Can. J. Math., Vol. XXXIV, No. 6, 1982, pp. 1390–1395

A FURTHER GENERALIZATION OF AN IRREDUCIBILITY THEOREM OF A. COHN

MICHAEL FILASETA

Let $d_n d_{n-1} \ldots d_0$ be the b-ary representation of a positive integer N. Call $f(x) = \sum_0^n d_k x^k$ the polynomial obtained from N base b. In the case the base is 10, $f(x)$ will be called the polynomial obtained from N. Pólya and Szegö attribute the following theorem to A. Cohn [**2**, b. 2, VIII, 128]:

THEOREM 1. *A polynomial obtained from a prime is irreducible.*

This theorem was generalized in two different ways by John Brillhart, Andrew Odlyzko, and myself [**1**]. One way was by proving the theorem remains true regardless of the base being used. The second way was by permitting the coefficients of $f(x)$ to be different from digits. Thus, for example, if $f(x) = \sum_0^n d_k x^k$, where $0 \leqq d_k \leqq 167$ for all k, and if $f(10)$ is prime, then $f(x)$ is irreducible. In this paper, Theorem 1 will be generalized in another way by considering composite N. In particular, the following two results will be proven:

THEOREM 2. *Let $f(x)$ be a polynomial obtained from wp base b, where w and b are positive integers, $w < b$, and p is a prime. Then $f(x)$ is irreducible over the rational numbers.*

THEOREM 3. *Let $f(x)$ be a polynomial obtained from wp, where w is a positive integer $\leqq 90$ and p is a prime. Suppose $f(x) = g(x)h(x)$, where $g(x)$ and $h(x) \in \mathbf{Z}[x]$ having positive leading coefficients. If $w \neq 73$, 82, 83, 84, or 85, then $g(x)$ or $h(x)$ is a polynomial obtained from a divisor of w and therefore of degree $\leqq 1$. If $w = 73$, 82, 83, 84, or 85, then either $g(x)$ or $h(x)$ is a quadratic depending only on w or $g(x)$ or $h(x)$ is a polynomial obtained from a divisor of w.*

We first begin with the case of a general base b, then turn to the case $b = 10$, and finally discuss an irreducibility test for small degree polynomials.

1. To prove Theorem 2, we shall make use of a lemma (for a proof, see the proof of Theorem 3 in [**1**]).

Received January 4, 1982.

LEMMA. *Let* $f(x) = \sum_0^n d_k x^k \in \mathbf{Z}[x]$, *where* $d_n > 0$, $d_{n-1} \geqq 0$, *and* $d_{n-2} \geqq 0$. *Let*

$$m = \max_{k \leqq n-2} \{|d_k|/d_n\},\ r_1 = (1 + \sqrt{4m+1})/(2\sqrt{2}),\ \textit{and}$$
$$r_2 = \{(s + \sqrt{s^2 - 4})/54\}^{1/3} + \{(s - \sqrt{s^2-4})/54\}^{1/3} + 1/3,$$

where $s = 27m + 2$. *Then each zero* α *of* $f(x)$ *satisfies*

$$\mathrm{Re}\ (\alpha) < \max\ \{r_1, r_2\}.$$

The lemma can be made more explicit by noting

$$(*) \quad \max\ \{r_1, r_2\} = \begin{cases} r_1 \text{ if } m \geqq 4 + 3\sqrt{2} \\ r_2 \text{ if } m < 4 + 3\sqrt{2}. \end{cases}$$

(*) is shown by using the fact that r_2 is the positive zero of $g(x) = x^3 - x^2 - m$. Since $g(r_1) \geqq 0$ precisely when $m \geqq 4 + 3\sqrt{2}$, (*) follows.

For the proof of Theorem 2, write $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are polynomials in $\mathbf{Z}[x]$ having positive leading coefficients, $h(x)$ is irreducible, $p|h(b)$, and consequently $g(b)|w$. Suppose

$$g(x) = a_r x^r + a_{r-1}x^{r-1} + \ldots + a_0,$$

with $a_r > 0$. Now we consider two cases.

Case 1. $b \geqq 4$.

One checks directly by use of the lemma and (*) with $m = b - 1$ that if $b \geqq 4$, then each zero α of $f(x)$ satisfies $\mathrm{Re}\ (\alpha) < b - \sqrt{b}$. Then for each zero α of $g(x)$, $\mathrm{Re}\ (\alpha) < b - \sqrt{b}$ so that $g(x + b - \sqrt{b})$ has positive real coefficients. Thus,

$$g(x + b - \sqrt{b}) \geqq a_r x^r \quad \text{for all } x \geqq 0.$$

Take $x = \sqrt{b}$ to get $g(b) \geqq a_r b^{r/2}$. Now, $g(b) \leqq w < b$ so that $r = 0$ or 1. We want to show $r = 0$, so assume $r = 1$. Then $g(x) = a_1 x + a_0$ where $a_1 > 0$. But $f(x)$ has nonnegative coefficients so that $f(x)$ and therefore $g(x)$ have no positive real zeroes. Thus, $a_0 \geqq 0$ and $g(b) \geqq a_1 b \geqq b$, giving a contradiction.

