Parabola Volume 54, Issue 1 (2018)

Unimodular Roots and Arithmetic Progressions

Michael Barz[1]

1 Introduction

Michael Brilleslyper and Lisbeth Schaubroeck investigated polynomials of the form $z^n + z^k - 1$ in [1]. Specifically, they sought to find a way to determine when such a polynomial had at least one unimodular root – that is, a complex root r of the polynomial with $|r| = 1$. Their question was motivated by the polynomials of the form $z^n - 1$, whose roots (referred to as roots of unity) are all unimodular.

At the end of their paper, they posed four questions. In this paper, I will partially solve one of those questions, namely the question of when $z^n + z^k + z^j - 1$ has a unimodular root. Specifically, I will resolve this question for the case in which n, k, j is an arithmetic progression.

1.1 Main Result

I will call an ordered pair (n, d) of positive integers *unimodular* if $n > 2d$ and

$$z^n + z^{n-d} + z^{n-2d} - 1$$

has a unimodular root. My main result is the theorem below which shows how to determine whether or not a pair (n, d) is unimodular without having to actually find any roots.

Theorem 1. *Let n, d be positive integers with $n > 2d$, not both even.*
Then (n, d) is unimodular if and only if either n is even or $n \equiv d \pmod 4$.

This theorem follows directly from two lemmas, Lemma 3 and 4, that I will state and prove in Sections 4 and 5 below. First, however, I will first introduce the geometry of complex numbers, and provide a geometric motivation to show why it is interesting to look at unimodular pairs.

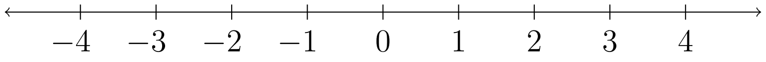
[1] Michael Barz is a student at the Northside College Preparatory High School, Chicago, USA.

2 The Geometry of Complex Numbers

2.1 The Geometry of Real Numbers

Complex numbers are often introduced algebraically, as solutions to the problem of negative square roots. Here, I will introduce them geometrically.

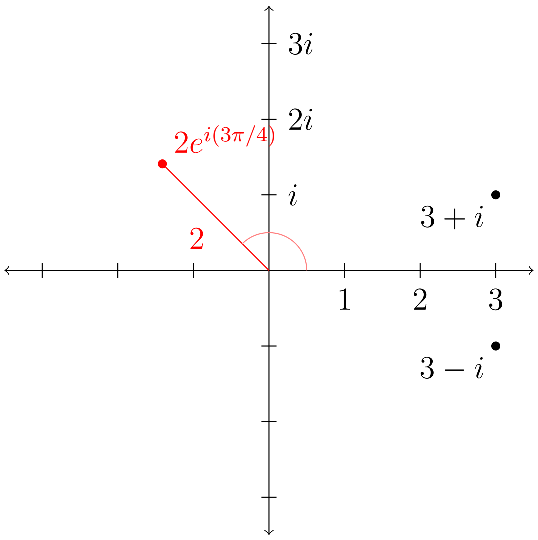
We often think of real numbers as being on the *real number line*, a one-dimensional continuum of numbers.



From this view, we may wonder whether there could be two-dimensional numbers.

2.2 The Complex Numbers

This leads to the *complex numbers.*



To present these, we introduce the imaginary number i satisfying $i^2 = -1$. This relation is motivated geometrically when I discuss polar forms below. Every *complex number* can then be written in the form $z = a + bi$ where a and b are both real numbers, and the number z can also be thought of a point in the plane with coordinates (a, b). For instance in the figure above,

$$0\,,\ 1\,,\ 2\,,\ 3\,,\ i\,,\ 2i\,,\ 3i\,,\ 3+i\,,\ 3-i\,,\ \text{and } 2e^{i(3\pi/4)} = -\sqrt{2} + \sqrt{2}\,i$$

are all complex numbers.

The numbers $3 + i$ and $3 - i$ are *complex conjugates* since you can reflect one of them over the real number line to get the other. In general, the conjugate of $a + bi$ is $a - bi$, and we denote the conjugate of any complex number z by $\overline{z}$.

