Polynomial Irreducibility via Shifts

January 12, 2024

Abstract

When factoring integer polynomials, it often helps to be able to tell if a polynomial is irreducible before trying (and failing) to find its factors. We examine one such irreducibility test presented by A. Bevelacqua and extend its applicability via shifts, or translations, of the polynomial. On the way there, we also encounter fixed divisors, Bunyakovsky's conjecture, and a bound on the size of the complex roots of the polynomial.

1 Introducing Shifts

Factoring integer polynomials can be a difficult problem, especially if the given polynomial is irreducible. It is easily determined, for instance, that $x^2 + 5x + 6$ is reducible as $(x + 2)(x + 3)$, but it may not be as obvious that the superficially similar polynomial $x^2 + 5x + 8$ has no such factorization over the integers. Attempting to factor the polynomial does not exclude the possibility that the correct factorization has simply not been found yet. To aid in the process of factoring integer polynomials, various criteria have been developed over the years which can positively identify irreducible integer polynomials (see [8], [1], [5]). More recently, the following irreducibility test was presented by A. Bevelacqua in [2] (and subsequently extended in [11]):

Theorem 1. *For any prime p and integers $a_1, \ldots, a_n$ sucn that $p \geq a_1 \geq \cdots \geq a_n \geq 1$, the polynomial $f = p + a_1x + \cdots + a_nx^n$ is irreducible in $\mathbb{Z}[x]$ if and only if the list $(p, a_1, \ldots, a_n)$ does not consist of $(n+1)/d$ consecutive constant lists of length $d > 1$.*

The edge case in which the coefficients form constant lists arises due to a trivial factorization of such polynomials. We can eliminate this edge case by making the inequalities strict, which leads to the following corollary.

Corollary 1.1. *For any prime p and integers $a_1, \ldots, a_n$ sucn that $p > a_1 > \cdots > a_n > 1$, the polynomial $f = p + a_1x + \cdots + a_nx^n$ is irreducible in $\mathbb{Z}[x]$.*

Here we aim to generalize Bevelacqua's result by allowing the polynomial to be translated, or shifted. This shifting is accomplished by adding an integer k to the input x of the polynomial, thereby changing the coefficients. It is straightforward to show that shifting the polynomial does not change its reducibility; nevertheless, we include the proof here for completeness.

Proposition 1. *For any $f(x) \in \mathbb{Z}[x]$ and any $k \in \mathbb{Z}$, $f(x)$ is reducible iff $f(x+k)$ is reducible.*

Proof. Suppose $f(x)$ is reducible, *i.e.* $f(x) = g_1(x)g_2(x)\cdots g_n(x)$ with all the $g_i \in \mathbb{Z}[x]$ and $n > 1$. Then $f(x+k) = g_1(x+k)g_2(x+k)\cdots g_n(x+k)$, and is therefore reducible. Conversely, suppose $f(x+k)$ is reducible, so that $f(x+k) = g_1(x)g_2(x)\cdots g_n(x)$ with all the $g_i \in \mathbb{Z}[x]$ and $n > 1$. Then $f(x) = g_1(x-k)g_2(x-k)\cdots g_n(x-k)$, and is therefore reducible. □

The above observation is sufficient to extend the scope of Theorem 1 and Corollary 1.1. If, for example, a polynomial has decreasing coefficients but the constant term is not prime, it can perhaps be shifted so that the constant term is prime. Then if this shifted polynomial still has decreasing coefficients, our proposition implies that the original polynomial was irreducible. In fact, since the constant term of $f(x+k)$ is $f(k)$, a natural way to check for shifts which give a prime constant term is to simply look for a prime value of the polynomial. However, it is not guaranteed that a prime value will be found, even if the polynomial is irreducible.

There are some integer polynomials whose output values all share a common factor $D > 1$. This common factor D is known as the fixed divisor (see [10], [12]). It may appear at first that the fixed divisor is the same as the gcd of the coefficients, but it is in fact possible for the fixed divisor to be greater than 1 even if the gcd of the coefficients is 1. For example, the polynomial $h(x) = x^2 + 9x + 6$ has fixed divisor 2, because x^2 and $9x$ have the same parity. Since the minimum positive value of h over the integers is 6, the value of h, and therefore the constant term of $h(x+k)$, will never be prime. It is known ([12]) that approximately 28% of integer polynomials have fixed divisor greater than 1, so we would like our method to apply to these polynomials as well. To this end, we first present a generalization of Lemma 2 of [2] which allows for the fixed divisor of the polynomial to be greater than 1. The proof involves the complex roots of the polynomial; nevertheless, all references to reducibility from this point on will continue to refer to reducibility in $\mathbb{Z}[x]$.

