-235.
6. O. Ore, *Einige Bemerkungen über Irreduzibilität*, Jahresbericht Der Deutschen Mathematiker-Vereinigung *44* (1934), 147-151.
7. G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis* (Springer-Verlag, Berlin, 1964).

University of South Carolina,
Columbia, South Carolina