THE CYCLOTOMIC EQUATION AND ITS SIGNIFICANCE TO SOLVING THE QUINTIC EQUATION

Jay Villanueva
Florida Memorial University
Miami, FL 33055
jvillanu@fmuniv.edu
ICTCM 2013

I. Introduction
A. The cyclotomic equation
B. The solution of polynomial equations by radicals

II. Solution of the cyclotomic equation
A. De Moivre
B. Vandermonde
C. Gauss

III. Significance of the cyclotomic equation
A. Construction of regular polygons by straightedge and compass
B. Solving the quintic equation

IV. Conclusions

****

I. Introduction

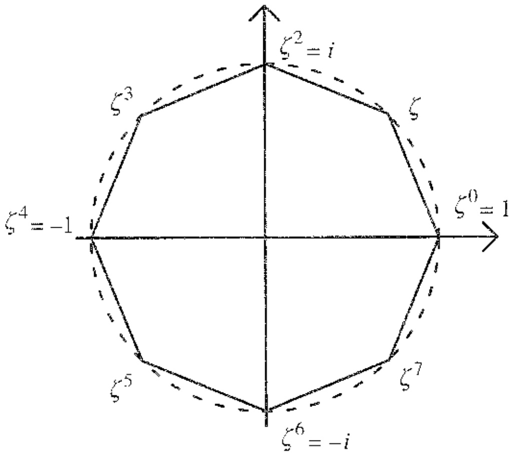
As teachers and researchers in mathematics we often need to solve equations. The linear and quadratic equations are easy. There are formulas for the cubic and quartic equations, though less familiar. There are no general methods to solve the quintic and other higher order equations. It would be good to have some readily solution to the solvable quintics, if we need them. The cyclotomic equation provides just that. In the field of complex numbers, the cyclotomic equation is:

$$(1) \qquad x^n - 1 = 0$$

where n is an integer, whose solutions are given by DeMoivre's theorem:

$$(2) \qquad x_k = \zeta_k = e^{2\pi i k/n} = cos\left(\frac{2\pi k}{n}\right) + i\ sin\left(\frac{2\pi k}{n}\right),\ k = 0, 1, 2, \ldots, n-1.$$

These are known as the roots of unity. In the complex plane, these roots of unity divide the arc of the unit circle into n segments of equal length, starting from (1, 0).



In the figure, the eighth roots of unity are shown, for $n = 8$.

The more general equation is:

(3) $$x^n - a = 0$$

and its zeros are:

(4) $$x_k = \sqrt{a}\,\zeta_k,$$

with ζ_k as above, and *a* a real number.

Since ancient times mathematicians have been concerned with solving polynomial equations. The solutions were written in terms of the coefficients of the equation and using only the operations of addition, subtraction, multiplication, division, and the extraction of roots; this is called the solution by radicals. The quadratic formula was known essentially to the Babylonians by 2000 BC; the cubic and quartic formulas were discovered during the Renaissance by Italian mathematicians. But there was no formula for the quintic equation. It was only to be found 300 years later that there cannot be a solution by radicals to the general quintic equation (Galois theory), although some specials forms of the quintic do have solutions. The cyclotomic equation is the simplest such solution.

II. Solutions to the cyclotomic equation

A. De Moivre

DeMoivre (1706) obtained solutions for small prime n. Since 1 is a solution of (1), we may divide $x^n - 1$ by $x - 1$ to get:

(5) $$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0.$$

Thus, for $n = 2$, the solution is -1, and for $n = 3$, the solution is $(-1 \pm i)/2$. For $n = 5$, he had a clever substitution. First, divide by x^2 (where the exponent is $\frac{n-1}{2} = 2$), and change variables to $y = x + x^{-1}$. Thus, Eq. (5) becomes:

(6) $$x^4 + x^3 + x^2 + x + 1 = 0, \rightarrow \quad x^2 + x + 1 + x^{-1} + x^{-2} = 0$$
$$\rightarrow \quad y^2 + y - 1 = 0,$$

a quadratic whose solutions are $y = \left(-1 \pm \sqrt{5}\right)/2$, and therefore,

(7) $$x_{2,3} = \left(\sqrt{5} - 1 \pm \sqrt{-10 - 2\sqrt{5}}\right)/4 \text{ and } x_{4,5} = \left(-\sqrt{5} - 1 \pm \sqrt{-10 + 2\sqrt{5}}\right)/4.$$

The next prime, $n = 7$, yields for $y = x + x^{-1}$, the cubic equation

(8) $$y^3 + y^2 - 2y - 1 = 0,$$

which can be solved by radicals; the 7th roots of unity can therefore be expressed by radicals. However, for the next prime, $n = 11$, DeMoivre's trick yields an equation of degree 5,

(9) $$y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1 = 0,$$

for which no general formula by radicals is known. Solving this equation was one of the greatest achievements of Vandermonde.

