ROOTS ON A CIRCLE

KEITH CONRAD

1. Introduction

The nth roots of unity obviously all lie on the unit circle (see Figure 1 with $n = 7$). Algebraic integers that are not roots of unity can also appear there. The quartic polynomial $z^4 - 2z^3 - 2z + 1$ has two roots on the unit circle (see Figure 2). To explain this, we use the symmetry in the coefficients of $z^4 - 2z^3 - 2z + 1$, which tells us that if α is a root then so is $1/\alpha$. Write the two real roots as α_1 and $1/\alpha_1$. If α_2 is a non-real root then so are $1/\alpha_2$ and $\overline{\alpha}_2$, neither of which is real or equal to α_2, so they must be equal. The condition $1/\alpha_2 = \overline{\alpha}_2$ is the same as $|\alpha_2| = 1$.

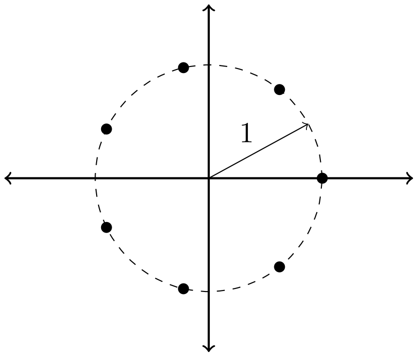

Figure 1. The 7th roots of unity.

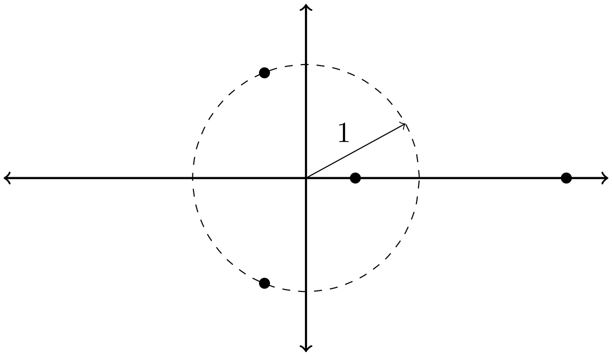

Figure 2. The roots of $z^4 - 2z^3 - 2z + 1$.

A famous polynomial with many, but not all, roots on the unit circle is Lehmer's polynomial [3, p. 477]

$$z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1,$$

whose roots are plotted in Figure 3. There are 2 real roots (approximately .850 and 1.176) and 8 roots on the unit circle. How do you prove those non-real roots are really on the unit circle? From the symmetry in the coefficients, the roots come in reciprocal pairs, and since the coefficients are real the non-real roots come in complex conjugate pairs. If α is one of the non-real roots, then $1/\alpha$ and $\overline{\alpha}$ are also roots, but it is not immediately clear how to show $1/\alpha = \overline{\alpha}$, so $|\alpha| = 1$. The argument we gave for the quartic does not apply in this case since there are too many non-real roots.

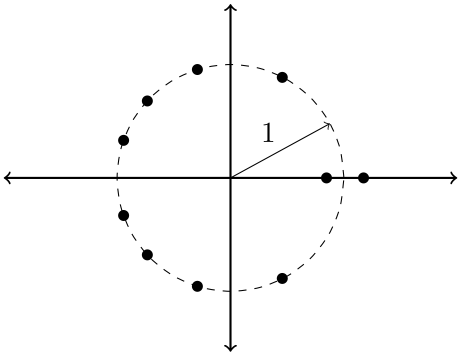

Figure 3. The roots of $z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1$.

Generally, we want to explain how to count the number of roots of a polynomial that lie on the unit circle. For an irreducible polynomial in $\mathbf{Q}[z]$, having a root on the unit circle imposes a symmetry property on the polynomial and a constraint on its degree, as follows.

Theorem 1.1. *Let $f(z) \in \mathbf{Q}[z]$ be irreducible with degree $n > 1$. If $f(z)$ has a root on the unit circle then n is even and $z^n f(1/z) = f(z)$.*

Proof. Let α be a root of $f(z)$ with $|\alpha| = 1$. Since f has real coefficients, $\overline{\alpha} = 1/\alpha$ is also a root of $f(z)$. The product $z^n f(1/z)$ is a polynomial in $\mathbf{Q}[z]$ of degree n (its leading coefficient is $f(0)$) with root α, so by irreducibility of $f(z)$, $z^n f(1/z) = cf(z)$ for some nonzero rational number c. Setting $z = 1$, $f(1) = cf(1)$. Since $f(1) \neq 0$ by our hypotheses, $c = 1$, so $f(z) = z^n f(1/z)$. Setting $z = -1$, we get $f(-1) = (-1)^n f(-1)$. Since $f(-1) \neq 0$, $(-1)^n = 1$, so n is even. □

In Section 2 we will describe a method of root counting on the unit circle that applies to all polynomials satisfying the conclusion of Theorem 1.1, whether or not they are irreducible in $\mathbf{Q}[z]$. In Section 3 we will describe two further methods that apply to more general polynomials. (A result needing polynomials with all roots on the unit circle is in [4].) Finally, Section 4 extends the ideas to circles of radius other than 1.

2. The Palindromic Case

It turns out that the conclusions in Theorem 1.1 essentially say $f(z)$ can be expressed in terms of $z + 1/z$, whether or not the coefficients are rational.

Theorem 2.1. *For a polynomial $f(z) = c_n z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ with coefficients in $\mathbf{C}$ and degree n, the following conditions are equivalent:*

1. *the polynomial has palindromic coefficients: $c_k = c_{n-k}$ for all k,*
2. *$z^n f(1/z) = f(z)$,*
3. *(if n is even) $f(z) = z^{n/2} g(z + 1/z)$ for a polynomial g with coefficients in $\mathbf{C}$ and degree $n/2$.*

Proof. It is simple to check that (1) and (2) are equivalent and that (3) ⇒ (2).

To prove (2) ⇒ (3), set $n = 2m$ and rewrite the equation $z^n f(1/z) = f(z)$ as $z^m f(1/z) = (1/z)^m f(z)$. Since $f(z)$ has degree $2m$,

$$\left(\frac{1}{z}\right)^m f(z) = c_{2m}z^m + c_{2m-1}z^{m-1} + \cdots + c_m + \cdots + \frac{c_1}{z^{m-1}} + \frac{c_0}{z^m}, \tag{2.1}$$

which is a polynomial in z and $1/z$ with degree m (this means the highest power of z and $1/z$ occurring is the mth power). The condition (1), which is equivalent to (2), tells us that the right side of (2.1) is has symmetric coefficients: z^i and z^{-i} have equal coefficients for all $i \leq m$. These properties are also true for $c_{2m}(z+1/z)^m$, which when expanded into a polynomial in z and $1/z$ has initial and final terms matching those in (2.1), so $(1/z)^m f(z) - c_{2m}(z+1/z)^m$ is a polynomial in z and $1/z$ of degree *less than* m with symmetric coefficients. Therefore by induction on the degree, we can write $(1/z)^m f(z) - c_{2m}(z + 1/z)^m = h(z + 1/z)$ where $h(z) \in \mathbf{C}[z]$ and either $h = 0$ or $\deg h < m$. Now add $c_{2m}(z + 1/z)^m$ to both sides. □

We will call a polynomial of degree n "palindromic" when its coefficients satisfy (1), and hence also (2) and (if n is even) (3).

Remark 2.2. If $f(z)$ is palindromic of odd degree n then $z^{2n} f(1/z^2) = f(z^2)$, so $f(z^2)$ is palindromic of even degree $2n$. Also the condition $z^n f(1/z) = f(z)$ forces $f(-1) = 0$, so $f(z) = (z+1)f_1(z)$, where $z^{n-1} f_1(1/z) = f_1(z)$, so $f_1(z)$ is palindromic of even degree $n-1$ and thus $f(z) = (z + 1)z^{(n-1)/2} g(z + 1/z)$ where $\deg g = (n - 1)/2$.

