COLLOQUIUM MATHEMATICUM

VOL. 143 2016 NO. 2

IRREDUCIBLE POLYNOMIALS WITH ALL BUT ONE ZERO CLOSE TO THE UNIT DISK

BY

DOYONG KWON (Gwangju)

Abstract. We consider a certain class of polynomials whose zeros are, all with one exception, close to the closed unit disk. We demonstrate that the Mahler measure can be employed to prove irreducibility of these polynomials over $\mathbb{Q}$.

1. Introduction and preliminaries. A few classes of polynomials have their irreducibility criteria over the field of rationals. The present paper introduces another irreducibility criterion for polynomials with one variable.

A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{R}[x]$ is said to be *reciprocal* (resp. *anti-reciprocal*) if $a_k = a_{n-k}$ (resp. $a_k = -a_{n-k}$) for every $k = 0, 1, \ldots, n$. Equivalently, a reciprocal (resp. anti-reciprocal) polynomial satisfies $x^n f(x^{-1}) = f(x)$ (resp. $x^n f(x^{-1}) = -f(x)$). Here, we do not assume $a_0 \neq 0$, and hence $\deg f \leq n$ with equality if and only if $a_0 \neq 0$. We consider the following class of polynomials with integer coefficients:

$$F_b(x) := x^n + b(a_{n-1}x^{n-1} + \cdots + a_1 x) + c =: x^n + br(x) + c \in \mathbb{Z}[x]$$

where $r(x)$ is reciprocal or anti-reciprocal, i.e., $x^n r(x^{-1}) = \pm r(x)$.

Let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = a_n \prod_{i=1}^n (x - \alpha_i) \in \mathbb{Z}[x]$ with $a_n \neq 0$. The *Mahler measure* of g is the real number ≥ 1 defined by

$$M(g) := |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}.$$

Clearly, the Mahler measures of cyclotomic polynomials are equal to 1. And the converse is also almost true by Kronecker's theorem [5]. Polynomials with Mahler measure 1 are cyclotomic polynomials possibly multiplied by

2010 *Mathematics Subject Classification*: Primary 11R06, 11R09; Secondary 30C15.
Key words and phrases: Mahler measure, irreducible polynomial.
Received 18 April 2015; revised 2 October 2015.
Published online 4 February 2016.

DOI: 10.4064/cm6604-11-2015

x^m for some $m \geq 1$. We also consider the following *modified Mahler measure*:

$$M'(g) := \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

that is, the leading coefficient is omitted.

In 1933, Lehmer [7] found a polynomial

$$l(x) := x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1, \tag{1}$$

whose Mahler measure is $\tau_0 \approx 1.17628$, its unique real zero greater than 1. The other zeros of $l(x)$ lie on the closed unit disk. We do not know yet whether the Mahler measure can have a value in the interval $(1, \tau_0)$. But polynomials with small Mahler measures are necessarily reciprocal as $l(x)$ is in the above.

PROPOSITION 1.1 ([9]). *Let $p(x) \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$ with $p(x) \neq x - 1$, and let $\theta_0 \approx 1.32472$ be the unique real root of $x^3 - x - 1 = 0$. If $M(p) < \theta_0$, then $p(x)$ is a reciprocal polynomial.*

The value θ_0 is known to be the smallest Pisot number [1].

2. Main results. We begin with a simple observation. The next proposition is elementary, but we include its proof for the reader's convenience. This is a variant of the continuity theorem for polynomials (see, e.g., [8, Section 1.3]).

PROPOSITION 2.1. *Let $f(x), g(x) \in \mathbb{C}[x]$ and $b \in \mathbb{C}$. Suppose $\deg f = n$ and $\deg g = m$ with $m < n$. Then some m (possibly multiple) zeros of $f(x) + bg(x)$ converge to each zero of $g(x)$ as $|b| \to \infty$.*

Proof. Assume that $g(x) = c\prod_{i=1}^{k}(x-\alpha_i)^{e_i}$ has distinct zeros $\alpha_1, \ldots, \alpha_k$. For each i, let C_i be a circle centered at α_i with radius ε_i sufficiently small so that no zeros of $g(x)$ other than α_i lie inside C_i. If $|bg(x)| > |f(x)|$ on every C_i, as this holds for sufficiently large $|b|$, then Rouché's theorem implies that $f(x) + bg(x)$ and $g(x)$ have the same number of zeros inside C_i. ∎

The goal of the present note is to give a class of irreducible polynomials over $\mathbb{Q}$ with finite and rather simple computations. We are now in a position to state our main theorem.

