Mathematical Enrichment Programme

U.C.D. April 6 2019

(Thomas J. Laffey).

Polynomials.

A polynomial has the form

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

where $n \geq 0$ is an integer, $a_0, a_1, \ldots, a_n$ are numbers and x is a symbol (or "indeterminate" or "variable").

If $a_0 \neq 0$, then n is the degree of $f(x)$.

One can add, subtract and multiply polynomials. Also, if $f(x)$, $g(x)$ are polynomials and $g(x) \neq 0$, we can find polynomials $h(x)$, $r(x)$ such that

$$f(x) = g(x)h(x) + r(x)$$

and $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$.

In this case, $r(x)$ is called the remainder of $f(x)$ on division by $g(x)$.

If $r(x) = 0$, we say that $g(x)$ divides $f(x)$.

We use long division to find $h(x)$ and $r(x)$.

$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ is called a monic polynomial if $a_0 = 1$.

α is a root (or zero) of $f(x)$ if $f(\alpha) = 0$.

The remainder theorem states that α is a root of $f(x)$ if and only if $x - \alpha$ divides $f(x)$.

Example: $f(x) = x^3 - 6x^2 + 11x - 6$ has roots 1, 2, 3 and

$$f(x) = (x-1)(x-2)(x-3).$$

In general, if $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ and $a_0 \neq 0$ and $f(x)$ has roots $\alpha_1, \alpha_2, \cdots, \alpha_n$, then

$$f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n). \quad (1)$$

A polynomial $f(x)$ of degree n has at most n distinct roots.

For example $f(x) = x^3 - 3x + 2$ has just two distinct roots, namely 1 and 2 and

$$f(x) = (x-1)^2(x+2). \quad (2)$$

The multiplicity of a root α of $f(x)$ is the number of times it occurs in a factorization (1). For example, the root 1 has multiplicity 2 in (2).

The factorization

$$f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$$

is unique up to the order of the factors $x-\alpha_1, \cdots, x-\alpha_n$.

For polynomials $f(x)$, $g(x)$, not both zero, one can calculate a polynomial $d(x)$ such that

(i) $d(x)$ is monic

(ii) $d(x)$ divides both $f(x)$ and $g(x)$ and

(iii) $d(x)$ has greatest possible degree among polynomials dividing both $f(x)$ and $g(x)$.

$d(x)$ is called the greatest common divisor (gcd) of $f(x)$, $g(x)$.

[It is also called the highest common factor (hcf) of $f(x)$, $g(x)$.]

Example ① $\gcd(x^3+1, x^3+3x^2+3x+1) = x+1$

② $\gcd(x^3-1, x^3+3x^2+3x+1) = 1$.

③ $\gcd(x^{10}-1, x^{14}-1) = x^2-1$.

For more than two thousand years, people have been interested in finding the roots of polynomials, both for the interest and challenge of the problem itself and because of the applications of the answer. At present, applications occur in all areas of science and engineering. For a randomly chosen polynomial, finding the roots (or good approximations of them) gets harder as one increases the degree.

For a polynomial $f(x) = a_0 x + a_1$ with $a_0 \neq 0$, there is obviously one root $\alpha = -a_1/a_0$.

For a polynomial $f(x) = a_0 x^2 + a_1 x + a_2$ ($a_0 \neq 0$) of degree 2, the roots are

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4 a_0 a_2}}{2 a_0}.$$

The number $a_1^2 - 4 a_0 a_2$ is called the discriminant of $f(x)$ in this case.

Suppose $f(x) = x^3 + a_1 x^2 + a_2 x + a_3$ is a monic polynomial of degree 3. We wish to find its roots. The first step is to write it in terms of $x + \frac{a_1}{3}$.

$$f(x) = \left(x + \frac{a_1}{3}\right)^3 + \left(a_2 - \frac{a_1^2}{3}\right)\left(x + \frac{a_1}{3}\right) + \left(a_3 - \frac{a_1 a_2}{3} + \frac{2a_1^3}{27}\right)$$

Let $x = y - \frac{a_1}{3}$. Then $f(x)$ becomes

$g(y) = y^3 + Hy + K$, where

$H = a_2 - \frac{a_1^2}{3}$, $K = a_3 - \frac{a_1 a_2}{3} + \frac{2a_1^3}{27}$.