Example 2.3. The polynomial $z^4 - 2z^3 - 2z + 1$ is palindromic of degree 4. Divide by z^2 to get $z^2 - 2z - 2/z + 1/z^2$. Subtract $(z + 1/z)^2$:

$$\left(z^2 - 2z - \frac{2}{z} + \frac{1}{z^2}\right) - \left(z + \frac{1}{z}\right)^2 = -2z - 2 - \frac{2}{z}.$$

This is $-2(z + 1/z) - 2$, so add $(z + 1/z)^2$ to both sides and multiply by z^2:

$$z^4 - 2z^3 - 2z + 1 = z^2\left(\left(z + \frac{1}{z}\right)^2 - 2\left(z + \frac{1}{z}\right) - 2\right).$$

Example 2.4. The polynomial $z^6 - z^4 - 2z^3 - z^2 + 1$ is palindromic of degree 6. Divide by z^3 to get $z^3 - z - 2 - 1/z + 1/z^3$. Now subtract $(z + 1/z)^3$:

$$\left(z^3 - z - 2 - \frac{1}{z} + \frac{1}{z^3}\right) - \left(z + \frac{1}{z}\right)^3 = -4z - 2 - \frac{4}{z}.$$

Next add $4(z + 1/z)$:

$$\left(z^3 - z - 2 - \frac{1}{z} + \frac{1}{z^3}\right) - \left(z + \frac{1}{z}\right)^3 + 4\left(z + \frac{1}{z}\right) = -2.$$

Bringing the powers of $z + 1/z$ to the right side and multiplying through by z^3, we get

$$z^6 - z^4 - 2z^3 - z^2 + 1 = z^3\left(\left(z + \frac{1}{z}\right)^3 - 4\left(z + \frac{1}{z}\right) + 2\right).$$

Example 2.5. The polynomial $z^8 - z^5 - z^4 - z^3 + 1$ is palindromic of degree 8. Divide by z^4 to get $z^4 - z - 1 - 1/z + 1/z^4$. Now subtract $(z + 1/z)^4$:

$$\left(z^4 - z - 1 - \frac{1}{z} + \frac{1}{z^4}\right) - \left(z + \frac{1}{z}\right)^4 = -4z^2 - z - 7 - \frac{1}{z} - \frac{4}{z^2}.$$

Next add $4(z + 1/z)^2$:

$$\left(z^4 - z - 1 - \frac{1}{z} + \frac{1}{z^4}\right) - \left(z + \frac{1}{z}\right)^4 + 4\left(z + \frac{1}{z}\right)^2 = -z + 1 - \frac{1}{z}.$$

Add $z + 1/z$:

$$\left(z^4 - z - 1 - \frac{1}{z} + \frac{1}{z^4}\right) - \left(z + \frac{1}{z}\right)^4 + 4\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) = 1.$$

Bringing all the powers of $z + 1/z$ to the right side and multiplying through by z^4, we have

$$z^8 - z^5 - z^4 - z^3 + 1 = z^4\left(\left(z + \frac{1}{z}\right)^4 - 4\left(z + \frac{1}{z}\right)^2 - \left(z + \frac{1}{z}\right) + 1\right).$$

In Theorem 2.1, we made no assumptions about irreducibility or that the coefficients are rational. (The theorem was, however, inspired by the situation of Theorem 1.1 where $f(z)$ is irreducible in $\mathbf{Q}[z]$.) Theorem 2.1 provides a bijection between the polynomials $g(z)$ in $\mathbf{C}[z]$ of degree m and the palindromic polynomials $f(z)$ in $\mathbf{C}[z]$ of degree $2m$. Obviously f is monic if and only if g is monic, and the nature of the recursive process to obtain g from f, as shown in Examples 2.3, 2.4, and 2.5, shows f has integral coefficients if and only if g has integral coefficients. If $f(z)$ is irreducible in $\mathbf{Q}[z]$ then $g(z)$ is also irreducible in $\mathbf{Q}[z]$ because the equation $f(z) = z^m g(z+1/z)$ forces f to factor nontrivially if g does. However, if $g(z)$ is irreducible in $\mathbf{Q}[z]$ then it does not follow that $f(z)$ is irreducible. For example, if $g(z) = z^2 - 5$ then $z^2 g(z + 1/z) = (z^2 - z - 1)(z^2 + z - 1)$.

Here is a link between roots on the unit circle and real roots.

Theorem 2.6. *Let $f(z) = c_n z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ have even degree $n = 2m$ and satisfy $c_k = c_{n-k}$ for all k. Write $f(z) = z^m g(z + 1/z)$ where $\deg g = m$. The roots of f on the unit circle, considered as pairs of reciprocals, correspond to the roots of g in the interval $[-2, 2]$ by $\{\alpha, 1/\alpha\} \leftrightarrow \alpha + 1/\alpha$.*

Proof. We have $f(z) = 0$ if and only if $g(z + 1/z) = 0$. (Note $f(0) = c_0 = c_n \neq 0$.)

If $|z| = 1$, so $z = \cos\theta + i\sin\theta$, then $z + 1/z = 2\cos\theta$ lies in the interval $[-2, 2]$. Conversely, if $-2 \leq t \leq 2$, so $t = 2\cos\theta$ for some angle θ, then $t = z + 1/z$ for the two numbers $z = \cos\theta \pm i\sin\theta$ (which are really one number when $t = \pm 2$, namely $z = 1$ for $t = 2$ and $z = -1$ for $t = -2$). □

Setting $z = \pm 1$ in the equation $f(z) = z^m g(z + 1/z)$, we get $f(\pm 1) = \pm g(\pm 2)$. Since we are usually interested in polynomials $f(z)$ that are irreducible over $\mathbf{Q}$ with degree greater than 1, $f(\pm 1)$ will not be 0, so $g(z)$ will not vanish at ± 2. Therefore the endpoints of $[-2, 2]$ will not really matter when we talk about roots, although we should specify that a root of $g(z)$ is in $(-2, 2)$, not just $[-2, 2]$, to be sure it has the form $z + 1/z$ for *two* values of z.

Remark 2.7. The multiplicity of a root of g in $(-2,2)$ equals the multiplicity of the corresponding root of f on the unit circle, and if 2 or -2 is a root of g with multiplicity k then 1 or -1 is a root of f with multiplicity $2k$.

Example 2.8. The polynomial z^4-2z^3-2z+1 from Figure 2 is palindromic. By Example 2.3,

$$z^4-2z^3-2z+1 = z^2\left(\left(z+\frac{1}{z}\right)^2 - 2\left(z+\frac{1}{z}\right) - 2\right),$$

so the roots of z^4-2z^3-2z+1 on the unit circle are related to the real roots of w^2-2w-2 in $[-2,2]$. This quadratic has roots $\approx -.732$ and 2.732. One of them is in $(-2,2)$, so there are two roots of the quartic on the unit circle.

Example 2.9. The palindromic polynomial $z^6-z^4-2z^3-z^2+1$ can be written as

$$z^6-z^4-2z^3-z^2+1 = z^3\left(\left(z+\frac{1}{z}\right)^3 - 4\left(z+\frac{1}{z}\right) - 2\right)$$

by Example 2.4, so the roots of $z^6-z^4-2z^3-z^2+1$ on the unit circle (see Figure 4) are related to the roots of w^3-4w-2 in $[-2,2]$. This cubic has roots ≈ -1.675, $-.539$, and 2.214. Two of the roots of w^3-4w-2 are in $(-2,2)$ so $z^6-z^4-2z^3-z^2+1$ has four roots on the unit circle.

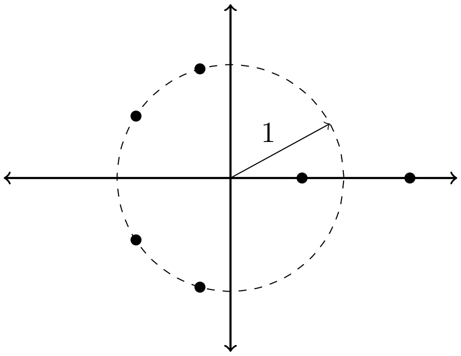

FIGURE 4. The roots of $z^6-z^4-2z^3-z^2+1$.

Example 2.10. The palindromic polynomial $z^8-z^5-z^4-z^3+1$ can be written as

$$z^8-z^5-z^4-z^3+1 = z^4\left(\left(z+\frac{1}{z}\right)^4 - 4\left(z+\frac{1}{z}\right)^2 - \left(z+\frac{1}{z}\right) + 1\right)$$

by Example 2.5, so roots of $z^8-z^5-z^4-z^3+1$ on the unit circle (see Figure 5) are related to the roots of w^4-4w^2-w+1 in $[-2,2]$. This quartic has roots ≈ -1.764, $-.693$, $.396$, 2.061. Three of the roots of w^4-4w^2-w+1 are in $(-2,2)$ so $z^8-z^5-z^4-z^3+1$ has six roots on the unit circle.

