# Solutions of Polynomial Equations

Donald Rideout, Memorial University of Newfoundland[1]

Polynomial equations have a lengthy history. A Babylonian tablet of 1600 B.C. poses problems which reduce to the solution of quadratic equations. It is clear that they could solve them, but they had no algebraic notion with which to express their solution. The ancient Greeks solved quadratics by geometric constructions and had methods applicable to cubic equations involving points of intersection of conics. Algebraic solutions of the cubic were unknown until the middle of the 16th century. The Italian school of Bologna, at the time of the Renaissance, discovered that the solution of the cubic could be reduced to that of three basic types:

$$x^3 + px = q, \quad x^3 = px + q, \quad x^3 + q = px.$$

They were forced to distinguish these cases because they did not recognize the existence of negative numbers. One of the group, Scipio del Ferro, is believed to have solved the equation $x^3 + px = q$. This solution was kept secret and was rediscovered by another of the group, Niccolo Fontana (nicknamed Tartaglia), in 1535. He communicated his solution to Girolano Cardano, having first sworn him to secrecy. But when Cardano's *Ars Magna* appeared in 1545, it contained a complete discussion of Fontana's solution, with acknowledgement to the discoverer. We will give his solution below, and we will make use of negative numbers, thereby combining the three cases above.

At the beginning of the last century, the central problem of the theory of equations was to find a formula that would express a root of the polynomial equation

$$x^n + a_1 x^{n-1} + \ldots + a_{n-2} x^2 + a_{n-1} x + a_n = 0$$

in terms of the coefficients $a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n$. It was assumed that such a formula could be written in terms of arithmetic operations of the coefficients and extraction of roots. What was wanted were analogues of the formulas

$$x = -a_1 \quad \text{and} \quad x = \frac{1}{2}(-a_1 \pm \sqrt{a_1^2 - 4a_2})$$

that solve the problem in cases $n = 1$ and $n = 2$, respectively. Even here we encounter some difficulties. We are assuming that the coefficients are real numbers, but the quadratic equation $x^2 + a_1 x + a_2 = 0$ may have complex number solutions. For example, the solutions of $x^2 + x + 1 = 0$ are $x = \frac{1}{2}(-1 \pm \sqrt{3}i)$ where $i$ is one of the solutions of $z^2 + 1 = 0$ and is sometimes written $i = \sqrt{-1}$.

The arithmetic of complex numbers is very straightforward if we remember to replace $i^2$ by $-1$. If $z_1 = x_1 + y_1 i$ and $z_2 = x_2 + y_2 i$ are two complex numbers, then

$$\begin{aligned} z_1 + z_2 &= (x_1 + x_2) + (y_1 + y_2)i \\ z_1 z_2 &= (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i. \end{aligned}$$

[1]Talk given at CMC Seminar, Waterloo, June 1997

If $= x + yi$, then $\overline{z} = x - yi$ is called the *conjugate* of $z$ and $|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}$ is called the *modulus* of $z$ and is usually denoted by $r$. If $z \neq 0$, then $r > 0$ and any number $\theta$ such that $\cos\theta = \frac{x}{r}$ and $\sin\theta = \frac{y}{r}$ is called an *amplitude* or *argument* of $z$. If $\theta$ is chosen so that $-\pi < \theta \leq \pi$, then $\theta$ is called the *principal amplitude* of $z$. In terms of $r$ and $\theta$, we have

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

So written, $z$ is said to be expressed in *modulus-ampitude* or *polar* form. For example, $z = 1 + i = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$, $z = \frac{1}{2}(-1 + \sqrt{3}i) = 1(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3})$, and $z = \frac{1}{2}(-1 - \sqrt{3}i) = 1(\cos\frac{-2\pi}{3} + i\sin\frac{-2\pi}{3})$. In the modulus-amplitude form, the arithmetic of complex numbers is made easy by the very fascinating de Moivre's Theorem which states that

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

where $n$ is any integer and $\theta$ is any real number. The formula also holds if the plus is replaced by a minus on both sides of the equation. We observe from de Moivre's formula that for any positive integer $n$,

$$(\cos\frac{\theta}{n} \pm i\sin\frac{\theta}{n})^n = \cos(n\cdot\frac{\theta}{n}) \pm i\sin(n\cdot\frac{\theta}{n}) = \cos\theta \pm i\sin\theta,$$

and more generally

$$(\cos\frac{\theta + 2k\pi}{n} \pm i\sin\frac{\theta + 2k\pi}{n})^n = \cos(\theta + 2k\pi) \pm i\sin(\theta + 2k\pi) = \cos\theta \pm i\sin\theta.$$

