Needham, Chapter 1, Exercise 34, p. 51
G. Palmer, March 12, 2020, 10 am PST

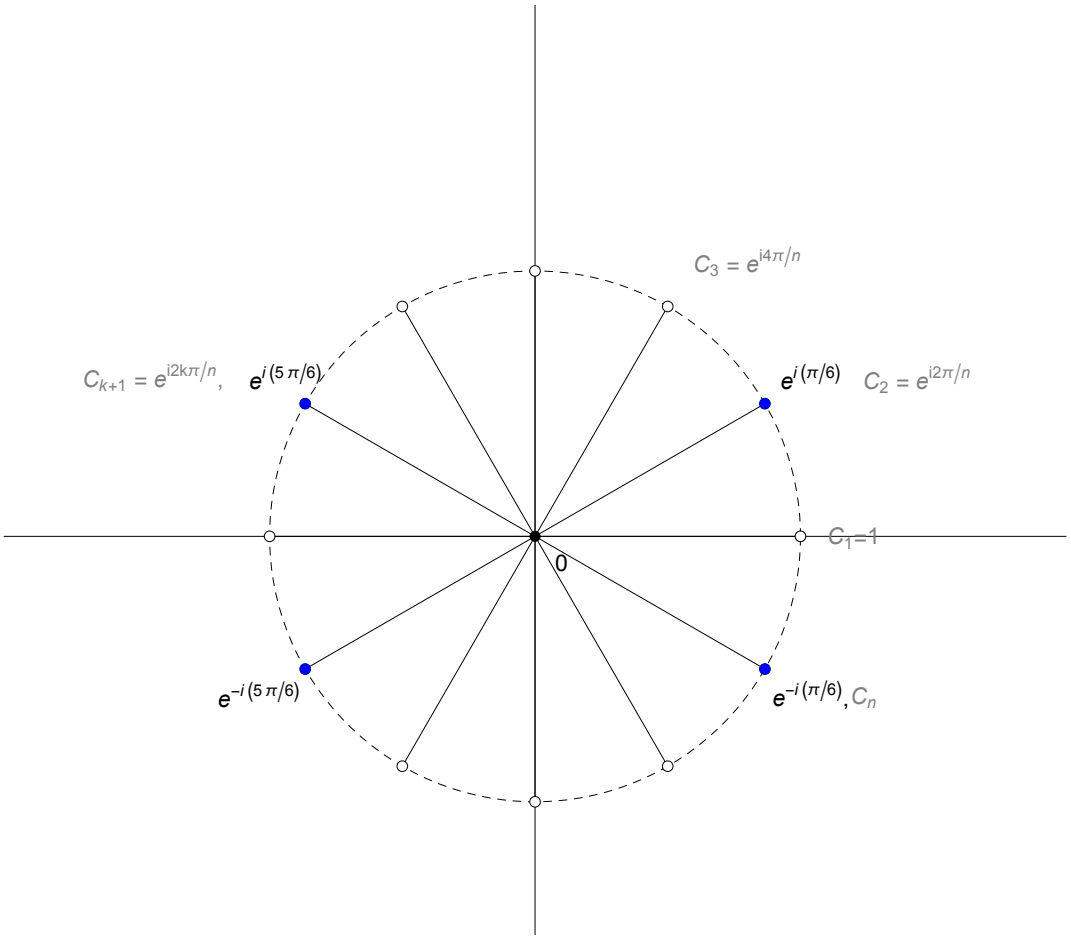


Figure 1. Partial copy of [19] with 12 roots of unity

34 Let S denote the set of 12th roots of unity shown in [19], one of which is $\xi = e^{i(\pi/6)}$. Note that ξ is a primitive 12th root of unity, meaning that its powers yield all of the 12th roots of unity: $S = \{\xi, \xi^2, \xi^3, ..., \xi^{12}\}$.

(i) Find all the primitive 12th roots of unity, and mark them on a copy of [19].

The primitive 12th roots of unity are: $S_p = \{e^{i(\pi/6)}, e^{-i(\pi/6)}, e^{i(5\pi/6)}, e^{-i(5\pi/6)}\}$. They are marked in blue. We can find them by a process of trial and elimination. Let PRU stand for "primitive root of unity".

