CYCLOTOMIC POLYNOMIALS AND REGULAR POLYGONS

Jay Villanueva

Miami Dade College

11011 SW 104 St.

Miami, FL 33176

jvillanu@mdc.edu

(*Abstract*.) The irreducible factors of the binomial equation $z^n - 1 = 0$ give the cyclotomic equations. Their solution gives *n* points around the circumference of the unit circle, which locate the vertices of the regular polygon of *n* sides inscribed in the circle. Thus, solving the cyclotomic equations solves the regular *n* – gon, and getting the distance between neighboring vertices gives the side *L* of the regular polygon. The harder problem is to express this side *L* in terms of radicals. We will demonstrate this for two cases: (a) for *n* = 5 and (b) for *n* =17. For the pentagon we will use a trick from De Moivre, and for the 17 – gon, we will use the more general method of Gauss. We will then assert that in general the cyclotomic equation of any degree *n* is solvable, and that the side *L* of any constructible polygon of *n* sides

$$n = 2^r p_1 p_2 \dots p_m,\ r, m = integers,\ \ p_m = 2^{2^m} + 1,$$

may be expressed in terms of radicals.

The binomial equation $z^n - a = 0$ is among the simplest polynomial equation, yet its study could get quite involved especially when $a \neq 1$. When $a = 1$, its roots are given by De Moivre's formula, known as the *n*th roots of unity, consisting of $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ and its first *n* powers, $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$. Clearly, when *n* is a prime, every *n*th root of unity (except 1) is a root of

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1,$$

which is irreducible. In factored form

$$x^n - 1 = \prod\left(x - \zeta_n^i\right),\quad 0 \leq i < n.$$

We define the *n*th cyclotomic polynomial $\Phi_n(x)$ to be the product

$$\Phi_n(x) = \prod\left(x - \zeta_n^i\right), \quad 0 \le i < n, \gcd(i,n) = 1.$$

Thus the roots of $\Phi_n(x)$ are ζ_n^i for those $0 \le i < n$ relatively prime to *n*. For example,

$\Phi_1 = x - 1,\ \Phi_2 = x + 1,\ \Phi_3 = x^2 + x + 1,\ \Phi_4 = x^2 + 1$, we will show

$\Phi_5 = x^4 + x^3 + x^2 + x + 1,\ \Phi_6 = x^2 - x + 1.$

The roots of $z^n - 1 = 0$ are given by

$$z_k = \zeta_n^k = e^{2\pi ik/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0,1,2,\ldots,n-1.$$

In the complex plane their locations give the vertices of the regular polygon of *n* sides inscribed in the unit circle. Finding the side *L* of the regular polygon inscribed in the unit circle is easy for $n = 3, 4, \& 6$. It is a challenge to find a rational expression for $n = 5$, which we will show, and also for $n = 17$.

(i) For a triangle ($n = 3$), the central angle is $\theta = 2\pi/3$:

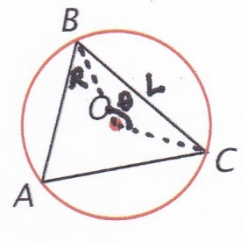

Figure 1. Finding the side *L* of a regular triangle inscribed in a unit circle.

$$\frac{L}{2} = R\sin\frac{\theta}{2} = R\sin\frac{\pi}{3} \ \Rightarrow\ L = R\sqrt{3}.$$

(ii) For a square ($n = 4$), $\theta = 2\pi/4$:

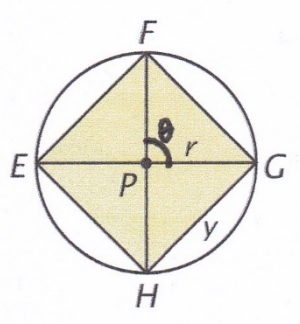

Figure 2. A square in a unit circle.

$$\frac{L}{2} = R\sin\frac{\theta}{2} = R\sin\frac{\pi}{4} \;\Rightarrow\; L = R\sqrt{2}.$$

(c) For a hexagon $(n = 6), \theta = 2\pi/6$:

Figure 3. A regular hexagon in a unit circle.

$$\frac{L}{2} = R\sin\frac{\theta}{2} = R\sin\frac{\pi}{2} \;\Rightarrow\; L = R.$$

Finding L for the pentagon is challenge. First of all, $\theta = 2\pi/5$ is not a special angle. Second, the cyclotomic equation is of degree 4:

(1) $$\frac{z^5-1}{z-1} = z^4 + z^3 + z^2 + z + 1 = 0.$$

We use a neat trick from De Moivre. Let

(2) $$t = z + \frac{1}{z}, \;\; t^2 = z^2 + 2 + \frac{1}{z^2}.$$

And (1) becomes

$$t^2 + t - 1 = 0 \quad \text{with solutions} \quad t = \frac{-1\pm\sqrt{5}}{2}.$$