Proposition 2. *Let $f(x) \in \mathbb{Z}[x]$ have fixed divisor D. Suppose that $f(0) = Dp$ for some prime p, and that all roots $\theta \in \mathbb{C}$ of f have $|\theta| > D$. Then f is irreducible.*

Proof. Suppose on the contrary that f is reducible, *i.e.* for some $r > 1$, there are integer polynomials $g_i(x)$ such that $f(x) = g_1(x)g_2(x)\cdots g_r(x)$. Then $|f(0)| = |g_1(0)||g_2(0)|\cdots|g_r(0)| = Dp$. For each g_i, let c_i be the leading coefficient of g_i. By Vieta's formulas, we have that $|g_i(0)/c_i|$ is the product of all the complex roots of g_i. Now the roots of each of the g_i are also roots of f, so we get

$$|g_i(0)/c_i| > D \Rightarrow |g_i(0)| > D|c_i| \geq D,$$

where in the last step we use the fact that $c_i \in \mathbb{Z} \setminus \{0\}$. Now p must divide one of the $g_i(0)$; WLOG suppose $p \mid g_1(0)$. Then there is a positive integer b such that $D = b|g_2(0)| \cdots |g_r(0)|$. But this is impossible, since all the $|g_i(0)|$ are greater than D. By contradiction, f is irreducible. □

From these two propositions, along with the observation that the fixed divisor is invariant under shifts, our main result follows:

Theorem 2. *Let $f(x) \in \mathbb{Z}[x]$ have fixed divisor D. Then f is irreducible if there exists a $k \in \mathbb{Z}$ such that $f(k) = Dp$ for some prime p and all complex roots of $f(x+k)$ have norm greater than D.*

In [2] it was shown that if the coefficients of the polynomial are strictly decreasing, then all complex roots have norm greater than 1; therefore the special case $k = 0$, $D = 1$ of Theorem 2 implies Corollary 1.1.

2 Finding Shifts

We now address the practical utility of Theorem 2. Firstly, one may wonder about the commonality of values of k for which $f(k) = Dp$. To address this question, we appeal to Bunyakovsky's conjecture (first stated in [3] and discussed further in [9]), which hypothesizes that any irreducible integer polynomial will have infinitely many such values. More importantly, however, this result seems to require us to find the complex roots of the polynomial in order to be of any use. On the contrary, all that is necessary is an upper bound on the real parts of the complex roots, as detailed in the following proposition:

Proposition 3. *Let $f(x) \in \mathbb{C}[x]$ and $s \in \mathbb{R}^+$. Let z_0 be the root of f with maximal real part $Re(z_0)$, and let $m \geq \lfloor Re(z_0) \rfloor + s + 1$. Then all roots w of $f(x+m)$ have $|w| > s$.*

Proof. For a given root z of f, let w be the corresponding root of $f(x+m)$, *i.e.* $w = z - m$. Then $\mathrm{Re}(w) = \mathrm{Re}(z-m) = \mathrm{Re}(z) - m \leq \mathrm{Re}(z_0) - \lfloor \mathrm{Re}(z_0) \rfloor - s - 1 < 1 - s - 1 = -s$. Hence for all w, we have $|w| = \sqrt{\mathrm{Re}(w)^2 + \mathrm{Im}(w)^2} \geq |\mathrm{Re}(w)| > s$. □

Since the above result holds for all $m \geq \lfloor \mathrm{Re}(z_0) \rfloor + s + 1$, using an upper bound for $\mathrm{Re}(z_0)$ will still yield an acceptable shift. Furthermore, since $\mathrm{Re}(z_0) \leq |z_0|$, an upper bound on the norms of the roots is also an upper bound on the real parts. There are many methods for bounding the norms of the roots given the coefficients of the polynomial (see [6], [7]); here we will use Cauchy's bound (first presented in [4]). Using this bound, we find that if $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, with $(a_n \neq 0)$, then

$$\mathrm{Re}(z_0) \leq |z_0| \leq 1 + \max \left\{ \left| \frac{a_{n-1}}{a_n} \right|, \left| \frac{a_{n-2}}{a_n} \right|, \cdots, \left| \frac{a_0}{a_n} \right| \right\}, \tag{1}$$

which together with Proposition 3, leads us to the following corollary.

Corollary 2.1. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ have fixed divisor D. Let*

$$M = 1 + \max\left\{\left|\frac{a_{n-1}}{a_n}\right|, \left|\frac{a_{n-2}}{a_n}\right|, \cdots, \left|\frac{a_0}{a_n}\right|\right\}$$

and $m = \lfloor M \rfloor + D + 1$. If there exists a $k \in \mathbb{Z}^+$ such that $f(m+k) = Dp$ for some prime p, then f is irreducible.

Proof. From (1) we get $m \geq \mathrm{Re}(z_0)+D+1$, and therefore $m+k \geq \mathrm{Re}(z_0)+D+1$ for any $k \in \mathbb{Z}^+$. Then applying Proposition 3 with $s = D$, we see that all complex roots of $f(x + m + k)$ will have norm greater than D. Finally, if $f(m+k) = Dp$ for some prime p, we get that f is irreducible by Theorem 2. □

The above result no longer references the complex roots of the polynomial, only the coefficients; this allows us to find acceptable shifts without calculating the complex roots. For our earlier polynomial $h(x) = x^2+9x+6$, we have $D = 2$ and $m = 13$. From there, the smallest k such that $h(m + k) = Dp$ is $k = 6$, which gives $h(19) = 538 = 2 \cdot 269$. If we have information about the roots of the polynomial, however, we can find a smaller shift. It turns out that the smallest k such that all roots of $h(x+k)$ have norm greater than 2 is $k = 2$. From there, we get $h(4) = 58 = 2 \cdot 29$. So both methods show that h is irreducible.

