Ruler + compass construction of regular 17-sided polygon
(from: The Theory of Numbers, by Hardy & Wright)

Talk about constructing angle $\alpha = 2\pi/n$.

Suppose that $(n_1, n_2) = 1$ and that the problem is soluble for $n = n_1$ and for $n = n_2$. There are integers r_1 and r_2 such that

$$r_1 n_1 + r_2 n_2 = 1$$

or

$$r_1 \alpha_2 + r_2 \alpha_1 = r_1 \frac{2\pi}{n_2} + r_2 \frac{2\pi}{n_1} = \frac{2\pi}{n_1 n_2}.$$

Hence, if the problem is soluble for $n = n_1$ and $n = n_2$, it is soluble for $n = n_1 n_2$. It follows that we need only consider cases in which n is a power of a prime. In what follows we suppose $n = p$ prime.

We can construct α if we can construct $\cos\alpha$ (or $\sin\alpha$); and the numbers

$$\cos k\alpha + i \sin k\alpha \quad (k = 1, 2, \dots, n-1)$$

are the roots of

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + 1 = 0. \tag{5.8.1}$$

Hence we can construct α if we can construct the roots of (5.8.1).

'Euclidean' constructions, by ruler and compass, are equivalent analytically to the solution of a series of linear or quadratic equations.† Hence our construction is possible if we can reduce the solution of (5.8.1) to that of such a series of equations.

The problem was solved by Gauss, who proved (as we stated in § 2.4) that the reduction is possible if and only if n is a 'Fermat prime'‡

$$n = p = 2^{2^h} + 1 = F_h.$$

The first five values of h, viz. 0, 1, 2, 3, 4, give

$$n = 3,\ 5,\ 17,\ 257,\ 65537,$$

all of which are prime, and in these cases the problem is soluble.

The constructions for $n = 3$ and $n = 5$ are familiar. We give here the construction for $n = 17$. We shall not attempt any systematic exposition of Gauss's theory; but this particular construction gives a fair example of the working of his method, and should make it plain to the reader that (as is plausible from the beginning) success is to be expected when $n = p$ and $p-1$ does not contain any prime but 2. This requires that p is a prime of the form $2^m + 1$, and the only such primes are the Fermat primes.||

Suppose then that $n = 17$. The corresponding equation is

$$\frac{x^{17} - 1}{x - 1} = x^{16} + x^{15} + \dots + 1 = 0. \tag{5.8.2}$$

† See § 11.5.

‡ See § 2.5.

|| See § 2.5, Theorem 17.

We write $\alpha = \dfrac{2\pi}{17}$, $\epsilon_k = e\left(\dfrac{k}{17}\right) = \cos k\alpha + i \sin k\alpha,$

so that the roots of (5.8.2) are

(5.8.3) $$x = \epsilon_1, \epsilon_2, \ldots, \epsilon_{16}.$$

From these roots we form certain sums, known as *periods*, which are the roots of quadratic equations.

The numbers $3^m \quad (0 \leqslant m \leqslant 15)$

are congruent (mod 17), in some order, to the numbers $k = 1, 2, \ldots, 16$,† as is shown by the table

$$\begin{array}{l} m = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15, \\ k = 1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11,\ 16,\ 14,\ 8,\ 7,\ 4,\ 12,\ 2,\ 6. \end{array}$$

We define x_1 and x_2 by

$$x_1 = \sum_{m \text{ even}} \epsilon_k = \epsilon_1+\epsilon_9+\epsilon_{13}+\epsilon_{15}+\epsilon_{16}+\epsilon_8+\epsilon_4+\epsilon_2,$$

$$x_2 = \sum_{m \text{ odd}} \epsilon_k = \epsilon_3+\epsilon_{10}+\epsilon_5+\epsilon_{11}+\epsilon_{14}+\epsilon_7+\epsilon_{12}+\epsilon_6;$$

and y_1, y_2, y_3, y_4 by

$$y_1 = \sum_{m \equiv 0 (\text{mod } 4)} \epsilon_k = \epsilon_1+\epsilon_{13}+\epsilon_{16}+\epsilon_4,$$

$$y_2 = \sum_{m \equiv 2 (\text{mod } 4)} \epsilon_k = \epsilon_9+\epsilon_{15}+\epsilon_8+\epsilon_2,$$

$$y_3 = \sum_{m \equiv 1 (\text{mod } 4)} \epsilon_k = \epsilon_3+\epsilon_5+\epsilon_{14}+\epsilon_{12},$$

$$y_4 = \sum_{m \equiv 3 (\text{mod } 4)} \epsilon_k = \epsilon_{10}+\epsilon_{11}+\epsilon_7+\epsilon_6.$$