The first, unquestioned PRU is $e^{ik2\pi/n} = e^{i\pi/6} = \xi$, where k = 1 and n = 12. Let m be the power of ξ. I will refer to ξ as one "step". As we cycle through $\left(e^{i(\pi/6)}\right)^m$, each increment of m takes us to the next root of unity. For each value of k tested, m varies from 1 to 12. Since m = n = 12, $e^{i\pi/6}$ is a PRU. We

have just tested the root associated with k = 1.

For k = 2, the first root is $e^{i\pi/3}$, which is two steps. In taking two steps with each increment of m with $\left(e^{i\pi/3}\right)^m = e^{im\pi/3}$ we skip over one root each turn. The marker lands on only half the roots of unity in the first wind of 6 steps and repeats the exact same pattern on subsequent winds. $e^{i\pi/3}$ is not a PRU. It is also clear that any multiple of k, as in $e^{ik\pi/3}$ will fall on one of the values for k = 2, so multiples of 2 cannot be PRUs. We can therefore rule out $e^{ik2\pi}$ for even k.

For k = 3, the first root is $e^{i\pi/2}$ = i. The powers of $e^{i\pi/2}$ hit only members of {i, -1, -i, 1}. $e^{i\pi/2}$ is not a PRU nor is any $e^{ik\pi/2}$ where k is a multiple of 3. We can therefore rule out $e^{ik2\pi}$ where k = {3, 6, 9, 12}.

We have now eliminated $e^{ik2\pi/n}$, where k = {2, 3, 4, 6, 8, 9, 10, and 12} from the candidates for PRU. We know that k = 1 works. That leaves just 5, 7, and 11 left to test.

For k = 5, the first root is $e^{i5\pi/6}$. Even though $e^{i5\pi/6}$ skips over four roots of unity with each increment of m, $e^{im5\pi/6}$ eventually falls on all the roots of unity. Therefore, $e^{i5\pi/6}$ is a PRU. The conjugate of $e^{i5\pi/6}$ is $e^{i7\pi/6} = e^{-i(5\pi/6)}$, which increases our confidence. We find empirically that 12 successive powers of $e^{i7\pi/6}$ fall on all the roots of unity. The same is true of $e^{i11\pi/6} = e^{-i(\pi/6)}$, which is the conjugate of $e^{i\pi/6}$. Thus, the final roster of PRUs contains two conjugate pairs: $\{e^{i(\pi/6)}, e^{-i(\pi/6)}, e^{i(5\pi/6)}, e^{-i(5\pi/6)}\}$.

(ii) Write down in the form of (16), the factorization of the polynomial $\Phi_{12}(z)$, whose roots are the primitive 12th roots of unity. [In general, $\Phi_n(z)$ is the polynomial (with the coefficient of the highest power of z equal to 1) whose roots are the primitive n^{th} roots of unity; it is called the n^{th} cyclotomic polynomial.

$$\Phi_{12}(z) = (z - e^{i(\pi/6)})\left(z - e^{i(5\pi/6)}\right)(z - e^{-i(\pi/6)})\left(z - e^{-i(5\pi/6)}\right)$$

(iii) By first multiplying out pairs of factors corresponding to conjugate roots, show that $\Phi_{12}(z) = z^4 - z^2 + 1$.

Let a = $(z - e^{i(\pi/6)})(z - e^{-i(\pi/6)}) = z^2 - z e^{i(\pi/6)} - z e^{-i(\pi/6)} + 1$

$= z^2 - 2\, z \cos(\pi/6)\, e^{i(\pi/6)} + 1 = z^2 - z\sqrt{3} + 1$

Let b = $\left(z - e^{i(5\pi/6)}\right)\left(z - e^{-i(5\pi/6)}\right) = z^2 + z\sqrt{3} + 1$

Multiply b by the parts of a:

z^2**b**	$z^4 + z^3\sqrt{3} + z^2$

– z $\sqrt{3}$ b $\quad -z^3\sqrt{3} - 3z^2 - z\sqrt{3}$

1 b $\quad z^2 + z\sqrt{3} + 1$

$$\Phi_8(z) = z^4 + \left(z^3\sqrt{e} - z^3\sqrt{e}\right) + (2z^2 - 3z^2) - (z\sqrt{3} - z\sqrt{3}) + 1$$

$$= z^4 - z^2 + 1$$

This is what we wanted.

