Elemente der Mathematik 77 (2022), 20–26
DOI 10.4171/EM/436

Further explorations of unimodular roots

Adam Glesser and Heather Stemen

Adam Glesser is a professor of mathematics at California State University, Fullerton. He earned his doctorate from the University of California, Santa Cruz in 2006 studying the representation theory of finite groups. He has since written on an eclectic list of topics and was awarded the 2020 George Pólya Award for expository excellence by the Mathematical Association of America.

Heather Stemen is a high school mathematics teacher at the Cobalt Institute of Math & Science, and an adjunct professor in the Mathematics Department at Victor Valley Community College. She obtained her Bachelor's Degree in Pure Mathematics in 2015, and her Masters Degree in Mathematics in 2019, both from California State University, Fullerton.

1 Introduction

In [1], the authors define a (complex) root of a polynomial to be *unimodular* if it lies on the unit circle in the complex plane or is, equivalently, a complex number of the form $e^{i\theta}$ for $\theta \in \mathbb{R}$. They then give a complete classification of the pairs (n, k) for which the polynomial $z^n + z^k - 1$ has a unimodular root. Moreover, they determine the exact locations of the unimodular roots for each such pair (n, k). We refer to their paper for an explanation of the historical significance of the problem of finding roots of trinomials. To describe their main theorem, we use the following notation. First, for two integers n and

Das Studium der Wurzeln von Polynomen reicht zurück bis in die Anfänge der Mathematik. Im 19. Jahrhundert begann man speziell Trinome von hohem Grad zu betrachten. 2014 untersuchten Brilleslyper und Schaubroeck komplexe Polynome der Form $z^n + z^k - 1$ und formulierten Bedingungen an die ganzen Zahlen n und k, sodass das Polynom *unimodulare Wurzeln* hat, d. h. Wurzeln auf dem komplexen Einheitskreis. In der vorliegenden Arbeit verallgemeinern die Autoren die Theorie auf Polynome der Form $z^n + z^k - c$, für $c \in \mathbb{Q}$. Sie finden notwendige und hinreichende Bedingungen an n und k, sodass unimodulare Wurzeln existieren und beschrieben, wo diese dann genau liegen. Die Analyse kommt dabei ohne den Schur–Cohn Algorithmus aus, der normalerweise verwendet wird, um Wurzeln im respektive auf dem Einheitskreis zu finden.

k, we let $\gcd(n,k)$ denote the greatest common divisor of n and k. Next, for a complex number, $z = re^{i\theta} = r\big(\cos(\theta) + i\sin(\theta)\big)$, we denote the complex conjugate of z by $\bar{z} = re^{-i\theta} = r\big(\cos(\theta) - i\sin(\theta)\big)$. Finally, for a positive integer m, the set of mth roots of unity, i.e., the set of complex numbers whose mth power is 1, is denoted by μ_m. Thus, we have

$$\mu_m = \left\{ e^{2\pi i s/m} \mid 0 \le s \le m-1 \right\}.$$

Theorem 1.1 ([1], Theorem 2)**.** *Let n and k be integers such that $1 \le k < n$. Let $g = \gcd(n,k)$. The polynomial $p(z) = z^n + z^k - 1$ has unimodular roots if and only if $(n+k)/g$ is divisible by 6. If the polynomial p does have unimodular roots, then p has exactly $2g$ unimodular roots. The roots of p come in pairs $(z_m, \overline{z}_m)$ where*

$$z_m = e^{\pi i/(3g)}\mu_g.$$

In this paper, we generalize Theorem 1.1 by considering any trinomial of the form $p(z) = z^n + z^k - c$ where $c \in \mathbb{Q}$.

2 Statement of Main Theorem

We quickly see that the possible values for c are bounded quite tightly. In fact, if p has a unimodular root, then $|c| \le 2$. We prove this by first examining a general nth degree polynomial. This would be useful if one wanted to extend this work in the direction indicated in ([1], Problems for Investigation 2).

Lemma 2.1. *If $p(z) = a_n z^n + \cdots + a_1 z - a_0 \in \mathbb{C}[z]$ has a unimodular root, then*

$$|a_0| \le |a_n| + \cdots + |a_1|.$$

In particular, if n and k are integers such that $1 \le k < n$ and such that $z^n + z^k - c$ has a unimodular root, then $|c| \le 2$.

