MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 152
OCTOBER 1980, PAGES 1379–1381

Note on Irreducibility Testing

By John Brillhart

Abstract. An effective method is developed for deducing the irreducibility of a given polynomial with integer coefficients from a single occurrence of a prime value of that polynomial.

1. Introduction. It is usually true that a reducible polynomial $F(x)$ with integer coefficients, say

$$F(x) = G(x)H(x), \tag{1}$$

where $G(x)$ and $H(x)$ are nonconstant polynomials with integer coefficients, cannot take a prime value for an integer value of x. The exceptions to this (and these are the only exceptions) occur when one of the factors in (1) has a value ± 1 and the other factor is a prime. Since $|G(x)|$ and $|H(x)|$ are large when $|x|$ is large, it is clear that there are only a finite number of *exceptional* x for which this can happen. It follows then, that a polynomial of unknown nature which *does* take a prime value for an integral x, where $|x|$ is large enough to avoid being exceptional, will have to be irreducible in $Z[x]$.

2. A Determination of "Large Enough". Rather than trying to find the exceptional values of x so as to be able to avoid them, it is sufficient to find a circle about the origin in the complex plane inside of which they all lie. Then, any integer at least one unit away from this circle will be nonexceptional, as will be proved in Theorem 1.

LEMMA 1. *Let $G(z)$ be a nonconstant polynomial with integer coefficients, and let m be a positive number exceeding the moduli of the zeros of $G(z)$. If $|z| \geqslant m + 1$, then $|G(z)| > 1$.*

Proof. Let α_i be the zeros of $G(z)$. Then $|G(z)| = |a_0| \prod |z - \alpha_i| > 1$, since $|a_0| \geqslant 1$ and each linear factor on the right exceeds 1 when $|z| \geqslant m + 1$. Q.E.D.

THEOREM 1. *Let $f(x)$ be a nonconstant polynomial with integer coefficients, and let m be a positive integer exceeding the moduli of the zeros of $f(x)$. If $f(x_0)$ is a prime for some integer x_0 such that $|x_0| \geqslant m + 1$, then $f(x)$ is irreducible in $Z[x]$.*

Proof. Suppose $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials with integer coefficients and $\deg h \geqslant 1$. Then, certainly, m exceeds the moduli of the zeros of $g(x)$ and $h(x)$. Also, prime $= |f(x_0)| = |g(x_0)|\,|h(x_0)|$, so by Lemma 1 the second

Received October 14, 1979, revised January 10, 1980.
1980 *Mathematics Subject Classification.* Primary 12A20.
Key words and phrases. Irreducibility testing.

0025-5718/80/0000-0179/$01.75

factor is an integer > 1, i.e. $|h(x_0)| =$ prime, which implies deg $g = 0$, since otherwise Lemma 1 would imply $|g(x_0)| > 1$. Thus, $g(x) \equiv \pm 1$, which gives the theorem. Q.E.D.

3. Computation of m. Let $f(x) = a_0x^n + \cdots + a_n$ be a polynomial with integer coefficients. Then a value for m can easily be obtained from the inequality of Cauchy [5]:

$$m \geqslant 1 + \max_k |a_k/a_0|, \quad \text{for } 1 \leqslant k \leqslant n.$$

(Also see [4, pp. 137–139].) The value of m given by this rough estimate is often too large to be convenient, so another method may be used, which is also due to Cauchy [5] (also see [2, p. 73]). Let $f(x) = a_0x^n + \cdots + a_n$, $a_0 \geqslant 1$, as in Theorem 1. Construct $f^*(x) = a_0x^n - \sum_{s=1}^{n} |a_s|x^{n-s}$, and find the smallest positive integer m such that, when $f^*(x)$ is divided by $x - m$, the resulting quotient will have nonnegative coefficients and resulting remainder will be positive, i.e.

$$f^*(x) = (x - m)(a_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}) + R,$$

where $b_1, \ldots, b_{n-1}$ are nonnegative and $R > 0$. (Such an m can readily be found by synthetic division.) This m will then exceed the moduli of the zeros of $f(x)$, since

$$|f(x)| \geqslant a_0|x|^n - \sum_{s=1}^{n} |a_s|\,|x|^{n-s}$$

$$= (|x| - m)(a_0|x|^{n-1} + b_1|x|^{n-2} + \cdots + b_{n-1}) + R,$$

so that $|f(x)| > 0$ for $|x| \geqslant m$.

Example (see [2, p. 74]). Let $f(x) = 2x^6 - 7x^5 - 10x^4 + 30x^3 - 60x^2 + 10x - 50$. Then the first method gives the poor value $m = 31$. The second method, with $f^*(x) = 2x^6 - 7x^5 - 10x^4 - 30x^3 - 60x^2 - 10x - 50$ and the calculation

6	2	−7	−10	−30	−60	−10	−50
	2	5	20	90	480	2870	17170

gives $m = 6$. Thus, setting $x = \pm 7, \pm 8, \ldots$, we find $f(7) = 101009$ is a prime, so $f(x)$ is irreducible in $Z[x]$. If the degree of $f(x)$ is high, or if there are no prime values of $f(x)$ for any x values tried, beginning with $\pm(m + 1)$, it may be advisable to compute the smallest possible value for m. To do this, one may use a more elaborate third method, which will not, however, be discussed here; see [6, pp. 148–151].

Remarks. 1. A theorem similar to Theorem 1, in which the real parts of the zeros are employed, is given in [1].

2. The method discussed here in general reduces irreducibility testing in $Z[x]$ to primality testing in Z, although some polynomials, such as $x^2 + x + 4$, which are irreducible in $Z[x]$, cannot be shown to be such by this method, because they never take a prime value for an integral x.

3. For some polynomials it may be useful to use $x^nf(1/x)$ instead of $f(x)$ in this method.

4. Some values of $f(x)$ do not need to be tested for primality, since they are known in advance to be composite; for if a prime p divides $f(x_1)$, where $0 \leqslant x_1 \leqslant p - 1$,

then p will also divide $f(x_1 + kp)$, $k \in Z$. Thus, since $|f(x)|$ is increasing for $|x| \geqslant m + 1$, $f(x_1 + kp)$ will be composite, except possibly for the first value of $|x_1 + kp| \geqslant m + 1$, when $f(x_1 + kp)$ may equal $\pm p$.

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

1. G. PÓLYA & G. SZEGÖ, *Aufgaben und Lehrsätze aus der Analysis,* Springer-Verlag, Berlin, 1964, b. 2, VIII, p. 127.

2. J. V. USPENSKY, *Theory of Equations,* McGraw-Hill, New York, 1948.

3. JOHN BRILLHART, MICHAEL FILASETA & ANDREW ODLYZKO, "On an irreducibility theorem of A. Cohn," *Canad. J. Math.* (To appear.)

4. D. K. FADDEEV & I. S. SOMINSKIĬ, *Problems in Higher Algebra,* Freeman, San Francisco, Calif., 1965.

5. A. L. CAUCHY, "Exercises de mathématiques," 1829 Oeuvres (2), v. 9, p. 122; *Journ. École Poly.,* v. 25, 1837, p. 176.

6. M. MARDEN, *The Geometry of the Zeros of a Polynomial in a Complex Variable,* Math. Surveys, no. 3, Amer. Math. Soc., Providence, R.I., 1949; revised 1966.