Example 2.11. To prove Lehmer's polynomial $z^{10}+z^9-z^7-z^6-z^5-z^4-z^3+z+1$ has 8 roots on the unit circle, we express this polynomial in terms of $z+1/z$. Carrying out

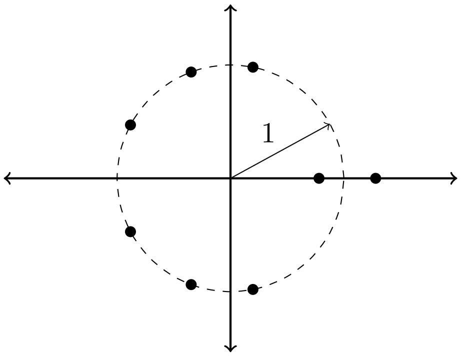

FIGURE 5. The roots of $z^8 - z^5 - z^4 - z^3 + 1$.

the method of Examples 2.3, 2.4, and 2.5 on Lehmer's polynomial, it is equal to

$$z^5\left(\left(z+\frac{1}{z}\right)^5+\left(z+\frac{1}{z}\right)^4-5\left(z+\frac{1}{z}\right)^3-5\left(z+\frac{1}{z}\right)^2+4\left(z+\frac{1}{z}\right)+3\right).$$

The polynomial $w^5 + w^4 - 5w^3 - 5w^2 + 4w + 3$ has all real roots, which are approximately -1.886, -1.468, $-.584$, $.913$, 2.026. Since 4 of the roots are in $(-2, 2)$, there are 8 roots of Lehmer's polynomial on the unit circle.

Lehmer does not say in [3] how he determined that his polynomial has all but two roots on the unit circle, but I suspect it was by the method we just used. This method appears in [1, p. 297] and [2, Prop. 8].

A real number α is called a *Salem number* if $\alpha > 1$, α is the root of a monic polynomial in $\mathbf{Z}[x]$ whose other roots include $1/\alpha$, and all further roots are on the unit circle. The root of Lehmer's polynomial that is greater than 1 is a Salem number and it is conjectured to be the smallest Salem number. The paper [1] discusses many places where Salem numbers occur in mathematics and [5, Sect. 3.4] puts Lehmer's polynomial into the general setting of arithmetic dynamics.

So far our examples have had all but two roots on the unit circle and the remaining two roots are real. Is there an example where $f(z)$ is irreducible in $\mathbf{Q}[z]$ and all but two of its roots are on the unit circle and these other two roots are not real? No. Such a situation requires $g(z)$ to have all but one root in $[-2, 2]$ and therefore its remaining root must be real since $g(z)$ has real coefficients. When t is real and outside $[-2, 2]$, the solutions to $z + 1/z = t$ are both real (and reciprocals of each other).

Let's try to get an example with roots on the unit circle where all but four roots are on the unit circle and those other four roots are not real. A minimal example would be $f(z) = z^3g(z + 1/z)$ where $\deg g = 3$ with g having one root in $[-2, 2]$ and its other two roots not being real.

Example 2.12. The polynomial $g(z) = z^3 - z - 1$ has one real root, which is approximately 1.32 and is in $(-2, 2)$. Define

$$f(z) = z^3 g\left(z+\frac{1}{z}\right) = z^6 + 2z^4 - z^3 + 2z^2 + 1,$$

which happens to be irreducible in $\mathbf{Q}[z]$. Since g has 1 root in $(-2,2)$ and 2 non-real roots, f has 2 roots that are on the unit circle and 4 roots that are off the unit circle and are not real. See Figure 6.

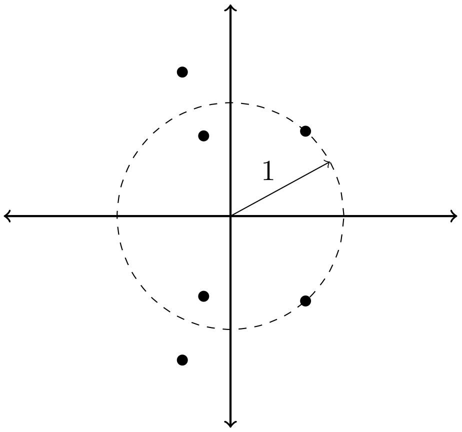

FIGURE 6. The roots of $z^6+2z^4-z^3+2z^2+1$.

Theorem 2.6 is easy to apply to a specific palindromic polynomial of even degree, but not to a family of palindromic polynomials (or a palindromic polynomial of odd degree). An example of such a family is $\sum_{k=0}^{n}\binom{n}{k}\lambda^{k(n-k)}z^k$ for $n\in\mathbf{Z}^+$, which has all of its roots on the unit circle when $\lambda\in[0,1]$. See `https://mathoverflow.net/questions/299304/a-family-of-polynomials-whose-zeros-all-lie-on-the-unit-circle/`.

3. The General Case

Since Theorem 2.6 only works on palindromic polynomials, we need new ideas to count roots on the unit circle of nonpalindromic polynomials.

Example 3.1. The polynomial $f(z)=z^{10}+5z^8+z^7+12z^6+2z^5+13z^4+z^3+8z^2-z+2$, which is not palindromic, appears to have 4 roots on the unit circle in Figure 7.

How can we verify there are 4 roots of $f(z)$ on the unit circle? One method is to factor $f(z)$ in $\mathbf{Q}[z]$. If it really has roots on the unit circle then it must be *reducible* in $\mathbf{Q}[z]$ since it is not palindromic. We can apply Theorem 2.6 to the irreducible factors of $f(z)$ in $\mathbf{Q}[z]$; the factors with roots on the unit circle must be palindromic of even degree. Using a computer algebra package, $f(z)$ factors in $\mathbf{Q}[z]$ as

$$(z^2+z+2)(z^8-z^7+4z^6-z^5+5z^4-z^3+4z^2-z+1), \tag{3.1}$$

where the first factor has no roots on the unit circle by the quadratic formula and the second factor is palindromic with even degree. We could apply the recursive method in the proof of Theorem 2.1 to write the second factor as $z^4g(z+1/z)$ for some $g(z)$ and then count roots of $g(z)$ in $[-2,2]$ in order to count the roots of $f(z)$ on the unit circle by Theorem 2.6. However, rather than show further details, let's admit that it would be good to have a method that can be applied to general polynomials without having to factor them. We will describe two methods, one told to me by François Brunault and the other by Fernando Rodriguez-Villegas.

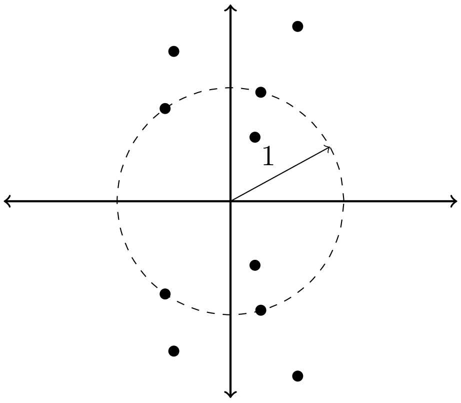

FIGURE 7. The roots of $z^{10} + 5z^8 + z^7 + 12z^6 + 2z^5 + 13z^4 + z^3 + 8z^2 - z + 2$.

Brunault's observation is that if $f(z)$ of degree $n > 0$ in $\mathbf{R}[z]$ does not have 0, 1, or -1 as roots (dividing $f(z)$ by enough powers of z, $z-1$, and $z+1$ can put us in that situation) then the (monic) polynomial $F(z) := \gcd(f(z), z^n f(1/z))$ fits the hypotheses of Theorem 2.6 and roots of $f(z)$ on the unit circle are the same as roots of $F(z)$ on the unit circle (although not necessarily with the same multiplicity), so we can use Theorem 2.6 to count roots of $F(z)$ on the unit circle in order to make that count for $f(z)$.

Theorem 3.2. *Let $f(z) \in \mathbf{R}[z]$ be nonconstant of degree n without 0, 1, or -1 as roots. The polynomial $F(z) := \gcd(f(z), z^n f(1/z))$ has even degree and is palindromic, and a number on the unit circle is a root of $f(z)$ if and only if it is a root of $F(z)$.*

Proof. Since $F(z)$ is a factor of $f(z)$ and 0, 1, and -1 are not roots of $f(z)$, they are not roots of $F(z)$ either. For nonzero α in $\mathbf{C}$ we have $F(\alpha) = 0$ if and only if $f(\alpha) = 0$ and $f(1/\alpha) = 0$, so $F(\alpha) = 0$ if and only if $F(1/\alpha) = 0$: the roots of $F(z)$ always come in reciprocal pairs $\{\alpha, 1/\alpha\}$, where $\alpha \neq 1/\alpha$ since $F(z)$ does not have 0, 1, or -1 as roots.

