The Three Famous Problems of Antiquity

1. Dupilication of the cube   2. Trisection of an angle   3. Quadrature of the circle

These are all construction problems, to be done with what has come to be known as *Euclidean tools*, that is, straightedge and compasses under the following rules:

- With the straightedge a straight line of indefinite length may be drawn through any two distinct points.
- With the compasses a circle may be drawn with any given point as center and passing through any given second point.

To expand on the problems somewhat, the duplication of the cube means to construct the edge of a cube having twice the volume of a given cube; the trisection of an angle means to divide an arbitrary angle into three equal parts; the quadrature of the circle means to construct a square having area equal to the area of a given circle.

The importance of these problems stems from the fact that all three are unsolvable with Euclidean tools, and that it took over 2000 years to prove this! Also, these are the problems that seem to attract amatuer mathematicians who, not believing the proofs of the impossibility of these constructions, (probably due to) expend much effort on "proofs" that one or more of these is indeed possible. Trisecting the angle is the favorite. Many of these attempts do produce very good approximations, but, as will be seen, cannot be exact.

Interestingly enough, the results needed to show that the three problems are impossible are not geometric, but rather are algebraic in nature. The two pertinent theorems are:

Theorem A: The magnitude of any length constructible with Euclidean tools from a given unit length is an algebraic number.

Theorem B: From a given unit length it is impossible to construct with Euclidean tools a segment the magnitude of whose length is a root of a cubic equation having rational coefficients but no rational root.

Notice that while Theorem A says any constructible number is algebraic, Theorem B says not all algebraic numbers are constructible. The proofs of these theorems will be postponed while the three famous problems are put to rest now.

Duplication of the cube: Let the edge of the given cube be the unit of length, and let x be the edge of the cube having twice the volume of the given cube. Then $x^3 - 2 = 0$. Since any rational root of this equation must have as numerator a factor of 2 and as denominator a factor of 1 the equation has no rational roots. Thus, according to Theorem B, x is not constructible.

Trisection of the angle: Some angles, such as $90\,^\circ$, can be trisected, but if it can be shown that some angle cannot be trisected, then the general trisection problem will have been proved impossible. Here it will be shown that a $60\,^\circ$ angle cannot be trisected. Recall the trigonometric identity

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3},$$

and take $\theta = 60\,^\circ$ and $x = \cos\frac{\theta}{3}$. The identity becomes

$$8x^3 - 6x - 1 = 0$$

and, as above, any rational root must have a factor of -1 as numerator and a factor of 8 as denominator. A check of the possibilities again shows that, by Theorem B, x is not constructible. It remains to show that the trisection of a $60\,^\circ$ angle is equivalent to constructing a segment of length $\cos 20\,^\circ$. In Figure 1 the radius of the circle is 1 and $\angle BOA = 60\,^\circ$. If the trisector OC can be constructed, then so can segment OD, where D is the foot of the perpendicular from C to OA. But $OD = x$.

The student should prove the following theorem on the rational roots of a polynomial, which was used in both of the above proofs.

Theorem C: If a polynomial equation

$$a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = 0$$

with integer coefficients $a_0, a_1, \dots, a_n$ has a reduced rational root $\frac{b}{c}$, then b is a factor of a_n and c is a factor of a_0.

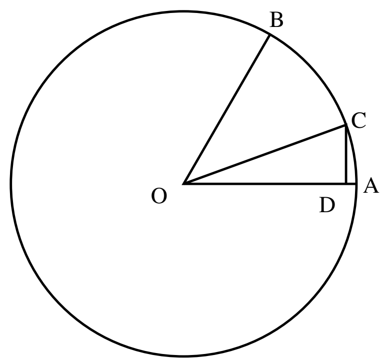

Figure 1

The quadrature of the circle: In the proof of Theorem A it will be seen that the constructibility of a number a is equivalent to the constructibility of $\sqrt{a}$. Thus, if the radius of the given circle is 1, the required square must have side $\sqrt{\pi}$; but π was shown to be transcendental in the last chapter, and so cannot be constructed, by Theorem A.

We now turn to the proofs of Theorems A and B.

Proof of Theorem A: Any Euclidean construction consists of some sequence of the following steps:

1. drawing a straight line between two points,
2. drawing a circle with a given center and a given radius,
3. finding the intersection points of two lines, a line and a circle, or two circles.

