Can. J. Math., Vol. XXXIII, No. 5, 1981, pp. 1055–1059

ON AN IRREDUCIBILITY THEOREM OF A. COHN

JOHN BRILLHART, MICHAEL FILASETA AND ANDREW ODLYZKO

1. Introduction. In [**1**, b.2, VIII, 128] Pólya and Szegö give the following interesting result of A. Cohn:

THEOREM 1. *If a prime p is expressed in the decimal system as*

$$p = \sum_{k=0}^{n} a_k 10^k, \quad 0 \leqq a_k \leqq 9,$$

then the polynomial $\sum_{k=0}^{n} a_k x^k$ is irreducible in $\mathbf{Z}[x]$.

The proof of this result rests on the following theorem of Pólya and Szegö [**1**, b.2, VIII, 127] which essentially states that a polynomial $f(x)$ is irreducible if it takes on a prime value at an integer which is sufficiently far from the zeros of $f(x)$.

THEOREM 2. *Let $f(x) \in \mathbf{Z}[x]$ be a polynomial with the zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$. If there is an integer b for which $f(b)$ is a prime, $f(b-1) \neq 0$, and* Re $(\alpha_i) < b - \frac{1}{2}$ *for $1 \leqq i \leqq n$, then $f(x)$ is irreducible in $\mathbf{Z}[x]$.*

Proof. Assume that $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbf{Z}[x]$, and deg g, deg $h \geqq 1$. If α_j are the zeros of $g(x)$, then Re $(\alpha_j) < b - \frac{1}{2}$. If $g(x)$ is factored over the complex field, it follows readily that $g(x + b - \frac{1}{2})$ has no missing terms and all the terms have the same sign. Also, the coefficients of $g(-x + b - \frac{1}{2})$ are strictly alternating. Thus,

$$|g(b - \tfrac{1}{2} - t)| < |g(b - \tfrac{1}{2} + t)| \quad \text{for any } t > 0.$$

For $t = \frac{1}{2}$, $|g(b-1)| < |g(b)|$, and since $g(b-1) \in \mathbf{Z}$ and $g(b-1) \neq 0$, it follows that $|g(b-1)| \geqq 1$ and $|g(b)| \geqq 2$. By the same agrument, it also follows that $|h(b)| \geqq 2$, which contradicts the assumption that $f(b)$ is a prime.

In this paper we obtain an irreducibility result (Theorem 3), which is derived from Theorem 2, for polynomials whose first three coefficients are non-negative. The new feature in this result is the lower bound for the integer b in Theorem 2 which is computed from the coefficient of $f(x)$. This theorem is then used to prove the generalization of Theorem 1 in

Received December 7, 1979 and in revised form May 12, 1981.

which the base 10 is replaced by any integral base $b \geqq 2$. We also discuss how these theorems can be used to test a given polynomial for irreducibility.

2. Generalizations and applications. In the next theorem a polynomial is given and conditions are derived for its irreducibility. In the corollaries that follow, a prime is given from which a polynomial is derived that is then shown to be irreducible.

THEOREM 3. *Let*

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

be a polynomial with $a_n > 0$, $a_{n-1} \geqq 0$, *and* $a_{n-2} \geqq 0$. *Let* $m = \max\{|a_k|/a_n\}$ *for* $0 \leqq k \leqq n-2$,

$$r_1 = (1 + \sqrt{4m+1})/2, \quad \text{and}$$
$$r_2 = [(s + \sqrt{s^2-4})/54]^{1/3} + [(s - \sqrt{s^2-4})/54]^{1/3} + \tfrac{1}{3},$$

where $s = 27m + 2$. *If there is an integer*

$$b > \max\{r_1/\sqrt{2}, r_2\} + \tfrac{1}{2}$$

for which $f(b)$ *is a prime and* $f(b-1) \neq 0$, *then* $f(x)$ *is irreducible in* $\mathbf{Z}[x]$.

Proof. We observe first that $r_1 \geqq 1$ and $r_2 \geqq 1$. Let

$$A = \{z \in \mathbf{C}: \operatorname{Re}(z) \leqq \max\{r_1/\sqrt{2}, r_2\}\}.$$

We will show that all the zeros of f lie in A by proving that $|f(z)| > 0$ for $z \in A^c$, the complement of A.