When α is on the unit circle, $1/\alpha = \overline{\alpha}$. Since $f(z)$ has real coefficients, $f(\overline{\alpha}) = \overline{f(\alpha)}$. Therefore when α is on the unit circle, $f(1/\alpha) = 0 \Leftrightarrow \overline{f(\alpha)} = 0 \Leftrightarrow f(\alpha) = 0$, so $F(\alpha) = 0$ if and only if $f(\alpha) = 0$.

To prove $F(z)$ has even degree and is palindromic, suppose α is a root of $F(z)$, so $1/\alpha$ is a root and $\alpha \neq 1/\alpha$. Factor the biggest powers of α and $1/\alpha$ out of $f(z)$: $f(z) = (z-\alpha)^i(z-1/\alpha)^j h(z)$ where $i \geq 1$ and $j \geq 1$ and $h(z)$ does not have α or $1/\alpha$ as roots. (Possibly $i \neq j$.) Computing degrees tells us $n = i + j + \deg h$, so

$$\begin{aligned}
z^n f(1/z) &= z^{i+j+\deg h}(1/z-\alpha)^i(1/z-1/\alpha)^j h(z) \\
&= z^i(1/z-\alpha)^i z^j(1/z-1/\alpha)^j z^{\deg h} h(1/z) \\
&= (1-\alpha z)^i(1-z/\alpha)^j z^{\deg h} h(1/z) \\
&= (-\alpha)^i(z-1/\alpha)^i(-1/\alpha)^j(z-\alpha)^j z^{\deg h} h(1/z) \\
&= (z-\alpha)^j(z-1/\alpha)^i((-\alpha)^i(-1/\alpha)^j) z^{\deg h} h(1/z),
\end{aligned}$$

where the polynomial $z^{\deg h} h(1/z)$ does not have α or $1/\alpha$ as roots. Therefore in $\mathbf{C}[z]$, $z-\alpha$ and $z-1/\alpha$ are factors of $F(z)$ with the same multiplicity $\min(i,j)$. Thus

$$F(z) = (z-\alpha)^{\min(i,j)}(z-1/\alpha)^{\min(i,j)} \gcd(h(z), z^{\deg h} h(1/z)).$$

So each root pair $\{\alpha, 1/\alpha\}$ of $F(z)$ contributes the factor $(z-\alpha)^{\min(i,j)}(z-1/\alpha)^{\min(i,j)}$ to $F(z)$. For $a \geq 1$ in $\mathbf{Z}$ and $\alpha \notin \{0, 1, -1\}$ the product $p(z) = (z-\alpha)^a(z-1/\alpha)^a$ of degree $2a$ satisfies $z^{2a}p(1/z) = p(z)$. Since $F(z)$ is a product of such (pairwise relatively prime) factors, $\deg F$ is even and $z^{\deg F}F(1/z) = F(z)$, so $F(z)$ is palindromic by Theorem 2.1. □

We can calculate $F(z)$ by Euclid's algorithm in $\mathbf{R}[z]$, so if $f(z) \in \mathbf{Q}[z]$ then $F(z) \in \mathbf{Q}[z]$.

Example 3.3. Let $f(z) = z^{10} + 5z^8 + z^7 + 12z^6 + 2z^5 + 13z^4 + z^3 + 8z^2 - z + 2$ from Example 3.1. From Figure 7 it seems to have 4 roots on the unit circle. To verify this, first note 0, 1, and -1 are not roots ($f(0) = 2$, $f(1) = 44$ and $f(-1) = 38$). We have $z^{10}f(1/z) = 2z^{10} - z^9 + 8z^8 + z^7 + 13z^6 + 2z^5 + 12z^4 + z^3 + 5z^2 + 1$, and using Euclid's algorithm we get

$$F(z) = \gcd(f(z), z^{10}f(1/z)) = z^8 - z^7 + 4z^6 - z^5 + 5z^4 - z^3 + 4z^2 - z + 1,$$

which has even degree and is palindromic.[1] By the proof of Theorem 2.1 we have $F(z) = z^4g(z+1/z)$ for $g(z) = z^4 - z^3 + 2z - 1$. The polynomial $g(z)$ has two real roots, approximately -1.153 and $.535$, which are both in the interval $(-2, 2)$, so $F(z)$ has four roots on the unit circle by Theorem 2.6 and thus $f(z)$ does as well by Theorem 3.2.

Example 3.4. The polynomial $f(z) = z^{10} - z^6 + 4z^4 - 3z^2 + 2$ is not palindromic and does not have 0, 1, or -1 as roots. To count the roots of $f(z)$ on the unit circle, we compute

$$F(z) = \gcd(f(z), z^{10}f(1/z)) = z^8 - 2z^6 + 3z^4 - 2z^2 + 1.$$

This is palindromic of degree 8, so $F(z) = z^4g(z + 1/z)$ where it turns out that $g(z) = z^4 - 6z^2 + 9$. The polynomial g has two double roots, approximately ± 1.732 (exactly, these are $\pm\sqrt{3}$). Both roots are in $(-2, 2)$, so each one leads to two double roots of $F(z)$ on the unit circle by solving $z + 1/z = w$ for z where w is a root of g.

Example 3.4 is the first time that we have met an example where $g(z)$ has a repeated root.

Example 3.5. Let $f(z) = z^6 + iz^5 + (3+i)z^4 + (1+i)z^3 + (1+3i)z^2 + z + i$. Here the coefficients are complex. The roots are plotted in Figure 8 and there appear to be two roots on the unit circle.

Although $f(z) \neq 0$ at $z = 0, 1$, and -1, we are not justified in applying Theorem 3.2 since $f(z)$ does not have real coefficients. Even though $\gcd(f(z), z^6f(1/z))$ makes sense, it is 1 and therefore its (empty set of) roots do not help us count roots of $f(z)$ on the unit circle. And $\gcd(f(z), z^6\overline{f(1/\overline{z})})$ does not help either since, in this case, $z^6\overline{f(1/\overline{z})} = -if(z)$.[2] But $f(z)\overline{f(\overline{z})}$ has real coefficients and is palindromic:

$$f(z)\overline{f(\overline{z})} = z^{12} + 7z^{10} + 4z^9 + 14z^8 + 16z^7 + 14z^6 + 16z^5 + 14z^4 + 4z^3 + 7z^2 + 1$$

This is $z^6g(z + 1/z)$ where $g(z) = z^6 + z^4 + 4z^3 - 5z^2 + 4z - 2$. There are two real roots of $g(z)$ in $[-2, 2]$, approximately -1.850 and $.684$, so $f(z)\overline{f(\overline{z})}$ has four roots on the unit circle. The roots of $f(z)$ and $\overline{f(\overline{z})}$ are complex conjugate to each other and $f(z)\overline{f(\overline{z})}$ has no repeated roots, so $f(z)$ has two roots on the unit circle.

[1] We have now rediscovered the second factor of $f(z)$ in (3.1), but without having to factor $f(z)$.

[2] The "double conjugate" $\overline{f(\overline{z})}$ is the polynomial with coefficients conjugate to $f(z)$ while $f(\overline{z})$ and $\overline{f(z)}$ are not polynoimals in z.

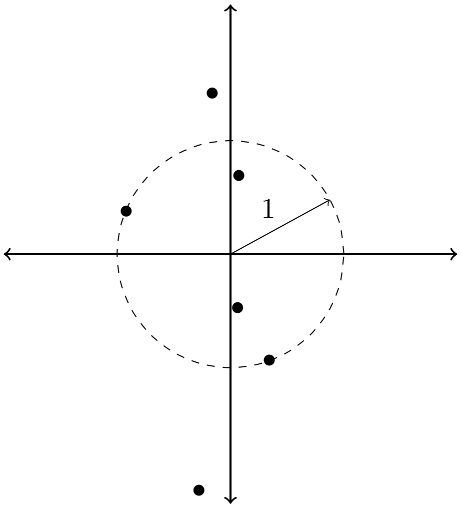

FIGURE 8. The roots of $z^6 + iz^5 + (3+i)z^4 + (1+i)z^3 + (1+3i)z^2 + z + i$.

Rodrigues-Villegas's suggestion for how to find roots of a polynomial on the unit circle is to apply a Möbius transformation to pass between the unit circle and the real line. The Möbius transformation

$$M(z) = \frac{z-i}{z+i},$$

which is illustrated in Figure 9, sends the upper half-plane onto the open unit disc and the real line onto the unit circle *without the point* 1 (although you could say ∞ is sent to 1). Its inverse is

$$M^{-1}(z) = \frac{i(1+z)}{1-z} = \frac{z+1}{i(z-1)},$$

which sends the unit circle without 1 onto the real line.