Further, every construction problem involves certain given geometric elements $a, b, c, \ldots$ and requires that certain other elements $x, y, z, \ldots$ be found. The conditions of the problem make it possible to set up one or more equations whose solutions allow the unknown elements to be expressed in terms of the given ones. At this point the student should show that, given segments of length a, b, and 1, segments of length $a+b$, $a-b$, ab, $\frac{a}{b}$ and $\sqrt{a}$ can be constructed. These turn out to be the basic operations. Assume that a coordinate system and a unit length are given, and that all the given elements in the construction are represented by rational numbers. Since the sum, difference, product, and quotient (dividing by 0 is of course excluded) of two rational numbers is another rational number, the rational numbers form a closed set under the 4 arithmetic operations. Any set which is closed with respect to these 4 fundamental operations is called a field, and the field of rational numbers will be denoted by Q_0. If two points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ in $Q_0 \times Q_0$ are given, then the equation of the line through them is $(y_2 - y_1)x + (x_1 - x_2)y + (x_2y_1 - x_1y_2) = 0$ or

$$ax + by + c = 0.$$

Clearly, a, b, and c are rational. The equation of a circle with rational radius r and center $(h, k) \in Q_0 \times Q_0$ is $x^2 + y^2 - 2hx - 2ky + h^2 + k^2 - r^2 = 0$ or

$$x^2 + y^2 + dx + ey + f = 0$$

where d, e, and f are rational. Now, finding the intersection of two lines involves arithmetic operations on the coefficients of the variables, and finding the intersection of two circles or of a circle and a line involves the extraction of square roots in addition to the 4 arithmetic operations. Thus, a proposed Euclidean construction is possible if and only if the numbers which define the desired elements can be derived from the given elements by a finite number of arithmetic operations and extractions of square roots.

If a unit length is given, then all rational numbers can be constructed, and if k is a rational number, $\sqrt{k}$ and $a + b\sqrt{k}$ can be constructed if a and b are in Q_0 (rationals). If $\sqrt{k}$ is not in Q_0 then all numbers of the form $a + b\sqrt{k}$ form a new field Q_1. (The student should prove this.) In fact, Q_1 contains Q_0 as a subfield. Next, all numbers of the form $a_1 + b_1\sqrt{k_1}$ where a_1 and b_1 are in Q_1 and k_1 is also in Q_1, but $\sqrt{k_1}$ is not in Q_1 also form a new field, Q_2, which contains Q_1 as a subfield. In this way a sequence of fields $Q_0, Q_1, \ldots,$ Q_n can be formed with the following properties:

(i) Q_0 is the rationals

(ii) Q_j is an extension of Q_{j-1}, $j = 1, 2, \ldots, n$

(iii) Every number in Q_j, $j = 0, 1, \ldots, n$ is constructible

(iv) For every number constructible in a finite number of steps, there exists an integer N such that the constructed number is in one of the fields $Q_0, \ldots, Q_N$.

Because the members of the field Q_j are all roots of polynomials having degree 2^j and rational coefficients, it follows that all constructible numbers are algebraic. This proves Theorem A.

Proof of Theorem B: Consider the general cubic with rational coefficients

$$x^3 + px^2 + qx + r = 0$$

and having no rational roots. Assume that one of the roots is constructible, say x_1. Then x_1 is in Q_n for some integer $n > 0$, where Q_n is one of the fields constructed in the proof of Theorem A. Also assume that none of the roots belong to Q_j, $j < n$. Thus,

$$x_1 = a + b\sqrt{k}$$

where a, b, and k belong to Q_{n-1}. Substituting $x_1 = a + b\sqrt{k}$ into the cubic yields $s + t\sqrt{k}$, and because x_1 is a root,

$$s = a^3 + 3ab^2k + pa^2 + pb^2k + qa + r = 0$$

and

$$t = 3a^2b + b^3k + 2pab + qb = 0.$$

(The student should fill in the details.) Now if $a - b\sqrt{k}$ is substituted into the left side of the cubic, the left side becomes $s - t\sqrt{k}$ and is zero. This means that $x_2 = a - b\sqrt{k}$ is also a root of the cubic. To get the third root, write the cubic as

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

and expand. The coefficient of x^2 turns out to be $-(x_1 + x_2 + x_3)$ which is equal to p. This and the fact that $x_1 + x_2 = 2a$ gives

$$x_3 = -2a - p$$

which means that x_3 belongs to Q_{n-1}, a contradiction. This completes the proof of Theorem B.