Proof. If ω is a unimodular root (so that $|\omega| = 1$), then the triangle inequality implies that

$$|a_0| = |a_n\omega^n + \cdots + a_1\omega| \le |a_n||\omega|^n + \cdots + |a_1||\omega| \le |a_n| + \cdots + |a_1|. \qquad \square$$

Within this reduced search radius there are only five values for c that allow for the existence of unimodular roots for some pair (n,k). Each of these values for c places a different restriction on the quotient $(n+k)/\gcd(n,k)$.

Theorem 2.2. *Let n and k be integers such that $1 \le k < n$, let $g = \gcd(n,k)$, and let $c \in \mathbb{Q}$. If $z^n + z^k - c$ has a unimodular root, then $c \in \{0, \pm 1, \pm 2\}$. The necessary and sufficient conditions on n and k for the existence of unimodular roots, as well as the locations of the unimodular roots are given in the following table.*

c	condition	#	unimodular roots
-2	$(n+k)/g \equiv 0 \pmod 2$	g	$\mu_{2g} \setminus \mu_g$
-1	$(n+k)/g \equiv 0 \pmod 3$	$2g$	$e^{\pm 2\pi i/(3g)}\mu_g$
0		$n-k$	$\mu_{2(n-k)} \setminus \mu_{n-k}$
1	$(n+k)/g \equiv 0 \pmod 6$	$2g$	$e^{\pm \pi i/(3g)}\mu_g$
2		g	μ_g

The proof of our main theorem closely follows that in the original paper, but with the extra help of Niven's theorem which classifies all rational angles whose cosine is also rational.

3 Proof of the Main Theorem

We begin by handling the simplest case, namely when $c = 0$.

Lemma 3.1. *Let n and k be integers such that $1 \le k < n$. The polynomial $p(z) = z^n + z^k$ has $n-k$ unimodular roots, namely the elements of $\mu_{2(n-k)}$ that are not in μ_{n-k}.*

Proof. Let $p(z) = z^n + z^k = 0$ where $1 \le k < n$. If ω is a root of p, then factoring gives

$$\omega^k(\omega^{n-k} + 1) = 0.$$

It follows that 0 is a root of p of multiplicity k, and that the other roots of k are the $n-k$ roots of $z^{n-k} + 1 = 0$. For $\omega \neq 0$, we have $\omega^{n-k} = -1$, and squaring gives $\omega^{2(n-k)} = 1$. Thus, $\omega \in \mu_{2(n-k)}$. However, the $(n-k)$th power of each of the elements in μ_{n-k} equals 1, not -1, and so the $n-k$ distinct elements of $\mu_{2(n-k)} \setminus \mu_{n-k}$ are the $n-k$ nonzero roots of p. □

Now, for $c \neq 0$, we reduce to the situation where n and k are relatively prime. The following lemma generalizes ([1], Lemma 2).

Lemma 3.2. *Let $n, k_1, \ldots, k_s$ be integers such that $1 \le k_1 < k_2 < \cdots < k_s < n$ and let $g = \gcd(n, k_1, \ldots, k_s)$. The function $\lambda \longmapsto \lambda^g$ is a g-to-one and onto map from the set of unimodular roots of $p(z) = z^n + z^{k_1} + \cdots + z^{k_s} - c \in \mathbb{C}[z]$ to the set of unimodular roots of $q(z) = z^{n/g} + z^{k_1/g} + \cdots + z^{k_s/g} - c$.*

Proof. Assume that λ is a unimodular root and that $p(\lambda) = 0$. We have

$$0 = p(\lambda) = q(\lambda^g),$$

and therefore, λ^g is a unimodular root of q.

Conversely, assume that γ is unimodular and that $q(\gamma) = 0$. Let ω be a gth root of any of the g unimodular roots of γ (guaranteed to exist by the fundamental theorem of algebra), so that $\gamma = \omega^g$. We have,

$$0 = q(\gamma) = q(\omega^g) = p(\omega).$$

Therefore, ω is a unimodular root of p. □

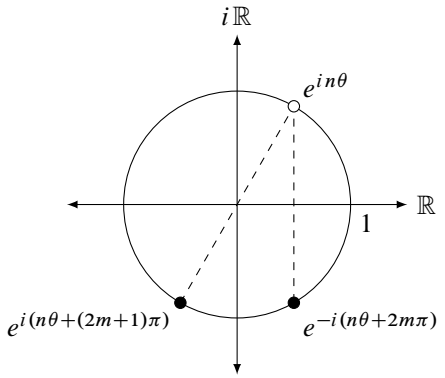

Fig. 1. Points on the unit circle whose imaginary parts are the negative of the imaginary part of $e^{in\theta}$.