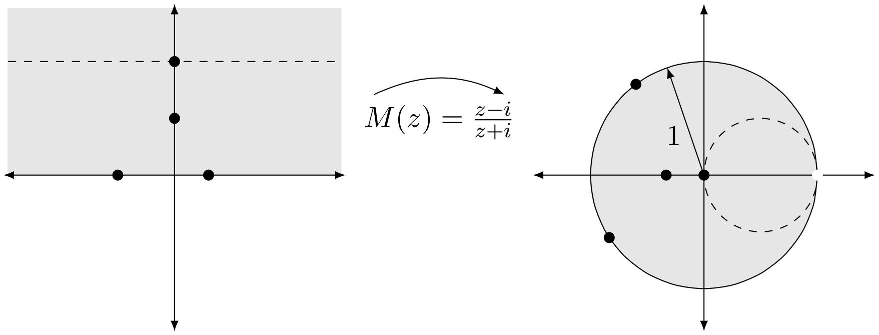

FIGURE 9. The Möbius transformation $M(z) = (z-i)/(z+i)$.

For a polynomial $f(z)$ of degree $n > 0$ (where $f(z)$ need not be palindromic and n need not be even), compose $f(z)$ with $M(z)$ and then multiply by $(z+i)^n$ to clear out the denominator: define

$$f^*(z) = (z+i)^n f(M(z)) = (z+i)^n f\left(\frac{z-i}{z+i}\right). \tag{3.2}$$

A real root of $f^*(z)$ is transformed by $M(z)$ into a root of $f(z)$ on the unit circle. Conversely, every root of f on the unit circle other than 1 has the form $(z-i)/(z+i)$ for some real number z that is a root of f^*. Therefore counting roots of f on the unit circle is the same as counting real roots of f^* as long as we remember to check separately whether or not 1 is a root of f (which is easy). There is no special role for the interval $[-2,2]$, we don't have to double the count when passing from real roots of the auxiliary polynomial to roots of f on the unit circle, and it doesn't matter whether or not f itself has real coefficients.

Writing $f^*(z) = a(z)+ib(z)$ where $a(z)$ and $b(z)$ have real coefficients, a real root of $f^*(z)$ is the same thing as a common real root of $a(z)$ and $b(z)$, that is, a root of the polynomial $\gcd(a(z), b(z))$. Thus counting roots of $f(z)$ on the unit circle is the same as checking if $f(1) = 0$ and counting real roots of $\gcd(a(z), b(z))$.

Example 3.6. Let $f(z) = z^4 - 2z^3 - 2z + 1$, from Example 2.8, so $f(1) \neq 0$. We have

$$f^*(z) = (z+i)^4 f\left(\frac{z-i}{z+i}\right) = -2z^4 - 12z^2 + 6 = -2(z^4 + 6z^2 - 3).$$

Here $b(z) = 0$. There are 2 real roots of $a(z) = f^*(z)$ (approximately $\pm.6812$; this isn't related to the Golden ratio, which is $1.61803\ldots$), so $f(z)$ has 2 roots on the unit circle.

Example 3.7. Let $f(z) = z^6 - z^4 - 2z^3 - z^2 + 1$, from Example 2.9, so $f(1) \neq 0$. Since

$$f^*(z) = (z+i)^6 f\left(\frac{z-i}{z+i}\right) = -2z^6 - 38z^4 + 26z^2 - 2 = -2(z^6 + 19z^4 - 13z^2 - 1),$$

again $b(z) = 0$ and $a(z) = f^*(z)$. The polynomial $a(z)$ has 4 real roots, so $f(z)$ has 4 roots on the unit circle.

Example 3.8. For the polynomial $f(z) = z^6 + 2z^4 - z^3 + 2z^2 + 1$ from Example 2.12, $f(1) \neq 0$ and

$$f^*(z) = 5z^6 - 29z^4 + 23z^2 - 7.$$

Once again $b(z) = 0$. The polynomial $a(z) = f^*(z)$ has 2 real roots, so $f(z)$ has 2 roots on the unit circle.

Example 3.9. For the polynomial $f(z) = z^8 - z^5 - z^4 - z^3 + 1$ from Example 2.10, $f(1) \neq 0$ and

$$f^*(z) = -z^8 - 64z^6 + 134z^4 - 56z^2 + 3.$$

Once more $b(z) = 0$. The polynomial $a(z) = f^*(z)$ has 6 real roots, so $f(z)$ has 6 roots on the unit circle.

Example 3.10. For Lehmer's polynomial $L(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1$, $L(1) \neq 0$ and

$$L^*(z) = (z+i)^{10} f\left(\frac{z-i}{z+i}\right) = -z^{10} - 149z^8 + 518z^6 - 314z^4 + 43z^2 - 1.$$

Yet again, $b(z) = 0$. There are 8 real roots of $a(z) = L^*(z)$, so $L(z)$ has 8 roots on the unit circle.

Example 3.11. We now turn to $f(z) = z^{10}+5z^8+z^7+12z^6+2z^5+13z^4+z^3+8z^2-z+2$, from Example 3.1. It is non-palindromic and seems to have 4 roots on the unit circle, with $f(1) \neq 0$. We counted its roots on the unit circle in Example 3.3 by using Theorem 3.2. To carry out this count using a Möbius transformation instead,

$$f^*(z) = (44z^{10}-198z^8+448z^6-548z^4+260z^2-38)+i(22z^9-88z^7+180z^5-184z^3+38z)$$

where $b(z)$ is (finally) not 0. Since $\gcd(a(z), b(z)) = 22z^8-88z^6+180z^4-184z^2+38 = b(z)/z$, which has 4 real roots, $f(z)$ has 4 roots on the unit circle.

Example 3.12. Let $f(z) = z^n - 1$, so $f(1) = 0$ and $f^*(z) = (z+i)^n - (z-i)^n$. Since the roots of $f(z)$ are all on the unit circle, $f^*(z)$ must have all real roots. Examples of the decomposition of $f^*(z)$ as $a(z) + ib(z)$ are given in Table 1. Unlike before, now it is $a(z)$ that is always 0. The roots of $b(z)$ are all real. In fact its roots are the numbers $\cot(\pi k/n)$ for $1 \leq k \leq n-1$.

n	$a(z)$	$b(z)$
1	0	-2
2	0	$-4z$
3	0	$-6z^2+2$
4	0	$-8z^3+8z$
5	0	$-10z^4+20z^2-2$
6	0	$-12z^5+40z^3-12z$

Table 1. Polynomials $a(z)$ and $b(z)$ for $z^n - 1$.

Example 3.13. Let $f(z) = z^{10}-z^6+4z^4-3z^2+2$ which is not palindromic and $f(1) \neq 0$. In Example 3.4 we showed $f(z)$ has four (double) roots on the unit circle. To show this using a Möbius transformation,

$$f^*(z) = (3z^{10}-87z^8+678z^6-678z^4+87z^2-3)+i(2z^9-56z^7+396z^5-56z^3+2z).$$

We have $\gcd(a(z), b(z)) = z^8-28z^6+198z^4-28z^2+1 = b(z)/(2z)$. Since 1 is not a root of $f(z)$, the roots of $f(z)$ on the unit circle are in bijection with the real roots of $\gcd(a(z), b(z))$. The polynomial $\gcd(a(z), b(z))$ has degree 8 and 4 real roots that are each double roots, so $f(z)$ has 4 roots on the unit circle and they are each a double root.

Example 3.14. Let $f(z) = z^6+iz^5+(3+i)z^4+(1+i)z^3+(1+3i)z^2+z+i$, a non-palindromic polynomial with $f(1) \neq 0$. We saw in Example 3.5 that $f(z)$ has two roots on the unit circle by looking at $f(z)\overline{f(\overline{z})}$. This can be done with a Möbius transformation, as follows. Since

$$f^*(z) = (1+i)(7z^6-6z^5-13z^4+12z^3+9z^2-14z-3),$$

$a(z)$ and $b(z)$ both equal $7z^6-6z^5-13z^4+12z^3+9z^2-14z-3$, which has two real roots. Therefore $f(z)$ has two roots on the unit circle.

Since we often saw in the examples that $b(z) = 0$, it is natural to ask what makes that happen (or what makes $a(z) = 0$).

