Again the reader is invited to draw up a chart or use a computer to see if any conclusions can be drawn or any further conjectures can be made. And always remember, mathematics is an experimental science!

DES MACHALE
Department of Mathematics, University College, Cork, Ireland
e-mail: *d.machale@ucc.ie*

95.26 Nice cubics

Introduction

A discussion with some other mathematics teachers raised the question whether it is possible to find a 'nice' cubic, that is one which has three rational zeros and two rational stationary points. The idea was to use it as an exercise for students to find the zeros and stationary points without having to substitute surds back into the cubic.

I was not aware of a solution without a repeated zero and my initial reaction was that it was not possible with three distinct zeros, but then a colleague managed to find one. So I decided to try and see if it was possible to find all solutions.

To simplify the problem, by a suitable transformation we can assume that one of the zeros is zero, the others are coprime integers and the cubic is monic (i.e. with a leading coefficient of 1). So the cubic can be assumed to be $y = x(x - a)(x - b) = x^3 - (a + b)x^2 + abx$ where a and b are coprime integers.

On differentiating and setting to zero, the stationary points are given by

$$3x^2 - 2(a + b)x + ab = 0, \tag{1}$$

which has roots $\frac{1}{3}\left(a + b \pm \sqrt{(a + b)^2 - 3ab}\right)$, which are rational if, and only if, $(a + b)^2 - 3ab = a^2 - ab + b^2$ is the square of a rational number (hence the square of an integer as a and b are integers).

So we need to find integer solutions of

$$a^2 - ab + b^2 = d^2. \tag{2}$$

Finding solutions

Such equations (solving polynomials in integers) are known as Diophantine equations (after Diophantus whose work Fermat annotated with his famous marginal note). A famous Diophantine equation is the Pythagoras equation and one method of finding Pythagorean triples is to factorise over the Gaussian integers, which are numbers of the form $a + bi$ where a and b are integers. To solve (2) we need to factorise in the ring of Eisenstein integers, $\mathbb{Z}[\omega]$, which are numbers of the form $p + q\omega$ where p and q are integers and ω is a complex cube root of one. Such structures are rings of algebraic integers. An algebraic integer is a zero of a monic polynomial with integer coefficients. Loosely speaking, a ring is an algebraic structure with an arithmetic similar to $\mathbb{Z}$.

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press

Note that $\omega^3 = 1$, and $\omega^2 + \omega + 1 = 0$. Note also that ω, ω^2 are complex conjugates.

Now

$$a^2 - ab + b^2 = (a + b\omega)(a + b\omega^2) \tag{3}$$

and we note that the factors are complex conjugates.

If (and that's a very big 'if'!!) we can carry over our ideas of factorising from the ordinary integers, $\mathbb{Z}$, we need

$$\pm(a + b\omega) = (p + q\omega)^2 \tag{4}$$

where p and q are integers.

Certainly this condition is sufficient as, by taking conjugates, we will also have $\pm(a + b\omega^2) = (p + q\omega^2)^2$ and hence

$$a^2 - ab + b^2 = (p + q\omega)^2(p + q\omega^2)^2 = (p^2 - pq + q^2)^2.$$

In fact condition (4) is also necessary, but that is far from trivial. In a general ring of algebraic integers factorisation may not be unique. Even if it is (as it is for the Eisenstein integers), there are some other details to be ironed out. I will defer these issues to later.

Expanding and using $\omega^2 = -1 - \omega$, we get

$$\pm(a + b\omega) = (p + q\omega)^2 = p^2 - q^2 + \omega(2pq - q^2).$$

So the solutions are given parametrically by

$$\pm a = p^2 - q^2$$

$$\pm b = 2pq - q^2$$

where p and q are integers, which must be coprime otherwise a and b would not be. The signs must be taken consistently.

It is convenient for the general problem to consider the distances between the zeros 0, a and b, which are $|a|$, $|b|$ and $|b - a|$. Now $\pm b = 2pq - q^2 = p^2 - (p - q)^2$. So let $c = b - a$ and $r = p - q$ and we get the distances between the zeros as

$$|a| = |p^2 - q^2|$$

$$|b| = |p^2 - r^2|$$

$$|c| = |q^2 - r^2|$$

where $p = q + r$.

From the symmetry of the solution, and remembering that we want three distinct zeros, we may assume $p > q > r > 0$ and the distances between the zeros in pairs are then given by

$$p^2 - q^2$$

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press

$$p^2 - r^2$$

$$q^2 - r^2$$

where $p = q + r, p > q > r > 0$.