We now solve $g(y) = 0$. [The fact that $g(y)$ has $0y^2$ makes it easier to solve].

The polynomial $z^3 - 1 = (z-1)(z^2 + z + 1)$

and $z^2 + z + 1 = 0$ has roots

$$\frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}$$

(where $i = \sqrt{-1}$). Write $\frac{-1 + i\sqrt{3}}{2} = \omega$.

Then $\omega^2 = \frac{(-1 + i\sqrt{3})^2}{4} = \frac{1 - 2i\sqrt{3} - 3}{4} = \frac{-1 - i\sqrt{3}}{2}$

So the two roots of $z^2 + z + 1 = 0$ are ω and ω^2, and $\omega^2 + \omega + 1 = 0$, $\omega^3 = 1$. $\{1, \omega, \omega^2\}$ is the set of cube roots of unity.

Now define three numbers

$$\lambda_1 = u+v, \quad \lambda_2 = \omega u + \omega^2 v, \quad \lambda_3 = \omega^2 u + \omega v .$$

We try and find u, v so that $\lambda_1, \lambda_2, \lambda_3$ are the roots of $g(y) = 0$.

We multiply out

$$G(y) = (y-\lambda_1)(y-\lambda_2)(y-\lambda_3) =$$

$$(y-(u+v))(y-(\omega u+\omega^2 v))(y-(\omega^2 u+\omega v)) .$$

The coefficient of y^2 in $G(y)$ is

$$-[u+v+\omega u+\omega^2 v+\omega^2 u+\omega v] =$$

$$-[u(1+\omega+\omega^2)+v(1+\omega+\omega^2)] = 0$$

since $1+\omega+\omega^2 = 0$.

The coefficient of y in $G(y)$ is

$$(u+v)(\omega u+\omega^2 v)+(u+v)(\omega^2 u+\omega v)+(\omega u+\omega^2 v)(\omega^2 u+\omega v)$$

$$= u^2(1+\omega+\omega^2) + uv(\omega+\omega^2+\omega+\omega^2+\omega+\omega^2) + v^2(1+\omega+\omega^2)$$

(using $\omega^3 = 1$, $\omega^4 = \omega$)

$$= -3uv, \quad \text{(using } 1+\omega+\omega^2 = 0\text{)}.$$

The coefficient of y^0 in $G(y)$ is

$$-(u+v)(\omega u+\omega^2 v)(\omega^2 u+\omega v)$$

$$= -[u^3 + u^2 v(1+\omega+\omega^2) + uv^2(1+\omega+\omega^2) + v^3]$$

$$= -(u^3+v^3) .$$

Hence

$$G(y) = y^3 - 3uvy - (u^3+v^3) .$$

To make $G(y)$ the same as $g(y)$

$= y^3 + Hy + K$, we need to choose u, v so that

$$-3uv = H \quad \text{and} \quad -(u^3+v^3) = K.$$

So we need the polynomial

$$T(t) = (t-u^3)(t-v^3) = t^2 - (u^3+v^3)t + u^3v^3$$
$$= t^2 + Kt - \frac{H^3}{27}.$$

So we must choose u^3, v^3 to be the solutions of the quadratic equation $T(t) = 0$, that is,

$$u^3, v^3 = \frac{-K \pm \sqrt{K^2 + \frac{4H^3}{27}}}{2}.$$

Take $u = \sqrt[3]{\frac{-K + \sqrt{K^2 + \frac{4H^3}{27}}}{2}}$, $v = \sqrt[3]{\frac{-K - \sqrt{K^2 + \frac{4H^3}{27}}}{2}}$.

Note that $x = y - \frac{a_1}{3}$, and $f(x) = 0$ if $g(y) = 0$, so the roots of $f(x) = 0$ are $-\frac{a_1}{3} + u + v$, $-\frac{a_1}{3} + \omega u + \omega^2 v$, $-\frac{a_1}{3} + \omega^2 u + \omega v$.

This is Cardano's formula, published in 1545. The trick for solving $y^3 + Hy + K = 0$ is attributed to del Ferro and Tartaglia.