Let A^c be partitioned into the two sets $A^c \cap B$ and $A^c \cap B^c$, where

$$B = \{z \in \mathbf{C}: \operatorname{Re}(z) < 0 \text{ or } |z| \leqq r_1\}.$$

If $z \in A^c \cap B^c$, then $\operatorname{Re}(1/z) > 0$ and

$$\left|\frac{f(z)}{z^n}\right| \geqq \left|a_n + \frac{a_{n-1}}{z}\right| - \sum_{k=2}^{n} \frac{|a_{n-k}|}{|z|^k} > \operatorname{Re}\left(a_n + \frac{a_{n-1}}{z}\right) - \sum_{k=2}^{\infty} \frac{ma_n}{|z|^k}$$
$$\geqq a_n - \frac{ma_n}{|z|^2 - |z|} = \frac{a_n(|z|^2 - |z| - m)}{|z|^2 - |z|} > 0,$$

since $|z| > r_1$, the positive zero of $x^2 - x - m$.

If $z \in A^c \cap B$, then $|\arg(z)| < \pi/4$, so $\operatorname{Re}(1/z)$ and $\operatorname{Re}(1/z^2)$ are $\geqq 0$. Thus,

$$\left|\frac{f(z)}{z^n}\right| > \operatorname{Re}\left(a_n + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2}\right) - \sum_{k=3}^{\infty} \frac{ma_n}{|z|^k} \geqq a_n - \frac{ma_n}{|z|^3 - |z|^2}$$
$$= \frac{a_n(|z|^3 - |z|^2 - m)}{|z|^3 - |z|^2} > 0,$$

https://doi.org/10.4153/CJM-1981-080-0 Published online by Cambridge University Press

since $|z| > r_2$, the positive zero of $x^3 - x^2 - m$. Thus, the hypotheses of Theorem 2 are satisfied for the integer b, which proves the theorem.

Remarks. 1. It should be noted that the size of a_{n-1} does not enter into Theorem 3.

2. In the part of the proof of Theorem 3 where $z \in A^c \cap B^c$, the stronger statement that $|f(z)| > 0$ for any $z \in B^c$ is actually true, though not necessary to the proof.

COROLLARY 1. *Let $b \geqq 2$ be an integer and let $B = 1$ if $b = 2$ and $B = [(2b - 1)(2b - 1 - \sqrt{2})/2]$ if $b \geqq 3$, where the brackets are the greztest integer function. Also, let a prime p be expressed as*

$$p = \sum_{k=0}^{n} a_k b^k,$$

where $a_n > 0$, $a_{n-1} \geqq 0$, $a_{n-2} \geqq 0$, and $|a_k|/a_n \leqq B$ for $0 \leqq k \leqq n - 2$, and define

$$f(x) = \sum_{k=0}^{n} a_k x^k.$$

If $f(b - 1) \neq 0$, then $f(x)$ is irreducible in $\mathbf{Z}[x]$.

Proof. Since all of the hypotheses of Theorem 3 except one are given, it is only necessary to show that

$$b > \max \{r_1/\sqrt{2}, r_2\} + \tfrac{1}{2}.$$

Let r_1^* and r_2^* be the positive zeros of $x^2 - x - B$ and $g(x) = x^3 - x^2 - B$, respectively. Then, since $m \leqq B$, we have that $r_1 \leqq r_1^*$ and $r_2 \leqq r_2^*$. Thus, we have only to show

$$b > \max \{r_1^*/\sqrt{2}, r_2^*\} + \tfrac{1}{2}.$$

Now, $r_1^*/\sqrt{2}$ is a zero of $h(x) = 2x^2 - \sqrt{2}x - B$. Since

$$h(b - \tfrac{1}{2}) = \tfrac{1}{2}(2b - 1)(2b - 1 - \sqrt{2}) - B > 0$$

and

$$g(b - \tfrac{1}{2}) = (b - \tfrac{1}{2})^2(b - \tfrac{3}{2}) - B > 0$$

for $b \geqq 2$, we then have that

$$b - \tfrac{1}{2} > \max \{r_1^*/\sqrt{2}, r_2^*\}.$$

Remark. We observe that the bound B is a quadratic function of b. Thus, say, for the bases $b = 2, 3, 4, 5, 10, 50$, and 100, the corresponding values of B are $1, 8, 19, 34, 167, 4830$, and 19659.

We can now give a simple and direct generalization of Theorem 1.

https://doi.org/10.4153/CJM-1981-080-0 Published online by Cambridge University Press

COROLLARY 2. *If a prime p is expressed in the number system with base $b \geqq 2$ as*

$$p = \sum_{k=0}^{n} a_k b^k, \quad 0 \leqq a_k \leqq b - 1,$$

then the polynomial $\sum_{k=0}^{n} a_k x^k$ is irreducible in $\mathbf{Z}[x]$.

Proof. This follows directly from Corollary 1.