Back to *z,* we get two equations:

$$z^2 - vz + 1 = 0 \quad \text{with} \quad v = \frac{-1+\sqrt{5}}{2}, \text{ and}$$

$$z^2 - v'z + 1 = 0 \quad \text{with} \quad v' = \frac{-1-\sqrt{5}}{2},$$

with solutions

$$z_{1,4} = \frac{\sqrt{5}-1\pm\sqrt{-10-2\sqrt{5}}}{4} \quad \text{and} \quad z_{2,3} = \frac{-\sqrt{5}-1\pm\sqrt{-10+2\sqrt{5}}}{4}.$$

Now, all five vertices of the pentagon are found. The side L is the distance between adjacent vertices. This is easiest done for $L = |z_2 - z_3| = \sqrt{\frac{5-\sqrt{5}}{2}}$.

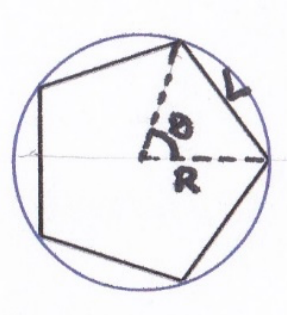

Figure 4. A regular pentagon inscribed in a unit circle.

As a check, from previous results for $n = 4$ & 6:

$$1R < L < \sqrt{2}\,R, \;\; R = 1,$$

and $$L = \sqrt{\frac{5-\sqrt{5}}{2}}\,R = 1.175571R.$$

Or, we can evaluate

$$L = 2R\sin\frac{\theta}{2} = 2(1)\sin\frac{2\pi}{2(5)} = 1.175571.$$

One remarkable achievement by Gauss is the discovery that the regular polygon of 17 sides is constructible, that is, its side L is expressible in radicals. (Since Euclid's time no mathematician has thought about this.) To show this.

First, its cyclotomic equation is of degree 16:

$$\frac{z^{17}-1}{z-1} = z^{16} + z^{15} + \cdots + z + 1 = 0.$$

De Moivre's trick will not work here for we will end up with an equation of degree 8. For the case $n = 17$, we will use the more general method of Gauss's law of periods of the cyclotomic equations. Gauss showed that the cyclotomic equations of prime degree p may be reduced to equations of degree equal to the prime factors of $p - 1$. In particular, the 17th

roots of unity are determined by solving successively 4 quadratic equations: $17 - 1 = 2^4$. We will do the computations now and justify the theory later.

Note that the 17th roots of unity are given by $g = 3$, i.e., the powers of 3 mod 17 are:

m	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
3^m	1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6.

Now, let $\zeta^k = e^{i2\pi k/17}$,

$$y_1 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

$$y_2 = \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 + \zeta^1.$$

Then, using the identities

$$e^{i\frac{2\pi k}{17}} + e^{-i\frac{2\pi(17-k)}{17}} = 2\cos\frac{2\pi k}{17} \quad \text{and}$$

$2\cos\alpha\cos\beta = \cos(\alpha+\beta) + \cos(\alpha-\beta)$, we get

$$y_1 + y_2 = -1, \;\; y_1 y_2 = -4.$$

Thus, y_1 and y_2 satisfy the quadratic equation:

(3) $$y^2 + y - 4 = 0,$$

and therefore $y_1 = \frac{-1-\sqrt{17}}{2}$ and $y_2 = \frac{-1+\sqrt{17}}{2}$.

In y_1 and y_2, take:

$$y_{11} = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}$$

$$y_{12} = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6$$

$$y_{21} = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$$

$$y_{22} = \zeta^{13} + \zeta^{16} + \zeta^4 + \zeta^1.$$

Then: $y_{11} + y_{12} = y_1$ and $y_{11}y_{12} = -1$.

And y_{11}, y_{12} satisfy

(4) $$y^2 - y_1 y - 1 = 0,$$

And therefore $y_{11} = \frac{y_1+\sqrt{y_1^2+4}}{2}$ and $y_{12} = \frac{y_1-\sqrt{y_1^2+4}}{2}$.

Similarly,

(5) $y_{21} = \frac{y_2+\sqrt{y_2^2+4}}{2}$ and $y_{22} = \frac{y_2-\sqrt{y_2^2+4}}{2}$

The next period:

$$y_{111} = \zeta^3 + \zeta^{14} \qquad y_{211} = \zeta^9 + \zeta^8$$
$$y_{112} = \zeta^5 + \zeta^{12} \qquad y_{212} = \zeta^{15} + \zeta^2$$
$$y_{121} = \zeta^{10} + \zeta^7 \qquad y_{221} = \zeta^{13} + \zeta^4$$
$$y_{122} = \zeta^{11} + \zeta^6 \qquad y_{222} = \zeta^{16} + \zeta^1.$$

The last two:

$y_{221} + y_{222} = y_{22}$ and $y_{221}y_{222} = y_{11}$ satisfy

(6) $y^2 - y_{22}y + y_{11} = 0.$

And ther6efore $y_{221} = \frac{y_{22}-\sqrt{{y_{22}}^2-4y_{11}}}{2}$ and $y_{222} = \frac{y_{22}+\sqrt{{y_{22}}^2-4y_{11}}}{2}$.