Note that a common factor of q and r would divide p also, hence q and r are coprime. Substituting into the roots of (1), we get that the stationary points occur at $x = qr$ and $x = \frac{1}{3}(2q + r)(q + 2r)$ and the latter is equal to $q^2 + qr + r^2 - \frac{1}{3}(q - r)^2$ and so the stationary points occur at integer values if, and only if, $q - r$ is divisible by 3.

However, having solved the problem for coprime a and b, we can now generate any solution by multiplying by some rational number. So assuming the necessity of (4), we finally arrive at the following.

General solution for nice cubics

Given a cubic with rational zeros $\alpha < \beta < \gamma$, its derivative has rational zeros if, and only if, the differences between α, β and γ (in pairs) are given by:

$$\lambda(p^2 - q^2)$$

$$\lambda(p^2 - r^2)$$

$$\lambda(q^2 - r^2)$$

where λ is rational, q and r are coprime integers, $q > r > 0$ and $p = q + r$.

The zeros of the derivative are $\alpha + qr\lambda$ and $\alpha + \frac{1}{3}(2q + r)(q + 2r)\lambda$.

For the cubic to have integer zeros, then α and λ must be integers and then the derivative has integer zeros if, and only if, λ or $q - r$ is divisible by 3.

Some examples

r	q	p	$q^2 - r^2$	$p^2 - r^2$	$p^2 - q^2$	qr	$\frac{1}{3}(2q+r)(q+2r)$
1	2	3	3	5	8	2	$\frac{20}{3}$
1	3	4	8	7	15	3	$\frac{35}{3}$
2	3	5	5	16	21	6	$\frac{56}{3}$
1	4	5	15	9	24	4	18

So, looking at the first row, any cubic (with rational zeros) with gaps of 3 between two adjacent zeros and 5 between the other adjacent zeros (and hence 8 between the non-adjacent zeros) will have stationary points with rational x-coordinates. An example is given by $x(x-3)(x-8)$, which has stationary points at $x = 2$ and $x = \frac{20}{3}$.

For the third row, for example, if we take the zeros of the cubic as -4, 12 and 17 (which have pairwise gaps of 5, 16 and 21), we find the stationary points are at $x = -4 + 6$ and $x = -4 + \frac{56}{3} = \frac{44}{3}$.

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press

Unique factorisation, primes, irreducibles, associates and units

The preceding solution certainly provides an infinite supply of nice cubics, but to establish that there are no further solutions, we need to consider equations (3) and (4) in more detail. This can get quite technical, so I will use three Lemmas, whose proofs I will defer to the appendix which readers can omit if they wish. The general theory I refer to in this section and the appendix is gleaned from [1].

In the set of ordinary integers, $\mathbb{Z}$, we have uniqueness of factorisation into primes apart from order. When we move into rings of algebraic integers such as $\mathbb{Z}[\omega]$, we need to exercise a bit of care as this is not necessarily the case.

For example, consider $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. We can factorise 6 in two ways, as 2×3 or as $(1 + \sqrt{-5})(1 - \sqrt{-5})$ and none of these factors can be factorised any further (without using ± 1) (see [1, p. 89]).

The definition of a prime in $\mathbb{Z}$ can take two forms:

either $\quad p = ab \Rightarrow a = \pm p$ or $b = \pm p$

or $\quad p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Note the symbol $\mid$ means 'is a divisor of', or more simply 'divides'.

In $\mathbb{Z}$ these definitions are equivalent, but in more general rings they are not. The first says that p is irreducible; the second says that p is prime. Every prime is irreducible, but it is not necessarily the case that every irreducible is a prime. If factorisation into irreducibles is possible, then factorisation is unique if, and only if, every irreducible is prime. (See [1, pp. 78, 95-96].)

For our purposes we have the following result.

Lemma 1: $\mathbb{Z}[\omega]$ is a unique factorisation domain.

However we also we need to consider the presence of units. A unit is a divisor of 1. In $\mathbb{Z}$ units are not really an issue as the only units are ± 1 and these are traditionally omitted in factorisations. Related to these we have associates. We say that u and v are associates if $u = \varepsilon v$ where ε is a unit. In $\mathbb{Z}$, u and v are associates if $u = \pm v$.

Uniqueness of factorisation is unique only up to associates and units.

For example, even in $\mathbb{Z}$, $10 = (2)(5) = (-2)(-5) = (1)(2)(5) = (-1)(-2)(5)$, but clearly these are equivalent. The numbers 1 and -1 are units, -2 and 2 are associates and -5 and 5 are associates.

In $\mathbb{Z}$ we can get round this by excluding negative numbers and 1, but in a more general ring of algebraic integers this may not be possible as there may be other units and if we are dealing with complex numbers we cannot make a sensible definition of positive.