THEOREM 2.2. *Let*

$$F_b(x) := x^n + b(a_{n-1}x^{n-1} + \cdots + a_1x) + c =: x^n + br(x) + c \in \mathbb{Z}[x],$$

where $a_{n-1} \neq 0$ and $r(x)$ is reciprocal or anti-reciprocal, i.e., $x^n r(x^{-1}) = \pm r(x)$. Assume that $\gcd(r(x), x^n + c) = 1$, and that $c \neq 1$ (resp. $c \neq -1$) if $x^n r(x^{-1}) = r(x)$ (resp. $x^n r(x^{-1}) = -r(x)$). Suppose that the modified Mahler measure $M'(r)$ of $r(x)$ is less than θ_0. Then for all b with sufficiently large $|b|$, the polynomial $F_b(x)$ is irreducible over $\mathbb{Q}$.

The Euclidean algorithm gives us $\gcd(r(x), x^n + c)$. If it is a nonconstant polynomial, then $F_b(x)$ is reducible. The hypothesis $\gcd(r(x), x^n + c) = 1$ in the above theorem excludes this trivial case. If $c = 1$ and $x^n r(x^{-1}) = r(x)$ (resp. $c = -1$ and $x^n r(x^{-1}) = -r(x)$), then $F_b(x)$ itself is reciprocal (resp. anti-reciprocal). If $x^n r(x^{-1}) = -r(x)$, then $x - 1$ is a factor of $x^n + br(x) - 1$. On the other hand, if $x^n r(x^{-1}) = r(x)$ and $n \in \mathbb{N}$ is odd, then $x + 1$ is a factor of $x^n + br(x) + 1$. The remaining case where $x^n r(x^{-1}) = r(x)$ and $n = 2m \in \mathbb{N}$ has been studied in the literature. We refer to, e.g., [2] and [4].

Proof of Theorem 2.2. Suppose that $F_b(x)$ is reducible, say, $F_b(x) = f_b(x)g_b(x)$ for some nonconstant monic polynomials $f_b(x), g_b(x) \in \mathbb{Z}[x]$, where $g_b(x)$ is irreducible. Applying Proposition 2.1, we assume that $|b|$ is large enough that $n - 1$ zeros of $F_b(x)$ are sufficiently close to those of $r(x)$. With no loss of generality, we may assume that all the zeros of $g_b(x)$ are close to some zeros of $r(x)$. Since $g_b(x)$ is monic and $M'(r) < \theta_0$, the Mahler measure $M(g_b)$ is less than θ_0 if $|b|$ is large enough. Accordingly, $g_b(x)$ is reciprocal by Proposition 1.1. For any zero γ of $g_b(x)$, we also have $g_b(\gamma^{-1}) = 0$. In what follows, double signs should be read in the same order, coherently. Since $F_b(\gamma) = 0 = F_b(\gamma^{-1})$ and $\gamma^n r(\gamma^{-1}) = \pm r(\gamma)$, one deduces that

$$\gamma^n + c = -br(\gamma) = \mp b\gamma^n r(\gamma^{-1}) = \pm\gamma^n(\gamma^{-n} + c) = \pm(1 + c\gamma^n),$$

which implies $(\pm c - 1)(\gamma^n \mp 1) = 0$. Because $\pm c - 1 \neq 0$, we find that $\gamma^n = 1$ if $x^n r(x^{-1}) = r(x)$, and that $\gamma^n = -1$ if $x^n r(x^{-1}) = -r(x)$. One observes that $r(\gamma)$ never vanishes for the zero γ of $g_b(x)$. In fact, if $r(\gamma) = 0$, then $\gcd(r(x), x^n + c)$ is a nonconstant polynomial, which contradicts our hypothesis.