Case 2. $b = 2$ or 3.

The case $b = 2$ follows from the generalization of Cohn's Theorem to an arbitrary base [**1**].

For $b = 3$, the lemma shows that each zero α of $g(x)$, being a zero of $f(x)$, satisfies $\mathrm{Re}\ (\alpha) < 1.7$ so that $g(x + 1.7) \geqq a_r x^r$ for all $x \geqq 0$. This gives $g(3) \geqq a_r(1.3)^r$ so that $r \leqq 2$. If $r = 0$, then we're through. If $r = 1$, then as in Case 1, $a_0 \geqq 0$ and $g(3) \geqq 3$, giving a contradiction. So assume $r = 2$. Then $g(3) \geqq a_2(1.3)^2$ so $a_2 = 1$. Also, $a_0 \neq 0$ since $g(3) \not\equiv 0 \pmod 3$. But a_0 divides the constant term of $f(x)$, and since $f(x)$ has no positive real zeroes, $a_0 \geqq 0$. Thus, $a_0 = 1$ or 2. Now,

$$g(x + 1.7) = x^2 + (3.4 + a_1)x + (2.89 + 1.7a_1 + a_0) \in \mathbf{R}^+[x]$$

so $a_1 > -3.4$. Also,

$$g(3) = 9 + 3a_1 + a_0 \leqq w \leqq 2$$

so

$$a_1 \leqq (-7 - a_0)/3 \leqq -2.6.$$

Therefore, $a_1 = -3$, and $g(x) = x^2 - 3x + 1$ or $g(x) = x^2 - 3x + 2$. Both of these choices for $g(x)$ have a positive real zero, giving a contradiction.

2. For $b = 10$ the lemma in the previous section gives an upper bound of ≈ 2.504 for the real part of a zero of $f(x)$. The actual bound can be sharpened to <2.5 by using methods similar to those used in [**1**]. The bound 2.5 isn't necessary to obtain the results of this section but will be used for convenience.

In Theorem 3 let $h(x)$ be such that $p|h(10)$ and write

$$g(x) = a_r x^r + a_{r-1}x^{r-1} + \ldots + a_0,$$

with $a_r > 0$. If $r < 2$, then $g(x) = a_1 x + a_0$ where both a_1 and a_0 are digits (base 10). Thus, $g(x)$ is a polynomial obtained from $g(10)$, a divisor of w.

Now, suppose $r \geqq 2$. Since $g(10) \geqq a_r(7.5)^r > 421$ for $r \geqq 3$, $r = 2$. Thus, $g(x) = a_2 x^2 + a_1 x + a_0$ and

$$g(x + 2.5) = a_2 x^2 + (5 + a_1)x + (6.25 + 2.5a_1 + a_0) \in \mathbf{R}^+[x].$$

This gives $g(10) \geqq a_2(7.5)^2$. Since $g(10) \leqq 90$, $a_2 = 1$. Also, $5 + a_1 > 0$ so $a_1 \geqq -4$. Therefore, $g(10) \geqq (7.5)^2 + (7.5) = 63.75$, proving Theorem 3 for $w \leqq 63$.

For any $w \leqq 90$, we have $g(10)|w$ and $g(10) > 63$ so $g(10) = w$. If $w = c_1 10 + c_0$ where c_1 and c_0 are digits, then

$$g(10) \equiv a_0 (\text{mod } 10) \text{ and } w \equiv c_0 (\text{mod } 10)$$

so $a_0 = c_0$ and consequently $a_1 = c_1 - 10$. Thus, $g(x)$ is a quadratic depending only on w, proving Theorem 3 for $w = 73$, 82, 83, 84, and 85.

It remains to show that for the remaining $w \leqq 90$ in Theorem 3 the corresponding quadratic $g(x)$ is not a possible factor of $f(x)$. We give an example of three possible procedures which may be used to handle the remaining w:

(i) For $w = 64$, $g(x) = x^2 - 4x + 4 = (x - 2)^2$ so $g(x)$ has a positive real zero and cannot be a factor of $f(x)$.