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press

So if $a + b\omega$ and $a + b\omega^2$ have no common factors (other than units) then from (3) we can deduce a modified version of (4):

$$\pm(a + b\omega) = \varepsilon(s + t\omega)^2$$

where ε is a unit and s, t are integers.

We now need:

Lemma 2: In $\mathbb{Z}[\omega]$ the only units are ± 1, $\pm\omega$, $\pm\omega^2$.

So (4) becomes $\pm(a + b\omega) = \omega^j(p + q\omega)^2$ where $j = 0$, 1 or 2. The case $j = 0$ we have already dealt with. The other two cases are equivalent to this as $\omega^2(s + t\omega)^2 = (s\omega + t\omega^2)^2 = (p + q\omega)^2$ where $p = -t$, $q = s - t$ and $\omega(s + t\omega)^2 = (\omega^2)^2(s + t\omega)^2 = (s\omega^2 + t)^2 = (p + q\omega)^2$ where $p = t - s$, $q = -s$.

However another issue is that if a and b are coprime integers then $a + b\omega$ and $a + b\omega^2$ may have a common factor which is not a unit. We need the following result.

Lemma 3: If a and b are coprime in $\mathbb{Z}$ then any common divisor of $a + b\omega$ and $a + b\omega^2$ in $\mathbb{Z}[\omega]$ is either a unit or an associate of $1 - \omega$.

So to finish our solution we need to consider the equation

$$\pm(a + b\omega) = (1 - \omega)(p + q\omega)^2.$$

Taking conjugates we get $\pm(a + b\omega^2) = (1 - \omega^2)(p + q\omega^2)^2$ and multiplying gives $a^2 - ab + b^2 = 3(p^2 - pq + q^2)^2$ but 3 is not the square of an integer and hence we get no further solutions.

Appendix: Proofs of the lemmas

To prove the lemmas, it is helpful to introduce the concept of the norm of an element of $\mathbb{Z}[\omega]$. We define the norm of $a + b\omega$ by

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2).$$

Note that also $N(a + b\omega) = a^2 - ab + b^2 = |a + b\omega|^2$ and so the norm of every non-zero element is a positive integer.

Now by the properties of modulus we have $N(uv) = N(u)N(v)$. Hence we can deduce the two useful properties:

1. $u \mid v$ in $\mathbb{Z}[\omega] \Rightarrow N(u) \mid N(v)$ in $\mathbb{Z}$,
2. u is a unit $\Rightarrow N(u) = 1$.

I will prove Lemmas 2 and 3 first.

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press

Lemma 2: In $\mathbb{Z}[\omega]$ the only units are ± 1, $\pm\omega$, $\pm\omega^2$.

Proof:

Since $1 = (1)(1) = (-1)(-1) = (\omega)(\omega^2) = (-\omega)(-\omega^2)$ the stated elements are all units. Conversely, if $\alpha + b\omega$ is a unit, then $N(\alpha + b\omega) = 1 \Rightarrow \alpha^2 - \alpha\beta + \beta^2 = 1 \Rightarrow 3(\alpha - \beta)^2 + (\alpha + \beta)^2 = 4$.

The integer solutions of this are either $\alpha - \beta = \pm 1$, $\alpha + \beta = \pm 1$ (where the signs can be chosen independently) or $\alpha - \beta = 0$, $\alpha + \beta = \pm 2$.

Solving these gives $\alpha = \pm 1$, $\beta = 0$ or $\alpha = 0$, $\beta = \pm 1$ or $\alpha = \beta = \pm 1$, giving the possible units as ± 1, $\pm\omega$ and $\pm(1 + \omega) = \mp\omega^2$.

Lemma 3: If a and b are coprime in $\mathbb{Z}$ then any common divisor of $a + b\omega$ and $a + b\omega^2$ in $\mathbb{Z}[\omega]$ is either a unit or an associate of $1 - \omega$.

Proof:

Let $u = a + b\omega$, $v = a + b\omega^2$ and suppose $\lambda \mid u$ and $\lambda \mid v$.

Then $\lambda \mid (u - v) = \omega b(1 - \omega)$ and $\lambda \mid (\omega v - \omega^2 u) = \omega a(1 - \omega)$.

Now $N(\omega a(1 - \omega)) = N(\omega)N(a)N(1 - \omega) = (1)(a^2)(3) = 3a^2$ and similarly $N(\omega b(1 - \omega)) = 3b^2$.

So $N(\lambda)$ divides both $3a^2$ and $3b^2$. But $N(\lambda)$ is a positive integer so must be 1 or 3 as a and b are coprime.

If $N(\lambda) = 1$ then, from the proof of lemma 2, λ is a unit.