The "length" of a complex number z, called the *modulus* of z, is denoted by $|z|$. It is the distance from that complex number to the point 0, just like the absolute value of a real number $|x|$. By Pythagoras' Theorem,

$$|a + bi| = \sqrt{a^2 + b^2}\,.$$

For instance, $|1| = 1$, $|0| = 0$, and $|1 + i| = \sqrt{2}$. Conjugates and the modulus relate to each other very nicely. In particular, if $z = a + bi$, then

$$z\overline{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2\,.$$

2.3 Polar Forms of Complex Numbers

I have so far been writing complex numbers z in the form $z = a + bi$, their rectangular or *Cartesian* form. Complex numbers can also be written in their *polar form*, as

$$z = r(\cos\theta + i\sin\theta)\,,$$

where $r = |z|$ is the modulus of z and θ is the anti-clockwise angle from the positive x-axis direction to the direction of z when seen from 0.

The number $\cos\theta + i\sin\theta$ is the complex number obtained by rotating the number 1 in anti-clockwise direction about the origin (the real number 0) by the angle θ. This can be thought of as the "direction" of our complex number. Then, we multiply by r to get the correct "length". See the red point $z = 2e^{i(3\pi/4)}$ in the complex plane above for an example. It has modulus $|z| = 2$ and angle $3\pi/4$ to the positive x-axis, so we can also write z as

$$z = 2\big(\cos(3\pi/4) + i\sin(3\pi/4)\big) = -\sqrt{2} + \sqrt{2}\,i\,.$$

The polar form of a complex number is a very nice representation to use algebraically, since $\cos x + i\sin x$ is a very nicely behaving function. You can verify, using trigonometric identities or by geometrically by interpreting it as a rotation, that $\cos x + i\sin x$ behaves, very surprisingly, much like an exponential function. If we define $f(x) = \cos x + i\sin x$, then $f(a + b) = f(a)f(b)$ and $f(0) = 1$. Also, $f(-x) = 1/f(x)$ and $(f(x))^n = f(nx)$. These properties make algebraic calculations with $\cos x + i\sin x$ very easy. They might also lead us to suspect Euler's formula, which states [3] that

$$e^{ix} = \cos x + i\sin x$$

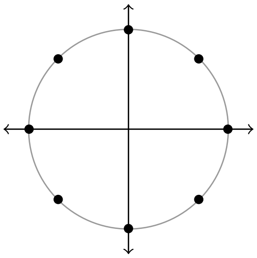
for any real number x. These polar forms help reinforce the notion of multiplication as rotating and scaling. If $z = re^{i\theta}$ and $w = se^{i\phi}$, then

$$zw = rse^{i(\theta+\phi)}\,,$$

which can be found by scaling z by the factor s, and then rotating it by the angle ϕ.

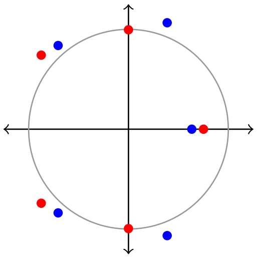
2.4 Some Geometric Motivations for Unimodular Roots

The polynomials of the form $z^n - 1$ have roots which are all on the *unit circle*, the circle centered at 0 with radius 1 in the complex plane. Moreover, all of these roots are distributed evenly about the unit circle. Below, I have drawn the unit circle, as well as the roots of $z^8 - 1$.



This symmetric geometry of the roots of $z^n - 1$ is what prompted Brilleslyper and Schaubroeck to investigate $z^n + z^k - 1$, and to investigate the conditions for when those polynomials had roots on the unit circle.

According to Theorem 1, $z^5 + z^4 + z^3 - 1$ will have at least one root on the unit circle but $z^5 + z^3 + z - 1$ will not, for instance. The roots of both these polynomials are drawn below, the roots of $z^5 + z^4 + z^3 - 1$ in red, and those of $z^5 + z^3 + z - 1$ in blue.