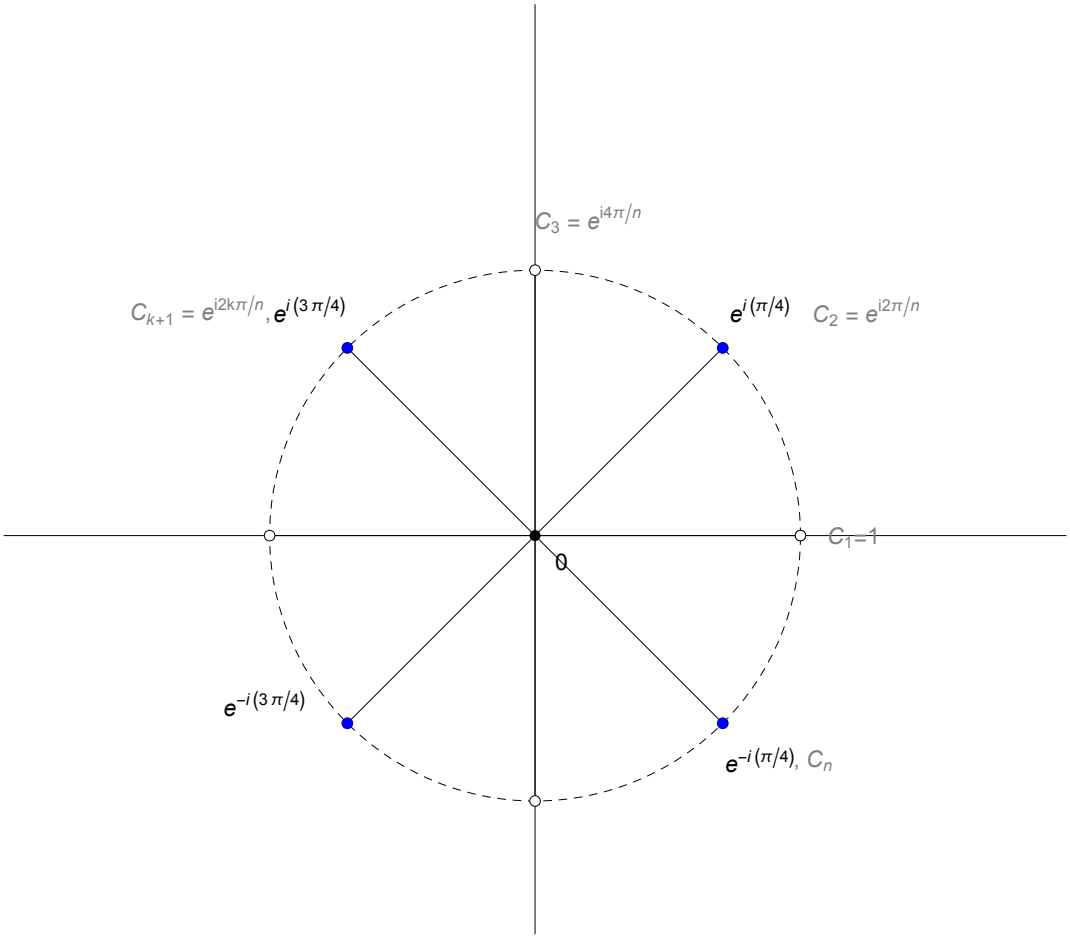


Figure 2. Partial copy of [19] with 8 roots of unity

(iv) By repeating the above steps, show that $\Phi_8(z) = z^4 - 1$.

Figure 2, the primitive roots of unity are again shown in blue.

$\Phi_8(z)$ has 8 roots of unity, so a root can be described as $e^{ik2\pi/8}$. The first root of unity is $e^{i\pi/4}$, which is a PRU because it requires only one additional power to fall on the next root of unity in the anti-clockwise direction. The conjugate $e^{-i\pi/4} = e^{i7\pi/4}$ is also a PRU. Each additional power of $e^{-i\pi/4}$

creates a root one step in the clockwise direction.

k = 2 produces $e^{i\pi/2} = i$, which is not a root of unity, because each power of $\left(e^{i\pi/2}\right)^m$ skips over a root and the identical pattern repeats with each wind. The powers are {i, –1, –i, 1}. We can eliminate $e^{ik2\pi/8}$ where k even.

k = 3 produces $e^{i3\pi/4}$, which is symmetrical about the y axis with the first PRU. This is a PRU and so is $e^{-i3\pi/4}$. That exhausts th candidates for PRU.