The last periods are ζ^1 and ζ^{16}, with $\zeta^1 + \zeta^{16} = y_{222}$ and $\zeta^1\,\zeta^{16} = 1$. Thus,

$$\zeta^1 = \frac{y_{222}+\sqrt{{y_{222}}^2-4}}{2}.$$

$$\Rightarrow \cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17} + \frac{1}{8}\sqrt{17} + 3\sqrt{17} - 2\sqrt{34 + 2\sqrt{17}}}.$$

The law of periods of Gauss follows from group theory. The roots of unity $\zeta^k = e^{i2\pi k/n}$, $k = 0,1, \dots, n-1$, form a cyclic group Z_n whose order is $|Z_n| = \varphi(n)$, the number of integers *i,* $0 \le i < n$, relatively prime to *n* ($\varphi(n)$ is Euler's totient function). Because

$$\zeta^k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n},$$

$$e^{i\frac{2\pi k}{n}} + e^{-i\frac{2\pi(n-k)}{n}} = 2\cos\frac{2\pi k}{n}, \quad \text{and}$$

$$2\cos\alpha\cos\beta = \cos(\alpha+\beta) + \cos\alpha\ -\beta),$$

we get periods for the roots. For example, for $n = 7$, we get $n - 1 = 6 = 3 \cdot 2$, i.e., 3 2-periods; for $n = 17$, we get $n - 1 = 16 = 2^4$, or 4 quadratic equations to solve, as we have illustrated.

Concluding remarks. The more general binomial equation $z^n - a = 0$, for some element *a* in a field *F*, has roots given by De Moivre's formula. If one root is given, then all the roots are known, for, if $b = \sqrt[n]{a}$, the real root and $\zeta^k = e^{i2\pi k/n}$, then all the other roots are $b, b\zeta, b\zeta^2, \ldots, b\zeta^{n-1}$, ad all these rots are also in *F.* In the complex plane, the points $\left(\cos\frac{2\pi k}{n}, \sin\frac{2\pi k}{n}\right)$ for $k = 0,1,2, \ldots, n-1$, which represent the *n*th roots of unity, are the vertices of a regular polygon with *n* sides: they divide the circumference into *n* equal parts. For this reason, the theory which is concerned with *n*th roots of unity, or with the sine and cosine of $2\pi k/n$ for integers *k, n,* is called *cyclotomy,* meaning 'division of the circle' into equal parts.

- All roots of $z^n - a = 0$ are known for any integer *a.*
- All roots of the cyclotomic equation $\Phi_n = 0$ are known for arbitrary integer *n.*
- The roots of unity $\zeta^k = e^{i2\pi k/n}$ are solutions to the binary equation $z^n - 1 = 0$, and represent the vertices of a regular polygon of *n* sides inscribed in a unit circle.
- All roots of the cyclotomic equation $\Phi_n = 0$ are expressible as radicals.
- When the roots of unity are expressible in radicals this means the corresponding regular polygon is constructible by straightedge and compass.
- We demonstrated by an explicit calculation that the side of a regular pentagon is expressible in radicals, and that the pentagon is constructible.
- We also showed by an actual calculation that the regular 17-gon is constructible.
- A regular *n*-gon is constructible if the number of sides is given by

  $n = 2^r p_1 p_2 \ldots p_m$, r a + integer, and

  $p_m = 2^{2^m} + 1$, $m \geq 0$ integer.

References

1. B. Bold, 1969. *Famous Problems in Geometry & How to Solve Them.* NY: Dover.
2. JA Beachy & WD Blair, 1996. *Abstract Algebra.* IL: Waveland Press.
3. F Butin, 2019. *Algebra.* NY: Dover.
4. R Courant, H Robbins, & I Stewart, 1996. *What Is Mathematics?* Oxford University Press.
5. D Cox, 2004. *Galois Theory.* NJ: J Wiley & Sons.
6. JB Fraleigh, 1999. *A First Course in Abstract Algebra.* MA: Addison Wesley.
7. CR Hadlock, 1978. *Field Theory and its Classical Problems.* Math Asso America.

8. JM Howie, 2006. *Fields & Galois Theory.* NY: Springer Verlag.
9. HR Jacobs, 2003. *Geometry.* NY: Freeman & Co.
10. F Klein, 1930. *Famous Problems of Elementary Geometry.* NY: Stecher.
11. JE Maxfield & MW Maxfield, 1971. *Abstract Algebra & Solution by Radicals.* NY: Dover.
12. CC Pinter, 1982. *A Book of Abstract Algebra.* NY: Dover.
13. I Stewart, 2015. *Galois Theory*. FL: CRC Press.
14. JP Tignol, 2001. *Galois Theory of Algebraic Equations.* NJ: World Scientific Publ Co.