Maths Circle: What is Euclidean Construction? Part III

Parthanil Roy, Indian Statistical Institute

1 A Quick Recap

Euclidean construction starts with two points at unit distance. Without loss of generality, we shall assume these two points to be $(0,0)$ and $(1,0)$ in the Cartesian coordinate system. Euclidean construction proceeds with the repeated applications of five basic constructions. These are:

1. Creating the line through two existing points.
2. Creating the circle through one point with centre at another point.
3. Creating the point which is the intersection of two existing, non-parallel lines.
4. Creating the one or two points in the intersection of a line and a circle (if they intersect).
5. Creating the one or two points in the intersection of two circles (if they intersect).

In other words, we keep on using the points, lines and circles that have already been constructed and get to construct new ones using the five basic constructions $(1-5)$ above.

Definition. *We say that a point in the plane is constructible if it is either* $(0,0)$ *or* $(1,0)$ *or it can be obtained as a new point of intersection in 3 – 5 above after repeating any of 1 – 5 finitely many times in any order.*

Definition. *We say that a real number* r *is constructible if the point* $(r,0)$ *is constructible as defined above.*

Theorem 1. *A real number* α *is constructible if and only if* α *can be written using integers and the mathematical operations* $+$, $-$, $\times$, $\div$ *and* $\sqrt{}$ *(each used finitely many times in any order).*

2 The Minimal Polynomial

Theorem 2 (Division for Polynomials)**.** *If* $g(x) \neq 0$ *and* $f(x)$ *are two polynomials with rational coefficients, then there exist polynomials* $q(x)$ *and* $r(x)$ *also with rational coefficients such that*

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

and $degree(r(x)) < degree(g(x))$.

The polynomials $q(x)$ and $r(x)$ are called quotient and remainder, respectively, when $f(x)$ is divided by $g(x)$.

Problem 1. *Prove Theorem 2.*

[**Hint:** Fix $g(x) \neq 0$. If $degee(f(x)) < degree(g(x))$, then take $q(x) = 0$ and $r(x) = f(x)$. If $degee(f(x)) \geq degree(g(x))$, then use induction on $degree(f(x))$.]

Suppose a real number α is a root of a polynomial $f(x)$ with rational coefficients. This means that there are rational numbers $a_0, a_1, \ldots, a_m$ such that $a_m \neq 0$ and

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m = 0.$$

For such a number α, a minimal polynomial is defined as a nonzero polynomial $g(x)$ with rational coefficients and minimum degree such that $g(\alpha) = 0$. **Why would it exist?**

Problem 2. *Suppose a real number α is a root of polynomial $f(x)$ with rational coefficients and $g(x)$ is a minimal polynomial for α. Then show that there exists a polynomial $q(x)$ with rational coefficients such that $f(x) = g(x)q(x)$. Using this, show that any two minimal polynomials of α are just rational multiples of each other.*

Problem 3. *Find a minimal polynomial for each of these constructible numbers:*

- $\alpha = \sqrt{2+\sqrt{3}}$.
- $\alpha = \sqrt{5+\sqrt{2+\sqrt{3}}}$.
- $\alpha = \sqrt{2}+\sqrt{3}$.
- $\alpha = \sqrt{5}+\sqrt{\sqrt{2}}$.

Just finding them would be enough - you do not have to formally prove that these are actually minimal polynomials.

What do you observe from Problem 3? ***The degree of minimal polynomials of all of these constructible numbers are powers of** 2**. This is actually true for every constructible number.*** The reason is simple - in order to rationalize, we have to keep on squaring till all the "$\surd$" signs are removed. Each squaring will add a power of 2 in the degree of the minimal polynomial. This is summarized in the following result.

Theorem 3. *Every constructible number has a minimal polynomial and the degree of this polynomial is a power of* 2.

We shall use Thorem 3 to establish that 60° cannot be trisected using Euclidean construction.

3 Impossibility of Trisection of 60°

Definition 1. *An angle θ is called constructible if there are three constructible points A, B and C in the plane such that $\angle ABC = \theta$.*

Note that without loss of generality, we may assume that $B = (0,0)$ and $C = (r,0)$ for some constructible number r.

Problem 4. *Show that an angle θ can be constructed using the Euclidean method if and only if $\cos\theta$ is a contructible number.*

Now we would show that 60° cannot be trisected using Euclidean construction. Note that this is same as proving 20° is not constructible and hence by Problem 4, we have to establish $\cos 20^\circ$ is not a constructible number. Keeping this in mind, we turn our attention to $\cos 20^\circ$.

Problem 5. *Using the formula $\cos 3\theta = 4(\cos\theta)^3 - 3\cos\theta$, show that $\beta = \cos 20^\circ$ is a root of the polynomial $g(x) = 8x^3 - 6x - 1$, i.e., $g(\beta) = 0$.*

We shall now show that $g(x)$ is a minimal polynomial of β and hence by Theorem 3, it would follow that $\beta = \cos 20^\circ$ is not a constructible number establishing the impossibility of the trisection of 60° using Euclidean method.

Problem 6. *Show that the polynomial $g(x) = 8x^3 - 6x - 1$ does not have any rational root.*

[**Hint:** Suppose, if possible, $g(\gamma) = 0$ for some rational number γ. Write γ in its reduced form, i.e., $\gamma = p/q$, where p, q are integers such that $q > 0$ and $gcd(p,q) = 1$. Using $g(p/q) = 0$, the fact that p and q are relatively prime, and a bit of algebra, show that p must divide 1 and q must divide 8. Using these, enumerate all the possibilities for γ and verfify they are not roots of $g(x)$.]

Problem 7. *Using Problem 6, show that the cubic polynomial* $g(x) = 8x^3 - 6x - 1$ *is irreducible in the sense that* $g(x)$ *cannot be written as* $g(x) = p(x)q(x)$, *where both* $p(x)$ *and* $q(x)$ *are nonconstant polynomials with rational coefficients.*

Problem 8. *Using Problem 2 and Problem 7, show that* $g(x) = 8x^3 - 6x - 1$ *is the minimal polynomial for* $\beta = \cos 20°$. *From this, establish, using Theorem 3, that* $\cos 20°$ *is not a constructible number and then applying Problem 4, prove that* $60°$ *cannot be trisected using Euclidean construction.*

We saw how a question from Euclidean geometry was answered using algebra – more precisely with the help of minimal polynomials. This just a glimpse of a beautiful and elegant theory, initiated by Évariste Galois in his rather short span of life (25 October 1811 – 31 May 1832), now known as Galois theory.

4 Descartes' Rational Root Theorem

Using the solution of Problem 6 outlined above, one can actually establish the following result.

Theorem 4. *If a nonzero polynomial*

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots a_mx^m$$

with integer coefficients (and $a_m \neq 0$*) has a rational root* $\gamma = p/q$ *written in its reduced form (i.e.,* p, q *are integers such that* $q > 0$ *and* $gcd(p, q) = 1$*), then*

- p *must divide the constant term* a_0, *and*
- q *must divide the leading coefficeinet* a_m.

Problem 9. *Prove Theorem 4.*