3 The Problem of Unimodular Roots

3.1 A Quick Reduction

Before continuing on to look at arithmetic progressions, I will include one theorem that applies to the general case of the problem. This theorem allows us to only have to deal with cases in which the three exponents are relatively prime.

Theorem 2. *Let n, j, k, and a be positive integers. Then, the polynomial $p(z) = z^{an} + z^{ak} + z^{aj} - 1$ has unimodular roots if and only if $f(z) = z^n + z^k + z^j - 1$ does.*

Proof. The key observation to make in this proof is that, if $z = e^{i\theta}$ is a root of p, then $e^{ia\theta}$ is a root of f (and vice versa). To see this, just note that $p(e^{i\theta}) = 0$ implies that

$$e^{(an)(i\theta)} + e^{(ak)(i\theta)} + e^{(aj)(i\theta)} - 1 = 0\,,$$

and thus $f(e^{i(a\theta)}) = 0$, so f has a unimodular root as well. The other direction is very similar, concluding this proof. □

4 Parity and Experimental Data

When first working on this problem, I used Python and WolframAlpha to gather "experimental data" about when a pair (n, d) is unimodular. By looking at data, I noticed that the parity of n and d seemed to correlate with whether or not (n, d) is unimodular, and so I divided my work into parity-based cases.

4.1 n even, d even

In the case, as Theorem 2 shows, (n, d) will be unimodular if and only if $(n/2, d/2)$ is unimodular. So, we keep dividing by two until one of n or d is odd, and then this will fall into another case!

4.2 n even, d odd

This case is very easy to resolve; -1 is always a unimodular root!

Lemma 3. *If n, d are positive integers with $n > 2d$, and n is even but d is odd, then (n, d) is unimodular.*

Proof. To see this, note that n will be even, $n - d$ will be odd, and $n - 2d$ will be even. Also, -1 raised to an even power is 1, while -1 raised to an odd power is -1. Thus, we have that

$$(-1)^n + (-1)^{n-d} + (-1)^{n-2d} - 1 = 1 - 1 + 1 - 1 = 0\,.$$

□

4.3 n odd

For this case, let us first look at some examples. If $n = 7$ and $d = 1$, then the polynomial $z^7 + z^6 + z^5 - 1$ has no unimodular roots (according to WolframAlpha [4]). However, for $n = 5$ and $d = 1$, the polynomial $z^5 + z^4 + z^3 - 1$ does have a unimodular root: i [5].

Using my Python program to generate data for many polynomials with odd degree n, I conjectured that (n, d) is unimodular if and only if n and d leave the same remainder when divided by 4. This result, Lemma 4 below, is stated formally and proven in the next section.

5 Odd n

Lemma 4. *Let n, d be positive integers with $n > 2d$ and n odd.*
Then, (n, d) is unimodular if and only if $n \equiv d \pmod 4$.

Proof. The proof is split up into two parts. First, we show that a unimodular root exists if $n \equiv d \pmod 4$; then, we show that no unimodular root exists if $n \not\equiv d \pmod 4$.

So, suppose that $n \equiv d \pmod 4$. Write $n = 4k + a$ and $d = 4j + a$ where $0 \leq a < 4$ and where a, j, and k are all integers. Then, since $i^4 = 1$,

$$i^{4k+a} + i^{4(k-j)} + i^{4(k-2j)-a} - 1 = i^{4k}i^a + i^{4(k-j)} + i^{4(k-2j)}i^{-a} - 1 = i^a + i^{-a}\,.$$

As n is odd, either $a = 1$ or $a = 3$. If $a = 1$, then $i^a + i^{-a} = i + 1/i = i - i = 0$. Similarly, if $a = 3$, then $i^3 + i^{-3} = -i + i = 0$. In either case, i is a unimodular root. This completes the first half of the proof.

Now suppose that $n \not\equiv d \pmod 4$. I wish to show that (n, d) is not unimodular.