Theorem 3.15. *For $f(z) = \sum_{k=0}^n c_k z^k$ of degree n, write $f^*(z) = a(z) + ib(z)$, where $a(z)$ and $b(z)$ have real coefficients.*

(1) *$f(z)$ has real coefficients if and only if $f^*(-\overline{z}) = (-1)^n\overline{f^*(z)}$. Concretely: when n is even, $f(z)$ is real if and only if $a(z)$ is even and $b(z)$ is odd, and when n is odd, $f(z)$ is real if and only if $a(z)$ is odd and $b(z)$ is even.*

(2) *$a(z) = 0$ if and only if $f(z) = -z^n\overline{f(1/\overline{z})}$, while $b(z) = 0$ if and only if $f(z) = z^n\overline{f(1/\overline{z})}$. Concretely, $a(z) = 0$ if and only if $c_k = -\overline{c}_{n-k}$ for all k, while $b(z) = 0$ if and only if $c_k = \overline{c}_{n-k}$ for all k.*

(3) *If 1 is a root of f with multiplicity m then $\deg(f^*) = n - m$. In particular, f^* has degree n if and only if $f(1) \neq 0$.*

(4) *The leading coefficient of f is $f^*(-i)/(-2i)^n$.*

(5) *f has coefficients in $\mathbf{Q}(i)$ if and only if f^* has coefficients in $\mathbf{Q}(i)$.*

(6) *f has coefficients in $\mathbf{Z}[1/2, i]$ if and only if f^* has coefficients in $\mathbf{Z}[1/2, i]$.*

Part 3 explains why $b(z)$ for $z^n - 1$ in Table 1 has degree $n - 1$ rather than n.

Proof. This will involve a bit of careful computations with complex conjugation.

(1): To say $f(z)$ has real coefficients is equivalent to $f(z) = \overline{f(\overline{z})}$. This is equivalent to $f(M(z)) = \overline{f(\overline{M(z)})}$. Since $\overline{M(z)} = M(-\overline{z})$ by a direct calculation,

$$\overline{f(\overline{M(z)})} = \overline{f(M(-\overline{z}))} = \overline{\left(\frac{f^*(-\overline{z})}{(-\overline{z}+i)^n}\right)} = \frac{\overline{f^*(-\overline{z})}}{(-z-i)^n} = \frac{(-1)^n\overline{f^*(-\overline{z})}}{(z+i)^n},$$

so $f(z)$ has real coefficients if and only if $\overline{f^*(-\overline{z})} = (-1)^n(z+i)^n f(M(z)) = (-1)^n f^*(z)$. In terms of $a(z)$ and $b(z)$, $\overline{f^*(-\overline{z})} = a(-z) - ib(-z)$, so $f(z)$ has real coefficients if and only if $a(-z) = (-1)^n a(z)$ and $b(-z) = (-1)^{n-1}b(z)$.

(2): The equations $f^*(z) = a(z) + ib(z)$ and $\overline{f^*(\overline{z})} = a(z) - ib(z)$ let us solve for $a(z)$ and $b(z)$:

$$a(z) = \frac{f^*(z) + \overline{f^*(\overline{z})}}{2} \quad \text{and} \quad b(z) = \frac{f^*(z) - \overline{f^*(\overline{z})}}{2i}.$$

Therefore $a(z) = 0$ if and only if $\overline{f^*(\overline{z})} = -f^*(z)$ and $b(z) = 0$ if and only if $\overline{f^*(\overline{z})} = f^*(z)$.

For $\varepsilon = \pm 1$, the equation $\overline{f^*(\overline{z})} = \varepsilon f^*(z)$ is equivalent to

$$\overline{(\overline{z}+i)^n f(M(\overline{z}))} = \varepsilon(z+i)^n f(M(z)). \tag{3.3}$$

Since $M(\overline{z}) = \overline{M(-z)} = 1/\overline{M(z)}$, (3.3) is the same as

$$\overline{f(1/\overline{M(z)})} = \varepsilon\frac{(z+i)^n}{(z-i)^n} f(M(z)). \tag{3.4}$$

Replacing z with $M^{-1}(z) = (z+1)/(i(z-1))$ in (3.4), it becomes

$$z^n\overline{f(1/\overline{z})} = \varepsilon f(z).$$

For $\varepsilon = 1$ we get the condition for when $b(z) = 0$ and for $\varepsilon = -1$ we get the condition for when $a(z) = 0$.

(3): Write $f(z) = (z-1)^m q(z)$, where $q(1) \neq 0$. The operation $f \rightsquigarrow f^*$ is multiplicative, so $f^*(z) = ((z-1)^*)^m q^*(z) = (-2i)^m q^*(z)$. By an explicit calculation with polynomials, if $q(z)$ has degree d then the coefficient of z^d in $q^*(z)$ is $q(1) \neq 0$, so $q^*(z)$ has the same degree as q.

(4), (5), (6): These are explained by the formulas connecting $f(z)$ and $f^*(z)$:

$$f^*(z) = (z+i)^n f\left(\frac{z-i}{z+i}\right) \quad \text{and } f(z) = \left(\frac{i(z-1)}{2}\right)^n f^*\left(\frac{z+1}{i(z-1)}\right). \tag{3.5}$$

The second formula is derived by replacing z with $M^{-1}(z) = (z+i)/(i(z-1))$ in the definition $f^*(z) = (z+i)^n f(M(z))$. □

Is every polynomial $F(z)$ of the form $f^*(z)$ for some f? There is one constraint F has to satisfy, by the leading coefficient formula in the previous theorem: $F(-i) \neq 0$. This is the only obstruction.

Corollary 3.16. *For a polynomial $F(z)$ with degree N that satisfies $F(-i) \neq 0$, the polynomials $f(z)$ that satisfy $f^*(z) = F(z)$ are*

$$\left(\frac{i(z-1)}{2}\right)^{N+m} F\left(\frac{z+1}{i(z-1)}\right)$$

for $m \geq 0$. In particular, there is a unique $f(z)$ of the same degree as $F(z)$ such that $f^*(z) = F(z)$.

Proof. Since $\deg(f^*) \leq \deg f$, f needs to have degree at least N. If $f_1^*(z) = f_2^*(z)$ and $f_1(z)$ and $f_2(z)$ have the same degree then $f_1(z) = f_2(z)$. Since $(i(z-1)/2)^* = 1$, it suffices to show the polynomial

$$\left(\frac{i(z-1)}{2}\right)^{N} F\left(\frac{z+1}{i(z-1)}\right)$$

has degree N and satisfies $f^* = F$. Its degree is certainly at most N and the coefficient of z^N is $(i/2)^N F(-i) \neq 0$, so the degree is N. The reader can check this polynomial satisfies $f^*(z) = F(z)$.

□

On polynomials of a fixed degree, $f(z) \rightsquigarrow f^*(z)$ is a bijection. While it's true that if $f(z)$ has coefficients in $\mathbf{Z}[i]$ then $f^*(z)$ has coefficients in $\mathbf{Z}[i]$, the converse is false in general.

Example 3.17. When $F(z) = z^4 - 4z^2 + 2$, the solution to $f^*(z) = F(z)$ with degree 4 is

$$\left(\frac{i(z-1)}{2}\right)^{4} F\left(\frac{z+1}{i(z-1)}\right) = \frac{7}{16}z^4 - \frac{1}{4}z^3 + \frac{5}{8}z^2 - \frac{1}{4}z + \frac{7}{16}$$

In general, if $F(z) = \sum_{k=0}^N a_k z^k$ then

$$\left(\frac{i(z-1)}{2}\right)^{N} F\left(\frac{z+1}{i(z-1)}\right) = \frac{i^N}{2^N}\sum_{k=0}^{N} a_k(-i)^k(z+1)^k(z-1)^{N-k},$$

and asking for this to have z-coefficients in $\mathbf{Z}[i]$ amounts to some 2-power congruence conditions on linear combinations of the a_k's. (It's best to expand this polynomial in powers of $z-1$ rather than z, which doesn't affect whether or not coefficients are in $\mathbf{Z}[i]$.) To make sure the coefficients are in $\mathbf{Z}$ and not just $\mathbf{Z}[i]$, make sure the real and imaginary parts of $F(z)$ satisfy the even/odd conditions from Theorem 3.15, depending on the parity of N.

We can invert the process $f(z) \rightsquigarrow f^*(z)$ to generate examples of polynomials $f(z)$ in $\mathbf{Q}[z]$ with a specified number of roots on the unit circle starting with a polynomial in $\mathbf{Q}[z]$ having a specified number of real roots, but there is a lot more we have to keep track of compare to directly computing $z^m g(z+1/z)$ when $g(z)$ has enough roots in $(-2,2)$, especially if you want $f(z)$ to be monic with integral coefficients.

4. Beyond the Unit Circle

In number theory and algebraic geometry there are certain problems over finite fields that give rise to polynomials whose roots all have the same absolute value equal to a number *other than* 1, and this phenomenon has practical applications in coding theory (google "Hasse–Weil bound" and "coding theory"). An example of such a polynomial is $9z^4 + 9z^3 + 7z^2 + 3z + 1$, whose roots all lie on the circle $|z| = 1/\sqrt{3}$ (see Figure 10).[3] To verify this, we want to generalize the earlier theorems to roots on a circle r where $r \neq 1$.