Let $p(z) = z^n + z^k - c$ with $c \in \mathbb{Q}$, and assume $p(z)$ has a unimodular root, $e^{i\theta}$. Substituting $e^{i\theta}$ into $p(z)$ gives $e^{in\theta} + e^{ik\theta} - c = 0$. Rewriting $e^{in\theta} + e^{ik\theta} = c$ and rearranging terms, we have

$$c = [\cos(n\theta) + \cos(k\theta)] + i[\sin(n\theta) + \sin(k\theta)].$$

Equating the imaginary part with 0, we have $\sin(n\theta) + \sin(k\theta) = 0$.

This implies (see Figure 1) that either $k\theta = -n\theta + 2m\pi$ for some $m \in \mathbb{Z}$, or that $k\theta$ and $n\theta$ differ by an odd multiple of π. In the latter case, we would have $0 = \cos(n\theta)+\cos(k\theta)$. In light of Lemma 3.1, we may assume that $c \neq 0$. Thus, $k\theta = -n\theta \pmod{2\pi}$.

It follows that

$$\begin{aligned} c &= \cos(n\theta) + \cos(k\theta) \\ &= \cos(n\theta) + \cos(-n\theta) \\ &= 2\cos(n\theta), \end{aligned}$$

and so

$$n\theta \equiv \pm\cos^{-1}(c/2) \pmod{2\pi}.$$

Thus, there exist integers α and β such that

$$n\theta = \pm\cos^{-1}(c/2) + 2\pi\alpha$$

and

$$k\theta = \mp\cos^{-1}(c/2) + 2\pi\beta.$$

Solving both of these equations for θ and equating gives

$$[\pm\cos^{-1}(c/2) + 2\pi\alpha]/n = [\mp\cos^{-1}(c/2) + 2\pi\beta]/k.$$

Multiplying by nk gives $\pm k\cos^{-1}(c/2)+2k\pi\alpha = \mp n\cos^{-1}(c/2)+2n\pi\beta$. Rearranging, we obtain

$$\pm\cos^{-1}(c/2)(n+k) = 2\pi(n\beta - k\alpha).$$

Solving for $n+k$, we have (for $c \neq 2$)

$$n+k = \frac{2\pi}{\pm\cos^{-1}(c/2)}(n\beta - k\alpha), \tag{1}$$

with $n+k, n\beta - k\alpha \in \mathbb{Z}$. It follows that $\cos^{-1}(c/2)$ is a rational multiple of π. As $c \in \mathbb{Q}$, this gives us the opportunity to employ Niven's theorem.

Theorem 3.3 (Niven's Theorem, [3])**.** *The only pairs of the form* $(\theta, \cos(\theta))$ *where* $0 \leq \theta \leq \pi$ *is a rational multiple of* π *and* $\cos\theta$ *is rational are:*

$$(0,1), \left(\frac{\pi}{3}, \frac{1}{2}\right), \left(\frac{2\pi}{3}, -\frac{1}{2}\right), \left(\frac{\pi}{2}, 0\right), (\pi, -1).$$

It follows that there are only five possible values for $c/2$, namely $0, \pm\frac{1}{2}, \pm 1$, and hence we get the five possible values for c as stated in Theorem 2.2. Theorem 1.1 and Lemma 3.1 handle the cases where $c = 1$ and $c = 0$, respectively. We explore each of the three remaining cases ($c = -1, \pm 2$) separately.

If $c = -1$, then (1) implies that

$$n+k = \pm 3(n\beta - k\alpha), \tag{2}$$

and hence $n+k \equiv 0 \pmod 3$.

Lemma 3.4. *Let* n *and* k *be relatively prime integers such that* $1 \leq k < n$*. If* $n+k \equiv 0 \pmod 3$*, then the unimodular roots of* $z^n + z^k + 1$ *are* $e^{\pm 2\pi i/3}$.

Proof. Since n and k are relatively prime and $n+k \equiv 0 \pmod 3$, both n and k are congruent to $\pm 1 \pmod 3$. So there exist nonnegative integers s and t such that $n = 3s \pm 1$ and $k = 3t \mp 1$. We assume that $n = 3s+1$ and $k = 3t-1$, and the other case is similar. We have

$$p(z) = z^{3s+1} + z^{3t-1} + 1 = z^{3s}z + z^{3t}\left(\frac{1}{z}\right) + 1.$$

By direct calculation, we have $p(e^{\pm 2\pi i/3}) = 0$.