(ii) For $w = 78$, $g(x) = x^2 - 3x + 8$. Let $z = (3 + \sqrt{23}i)/2$ so that $g(z) = 0$. Then $|z| = \sqrt{8}$ and $\theta = \arg(z) \approx 1.012$. If $f(x) = \sum_0^n d_k x^k$,

https://doi.org/10.4153/CJM-1982-097-3 Published online by Cambridge University Press

then

$$\left|\frac{f(z)}{z^n}\right| \geqq \operatorname{Re}\left(d_n + \frac{d_{n-1}}{z} + \ldots + \frac{d_{n-7}}{z^7}\right) - \sum_8^n \frac{d_{n-k}}{|z|^k}$$

$$> 1 + 9\cos 2\theta/8 + 9\cos 3\theta/8^{3/2} + 9\cos 4\theta/8^2 - \sum_8^\infty \frac{9}{8^{k/2}}$$

$$\approx 0.022 > 0.$$

This means $f(z) \neq 0$ so $g(x) \nmid f(x)$.

(iii) For $w = 86$, suppose $f(x) = g(x)h(x)$ where

$$g(x) = x^2 - 2x + 6 \quad \text{and} \quad h(x) = \sum_0^{n-2} b_k x^k.$$

Then $b_{n-3} \geqq 2$. Let t be such that $|b_t| \geqq 2$ and $|b_j| \leqq 1$ for $j < t$. If $b_t \geqq 2$, then

$$9 \geqq 6b_t - 2b_{t-1} + b_{t-2} \geqq 12 - 2 - 1 = 9$$

so $b_{t-1} = 1$ and $b_{t-2} = -1$. Also,

$$0 \leqq 6b_{t-2} - 2b_{t-3} + b_{t-4} \leqq -6 + 2 + 1 = -3,$$

giving a contradiction. If $b_t \leqq -2$, then

$$0 \leqq 6b_t - 2b_{t-1} + b_{t-2} \leqq -12 + 2 + 1 = -9,$$

giving a contradiction.

Comments. (1) For $w = 82$ and $p = 122321$, the polynomial obtained from wp has a quadratic factor. Similarly, for $w = 83$ and $p = 121333$, and for $w = 84$ or 85 and $p = 12211$. The author knows of no example for $w = 73$.

(2) The results of this section may be extended to $w > 90$. For example, if $91 \leqq w \leqq 99$ and $f(x)$ is the polynomial obtained from wp for some prime p, then $g(x)$ or $h(x)$ is a quadratic depending only on w or $g(x)$ or $h(x)$ is a polynomial obtained from a divisor of w. Furthermore, the quadratic occurs as a factor when $p = 11$. Also, for $w = 100 + c_1 10 + c_0 \leqq 150$, where c_1 and c_0 are digits, and for any prime p, if the polynomial $f(x)$ has no rational zeroes and if $x^2 + c_1 x + c_0$ is not a divisor of $f(x)$ in $\mathbf{Z}[x]$, then $f(x)$ is irreducible over the rationals.

(3) A result of a slightly different flavor is the following: If p and q are primes such that $p \not\equiv 1 \pmod{10}$ and $q \not\equiv 1, 2$, or $3 \pmod{10}$, then the polynomial $f(x)$ obtained from pq is irreducible. To show this, assume $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbf{Z}[x]$ with positive leading coefficients and $g(x) \not\equiv 1$ and $h(x) \not\equiv 1$. If $g(10) = 1$, then $g(x + 7)$ having positive integral coefficients guarantees that $g(x) \equiv 1$, a contradiction. Thus, $g(10) > 1$ and similarly $h(10) > 1$. We may take

https://doi.org/10.4153/CJM-1982-097-3 Published online by Cambridge University Press

$g(10) = p$ and $h(10) = q$. Write

$$g(x) = \sum_0^r a_k x^k \quad \text{and} \quad h(x) = \sum_0^{n-r} b_k x^k.$$

Then $a_0 \equiv g(10) = p \pmod{10}$ and $b_0 \equiv h(10) = q \pmod{10}$. Since $f(x)$ has no positive real zeroes, $a_0 \geqq 0$ and $b_0 \geqq 0$. The conditions $p \not\equiv 1 \pmod{10}$ and $q \not\equiv 1, 2$, or $3 \pmod{10}$ imply $a_0 \geqq 2$ and $b_0 \geqq 5$. This contradicts $a_0 b_0$ being the constant term of $f(x)$, i.e., a digit.

(4) Some simple but similar results on irreducibility can be made if we restrict the degree of $f(x)$ to being small. For example, if $f(x)$ is any quadratic with positive integral coefficients which takes on a prime value at any positive integer, then $f(x)$ is irreducible. This same result holds true if $f(x)$ is a cubic rather than a quadratic but for no higher degree.