Since n is odd, either $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$. Suppose that $n \equiv 1 \pmod 4$ and write $n = 4k + 1$ and $d = 4j + b$ where $0 \leq b < 4$. Then (n, d) is unimodular if and only if the polynomial

$$z^{4k+1} + z^{4(k-j)+1-b} + z^{4(k-2j)+1-2b} - 1$$

has a unimodular root. For sake of contradiction, assume that the polynomial does have a unimodular root. Then, there is some complex number w such that $|w| = 1$ and

$$w^{4k+1} + w^{4(k-j)+1-b} + w^{4(k-2j)+1-2b} = 1\,,$$

or, in other words,

$$w^{4(k-2j)+1-2b}(w^{8j+2b} + w^{4j+b} + 1) = 1\,.$$

Then

$$|w^{8j+2b} + w^{4j+b} + 1| = \left|\frac{1}{w^{4(k-2j)+1-2b}}\right| = |w|^{-(4(k-2j)+1-2b)} = 1^{-(4(k-2j)+1-2b)} = 1\,.$$

Write $u = w^{4j+b}$. Then

$$|u^2 + u + 1| = 1\,.$$

Note that $u \neq 1$ and that

$$|u^3 - 1| = |(u-1)(u^2 + u + 1)| = |u - 1||u^2 + u + 1| = |u - 1|\,.$$

Therefore,

$$(u^3 - 1)(\overline{u^3 - 1}) = |u^3 - 1|^2 = |u - 1|^2 = (u - 1)(\overline{u - 1})\,.$$

Since $|u| = |w^{4j+b}| = |w|^{4j+b} = 1^{4j+b} = 1$, it follows that $u\overline{u} = |u|^2 = 1$, so $\overline{u} = \frac{1}{u}$. Therefore,

$$(u^3 - 1)(1/u^3 - 1) = (u - 1)(1/u - 1)\,.$$

Now multiply by u^3 to get

$$(u^3 - 1)(1 - u^3) = (u - 1)(u^2 - u^3)\,.$$

By expanding each side of this equation and tidying up, we get

$$(u^2 + 1)(u^2 - 1)^2 = u^6 - u^4 - u^2 + 1 = 0\,.$$

Thus, $u^2 = -1$ or $u^2 = 1$. Since $u \neq 1$, this means that $u \in \{\pm i, -1\}$. Something particularly interesting about this discovery is that it implies that w is a root of unity – that is, there is some integer p such that $w^p = 1$.

Now, I will look at several subcases to show that no unimodular root can exist. The general structure of my argument is to use a lot of algebra to arrive at a contradiction claiming that some odd number is even.

First, suppose that $d \equiv 1 \pmod 4$ (i.e., that $b = 1$), and suppose that $u = w^{4j+1} = -1$. Then

$$\begin{aligned} w^{4k+1} + w^{4k+1-(4j+1)} + w^{4k+1-2(4j+1)} &= w^{4k+1} + w^{4k+1}/w^{4j+1} + w^{4k+1}/(w^{4j+1})^2 \\ &= w^{4k+1} - w^{4k+1} + w^{4k+1} \\ &= w^{4k+1}\,. \end{aligned}$$

Thus, $w^{4k+1} = 1$. Write $w = e^{i\theta}$. Then $e^{i(4k+1)\theta} = w^{4k+1} = 1$, so

$$\cos\big((4k+1)\theta\big) + i\sin\big((4k+1)\theta\big) = 1\,,$$

which implies that $\sin\big((4k+1)\theta\big) = 0$. Thus,

$$(4k+1)\theta = 2x\pi$$

for some integer x. In other words,

$$\theta = \frac{2x}{4k+1}\pi\,.$$

However, we have that $w^{4j+1} = -1$, which for similar reasons implies that

$$(4j+1)\theta = (2m+1)\pi$$

for some integer m. Therefore,

$$\frac{2x}{4k+1}\pi = \theta = \frac{2m+1}{4j+1}\pi\,,$$

so

$$2x(4j+1) = (2m+1)(4k+1)\,.$$

This, however, produces a contradiction since the left-hand side of the above equation is even but the right-hand side is odd.