The formula is correct, but difficult to use. In particular, if the a_j are real numbers, the cubic $f(x)$ must have at least one real root, but it is difficult to recognize a real root from the formula.

For H, K real, we can try to solve

$$g(y) = y^3 + Hy + K = 0$$

by first getting a real root. Suppose that $\beta = w\cos\theta$, where w, θ are to be determined. We want to have

$$w^3\cos^3\theta + Hw\cos\theta + K = 0 \quad \ldots (X)$$

Recall the formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.

So $\cos^3\theta = \frac{1}{4}(\cos 3\theta + 3\cos\theta)$. Substituting into (X), we get

$$\frac{w^3}{4}(\cos 3\theta + 3\cos\theta) + Hw\cos\theta + K = 0$$

Choose w so that $\frac{3w^3}{4} + Hw = 0 \quad (w \neq 0)$

so $w = \pm\sqrt{\frac{-4H}{3}}$. Then the equation reduces to $\frac{w^3\cos 3\theta}{4} + K = 0$ and

$\cos 3\theta = -\frac{4K}{w^3}$ and if $\left|\frac{4K}{w^3}\right| \leq 1$, we can find a θ with $0 \leq \theta \leq \pi$ such that $\cos 3\theta = -\frac{4K}{w^3}$. Note that w is real if $H < 0$, so we get a real root $w\cos\theta$ in this case.

In attempting to solve IMO problems about roots of cubics, the formula is not applied directly, but instead the method of proof and some tricks on the specific equation are used.

Example: Suppose that α and β are real numbers such that $p(\alpha) = 0$, $q(\beta) = 0$ where

$$p(x) = x^3 - 6x^2 + 14x - 7,$$
$$q(x) = x^3 - 6x^2 + 14x - 17.$$

Find $\alpha + \beta$.

Solution: Note that

$$p(x) = (x-2)^3 + 2x + 1$$
$$= (x-2)^3 + 2(x-2) + 5, \text{ and}$$
$$q(x) = (x-2)^3 + 2(x-2) - 5.$$

Now $p(\alpha) = 0$ and $q(\beta) = 0$ implies

$$0 = p(\alpha) + q(\beta) = (\alpha-2)^3 + 2(\alpha-2) + 5 + (\beta-2)^3 + 2(\beta-2) - 5$$

$$= (\alpha-2)^3 + (\beta-2)^3 + 2(\alpha+\beta-4)$$

$$= (\alpha-2+\beta-2)\left((\alpha-2)^2 - (\alpha-2)(\beta-2) + (\beta-2)^2\right) + 2(\alpha+\beta-4)$$

$$= (\alpha+\beta-4)\left((\alpha-2)^2 - (\alpha-2)(\beta-2) + (\beta-2)^2 + 2\right) \quad \ldots (*)$$

Now for real numbers γ, δ we have

$$\gamma^2 - 4\delta + \delta^2 = \left(\gamma - \frac{\delta}{2}\right)^2 + \frac{3\delta^2}{4} \geq 0.$$

Hence the factor

$$(\alpha-2)^2 - (\alpha-2)(\beta-2) + (\beta-2)^2 + 2$$

in (Y) is positive. Hence (Y) implies that $\alpha + \beta - 4 = 0$, so $\alpha + \beta = 4$.

For a polynomial

$$f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4,$$

one can find formulae for its roots, but they are a lot more complicated than Cardano's. It was found by a student of Cardano, called Ferrari and both formulae were first published in a book called Ars Magna in 1545.

For the next 300 years, researchers tried to find similar type of solutions for the quintic (degree 5) and higher degrees. In 1824, Abel proved that no formula of that type is possible for degree greater than 4. In 1846, a more understandable proof by Galois was

published posthumously – he wrote his proof in 1830 when aged 18, but it was rejected for publication by the French Academy of Sciences, and Galois himself was killed in a duel in 1832. Nowadays, in teaching undergraduates the result, it is Galois' proof that is used; it is now part of a subject called Galois theory. Marcus du Sautoy relates the story of Galois in his book "Finding moonshine"

Factoring polynomials over the complex numbers.

Fundamental Theorem of Algebra: Let

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

be a polynomial with $a_1, \cdots, a_n$ real or complex numbers. Then there exist complex numbers $\alpha_1, \cdots, \alpha_n$ such that $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$.