In the above example, the input at which the polynomial evaluated to a prime multiple of the fixed divisor was not much greater than the shift amount required to meet the first condition. As it turns out, this will not always be the case. For instance, take the polynomial $x^{12} + 4094$ (from [8]). We see that all the complex roots have norm $\sqrt[12]{4094} < 2$, so the smallest k required to meet the complex root condition is 3. In addition, since $D = 1$, our upper bound on this k is 4097. However, the polynomial does not attain a prime value until $k = 170625$!

3 More on Shifts

We have just shown how to achieve the conclusion of Bevelacqua's theorem (f is irreducible), as well as one of the hypotheses (the constant term is prime) using shifts. Now one may naturally wonder about achieving the other hypothesis of the theorem (the coefficients are decreasing) using shifts, so that Bevelacqua's original theorem can be applied directly. Here we do just that; we claim that for any integer polynomial $f(x)$ with positive leading coefficient, there is some positive integer k such that the coefficients of $f(x + k)$ are positive and strictly decreasing. First, let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where all the $a_i \in \mathbb{Z}$ and $a_n \in \mathbb{Z}^+$. Then

$$\begin{aligned} f(x+k) &= \sum_{j=0}^{n} a_j (x+k)^j \\ &= \sum_{j=0}^{n} \sum_{i=0}^{j} a_j \binom{j}{i} x^i k^{j-i} \\ &= \sum_{i=0}^{n} \sum_{j=i}^{n} a_j \binom{j}{i} x^i k^{j-i} \\ &= \sum_{i=0}^{n} x^i \sum_{j=i}^{n} a_j \binom{j}{i} k^{j-i}. \end{aligned}$$

So we see that the ith coefficient of $f(x+k)$ is

$$b_i = \sum_{j=i}^{n} a_j \binom{j}{i} k^{j-i} = a_n \binom{n}{i} k^{n-i} + \sum_{j=i}^{n-1} a_j \binom{j}{i} k^{j-i} = \Theta(k^{n-i}).$$

Now as i increases, the power of k in the big-theta expression decreases. Therefore there is some $k \in \mathbb{Z}^+$ such that $b_{i+1} < b_i$ for all $i \in \mathbb{Z}$ where $0 \leq i < n$, as was previously claimed. Now one may naturally wonder about an upper bound on the smallest such k. Indeed, the authors have identified an upper bound of $m+n+1$, where $m = \max(-\min\{a_0, a_1, \cdots a_n\}, 0)$, though the proof of this bound would be too lengthy to include here. We invite any interested readers to derive and potentially improve upon this bound for themselves.

References

[1] Leonard M. Adleman and Andrew M. Odlyzko. "Irreducibility testing and factorization of polynomials". In: *Mathematics of Computation* 41 (1983), pp. 699–709.

[2] Anthony J. Bevelacqua. "Another Irreducibility Criterion". In: *The American Mathematical Monthly* 120.7 (2013), pp. 648–650.

[3] Viktor Bunyakovsky. "Sur les diviseurs numériques invariables des fonctions rationnelles entières". In: *Mém. Acad. Sc. St. Pétersbourg* 6 (1857), pp. 305–329.

[4] Augustin-Louis Cauchy. "Exercices de mathématiques". In: *Oeuvres Complètes.* Vol. 2. 9. 1829, p. 122.

[5] H. L. Dorwart. "Irreducibility of Polynomials". In: *The American Mathematical Monthly* 42.6 (1935), pp. 369–381. DOI: 10.1080/00029890.1935.11987732.

[6] Matsusaburo Fujiwara. "Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung". In: *Tohoku Mathematical Journal* 1.10 (1916), pp. 167–171.

[7] Tetsuzo Kojima. "On the limits of the roots of an algebraic equation". In: *Tohoku Mathematical Journal* 1.11 (1917), pp. 119–127.

[8] Kevin S. McCurley. "Prime values of polynomials and irreducibility testing". In: *Bulletin of the American Mathematical Society* 11.1 (1984), pp. 155–158.

[9] P. Pollack. "Hypothesis H and an impossibility theorem of Ram Murty". In: *Rendiconti del Seminario Matematico* 68.2 (2010), pp. 183–197.

[10] Devendra Prasad, Krishnan Rajkumar, and A. Satyanarayana Reddy. "A survey on fixed divisors". In: *Confluentes Mathematici* 11.1 (2019), pp. 29–52.

[11] Jitender Singh and Sanjeev Kumar. "A Generalization of Bevelacqua's Irreducibility Criterion". In: *The American Mathematical Monthly* 127.5 (2020), pp. 456–459. DOI: 10.1080/00029890.2020.1718952.

[12] Jan Turk. "The Fixed Divisor of a Polynomial". In: *The American Mathematical Monthly* 93.4 (1986), pp. 282–286.