We set

$$\begin{aligned} \rho_+(b) &:= \min\{|r(\gamma)| : g_b(\gamma) = 0 \ \&\ \gamma^n = 1\} > 0 \qquad \text{if } x^n r(x^{-1}) = r(x), \\ \rho_-(b) &:= \min\{|r(\gamma)| : g_b(\gamma) = 0 \ \&\ \gamma^n = -1\} > 0 \quad \text{if } x^n r(x^{-1}) = -r(x). \end{aligned}$$

Then, for all $b \in \mathbb{Z}$, both $\rho_+(b)$ and $\rho_-(b)$ can assume a finite number of values, because of the constraints $\gamma^n = 1$ and $\gamma^n = -1$ respectively. Now we define

$$\rho_\pm := \min\{\rho_\pm(b) : b \in \mathbb{Z} \ \&\ F_b(x) \text{ is reducible}\} > 0.$$

In either case of $x^n r(x^{-1}) = \pm r(x)$, the zero γ of $g_b(x)$ satisfies

$$|c \pm 1| = |\gamma^n + c| = |b|\,|r(\gamma)| \geq |b|\rho_\pm. \tag{2}$$

Since $|c \pm 1|$ and $\rho_\pm$ are independent of b, we obtain a desired contradiction for all b with $|b|$ sufficiently large. ∎

In Theorem 2.2, if all the zeros of $r(x)$ are, in particular, on the closed unit disk, then the bound for $|b|$ is effectively computable, as the next theorem says.

THEOREM 2.3. *With the same notation and hypotheses as in Theorem 2.2, assume further that all the zeros of $r(x)$ lie on the closed unit disk. Let*

$$R := \min_{|z|=\theta_0^{1/(n-1)}} |r(z)| > 0, \qquad C := \max_{|z|=\theta_0^{1/(n-1)}} |z^n + c| > 0,$$

where θ_0 is the smallest Pisot number. Also, set

$$\rho_\pm := \min\{|r(\gamma)| : \gamma^n = \pm 1 \ \&\ r(\gamma) \neq 0\} > 0,$$

according as $x^n r(x^{-1}) = \pm r(x)$. If $|b| > \max\{C/R, |c \pm 1|/\rho_\pm\}$, then $F_b(x) = x^n + br(x) + c$ is irreducible over $\mathbb{Q}$.

Proof. We suppose $F_b(x) = f_b(x)g_b(x)$ for some nonconstant monic polynomials $f_b(x), g_b(x) \in \mathbb{Z}[x]$, and follow the proof of Theorem 2.2. First, note that $R > 0$. Assume that $r(\gamma) = 0$ with $\gamma^n = \pm 1$. There are at most $n-2$ such γ's, and γ cannot be a zero of $F_b(x)$ because $\gcd(r(x), x^n + c) = 1$. Hence, $\rho_\pm > 0$. If $|b| > C/R$, then Rouché's theorem implies that $r(x)$ and $F_b(x)$ have the same number of zeros inside the circle $|z| = \theta_0^{1/(n-1)}$, i.e., $n-1$ zeros. Therefore, $M(g_b) < \theta_0$, and $g_b(x)$ is reciprocal. Now the hypothesis $|b| > |c \pm 1|/\rho_\pm$ contradicts (2). ∎

3. Examples. Let $\mathbf{a} = (a_0, a_1, \ldots, a_d) \in \mathbb{R}^{d+1}$ be a vector, and suppose that σ is a permutation on $\{0, 1, \ldots, d\}$ satisfying $a_{\sigma(0)} \leq a_{\sigma(1)} \leq \cdots \leq a_{\sigma(d)}$. We define

$$\underline{m}(\mathbf{a}) := a_{\sigma(\lfloor d/2 \rfloor)} \quad \text{and} \quad \overline{m}(\mathbf{a}) := a_{\sigma(\lceil d/2 \rceil)}.$$

Note that $\underline{m}(\mathbf{a}) = \overline{m}(\mathbf{a})$ whenever d is an even number. Then a real function $H(y) := \sum_{j=0}^d |y - a_j|$ attains its minimum when y belongs to the closed interval or the singleton $[a_{\sigma(\lfloor d/2 \rfloor)}, a_{\sigma(\lceil d/2 \rceil)}]$. We denote this minimum by $L(\mathbf{a})$.

PROPOSITION 3.1 ([6]). *Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{R}[x]$ be a reciprocal polynomial with $a_d > 0$, and let $\mathbf{a} = (a_0, a_1, \ldots, a_d)$ and $\mathbf{a}' = (a_1, \ldots, a_{d-1})$. If one of the following conditions holds, then all the zeros of f lie on the unit circle:*

(a) $\overline{m}(\mathbf{a}) \geq L(\mathbf{a})$,
(b) $f(1) \geq 0$ *and* $2a_d \geq L(\mathbf{a}') + \underline{m}(\mathbf{a}')$.

Our first example makes use of the above proposition.