B. Vandermonde

DeMoivre had shown that the problem of determining radical expressions for the roots of unity can be reduced to the solution by radicals of the alternate cyclotomic equation:

(10) $$\phi_n(x) = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

for n prime. And the substitution $y = (x + x^{-1})/2$ converts the equation above into an equation of degree $(n-1)/2$. Moreover, since the roots of ϕ_n are the complex numbers

$$e^{2\pi ik/n}, \quad \text{for } k = 1, 2, \ldots, (n-1)/2,$$

it follows that the roots of the equation in y are the values

(11) $$2cos(2\pi ik/n), \quad \text{for } k = 1, 2, \ldots, (n-1)/2.$$

Vandermonde made use of these results to obtain the radical solutions for $n = 11$, Eq. (9). In fact, he used the equivalent substitution $z = -(x + x^{-1})$, which yields the equation:

(12) $$z^5 - z^4 - 4z^3 + 3z^2 + 3z - 1 = 0.$$

Vandermonde then chose the roots to be:

(13) $$a = -2cos\frac{2\pi}{11},\ \ b = -2cos\frac{4\pi}{11},$$
$$c = -2cos\frac{6\pi}{11},\ \ d = -2cos\frac{8\pi}{11},\ \ e = -2cos\frac{10\pi}{11}.$$

He noted that the trigonometric identity

(14) $$2cos\alpha cos\beta = \cos(\alpha+\beta) + \cos(\alpha-\beta)$$

can be used to obtain relations between the roots. In fact, he used the relations between the roots to express the 11th roots of unity in terms of radicals, and leaves the problem there. Thus, the solution of the cyclotomic equation for prime *n* up to 11 was known by 1771. The problem stayed there until 1796 when Gauss gave the full solution.

[Some authors lament the fact that although Vandermonde made two brilliant discoveries on the solution of equations, he did not quite understand the significance of his discoveries:

i. The existence of relations between the roots, which can be used to reduce to degree 1 each polynomial expression in the roots;
ii. The existence of a cyclic permutation of the roots which preserves the relations between them.

The existence of a cyclic permutation which preserves the relation between the roots is a remarkable, though mysterious, property of cyclotomic equations, which should have awakened Vandermonde's curiosity. If he investigated this property carefully, he could have developed the theory of cyclotomy about thirty years before Gauss. Moreover, Vandermonde had pinpointed the very basic idea of Galois theory: in order to determine the 'structure' of an equation, deciding eventually if it is solvable by radicals, one has to look at the permutation of the roots; we only need to consider those permutations which preserve the relations between the roots. Vandermonde had missed out at two very important opportunities of great achievements.]

C. Gauss

The contributions of Gauss to the theory of equations – namely, the fundamental theorem of algebra and the solution of cyclotomic equations, in particular – are among his outstanding achievements, and also his earliest (1796). Gauss' results on the cyclotomic equations show how to complete Vandermonde's methods for any higher prime *n*. They were a thorough description of the reduction of the cyclotomic equation of prime index to equations of smaller degree. He showed that the solution of $\phi_n(x) = 0$ can be reduced to the solution of equations of degree equal to the prime factors of $n-1$. In particular, the 17th roots of unity can be determined by solving successively four quadratic equations, since $17-1=2^4$. As an application of this result, he showed that the regular polygon of

17 sides can be constructed by ruler and compass, a result he derived in his teens and is said to have determined his choice of vocation.

Gauss published his definitive account of the solution of cyclotomic equations as the final section of his treatise on number theory, *Disquisitiones Arithmeticae* (1801). His principal results were: (i) that the cyclotomic equation of prime index n is irreducible, a key result; (ii) that the cyclotomic equation of index $n-1$ is reducible to equations of degree equal to the prime factors of $n-1$; and (iii) that the cyclotomic equation is solvable by radicals. In fact, since any integer can be shown to be the product of primes, the cyclotomic equation of any degree is now completely solved.

(i) The irreducibility theorem may be stated thus: For n a prime, The cyclotomic polynomial $\phi_n(x)$ is irreducible (not factorable) over the field of rational numbers. Over the years, the proof has been generalized and simplified by other mathematicians, among them Eisenstein, whose theorem is now: Let

$$P = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$$

be a monic polynomial (i.e., the leading coefficient is 1) with integer coefficients c_i. If there is a prime p which divides $c_i, i = 0, 1, \dots m-1$ but such that p^2 does not divide c_0, then P is irreducible over the rationals. The importance of Gauss' irreducibility theorem is that it allows us to reduce every rational expression in the n^{th} roots of unity to polynomials of lower degree.