The result was conjectured by the Bernoulli's in the 17th century and

over the next 200 years, several proofs by world famous mathematicians appeared, but all were found to have gaps. The first proof to be accepted as correct was by Gauss in 1799. His proof was based on geometry and topology, while the previous attempted proofs were by algebra. His proof lasted over a 100 years before a gap was discovered and in 1920, a correct version was published by Ostrowski. The easiest proofs to understand are based on complex analysis, a kind of calculus invented by Cauchy and many other French mathematics in the first half of the 19th century. A theorem in this area called Rouché's Theorem yields the Fundamental Theorem of Algebra as a simple corollary. In the 1930s, an algebraic proof, based on Galois theory, was found by Emil Artin.

Factoring polynomials over the rational numbers and integers.

Suppose that $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, where $a_1, \cdots, a_n$ are rational numbers. We wish to study factorization of $f(x)$ as a product of polynomials $g_1(x)\, g_2(x) \cdots g_t(x)$, where $g_1(x), \cdots, g_t(x)$ are polynomials of degree at least one, having rational coefficients, and having the smallest possible degree subject to this.

Example: $x^3 - 1 = (x-1)(x^2+x+1)$

The roots of $x^2+x+1=0$ are the complex numbers ω, ω^2 where $\omega = \frac{-1+i\sqrt{3}}{2}$, $(i = \sqrt{-1})$, so x^2+x+1 cannot be factored as $(x-\alpha)(x-\beta)$ with α, β real. So over the rational numbers, the factorization

$$x^3 - 1 = (x-1)(x^2+x+1)$$

is the best we can do.

Similarly $x^4 - 1 = (x-1)(x+1)(x^2+1)$ cannot be factored further over the rationals.

Definition A polynomial $f(x)$ having rational coefficients and degree at least one is said to be irreducible over the rationals if $f(x)$ cannot be factored as a product $g(x)\,h(x)$ of two polynomials $g(x)$, $h(x)$ with rational coefficients and each having degree at least one.

[Remember that every integer is a rational number, that every rational number is a real number, and that every real number is a complex number; in symbols $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.]

Example. A polynomial $x^2 + ax + b$ with a, b rational is irreducible over the rationals if and only if it has no root in the rational numbers; this happens if and only if $\sqrt{a^2 - 4b}$ is not rational.

One of the most important results in this area is

Gauss' Lemma. Suppose

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

where $a_1, \ldots, a_n$ are integers and suppose that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials with rational coefficients and degree of $g(x) = r$, degree $h(x) = n - r$, for some integer r with $1 \leq r \leq n-1$. Then there is a rational number $q \neq 0$ such that $q\,g(x)$ is a monic polynomial with integer coefficients and $(\frac{1}{q})h(x)$ is also a monic polynomial with integer coefficients.

Example $x^2 - 4 = g(x)h(x)$, where

$$g(x) = \frac{3}{2}x - 3, \quad h(x) = \frac{2}{3}x + \frac{4}{3}.$$

$q = 2/3$, $q\,g(x) = x - 2$, $(\frac{1}{q})h(x) = x + 2$.

This lemma reduces the problem of identifying the irreducibility of $f(x)$ over the rationals to investigation of factorization over the integers.

Gauss' Lemma has its own wikipedia page, section 1 of which includes the standard proof, so I will not include the proof here.

Some applications of Gauss' Lemma.

① Consider $f(x) = x^2 - 2$. If $f(x)$ is the product $g(x)\,h(x)$ where $g(x)$, $h(x)$ are polynomials of degree less than 2 with integer coefficients, then $g(x)$, $h(x)$ have degree 1 and $g(x) = ax+b$, $h(x) = cx+d$ for some integers a, b, c, d. Thus

$$x^2 - 2 = ac\,x^2 + (ad+bc)\,x + bd.$$

So $ac = 1$, $ad + bc = 0$ and $bd = -1$.

Since a and c are integers, $ac = 1$ implies $a = c = 1$ or $a = c = -1$.

If $a = c = 1$, then $ad + bc = 0$ implies $b + d = 0$, so $d = -b$ and then $bd = -2$ implies $b^2 = 2$, which is impossible, since b is an integer.