Hence the numbers $\cos\frac{\theta+2k\pi}{n} + i\sin\frac{\theta+2k\pi}{n}$ are called the $n$th roots of $\cos\theta + i\sin\theta$. The integers $k$ can be restricted so that $0 \leq k < n$, since other $k$'s will lead to duplicate complex numbers. Since $(\cos\frac{2k\pi}{3} + i\sin\frac{2k\pi}{3})^3 = \cos 2k\pi + i\sin 2k\pi = 1$, the numbers $\cos\frac{2k\pi}{3} + i\sin\frac{2k\pi}{3}$ for $0 \leq k \leq 2$ are called the cube roots of 1 or cube roots of unity. They are usually denoted by

$$1, \quad \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \ \text{ and } \ \omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

We will record for later use the cube roots of $\omega$. They are

$$\cos\left(\frac{\frac{2\pi}{3} + 2k\pi}{3}\right) + i\sin\left(\frac{\frac{2\pi}{3} + 2k\pi}{3}\right) = \cos\frac{(2+6k)\pi}{9} + i\sin\frac{(2+6k)\pi}{9}$$

for $0 \leq k \leq 2$. Similarly, $\cos\frac{(2+6k)\pi}{9} - i\sin\frac{(2+6k)\pi}{9}$ are the cube roots of $\omega^2$.

In high school, considerable time is spent finding rational roots of polynomial equations with rational (or integer) coefficients. Several worthwhile topics are usually taught or recalled at this time, namely, (i) the Fundamental Theorem of Arithmetic to prove the main theorem about possible rational roots, (ii) the relationship between roots and linear factors, and (iii) synthetic division[2] as a fast way of checking the

[2]There is a risk in mentioning synthetic division in high school for fear that someone night find the algorithm difficult or, worse still, something interesting. An understanding of the long division process is more valuable than using synthetic division with little understanding.

possible rational roots.[3] Our approach will be different since we are looking for formulas which will allow us to solve any equation, and not just select ones with rational coefficients.

We are now ready to consider cubic equations and to show that there is a solution of the general cubic equation

$$x^3 + a_1 x^2 + a_2 x + a_3 = 0$$

which is in a form similar to the solution of the quadratic equation. By taking $x = y - \frac{1}{3}a_1$, we can reduce it at once to the form

$$y^3 + (a_2 - \frac{1}{3}a_1^2)y + \frac{2}{27}a_1^3 - \frac{1}{3}a_1 a_2 + a_3 = 0.$$

This equation can now be written as

$$y^3 + py + q = 0 \tag{1}$$

which is usually called the *reduced* form of the cubic. Note that the square term is missing. If $a_2$ happens to be zero, it is quicker to put $x = \frac{1}{y}$ in order to reach a reduced form of the cubic equation. (If $a_3 = 0$, the solution can be found trivially.) Let $y = \alpha_1 + \alpha_2$, then

$$\begin{aligned} y^3 &= \alpha_1^3 + 3\alpha_1^2\alpha_2 + 3\alpha_1\alpha_2^2 + \alpha_2^3 \\ &= 3\alpha_1\alpha_2(\alpha_1 + \alpha_2) + \alpha_1^3 + \alpha_2^3 \\ &= 3\alpha_1\alpha_2 y + \alpha_1^3 + \alpha_2^3. \end{aligned} \tag{2}$$

Equation (2) may be regarded as a cubic equation in $y$ and is in reduced form. Equations (1) and (2) are the same, provided

$$\alpha_1^3 + \alpha_2^3 = -q \text{ and } 3\alpha_1\alpha_2 = -p.$$

If we can find $\alpha_1$ and $\alpha_2$ such that

$$\alpha_1^3 + \alpha_2^3 = -q \text{ and } \alpha_1^3\alpha_2^3 = -\frac{p^3}{27},$$

then we will have accomplished our task. But we can easily define a quadratic in $z$ with $\alpha_1^3$ and $\alpha_2^3$ as roots:

$$(z - \alpha_1^3)(z - \alpha_2^3) = z^2 - (\alpha_1^3 + \alpha_2^3)z + \alpha_1^3\alpha_2^3 = z^2 + qz - \frac{p^3}{27}.$$

Solving $z^2 + qz - \frac{p^3}{27} = 0$, we get

$$z = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

[3] The next natural follow-up to this topic at university is the more general algorithm known as Kronecker's Theorem for factoring completely into irreducible (prime) factors any polynomial with integer (or rational coefficents).

Letting $\alpha_1^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and $\alpha_2^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, then

$$y = \alpha_1 + \alpha_2 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

This is the famous formula of Cardan, another of the Italian school of Bologna, who brought it into prominence in 1573.