Example. Let $p = 397$. If we express p to various bases $b \geqq 2$, we obtain the following collection of irreducible polynomials:

p	Irreducible Polynomials
110001101_2	$x^8 + x^7 + x^3 + x^2 + 1$
112201_3	$x^5 + x^4 + 2x^3 + 2x^2 + 1$
12031_4	$x^4 + 2x^3 + 3x + 1$
3042_5	$3x^3 + 4x + 2$
1501_6	$x^3 + 5x^2 + 1$
1105_7	$x^3 + x^2 + 5$
615_8	$6x^2 + x + 5$
.	.
.	.
.	.

It is clear from the fact that the first three coefficients of $f(x)$ must be non-negative that Theorem 3 cannot be used to test the irreducibility of any polynomial. Accordingly, we prove the following theorem which has a more restrictive condition on the size of the coefficients but can be used to test any polynomial.

THEOREM 4. *Let $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbf{Z}[x]$ be a polynomial with $a_n > 0$ and $a_{n-1} \geqq 0$. If there exists an integer $b \geqq 2$ for which $f(b)$ is a prime, $f(b-1) \neq 0$, and $|a_k|/a_n \leqq (4b^2 - 8b + 3)/4$ for $0 \leqq k \leqq n - 2$, then $f(x)$ is irreducible in $\mathbf{Z}[x]$.*

Proof. Let $A = \{z \in \mathbf{C}: |z| < b - \frac{1}{2}\}$. If $z \in A^c$, then

$$\left| \frac{f(z)}{z^n} \right| > \operatorname{Re}\left(a_n + \frac{a_{n-1}}{z}\right) = \sum_{k=2}^{\infty} \frac{a_n(4b^2 - 8b + 3)/4}{|z|^k}$$

$$\geqq a_n - \frac{a_n(b^2 - 2b + \frac{3}{4})}{|z|^2 - |z|} = \frac{a_n[|z| - (b - \frac{1}{2})][|z| + (b - \frac{3}{2})]}{|z|^2 - |z|} \geqq 0.$$

Thus, the zeros α_i of $f(z)$ are all in A, so $\operatorname{Re}(\alpha_i) < b - \frac{1}{2}$ and $f(x)$ is irreducible by Theorem 2.

Remarks. 1. It should be noted that Theorem 4 omits the possibility of testing a polynomial in the very special case $a_n = 1$ and $b = 2$.

2. Any polynomial $f(x)$ can be tested by Theorem 4 since one of $\pm f(x)$ or $\pm f(-x)$ will have two non-negative leading coefficients. For example, let $f(x) = 2x^3 - 5x^2 + 107$. Since $-f(-x) = 2x^3 + 5x^2 - 107$, $-f(-9) \neq 0$, and $-f(-10) = 2393$ is a prime, then $f(x)$ is irreducible.

3. The above theorems will not always be successful in demonstrating the irreducibility of an irreducible polynomial, even if the size of the numbers involved is not too large. This is because irreducible polynomials exist which take no prime value at integral arguments. A simple example is $x^2 + x + 4$, which is irreducible, but for integral x is even and is never equal to ± 2. A more general example is $x^p + (p - 1)x + 6p$, where p is a prime $\equiv 1 \pmod{35}$. (Also see [**1**, b. 2, VIII, 120].)

4. The transformation $x = ay$ can sometimes aid in showing irreducibility. For example, using Theorem 4 with $f(x) = x^3 - x + 59$, we have $f(7) \neq 0$ and $f(8) = 563$, a prime. However, 59 exceeds the size of the coefficients allowed in Theorem 4 with base $b = 8$. If we set $x = 2y$, then $g(y) = f(2y) = 8y^3 - 2y + 59$, so $g(3) \neq 0$, $g(4) = 563$, and the bound on the coefficients is now 70, with permits 59. Thus, $f(x)$ is irreducible.

5. The reciprocal polynomial $x^n f(1/x)$ may sometimes aid in either increasing the size of the coefficients or in searching for prime values of $f(x)$.

6. In searching for prime values of $f(x)$, certain values of $f(x)$ do not need to be considered because they are known to be composite; for, if p is a prime divisor of $f(x_0)$, then p divides $f(x_0 + kp)$, $k \in \mathbf{Z}$, so $f(x_0 + kp)$ will be composite if $f(x_0 + kp) \neq \pm p$. The possibility that $f(x_0 + kp) = \pm p$ can be settled at the outset by noting that $f(x)$ is an increasing function to the right of the maximal real part of its zeros.

References

1. G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis* (Springer-Verlag, Berlin, 1964).

The University of Arizona,
Tucson, Arizona;
Bell Telephone Laboratories,
Murray Hill, New Jersey