EXAMPLE 1. Proposition 3.1 shows that every zero of $2x^3 + x^2 + x + 2$ lies on the unit circle. We set $r(x) := 2x^4 + x^3 + x^2 + 2x$ and

$$F_b(x) := x^5 + b(2x^4 + x^3 + x^2 + 2x) + 12.$$

Then x^5+12 and $r(x)$ are relatively prime. We compute

$$R := \min_{|z|=\theta_0^{1/4}} |r(z)| = 0.514079\dots, \qquad C := \max_{|z|=\theta_0^{1/4}} |z^5+12| = 13.421196\dots$$

and

$$\rho_+ := \min\{|r(\gamma)| : \gamma^5 = 1 \ \&\ r(\gamma) \neq 0\} = 0.381966\dots.$$

Consequently, $F_b(x)$ is irreducible if $|b| \geq 35$. Additional checks for $-34 \leq b \leq 34$ enable us to state the following:

> *$x^5 + b(2x^4+x^3+x^2+2x)+12$ with $b \in \mathbb{Z}$ is irreducible over $\mathbb{Q}$ if and only if $b \neq 2$. In the case of $b = 2$,*
>
> $$x^5+2(2x^4+x^3+x^2+2x)+12 = (x^2+2x+2)(x^3+2x^2-4x+6).$$

Filaseta and Gross [3] presented the following irreducibility criterion.

Proposition 3.2. *If $\sum_{k=0}^n a_k \cdot 10^k$ with*

$$0 \leq a_k \leq 49598666989151226098104244512918$$

is a prime number, then the polynomial $\sum_{k=0}^n a_k x^k$ is irreducible over $\mathbb{Q}$.

Example 2. By Proposition 3.1, every zero of $2x^4+2x^3+x^2+2x+2$ lies on the unit circle. Let $r(x) := 2x^5+2x^4+x^3+2x^2+2x$ and

$$F_b(x) := x^6 + b(2x^5+2x^4+x^3+2x^2+2x)+3,$$

where $\gcd(x^6+3, r(x)) = 1$. For, e.g., $0 \leq b \leq 100$, one verifies that $F_b(10)$ is a prime if and only if

$$b = 0, 1, 6, 7, 9, 19, 20, 21, 23, 28, 31, 36, 42, 45, 50, 58, 61, 62, 72, 77, 85, 94, 98.$$

So Proposition 3.2 guarantees that $F_b(x)$ is irreducible over $\mathbb{Q}$ for these b's. On the other hand, we compute

$$R := \min_{|z|=\theta_0^{1/5}} |r(z)| = 0.643147\dots, \qquad C := \max_{|z|=\theta_0^{1/5}} |z^6+3| = 4.401354\dots$$

and $\rho_+ := \min\{|r(\gamma)| : \gamma^6 = 1 \ \&\ r(\gamma) \neq 0\} = 1$. Hence, $F_b(x)$ is irreducible if $|b| \geq 7$. After irreducibility checks for $-6 \leq b \leq 6$, we conclude that

> *$x^6 + b(2x^5+2x^4+x^3+2x^2+2x)+3$ with $b \in \mathbb{Z}$ is irreducible over $\mathbb{Q}$ if and only if $b \neq 4$. In the case of $b = 4$,*
>
> $$x^6+4(2x^5+2x^4+x^3+2x^2+2x)+3 = (x+1)(x^2-x+1)(x^3+8x^2+8x+3).$$

Acknowledgements. This study was financially supported by Chonnam National University, 2013.

References

[1] M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, and J.-P. Schreiber, *Pisot and Salem Numbers*, Birkhäuser, Basel, 1992.

[2] L. E. Dickson, *Criteria for the irreducibility of a reciprocal equation*, Bull. Amer. Math. Soc. 14 (1908), 426–430.

[3] M. Filaseta and S. Gross, *49598666989151226098104244512918*, J. Number Theory 137 (2014), 16–49.

[4] H. Kleiman, *On irreducibility criteria of Dickson*, J. London Math. Soc. (2) 7 (1974), 467–475.

[5] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), 173–175.

[6] D. Y. Kwon, *Reciprocal polynomials with all zeros on the unit circle*, Acta Math. Hungar. 131 (2011), 285–294.

[7] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) 34 (1933), 461–479.

[8] Q. I. Rahman and G. Schmeisser, *Analytic Theory of Polynomials*, Clarendon Press, Oxford, 2002.

[9] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.

DoYong Kwon
Department of Mathematics
Chonnam National University
Gwangju 500-757, Republic of Korea
E-mail: doyong@jnu.ac.kr