The PRUs of $\Phi_8(z)$ are $\{e^{i\pi/4}, e^{-i\pi/4}, e^{i3\pi/4}, e^{-i3\pi/4}\}$. We can write

$$\Phi_8(z) = (z - e^{i\pi/4})(z - e^{-i\pi/4})(z - e^{i3\pi/4})(z - e^{-i3\pi/4})$$

Let $a = (z - e^{i(\pi/4)})(z - e^{-i(\pi/4)}) = z^2 - z e^{i(\pi/4)} - z e^{-i(\pi/4)} + 1$

$$= z^2 - 2\, z \cos(\pi/4) + 1 = z^2 - z\sqrt{2} + 1$$

Let $b = \left(z - e^{i(3\pi/4)}\right)\left(z - e^{-i(3\pi/4)}\right) = z^2 - z e^{i(3\pi/4)} - z e^{-i(3\pi/4)} + 1$

$$= z^2 - 2\, z \cos(3\pi/4) + 1 = z^2 + z\sqrt{2} + 1$$

Multiply b by the parts of a:

$\mathbf{z^2 b}$	$z^4 + z^3\sqrt{2} + z^2$
$\mathbf{-\, z\sqrt{2}\, b}$	$-z^3\sqrt{2} - 2z^2 - z\sqrt{2}$
1 b	$z^2 + z\sqrt{2} + 1$

$$\Phi_8(z) = z^4 + \left(z^3\sqrt{2} - z^3\sqrt{2}\right) + \left(2z^2 - 2z^2\right) - (z\sqrt{2} - z\sqrt{2}) + 1$$

$$= z^4 + 1$$

This is what we wanted.

(v) For a general value of n, explain the fact that if ξ is a primitive nth root of unity, then so is $\overline{\xi}$. Deduce that $\Phi_n(z)$ always has even degree and real coefficients.

If $e^{ik2\pi/n}$ is a primitive root of unity, then $\left(e^{ik2Pi/n}\right)^m = e^{ikm2Pi/n}$ is a root of unity, where m = 1..n and k = 1..n. This can only happen where (1) the primitive root of unity is $e^{i2\pi/n}$, meaning that k = 1, or (2) where the primitive root of unity is $e^{i(\pi - 2\pi/n)}$. In the latter case $e^{im(\pi - 2\pi/n)}$ advances (anticlockwise) by (π - 2π/n) to a new root of unity with each increment of m by 1. Then, since every primitive root of unity has a conjugate, $\Phi_n(z)$ always has even degree. $\Phi_n(z)$ always has real coefficients because the coefficients derive from conjugate pairs of primitive roots of unity which can be written as 2

cos(θ) or they derive from whole number coefficients of z and from 1.

Our two examples were both of degree four. Judging from part (vi), $\Phi_p(z)$ may have higher degrees.