To solve $x^3 + 3x + 8 = 0$, let $x = \alpha_1 + \alpha_2$. Then $\alpha_1^3 + \alpha_2^3 = -8, \alpha_1\alpha_2 = -1$ and $z^2 + 8z - 1 = 0$, so that $z = -4 \pm \sqrt{17}$, and hence,

$$x = \sqrt[3]{-4 + \sqrt{17}} + \sqrt[3]{-4 - \sqrt{17}}.$$

The Fundamental Theorem of Algebra, proved by Gauss in 1799 in his doctoral dissertation, states that every polynomial equation of degree $\geq 1$ has a root. This root may well be a complex number. The proof does not tell us how to find an exact solution, just that one exists. An easy consequence of this theorem is to prove that a polynomial of degree $n$ has at most $n$ roots, and in fact, $n$ roots if we count "repeats." So then, what are the other two roots of the cubic equation $x^3+px+q = 0$? Recall that the three cube roots of 1 are 1, $\omega$ and $\omega^2$. Hence, the three cube roots of $\alpha_1 = \sqrt[3]{-4 + \sqrt{17}}$ are $\alpha_1, \omega\alpha_1$, and $\omega^2\alpha_1$ since $\alpha_1^3 = (\omega\alpha_1)^3 = (\omega^2\alpha_1)^3 = -4 + \sqrt{17}$. Similarly, $\alpha_2^3 = (\omega\alpha_2)^3 = (\omega^2\alpha_3)^3 = -4 - \sqrt{17}$. So, at first sight it appears that there are nine possibilities for the solutions of $x^3 + 3x + 8 = 0$. But, whereas each of the nine ways will satisfy

$$\alpha_1^3 + \alpha_2^3 = -8 \text{ (eg. } (\omega\alpha_1)^3 + (\omega\alpha_2)^3 = -8),$$

only three ways will satisfy $\alpha_1\alpha_2 = -1$, namely, $\alpha_1$ with $\alpha_2, \omega\alpha_1$ with $\omega^2\alpha_2$, and $\omega^2\alpha_1$ with $\omega\alpha_2$. Hence the three roots of the cubic equation $x^3 + 3x + 8 = 0$ are

$$x = \sqrt[3]{-4 + \sqrt{17}} + \sqrt[3]{-4 - \sqrt{17}} = \alpha_1 + \alpha_2, x = \omega\alpha_1 + \omega^2\alpha_2, \text{ and } x = \omega^2\alpha_1 + \omega\alpha_2.$$

The next example will introduce other obstacles to solving the cubic. Solve

$$x^3 - 3x + 1 = 0.$$

Clearly there are no rational roots, so we must apply the formula above with $p = -3$ and $q = 1$ obtaining

$$\begin{aligned} x &= \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{27}{27}}} + \sqrt[3]{-\frac{1}{2} - \sqrt{\frac{1}{4} - \frac{27}{27}}} \\ &= \sqrt[3]{-\frac{1}{2} + \frac{\sqrt{3}}{2}i} + \sqrt[3]{-\frac{1}{2} - \frac{\sqrt{3}}{2}i}. \end{aligned}$$

Earlier we computed the three cube roots of $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. They were

$$\cos\frac{(2+6k)\pi}{9} + i\sin\frac{(2+6k)\pi}{9} \quad \text{and} \quad \cos\frac{(2+6k)\pi}{9} - i\sin\frac{(2+6k)\pi}{9}$$

respectively, for $0 \le k \le 2$. These cube roots must be paired properly, $\alpha_1$ with $\alpha_2$ so that $\alpha_1\alpha_2 = -\frac{p}{3} = 1$, and hence $x = \alpha_1 + \alpha_2 = 2\cos\frac{(2+6k)\pi}{9}$ for $0 \le k \le 2$. Note that the three roots are real![4] You should check on your calculator that $x = 2\cos\frac{2\pi}{9}, 2\cos\frac{8\pi}{9}$, and $2\cos\frac{14\pi}{9}$ are indeed the correct roots. You should also prove that all three roots of $x^3 + px + q = 0$ are real if and only if the *discriminant* $\frac{q^2}{4} + \frac{p^3}{27}$ is less than zero. (We are assuming still that $p$ and $q$ are real numbers.)

To check your understanding of the general method, try to solve $x^3+x^2-2x-1 = 0$ by first substituting $x = y - \frac{1}{3}$ and solving $y^3 - \frac{7}{3}x - \frac{7}{27}$. You should get the solutions[5] $x = \frac{2\sqrt{7}}{3}\cos\left(\frac{\theta+2k\pi}{3}\right) - \frac{1}{3}$, $k = 0, 1, 2$ where $\cos\theta = \frac{1}{2\sqrt{7}}$ and $\sin\theta = \frac{3\sqrt{3}}{2\sqrt{7}}$.