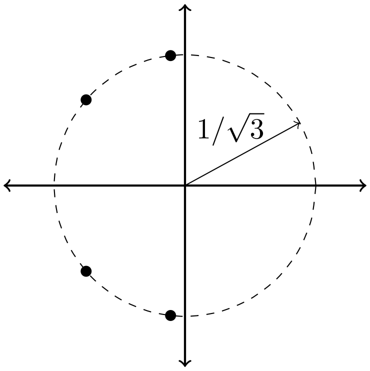

Figure 10. The roots of $9z^4 + 9z^3 + 7z^2 + 3z + 1$.

Theorem 4.1. *Let $f(z) \in \mathbf{Q}[z]$ be irreducible with degree $n > 1$. If $f(z)$ has a root with absolute value r, where $r^2 \in \mathbf{Q}$, then n is even and $(z/r)^n f(r^2/z) = f(z)$.*

Proof. Let α be a root of $f(z)$ with absolute value r, so $\overline{\alpha}$ is also a root and $\overline{\alpha} = r^2/\alpha$. The product $z^n f(r^2/z)$ is in $\mathbf{Q}[z]$ with degree n (the coefficient of z^n is $f(0)/r^n \neq 0$) and α is a root, so $z^n f(r^2/z) = cf(z)$ for some nonzero rational number c. Evaluating this equation at $z = r$ and then at $z = -r$, we see that $c = r^n$ and then that n is even. □

Theorem 4.2. *For $f(z) = c_n z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ with coefficients in $\mathbf{C}$ and degree n, and $r > 0$, the following conditions are equivalent:*

1. *$c_k = r^{n-2k} c_{n-k}$ for all k,*
2. *$(z/r)^n f(r^2/z) = f(z)$,*
3. *(if n is even) $f(z) = (z/r)^{n/2} g(z/r + r/z)$ for a polynomial g with coefficients in $\mathbf{C}$ and degree $n/2$.*

Proof. Apply Theorem 2.1 to $f(rz)$. □

A polynomial $f(z)$ fitting the first two properties in Theorem 4.2 is called "r-palindromic". Thus 1-palindromic means palindromic and $f(z)$ is r-palindromic if and only if $f(rz)$ is palindromic. Replacing $f(z)$ with $f(z/r)$, if $f(z)$ is palindromic then $f(z/r)$ is r-palindromic.

Remark 4.3. Generalizing Remark 2.2, if $f(z)$ is r-palindromic of odd degree n then $f(z^2)$ is $\sqrt{r}$-palindromic of even degree $2n$ and $f(z) = (z + r)f_r(z)$ where $f_r(z)$ is r-palindromic of even degree $n - 1$.

[3] This polynomial is the L-function of the quadratic character of the finite field $\mathbf{F}_3[t]/(t^5 - t - 1)$. Setting $z = 1/3^s$, the condition $|z| = 1/\sqrt{3}$ is equivalent to $\mathrm{Re}(s) = 1/2$, which resembles the classical Riemann hypothesis.

For a polynomial $f(z)$ fitting the conditions in Theorem 4.2, 0 is not a root and $f(\alpha) = 0 \iff f(r^2/\alpha) = 0$, so roots of $f(z)$ come in pairs $\{\alpha, r^2/\alpha\}$ (a singleton only for $\alpha = \pm r$).

Theorem 4.4. *For $f(z) = c_n z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ with coefficients in $\mathbf{C}$ that has even degree $n = 2m$ and is r-palindromic for an $r > 0$, write $f(z) = (z/r)^m g(z/r + r/z)$. Roots of f on the circle of radius r, considered as pairs $\{\alpha, r^2/\alpha\}$ (a singleton for $\alpha = \pm r$), are in bijection with the roots of g in the interval $[-2, 2]$ by $\{\alpha, r^2/\alpha\} \leftrightarrow \alpha/r + r/\alpha$.*

Proof. Apply Theorem 2.6 to $f(rz)$. □

Example 4.5. We will show $f(z) = 9z^4 + 9z^3 + 7z^2 + 3z + 1$ has all of its roots on the circle $|z| = 1/\sqrt{3}$ (see Figure 10). We first check $f(z)$ satisfies the first condition in Theorem 4.2 when $r = 1/\sqrt{3}$: $c_k = (1/3)^{2-k} c_{4-k}$ for $0 \leq k \leq 4$. The reader should confirm this for each k. Then Theorem 4.2 tells us $f(z)$ must satisfy the third condition, and explicitly $f(z) = (\sqrt{3}z)^2 g(\sqrt{3}z + 1/(\sqrt{3}z))$ for $g(w) = w^2 + \sqrt{3}w + 1/3$.[4] The polynomial g has two real roots (approximately -1.51 and $-.22$) and they are both in the interval $(-2, 2)$. Therefore $f(z)$ has all 4 roots on the circle of radius $1/\sqrt{3}$.

Example 4.6. We will show $z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$ has all of its roots on the circle $|z| = \sqrt{2}$ (see Figure 11).

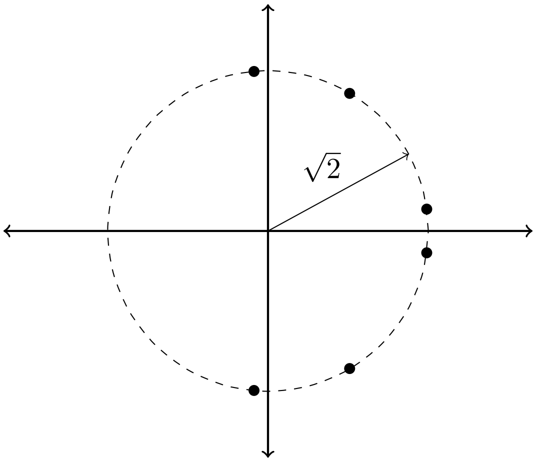

FIGURE 11. The roots of $z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$.

The polynomial satisfies the first condition of Theorem 4.2 for $r = \sqrt{2}$, so by the third condition $f(z) = (z/\sqrt{2})^3 g(z/\sqrt{2} + \sqrt{2}/z)$ for a polynomial $g(z)$. Explicitly, $g(w) = 8w^3 - 16\sqrt{2}w^2 + 12w + 2\sqrt{2}$ and this has all real roots (approximately $-.174, 1.021$, and 1.981) and they are all in $(-2, 2)$. Thus all the roots of $f(z)$ have absolute value $\sqrt{2}$.

For a polynomial that may not be r-palindromic, where $r > 0$, we can count its roots of absolute value r by generalizing the ideas of Brunault and Rodrigues-Villegas from Section 3.

[4] The second condition of Theorem 4.2 says $f(z) = (\sqrt{3}z)^4 f(1/(3z))$, which is called the functional equation for $f(z)$. When $z = 1/3^s$ as in the previous footnote and $F(s) = f(1/3^s)$, the functional equation for $f(z)$ is the same as $F(s) = 3^{2(1-2s)}F(1-s)$.

Theorem 4.7. *For $r > 0$, let $f(z) \in \mathbf{R}[z]$ have degree $n > 0$ without 0, r, or $-r$ as roots. The polynomial $F_r(z) := \gcd(f(z), (z/r)^n f(r^2/z))$ has even degree and is r-palindromic, and a complex number α of absolute value r is a root of $f(z)$ if and only if it is a root of $F_r(z)$.*

Proof. We can apply Theorem 3.2 to $f(rz)$, which does not have 0, 1, or -1 as roots: the polynomial $G_r(z) := \gcd(f(rz), z^n f(r/z))$ has even degree, is palindromic, and has the same roots of absolute value 1 as $f(rz)$.

The change of variables $z \mapsto z/r$ in polynomials does not change degrees and turns roots of absolute value 1 into roots of absolute value r (if you think this is wrong, consider $r = 2$ and the polynomial $z^2 + 1$). Therefore $F_r(z) := G_r(z/r) = \gcd(f(z), (z/r)^n f(r^2/z))$ has even degree, is r-palindromic, and has the same roots of absolute value r as $f(r(z/r))$, which is $f(z)$. □

Example 4.8. Let $f(z) = z^6 - 4z^4 + 6z^3 - 16z^2 - 60z + 25$. We will show 4 out of 6 roots have absolute value $r = \sqrt{5}$ without factoring $f(z)$.