Out[660]=

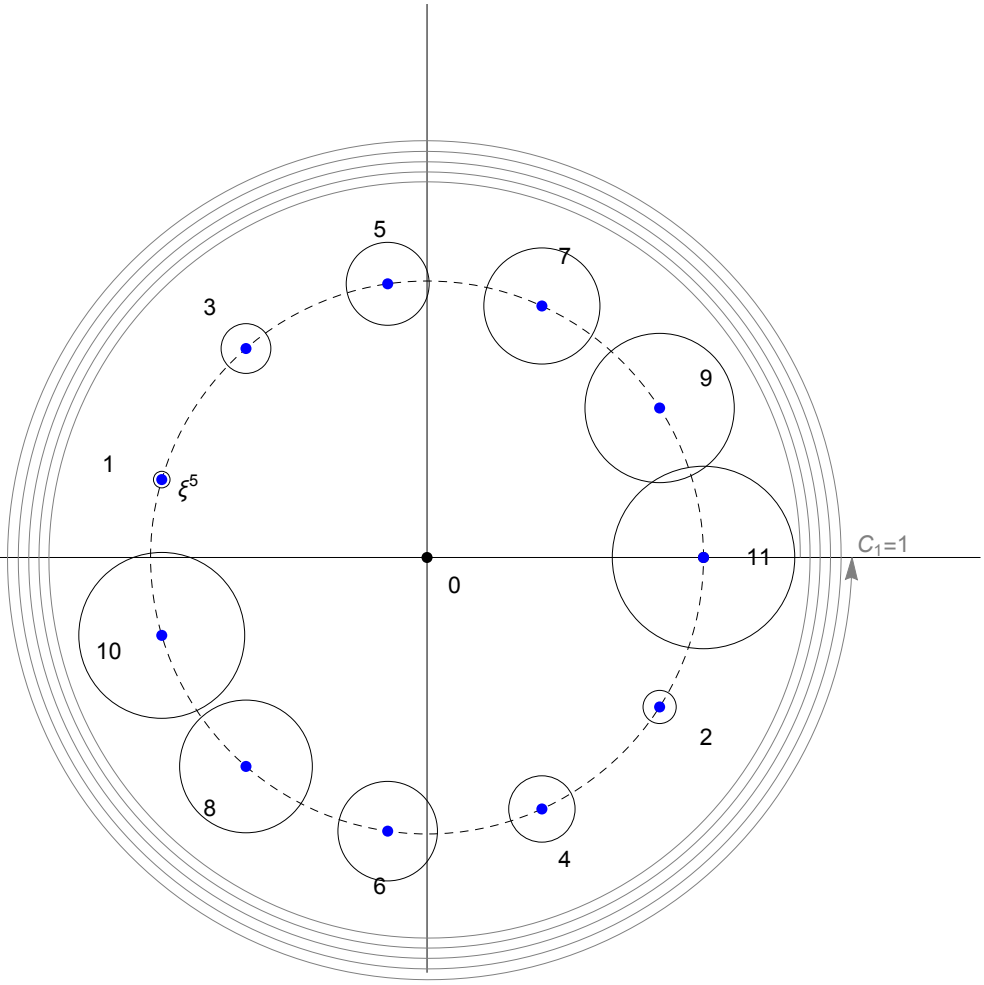


Figure 3. Partial copy of [19] with 11 roots of unity $\xi = e^{i2\pi/11}$
test root is ξ^5, a primitive root of unity

(vi) Show that if p is a prime number then $\Phi_p(z) = 1 + z + z^2 + \cdots + z^{p-1}$.

To solve this, we have to show two things: (1) That every root of unity save C_1 (see Figure 19) (the p^{th} root) is a primitive root of unity; and (2) that the factorization of $\Phi_p(z)$ multiplies out to $1 + z + z^2 + \cdots + z^{p-1}$.

If p is a prime number other than 2, then p is odd, so we set 2 aside as a special case. Since $\Phi_p(z)$ must have even degree (see part v) and p is odd, the highest power of $\Phi_p(z)$ must be no greater than (p – 1). It appears that a polynomial of degree p, where p is prime, has (p – 1) primitive roots of unity. Then every root but one is a PRU and there are (p – 1)/2 conjugate pairs.

There are p roots of unity. Test the roots $e^{\mathrm{i}k2\pi/p}$, k = 1..p by finding their powers $e^{\mathrm{i}mk2\pi/p}$, m = 1..p. For each k, if all the m powers fall on a root of unity, then $e^{\mathrm{i}mk2\pi/p}$ is a PRU.

k = 1; The second root by Figure [19] is the first $\xi = e^{\mathrm{i}2\pi/p}$. Every power $e^{\mathrm{i}k2\pi/p}$ in m = 1..p is a root of unity. Therefore, $e^{\mathrm{i}2\pi/p}$ is a PRU. [I think it would work better to name the roots with $C_n = 1$, but I will stick with Needham's scheme.]