If $a = c = -1$, we get $-b - d = 0$ and get the same conclusion. So no such factorization exists. But if $\sqrt{2}$ were a rational number r/s with integers r, s, then $x^2 - 2 = (x - \frac{r}{s})(x + \frac{r}{s})$

is a factorization with rational coefficients. But, by Gauss' Lemma, x^2-2 must have a factorization into two polynomials (with integer coefficients) of degree one. This is a contradiction. Hence $\sqrt{2}$ is not rational.

This example can be generalized to prove irrationality of many numbers

(2) $f(x) = x^3 - 3$. If $f(x) = g(x)h(x)$, where $g(x)$, $h(x)$ have degree less than 3 with integer coefficients, then one, $g(x)$ say, must have degree 1 and the other degree 2. So we can write

$$x^3 - 3 = (px+q)(rx^2+sx+t)$$

where p, q, r, s, t are integers. Then counting the number of x^3, $pr = 1$ and thus $p = r = 1$ or $p = r = -1$.

Counting the number of x^2, we get

$ps + qr = 0$, so $s + q = 0$ and $s = -q$.

Counting the number of x, we get

$pt + qs = 0$, so $t = q^2$ or $-q^2$,

since $s = -q$ and $p = \pm 1$.

Counting the coefficients of x^0 we get $qt = -3$ and $q^3 = \pm 3$. This is impossible

for q an integer. So no such factorization exists. But if $\alpha = \sqrt[3]{3}$ is rational, then

$$x^3 - 3 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$$

is a factorization of the same type with rational coefficients, so if α were rational, we would contradict Gauss' Lemma. Hence $\sqrt[3]{3}$ is not rational.

(3) Prove $\beta = \sqrt{2} + \sqrt[3]{3}$ is not rational

[Just because $\sqrt{2}$ and $\sqrt[3]{3}$ are not rational, it does not follow that their sum is irrational without (a lot) more calculation. [It is true that the sum of two rational numbers is rational, but the example $(1 + \sqrt{2}) + (3 - \sqrt{2}) = 4$ shows that the sum of two irrational numbers could be rational].

We first construct a polynomial with integer coefficients which β satisfies.

Now $(\beta - \sqrt{2})^3 = 3$, so

$$\beta^3 - 3\sqrt{2}\beta^2 + 6\beta - 2\sqrt{2} = 3.$$

This can be written as

$$\beta^3 + 6\beta - 3 = \sqrt{2}(3\beta^2 + 2)$$

Squaring we get

$$(\beta^3 + 6\beta - 3)^2 = 2(3\beta^2 + 2)^2, \text{ that is}$$

$$\beta^6 - 6\beta^4 - 6\beta^3 + 12\beta^2 - 36\beta + 1 = 0.$$

So β satisfies $f(\beta) = 0$ where

$$f(x) = x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1.$$

Suppose β is rational. Then $f(x)$ must have a factorization

$$f(x) = (x - \beta)(x^5 + l_1 x^4 + l_2 x^3 + l_3 x^2 + l_4 x + l_5)$$

with rationals $l_1, l_2, \cdots, l_5$.
But then in Gauss' Lemma, $q = 1$ since $x - \beta$ is already monic and β must be an integer, and also all the l_is must be integers. Comparing the coefficients of x^0, we get $\beta l_5 = -1$.
Since l_5 and β are integers and $\beta > 0$, we deduce that $\beta = 1$, which is clearly false. This contradiction proves that β is not rational.
[By more calculations, it is possible to prove that $f(x)$ is irreducible over the rationals]

It would be nice to have simple tests to decide if a given polynomial is irreducible over the rationals.

There are many tests, but the "nice" ones only apply to polynomials with some special conditions on their coefficients. The most famous one is:

Eisenstein's Irreducibility Criterion.

Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ where $a_0, a_1, \cdots, a_n$ are integers. Suppose there is a prime number p such that the following conditions hold.

(1) p does not divide a_0

(2) p divides each of $a_1, a_2, \cdots, a_n$ and

(3) p^2 does not divide a_n.

Then $f(x)$ is irreducible over the rationals.

[Like for Gauss' Lemma, there is a Wikipedia page for Eisenstein's criterion, containing the proof and examples.]

The drawback is that there are so many conditions before it can be applied.