We have $(z/r)^6 f(r^2/z) = (z^6/5^3) f(5/z) = (1/5)z^6 - (12/5)z^5 - (16/5)z^4 + 6z^3 - 20z^2 + 125$, and its greatest common divisor with $f(z)$ is $F_r(z) = z^4 + 3z^3 + 4z^2 + 15z + 25$. (This is r-palindromic, *i.e.*, $c_k = r^{4-2k} c_{4-k} = 5^{2-k} c_{4-k}$ for $0 \leq k \leq 4$, as Theorem 4.7 says it must be.) By Theorem 4.7, $f(z)$ has as many roots of absolute value r as $F_r(z)$ does, which by scaling is the same as the number of roots of absolute value 1 of

$$F_r(rz) = 25z^4 + 15\sqrt{5}z^3 + 20z^2 + 15\sqrt{5}z + 25.$$

This palindromic polynomial of degree 4 is $z^2 g(z + 1/z)$ for $g(z) = 25z^2 + 15\sqrt{5}z - 30$ and $g(z)$ has 2 real roots that are approximately -1.955 and $.613$. Both are in $(-2, 2)$, so $F_r(z)$ has 4 roots on the unit circle and thus $f(z)$ has 4 roots on the circle $|z| = r = \sqrt{5}$.

We can also count roots on the circle of radius r using the Möbius transformation

$$M_r(z) = r\frac{z - i}{z + i},$$

which sends the real line onto the circle of radius r, excluding the number r. Therefore the number of roots of $f(z)$ with absolute value r other than r itself equals the number of real roots of

$$(z + i)^n f\left(r\frac{z - i}{z + i}\right), \tag{4.1}$$

where $n = \deg f$.

Example 4.9. Let $f(z) = 9z^4 + 9z^3 + 7z^2 + 3z + 1$ as in Example 4.5. For $r = 1/\sqrt{3}$, $f(r) \approx 7.79 \neq 0$ and

$$(z + i)^4 f\left(r\frac{z - i}{z + i}\right) = \left(\frac{13}{3} + 2\sqrt{3}\right) z^4 - \frac{22}{3} z^2 + \left(\frac{13}{3} - 2\sqrt{3}\right).$$

This polynomial has 4 real roots, approximately ±.89 and ±.37, and $\deg f = 4$, so all the roots of f have absolute value $r = 1/\sqrt{3}$.

Example 4.10. We show $f(z) = z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$ from Example 4.6 has all roots with absolute value $r = \sqrt{2}$ by looking at real roots of (4.1): r is not a root of $f(z)$ since $f(r) \approx .318 \neq 0$, and

$$(z + i)^6 f\left(r\frac{z - i}{z + i}\right) = (88 - 62\sqrt{2})z^6 + (-168 + 70\sqrt{2})z^4 + (168 + 70\sqrt{2})z^2 + (-88 - 62\sqrt{2}).$$

This polynomial has 6 real roots and $\deg f = 6$, so all roots of f have absolute value $r = \sqrt{2}$.

Example 4.11. To count roots of $f(z) = z^6 - 4z^4 + 6z^3 - 16z^2 - 60z + 25$ with absolute value $r = \sqrt{5}$, we have $f(r) \approx -97.082 \neq 0$ and

$$(z+i)^6 f\left(r\frac{z-i}{z+i}\right) = a(z) + b(z)i$$

where

$$\begin{aligned} a(z) &= (-30-30\sqrt{5})z^6 + (-2430+390\sqrt{5})z^4 + (2430+390\sqrt{5})z^2 + (30-30\sqrt{5}) \\ &= (-30-30\sqrt{5})\left(z^6 + \frac{73-47\sqrt{5}}{2}z^4 + (4-17\sqrt{5})z^2 + \frac{3-\sqrt{5}}{2}\right) \end{aligned}$$

and

$$\begin{aligned} b(z) &= (-560-240\sqrt{5})z^5 + 2080z^3 + (-560+240\sqrt{5})z \\ &= (-560-240\sqrt{5})z\left(z^4 + \frac{-91+39\sqrt{5}}{2}z^2 + \frac{47-21\sqrt{5}}{2}\right). \end{aligned}$$

The real roots of $a(z)+b(z)i$ are the real roots of $\gcd(a(z), b(z))$, and this greatest common divisor is $b(z)/z$ since $a(z) = \frac{-96+48\sqrt{5}}{128}(z^2 + (2+\sqrt{5})^2)(b(z)/z)$. Check $b(z)/z$ has 4 real roots, so $f(z)$ has 4 roots with absolute value $r = \sqrt{5}$, as we found by another way in Example 4.9.

Appendix A. The Geometry of $z + 1/z$

The function $z + 1/z$, particularly how it relates the unit circle and $[-2, 2]$, was used in Section 2 to count roots of a polynomial on the unit circle. We take a closer look here at the geometric effect of this function on the complex plane.

On $\mathbf{C}$, inversion $z \mapsto 1/z$ exchanges the interior and exterior of the unit circle (ignoring the origin) and also the upper and lower half-planes. See Figure 12, where, for instance, the regions marked A and $1/A$ are exchanged. and try to get a feel for how the different parts of the plane get moved around (*e.g.*, regions A and B share a border and so do their inverse regions $1/A$ and $1/B$). This process is quite simple on the unit circle, where inversion is just reflection across the x-axis.

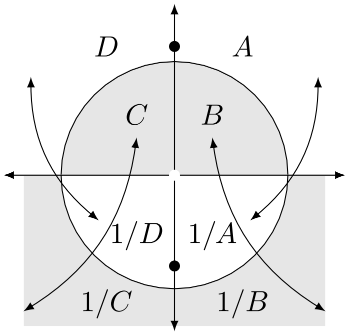

Figure 12. The function $1/z$.

If we look instead at the function $z \mapsto z + 1/z$ on the complex plane (ignoring the origin) then something quite different occurs. This function is 2-to-1 rather than 1-to-1: z and $1/z$ both go to the same place under $z + 1/z$, so the regions A and $1/A$ have the same values, and likewise for other pairs of inverse regions. What happens to the upper half-plane under $z \mapsto z + 1/z$ is illustrated in Figure 13: the regions B and C are spread out to the two quadrants in the lower half-plane and the regions A and D each fill up a whole quadrant in the upper half-plane. So $z + 1/z$ sends the upper half-plane onto the whole complex plane except for $(-\infty, -2]$ and $[2, \infty)$, which are doubly covered by the real line without 0. In the same way $z + 1/z$ on the lower half-plane fills up the complex plane.

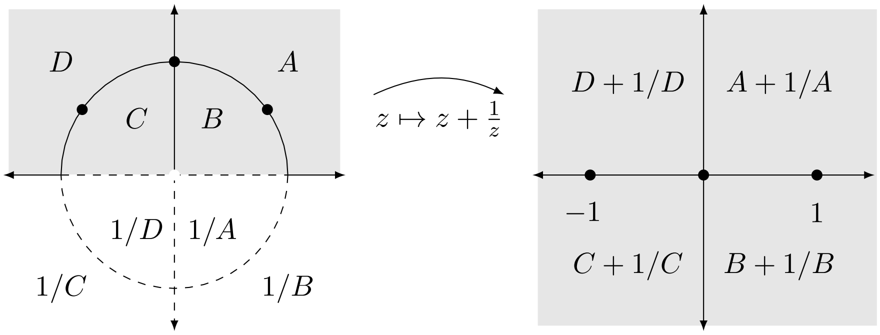

Figure 13. The function $z + 1/z$.

The circular arc from i to 1, which separates A and B, turns into the segment $[0, 2]$ on the real line. However, the boundary separating $A + 1/A$ and $B + 1/B$ is the whole positive x-axis, not just $[0, 2]$. Where did the part of the boundary $[2, \infty)$ between $A + 1/A$ and $B + 1/B$ come from? The explanation is that we should not forget the 2-to-1 nature of $z + 1/z$: we should look at where A has a common boundary with both B and $1/B$, not just $1/B$. That means not only the arc from i to 1 between A and B but also the interval $[1, \infty)$ between A and $1/B$. Under $z \mapsto z + 1/z$ the interval $[1, \infty)$ becomes $[2, \infty)$.

References

[1] E. Ghate and E. Hironaka, *The arithmetic and geometry of Salem numbers*, Bull. Amer. Math. Soc. **38** (2001), 293–314.

[2] G. Kuba, *Several types of algebraic numbers on the unit circle*, Arch. Math. **85** (2005), 70–78.

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

[4] F. Rodriguez-Villegas, *On the zeros of certain polynomials*, Proc. Amer. Math. Soc. **130** (2002), 2251–2254.

[5] J. H. Silverman, "The Arithmetic of Dynamical Systems," Springer-Verlag, NY, 2007.