Can the quartic equation, the case $n = 4$, be solved in a similar way? YES, it can! The method for solving the cubic involved the reduction of the cubic to the simpler quadratic equation. In a similar way, the solution of the quartic can be reduced to the solution of a cubic equation, called the *resolvent* of the quartic. We omit the details.

Since all equations of degree $\le 4$ are now solved, it is natural to ask how the quintic equation can be solved by radicals. Many mathematicians attacked the problem. The great Euler failed to solve the problem but found new methods for the quartic. Lagrange took an important step in 1770 when he unified the separate tricks used for the equations of degree $\le 4$. He showed that they depended on finding functions of the roots of the equation which were unchanged by certain permutations of those roots; and he showed that this approach failed when tried on the quintic. One of these important functions is the discriminant, defined for the cubic, for example, as

$$\Delta = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2,$$

where $r_1, r_2$ and $r_3$ are the three roots. Note that this function is unchanged by a permutation of the roots[6].

After this there was a general feeling that the quintic could not be solved by radicals, although there were many mathematicians who believed the desired formulas should exist. Both Abel in 1823 and Galois in 1828 believed that they had solved the quintic equation before they found their own errors and went on to clarify the real state of affairs. Abel proved in 1824 that there is no formula of the required kind for equations of degree 5. What he used was a result proved by Cauchy in 1815 involving simple calculations with permutations about the possibilities for the number of different functions that can be obtained from a given function of $n$ variables by permuting them among themselves.

The problem now arose of finding a way of deciding whether or not a given equation could be solved by radicals. Abel was working on it when he died in 1829. The young Galois discovered that there is a "group" naturally attached to each equation, and he

---

[4]Note that the method for solving the cubic involved the use of complex numbers, even though the roots may be real.

[5]A good exercise would be for you to prove that the roots can also be given as $x = 2\cos\frac{2\pi}{7}, 2\cos\frac{4\pi}{7}$ and $2\cos\frac{6\pi}{7}$.

[6]This function is symmetric with respect to these roots and hence can be written as a polynomial in the so-called elementary symmetric functions: $s_1 = r_1 + r_2 + r_3, s_2 = r_1r_2 + r_1r_3 + r_2r_3$ and $s_3 = r_1r_2r_3$. Note that $s_1 = -a_1, s_2 = a_2$ and $s_3 = -a_3$ where the cubic is $x^3 + a_1x^2 + a_2x + a_3$.

was able to analyse successfully how this group changed when the domain of certain known quantities was extended and to produce a necessary and sufficient condition for the solvability of a given equation by radicals. This condition was expressed in group-theoretic terms. This condition implied, for example, that the quintic equation $x^5 - 4x + 2 = 0$ cannot be solved by radicals simply because it has three real and two complex roots and it cannot be factored over the rationals (i.e. allowing only rational coeffients).

Évariste Galois(1811-1832) was born at Bourg-la-Reine near Paris on Friday, October 25, 1811. For the first twelve years of his life Galois was educated by his mother Adelaide-Marie who had a solid education in religion and classics. In October 1823 he entered the lycée Louis-le-Grand and performed well during his first two years obtaining a first prize in Latin. Then boredom set in with the structured classes, but at this time he began to take a serious interest in mathematics after reading a copy of Legendre's *Éléments de Géométrie*. At 15 years old he was reading material written for professional mathematicians, including works of Lagrange and Abel. He badly neglected his other studies. After failing the entrance exam to the prestigious École Polytechnique, he entered the École Normale in 1828. He was expelled in 1830 because of his radical political activities, since he always seemed to be in some sort of trouble with the authorities. Galois died tragically on Thursday, May 31, 1832 of peritonitis after being hit in the stomach during a gun duel the day before over a girl!

On January 17, 1831 Galois had sent to the famous Paris Academy a paper entitled *On the conditions of solvability of equations by radicals*. Finally on July 4, 1831 it was rejected by Poisson who declared it 'incomprehensible'. They just could not understand what he had written. On May 29, 1832, the eve of the dual, he wrote to his friend Auguste Chevalier, outlining his discoveries. In his letter he sketched the connection between groups and polynomial equations, stating that an equation is solvable by radicals provided its group is solvable.

Galois had over his short lifetime submitted three memoirs to the Academy of Sciences in Paris. His work was nearly lost to the mathematical world had not Joseph Liouville looked again at these manuscripts and addressed the Academy on Tuesday, July 4, 1843. His opening words were:

> *'I hope to interest the Academy in announcing that among the papers of Évareste Galois I found a solution, as precise as it is profound, of this beautiful problem: whether or not it is solvable by radicals....'*