Now, suppose that $u = i$. Then

$$\begin{aligned} w^{4k+1} + w^{4k+1-(4j+1)} + w^{4k+1-2(4j+1)} &= w^{4k+1} + w^{4k+1}/w^{4j+1} + w^{4k+1}/(w^{4j+1})^2 \\ &= w^{4k+1} + w^{4k+1}/i + w^{4k+1}/i^2 \\ &= w^{4k+1} - iw^{4k+1} - w^{4k+1} \\ &= -iw^{4k+1} . \end{aligned}$$

Thus,

$$w^{4k+1} = -1/i = i .$$

Again, let $w = e^{i\theta}$. Then

$$w^{4(k+j+1)} = w^{4k+1} \cdot w^{4j+1} = i \cdot i = -1 ,$$

so

$$4(k + j + 1)\theta = (2n + 1)\pi .$$

Also, note that

$$\cos((4k + 1)\theta) + i \sin((4k + 1)\theta) = e^{i(4k+1)\theta} w^{4k+1} = i ,$$

so $\sin\big((4k + 1)\theta\big) = 1$ and $\cos\big((4k + 1)\theta\big) = 0$, implying that $(4k + 1)\theta$ is an odd multiple of $\pi/2$. Therefore,

$$(4k + 1)\theta = (2m + 1)\frac{\pi}{2}$$

for some integer m. Thus,

$$\frac{2x + 1}{4(k + j + 1)}\pi = \theta = \frac{2m + 1}{4k + 1} \cdot \frac{\pi}{2} ,$$

and so

$$(2x + 1)(4k + 1) = 2(k + j + 1)(2m + 1) ,$$

which again is a contradiction as we have an even number on the right and an odd on the left.

The case in which $u = -i$ is similar, as are indeed the cases in which $d \equiv 0, 2, 3 \pmod 4$ and $n \equiv 3 \pmod 4$: the algebraic calculations are much the same, and all end in contradiction. Hence, (n, d) is not unimodular if $n \not\equiv d \pmod 4$.

This completes the proof of the lemma. □

6 Conclusion

In this paper, I have characterised when a pair (n, d) is unimodular, partially resolving the problem of finding when $z^n + z^k + z^j - 1$ has unimodular roots. Theorem 2 let me consider only those cases in which n, k, and j share no common factors, and Theorem 1 takes care of all other cases.

My proof for Lemma 2 broke into many cases at the end, so an interesting question would be to determine if there is a more streamlined way to prove this lemma. This might be possible since all of the cases had the same main idea but had tiny differences in calculation that necessitated the splitting into cases.

Another generalization of the problem would be adding more terms, considering $z^n + z^{n-d} + z^{n-2d} + z^{n-3d} - 1$, or a polynomial with even more terms. The techniques that I used in this paper could be extended to those for the most part, although it would introduce even more casework. If someone could find a proof without splitting into cases, then perhaps it will be very easy to generalize to an arithmetic progression of arbitrary length.

References

[1] M. Brilleslyper and L. Schaubroeck, Locating unimodular roots, *College Mathematics Journal* **45** (2014), 162–168.

[2] M. Brilleslyper and L. Schaubroeck, Counting interior roots of trinomials, *Mathematics Magazine* **91** (2018), 142–150.

[3] T. Rowland and E. Weisstein, Root of Unity, *MathWorld – A Wolfram Web Resource*, http://mathworld.wolfram.com/RootofUnity.html, last retrieved 27 April 2018.

[4] Wolfram Research, Inc. (n.d.), *WolframAlpha*, https://www.wolframalpha.com/input/?i=z%5E7+%2B+z%5E6+%2B+z%5E5+-+1+%3D0,+%7Cz%7C+%3D+1 last retrieved 10 October 2017.

[5] Wolfram Research, Inc. (n.d.), *WolframAlpha*, https://www.wolframalpha.com/input/?i=z%5E5+%2B+z%5E4+%2B+z%5E3+-+1+%3D0,+%7Cz%7C+%3D+1, last retrieved 10 October 2017.