k = 2. This is $\xi^2 = e^{\mathrm{i}4\pi/p}$. The p powers of ξ^2 are $\{e^{\mathrm{i}4\pi/p}, e^{\mathrm{i}2\cdot4\,\pi/p}, e^{\mathrm{i}3\cdot4\,\pi/p}, e^{\mathrm{i}4\cdot4\,\pi/p} \ldots (e^{\mathrm{i}p4\pi/p} = 1)\}$. Since the number of roots of unity is odd, and each power of m skips over one root of unity, the (p-1)/2 power skips the p^{th} root and matches the first root skipped on the first wind. Now the roots skipped over are the roots found on the first wind. At the end of the second wind (beginning at 1), the root $e^{\mathrm{i}m4\pi/p}$ reaches the p^{th} root. Every $e^{\mathrm{i}m4\pi/p}$ except 1 is a PRU. For example, if p = 3, the first root is $e^{\mathrm{i}4\pi3}$. Its square is $e^{\mathrm{i}8\pi/3}$, which skips over the p^{th} root $e^{\mathrm{i}6\pi/3}$. Its cube is $e^{\mathrm{i}12\pi/3} = e^{\mathrm{i}2\cdot3\,\pi/3} = e^{\mathrm{i}2\pi} = 1$, the third root of unity.

This is an empirical way of viewing the problem. But the key here is that p is prime, so no numbers except 1 and p divide p by a whole number. This includes all k in $e^{\mathrm{i}k\pi/p}$ and all powers $e^{\mathrm{i}mk\pi/p}$. No matter what k, other than 1 and p, is tested, powers m ∋ {1..p} of ξ^k fall on roots of unity, but in the traversal of the unit circle C, they also skip over roots of unity. (In Figure 3, test root ξ^5 is indexed with "1". The size of the circles provides a visual clue to the order of generation of roots.) Once a test root ξ^k reaches the p^{th} power, $\xi^{\mathrm{m}k}$ has generated every root exactly once. We know this because if the p powers of ξ^k must traverse the circle k times to get to (generate) the original starting point, then the same applies to every root of unity. When $\xi^{\mathrm{m}k}$ generates a root during the traversal, any root, it traverses the circle k times before generating it again. Since generation stops at C_1, there are too few trips around C to generate any point twice.

Therefore, all the roots of unity except $C_1 = 1$ (the p^{th} power of ξ^k), are primitive roots of unity. It follows that the factorization of the primitive polynomial is

$$\Phi_p(z) = (z - C_2)\,(z - C_3) \ldots \left(z - C_p\right)$$

The indexing here is the same as for Figure [19], with p replacing n. Note that $(z - C_1) = (z\text{-}1)$ is omitted from the primitive factorization. Then, by Descartes' Factor Theorem (p. 26)

$$z^n - 1 = (z - C_1)(z - C_2)\,(z - C_3) \ldots (z - C_n)$$

So we can write

$$\Phi_p(z) = (z - C_2)\,(z - C_3) \ldots \left(z - C_p\right) = \frac{z^p - 1}{z - 1} = 1 + z + z^2 + \cdots + z^{p-1} \quad \text{from Exercise 24.}$$

This is what we wanted.

Some related facts of possible interest

In the special case where p = 2, there can be no conjugate roots of unity.

$\Phi_2(z) = (z+1)$

(z = -1) is primitive.

primitive roots of unity = $\left\{e^{i2\pi/p}, e^{-i2\pi/p}, e^{i4\pi/p}, e^{-i4\pi/p}, \cdots, e^{i\frac{(p-1)}{2}2\pi/p}, e^{-i\frac{(p-1)}{2}2\pi/p}\right\}$

$\Phi_p(z) = (z-e^{i2\pi/p})(z-e^{-i2\pi/p})(z-e^{i(4\pi/p)})(z-e^{-i(4\pi/p)})\cdots (z-e^{i\frac{(p-1)}{2}2\pi/p})(z-e^{-i\frac{(p-1)}{2}2\pi/p})$

Products of conjugate pairs of primitive roots (if coefficients are all real):

1st pair: $z^2-2z\cos(2\pi/p)+1 = z^2-2\,\mathrm{Re}\left(e^{i2\pi/p}\right)z+1$

2nd pair: $z^2-2z\cos(4\pi/p)+1 = z^2-2\,\mathrm{Re}\left(e^{i2\pi/p}\right)z+1$

...

Since p is prime, and there are (p–1) conjugate pairs, (z-1) cannot be a member of such a pair because it lies on the real line.