If $N(\lambda) = 3$, let $\lambda = \alpha + \beta\omega$. Then $\alpha^2 - \alpha\beta + \beta^2 = 3$ and so $3(\alpha - \beta)^2 + (\alpha + \beta)^2 = 12$. The integer solutions of this are either $\alpha - \beta = \pm 2$, $\alpha + \beta = 0$ or $\alpha - \beta = \pm 1$, $\alpha + \beta = \pm 3$ (where the signs can be chosen independently). Solving for α, β gives the following solutions for λ:

$$\pm(1 - \omega), \pm(2 + \omega), \pm(1 + 2\omega).$$

But these are all associates of $1 - \omega$ as can be seen by multiplying it by each of the six units.

Lemma 1: $\mathbb{Z}[\omega]$ is a unique factorisation domain.

Proof:

I will prove that $\mathbb{Z}[\omega]$ is a Euclidean domain and by a standard piece of ring theory, this means that it will also be a unique factorisation domain (see [1, pp. 98-99]).

We need the definition of a Euclidean domain. It is an integral domain (i.e. a commutative ring with a multiplicative identity and no zero divisors) with a Euclidean function, ϕ, which is a function from the non-zero elements of the domain to $\mathbb{N}$ with the following two properties:

1. Given non-zero a, b, then $a \mid b \Rightarrow \phi(a) \leqslant \phi(b)$.
2. Given non-zero a, b, there exist q and r such that $a = qb + r$ and either $r = 0$ or $\phi(r) \leqslant \phi(b)$.

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press

Informally this says that we can divide and get a remainder of a smaller 'size' than the divisor.

For $\mathbb{Z}[\omega]$, we can use the norm as the Euclidean function. Now $a \mid b \Rightarrow N(a) \mid N(b) \Rightarrow N(a) \leqslant N(b)$, so the first property is satisfied. For the second property, given non-zero a and b in $\mathbb{Z}[\omega]$, let $Q = \frac{a}{b} = Q_1 + Q_2\omega$ in $\mathbb{C}$ where Q_1 and Q_2 are rational. Then take q_1 and q_2 to be the nearest integers to Q_1 and Q_2 respectively.

So we have $|Q_1 - q_1| \leqslant \frac{1}{2}$ and $|Q_2 - q_2| \leqslant \frac{1}{2}$, and $a = bQ = b(q_1 + q_2\omega) + b(Q_1 - q_1) + b(Q_2 - q_2)\omega$.

Let $q = q_1 + q_2\omega$ and $r = a - bq = b(Q_1 - q_1) + b(Q_2 - q_2)\omega$. Then $a = qb + r$ and

$$\begin{aligned} N(r) &= b^2\left[(Q_1 - q_1)^2 - (Q_1 - q_1)(Q_2 - q_2) + (Q_2 - q_2)^2\right] \\ &\leqslant b^2\left[(\tfrac{1}{2})^2 + (\tfrac{1}{2})(\tfrac{1}{2}) + (\tfrac{1}{2})^2\right] \\ &< b^2 = N(b). \end{aligned}$$

So $\mathbb{Z}[\omega]$ is a Euclidean domain and hence a unique factorisation domain.

Reference

1. I. N. Stewart and D. O. Tall, *Algebraic number theory* (2nd edn.), Chapman & Hall, 1987 (reprinted 1995).

C. JOHNSON
Hills Road Sixth Form College, Cambridge CB2 8PE

95.27 Symmetric rational expressions in polynomial sequences

Introduction

A recent *Gazette* article [1] considered the notion of *symmetric rational functions* in the variables $x_1, x_2, \ldots, x_n$. In this note we obtain some interesting results for the case in which these variables are specialised to finite sequences defined by polynomials. For the sake of clarity, we recapitulate some of the key definitions and results given in [1].

A rational function in the variables $x_1, x_2, \ldots x_n$ is called *symmetric* if it is left unchanged by any permutation of these variables. It is well known that any symmetric rational function may be written in terms of *elementary symmetric polynomials*. In fact, in [1] this result is proved for the special cases $n = 2$ and $n = 3$. The elementary symmetric polynomial $e_{k,n}$ is defined to be the sum of all possible products of k distinct elements from the set $x_1, x_2, \ldots, x_n$.

Let $f(x)$ be a polynomial function. In this note the variables $x_1, x_2, \ldots, x_n$ are specialised by setting $x_k = f(k)$, $k = 1, 2, \ldots, n$. We use $S_{k,n}$ to denote the elementary symmetric expression consisting of the sum of all possible products of k terms with distinct arguments from the

https://doi.org/10.1017/S002555720000303X Published online by Cambridge University Press