(5) Some interesting results for decimal representation of wp can be obtained by looking at bases other than 10. For example, Theorem 2 with $b = 100$ shows that since $73 \cdot 85711 = 6256903$, where 85711 is prime, $f(x) = 6x^3 + 25x^2 + 69x + 3$ is irreducible.

3. At the beginning of this paper two generalizations of Theorem 1 were mentioned where only prime values at integral arguments are taken into consideration. These generalizations can be used as an irreducibility test for a polynomial $f(x)$, but they fail to give any information when $f(x)$ is an irreducible polynomial which never takes on a prime value at an integral argument as is the case, for example, when $f(x) = x^2 + x + 4$. The results in this paper, however, are somewhat stronger. Theorem 2 shows that for $f(x) = x^2 + x + 4$, $f(x)$ is irreducible since $f(5) = 2 \cdot 17$. But one should note that if the degree of a polynomial $f(x)$ is large, one must be prepared in what follows to deal with large values of $f(x)$ at integral arguments. We are now ready to give an irreducibility test via a theorem.

THEOREM 4. *Let $f(x) = \sum_0^n d_k x^k \in \mathbf{Z}[x]$ such that $d_n > 0$ and $d_{n-1} \geqq 0$. Suppose $f(x)$ has no rational roots. Set*

$$m = (\max_{k \leqq n-2} \{|d_k|\})/d_n \text{ and}$$
$$B = (1 + \sqrt{4m + 1})/2.$$

If for any integer $b \geqq B$, $f(b) = wp$, where w is an integer $\leqq (b - B)^2$, and p is a prime, then $f(x)$ is irreducible over the rationals.

To prove Theorem 4, note that for $|z| \geqq B$,

$$\left| \frac{f(z)}{z^n} \right| \geqq \text{Re} \left(d_n + \frac{d_{n-1}}{z} \right) - \sum_2^n \frac{|d_{n-k}|}{|z|^k} > d_n - \frac{m d_n}{|z|^2 - |z|} \geqq 0.$$

Thus, each root α of $f(x)$ satisfies Re $(\alpha) < B$. If $f(x) = g(x)h(x)$, where

$g(x)$ and $h(x) \in \mathbf{Z}[x]$ such that $p|h(b)$, then $g(b) \leqq w$. The condition $w \leqq (b - B)^2$ guarantees $g(x)$ is of degree $\leqq 1$.

As an example, consider $f(x) = x^5 + 10x^4 - 3x^3 + 7x^2 - 1$. One checks that $f(x)$ has no rational roots. Here $m = 7$ and $B \approx 3.2$. Thus, we consider $f(5) = 2 \cdot 3 \cdot 11 \cdot 139$, $f(6) = 11 \cdot 43^2$, and finally $f(7) = 2 \cdot 5 \cdot 4013$. Since $(7 - B)^2 \approx 14.5 > 10$, $f(x)$ is irreducible.

In using Theorem 4 as an irreducibility test, we do not need to factor $f(b)$ completely. Instead we can make use of a primality test. Let $R = \prod_1^r p_j^{e_j}$, where p_j is the jth prime, $p_r \leqq (b - B)^2 < p_{r+1}$, and $e_j \in Z$ such that $p_j^{e_j} \| f(b)$. Let

$$s = \max_{j \leqq r} \{j : e_j \geqq 1\}.$$

If $f(b) = R$, set $\mathscr{P} = R/p_s$. If $f(b) \neq R$, set $P = R$. If $P > (b - B)^2$, then proceed to $f(b + 1)$. If $P \leqq (b - B)^2$, then consider $Q = f(b)/P$. If Q is prime, $f(x)$ is irreducible. If Q is composite, proceed to $f(b + 1)$. On the other hand, if $f(x)$ is reducible, some information can be gained about its factorization from divisors of $f(b)$ which are $> (b - B)^2$, as was done for $b = 10$ in Section 2. Finally, it should be noted that Theorem 4 can be applied to any polynomial $f(x) = \sum_0^n d_k x^k \in \mathbf{Z}[x]$ since $\pm f(x)$ or $\pm f(-x)$ will always have two nonnegative leading coefficients. In the case that $d_{n-2} \geqq 0$ as well as $d_n > 0$ and $d_{n-1} \geqq 0$, the role of B in Theorem 4 may be replaced by $\max \{r_1, r_2\}$ where r_1 and r_2 are as in the lemma of Section 1.

References

1. J. Brillhart, M. Filaseta and A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Can. J. Math. *33* (1981).
2. G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis* (Springer-Verlag, Berlin, 1964).

University of Illinois,
Urbana, Illinois