(ii) The cyclotomic polynomial $\phi_{n-1}(x)$, n a prime, may be decomposed into polynomials of lower degree which are the prime factors of $n-1$. This decomposition essentially simplifies the solution of the original equation for then the lower factors may be successively decomposed themselves into yet lower factors. Thus, a primitive 17th root of unity (an n^{th} root other than 1) can be determined by solving successively four quadratic equations ($n - 1 = 2^4$). This is the key fact which leads to the construction of the regular polygon of 17 sides by straightedge and compass alone. As a corollary, Wantzel published a result in 1837 (which was undoubtedly known to Gauss in 1796) that: The regular polygon of n sides can be constructed with ruler and compass if n is a product of distinct Fermat primes and a power of 2. (A Fermat prime is an integer of the form $2^{2^n} + 1$ for some integer n. These are indeed primes for $n = 0, 1, 2, 3, 4,$ but for $n = 5,$ Euler showed in 1732 that it is $= 641 \cdot 6700417,$ and since then it has been shown that there are no other Fermat primes for $5 \leq n \leq 16$.)

(iii) Gauss' final result is that the cyclotomic equation $\phi_n(x) = 0$ is solvable by radicals for every prime n. In fact, in full generality, for every integer n the n^{th} roots of unity can be expressed in terms of radicals. Taking the modern viewpoint, the Galois group of the cyclotomic equation of index p, $\phi_{p-1}(x) = 0$, over the rationals, is a cyclic group of order $p-1$. We now know that the general cyclic group is a solvable group. Thus, the cyclotomic equation is solvable by radicals.

III. Significance

The importance of the cyclotomic equation in the history of mathematics is that it provided us with the simplest example of a closed solution of the quintic equation by radicals. Although there are no formulas to solve a general quintic, the cyclotomic equation is an instance of a simple closed solution. There are other forms of the quintic equation that are solvable, but the cyclotomic equation is the simplest of these. In fact, since it is solvable for any integer *n,* it gave us a closed solution for a polynomial equation of any degree *n.* In addition, in Euclid's time, all known constructions of the regular polygon were restricted to the triangle, square, pentagon, and their multiples. Nothing was added to these for 2000 years. Gauss showed that there is a regular n-gon for every n a product of distinct Fermat primes and a power of 2. In particular, he demonstrated the construction of the regular heptadecagon $(n = 17)$.

As a summary of results: (i) the cyclotomic equation is readilty solved by DeMoivre's formula, which divides the arc of the unit circle into *n* equal parts; but these solutions are expressed in terms of trigonometric or complex exponential functions; (ii) the goal, as in classical algebra, is to write the solutions in terms of radicals; this was done by DeMoivre and Vandermonde, for small values of the degree *n,* and by Gauss, for all values *n;* (iii) Gauss also showed that the construction of regular polygons by straightedge and compass was related to the solution of the cylotomic equation; thus, he showed that the construction can be effected whenever the number of sides is a product of distinct Fermat primes and a power of 2; (iv) in modern times, Galois theory shows us why the cyclotomic equation is solvable by radicals for any integer *n.*

V. Conclusions

The roots of the cyclotomic equation (the roots of unity) can readily be found from DeMoivre's theorem, which solutions divide the arc of the unit circle into *n* equal parts. By a suitable transformation, the roots can be expressed in terms of radicals, which can be done for *n* a prime, and also for any integer *n.* The cyclotomic equation is significant in that it gave us the simplest closed-form solution to the quintic equation, which is an insolvable equation in terms of radicals (and other higher-order equations as well). Solving the cyclotomic equation also solved the classical problem of constructing the regular polygon by straightedge and compass. The construction is feasible whenever the number of sides is a product of distinct Fermat primes and a power of 2.

References:

1. JA Beachy and WD Blair, 1996. *Abstract Algebra.* IL: Waveland Press.
2. J Bewersdorf, 2006. *Galois Theory for Beginners*. Providence, RI: American Mathematical Society.
3. D Cox, 2004. *Galois Theory*. NJ: J Wiley & Sons.
4. J Fraleigh, 2000. *Abstract Algebra*. Reading, MA: Addison-Weslley.

5. JJ Rotman, 2000. *A first Course in Abstract Algebra*. Upper Saddle River, NJ: Prentice-Hall.
6. JP Tignol, 2001. *Galois' Theory of Algebraic Equations.* NJ: World Scientific.