Now assume $p\left(e^{i\theta}\right) = 0$. We will show that $\theta = \pm\frac{2\pi}{3}$ up to a multiple of 2π. Using (2), where the assumption was that p had a unimodular root, we have two diophantine equations in the variables α and β:

$$(-3k)\alpha + (3n)\beta = n+k, \tag{3}$$

$$(3k)\alpha + (-3n)\beta = n+k. \tag{4}$$

These have solutions since $\gcd(n,k) = 1$ implies that $\gcd(3n, 3k) = 3$, and we assumed that $n+k$ is divisible by 3. Since $n = 3s+1$ and $k = 3t-1$, we get that $\alpha = s$ and $\beta = t$ is a solution to (3) and $\alpha = n-s$ and $\beta = k-t$ is a solution to (4). So the complete set of integer solutions to (3) is

$$\alpha = s + m\cdot n, \qquad \beta = t + m\cdot k, \tag{5}$$

where $m \in \mathbb{Z}$. Similiarly, the complete set of integer solutions to (4) is

$$\alpha = n - s - m \cdot n, \qquad \beta = k - t - m \cdot k, \tag{6}$$

where $m \in \mathbb{Z}$. Now adding the equations

$$n\theta = \pm\frac{2\pi}{3} + 2\pi\alpha$$
$$k\theta = \mp\frac{2\pi}{3} + 2\pi\beta$$

and substituting $n = 3s + 1$ and $k = 3t - 1$ and solving for θ gives

$$\theta = \frac{2\pi}{3} \cdot \frac{\alpha + \beta}{s + t}. \tag{7}$$

Substituting the possible values for α and β from (5) and (6) into (7) gives

$$\theta \equiv \pm\frac{2\pi}{3} \pmod{2\pi}. \qquad \square$$

Combining Lemma 3.2 with Lemma 3.4, we obtain the result for $c = -1$ as stated in Theorem 2.2.

If $c = -2$, then, by (1), we have

$$n + k = \pm 2(n\beta - k\alpha),$$

and hence $n + k \equiv 0 \pmod 2$.

Lemma 3.5. *Let n and k be relatively prime integers such that $1 \leq k < n$ and such that $n + k \equiv 0 \pmod 2$. The polynomial $p(z) = z^n + z^k + 2$ has exactly one unimodular root, namely -1.*

Proof. If z is a unimodular root, then $2 = |z^n + z^k| \leq |z^n| + |z^k| = |z|^n + |z|^k = 2$. As the triangle inequality only becomes an equality when the arguments of summands are equal, it follows that $z^n = z^k$. In this case, we have $2z^n = -2$, and hence $z^n = -1$. Similarly, $z^k = -1$. As n and k are relatively prime, the only solution to both equations is $z = -1$. $\square$

Combining Lemma 3.2 with Lemma 3.5, we get the conclusion of Theorem 2.2 for $c = -2$.

Finally, if $c = 2$, we see immediately that 1 is a unimodular root of $z^n + z^k - 2$. Using the same argument as in the proof of Lemma 3.5, we see that 1 is the only such unimodular root. Combined with Lemma 3.2, we obtain the conclusion for $c = 2$ of Theorem 2.2. This completes the proof of our main theorem.

Work of the first author with Luis Gonzalez in [2] has uncovered that a similar result holds for the unimodular roots of $p(z) = z^n - z^k - c$, for rational c.

Acknowledgement

The authors would like to thank the Department of Mathematics at California State University, Fullerton for funding the research that led to this paper, as well as Luis Gonzalez for helping us to remove several typos from the original manuscript.

References

[1] M. Brilleslyper, L. Schaubroeck – *Locating unimodular roots*, The College Mathematics Journal 45, No. 3 (2014) 162–168

[2] A. Glesser, L. Gonzalez – *Even further explorations of unimodular roots*, preprint

[3] I. Niven – *Irrational numbers*, Wiley, 1956

Adam Glesser
800 N. State College Blvd.
Fullerton, CA 92831, USA
e-mail: aglesser@fullerton.edu

Heather Stemen
14045 Topaz Road
Victorville, CA 92392, USA
e-mail: hstemen@vvuhsd.org