Since $$\epsilon_k+\epsilon_{17-k} = 2\cos k\alpha,$$

we have

$$x_1 = 2(\cos\alpha+\cos 8\alpha+\cos 4\alpha+\cos 2\alpha),$$

$$x_2 = 2(\cos 3\alpha+\cos 7\alpha+\cos 5\alpha+\cos 6\alpha),$$

$$y_1 = 2(\cos\alpha+\cos 4\alpha), \qquad y_2 = 2(\cos 8\alpha+\cos 2\alpha),$$

$$y_3 = 2(\cos 3\alpha+\cos 5\alpha), \qquad y_4 = 2(\cos 7\alpha+\cos 6\alpha).$$

We prove first that x_1 and x_2 are the roots of a quadratic equation with rational coefficients. Since the roots of (5.8.2) are the numbers (5.8.3), we have

$$x_1+x_2 = 2\sum_{k=1}^{8} \cos k\alpha = \sum_{k=1}^{16} \epsilon_k = -1.$$

Again,

$$x_1 x_2 = 4(\cos\alpha+\cos 8\alpha+\cos 4\alpha+\cos 2\alpha)\times$$
$$\times(\cos 3\alpha+\cos 7\alpha+\cos 5\alpha+\cos 6\alpha).$$

If we multiply out the right-hand side and use the identity

(5.8.4) $$2\cos m\alpha \cos n\alpha = \cos(m+n)\alpha+\cos(m-n)\alpha,$$

† In fact 3 is a 'primitive root of 17' in the sense which will be explained in § 6.8.

we obtain $x_1 x_2 = 4(x_1+x_2) = -4.$

Hence x_1 and x_2 are the roots of

(5.8.5) $$x^2+x-4 = 0.$$

Also

$$\cos\alpha + \cos 2\alpha > 2\cos\tfrac{1}{4}\pi = \surd 2 > -\cos 8\alpha, \qquad \cos 4\alpha > 0.$$

Hence $x_1 > 0$ and therefore

(5.8.6) $$x_1 > x_2.$$

We prove next that y_1, y_2 and y_3, y_4 are the roots of quadratic equations whose coefficients are rational in x_1 and x_2. We have

$$y_1+y_2 = x_1,$$

and, using (5.8.4) again,

$$y_1 y_2 = 4(\cos\alpha + \cos 4\alpha)(\cos 8\alpha + \cos 2\alpha)$$
$$= 2\sum_{k=1}^{8} \cos k\alpha = -1.$$

Hence y_1, y_2 are the roots of

(5.8.7) $$y^2-x_1 y-1 = 0;$$

and it is plain that

(5.8.8) $$y_1 > y_2.$$

Similarly $y_3+y_4 = x_2, \qquad y_3 y_4 = -1,$

and so y_3, y_4 are the roots of

(5.8.9) $$y^2-x_2 y-1 = 0,$$

and

(5.8.10) $$y_3 > y_4.$$

Finally $$2\cos\alpha+2\cos 4\alpha = y_1,$$
$$4\cos\alpha\cos 4\alpha = 2(\cos 5\alpha+\cos 3\alpha) = y_3.$$

Also $\cos\alpha > \cos 4\alpha$. Hence $z_1 = 2\cos\alpha$ and $z_2 = 2\cos 4\alpha$ are the roots of the quadratic

(5.8.11) $$z^2-y_1 z+y_3 = 0$$

and

(5.8.12) $$z_1 > z_2.$$

We can now determine $z_1 = 2\cos\alpha$ by solving the four quadratics (5.8.5), (5.8.7), (5.8.9), and (5.8.11), and remembering the associated inequalities. We obtain

$$2\cos\alpha = \tfrac{1}{8}\{-1+\surd 17+\surd(34-2\surd 17)\}+$$
$$+\tfrac{1}{8}\surd\{68+12\surd 17-16\surd(34+2\surd 17)-2(1-\surd 17)\surd(34-2\surd 17)\},$$

an expression involving only rationals and square roots. This number may now be constructed by the use of the ruler and compass only, and so α may be constructed.

There is a simpler geometrical construction. Let C be the least positive acute angle such that

$$\tan 4C = 4,$$

so that C, $2C$, and $4C$ are all acute. Then (5.8.5) may be written

$$x^2+4x\cot 4C-4 = 0.$$

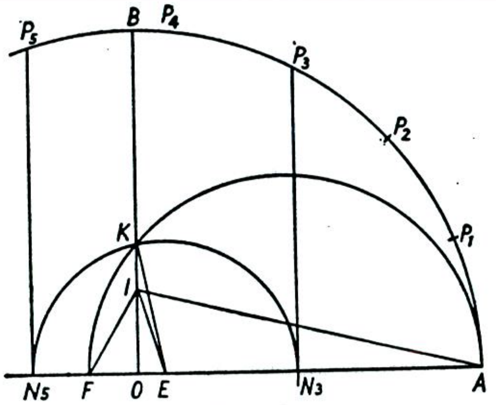

FIG. 6

The roots of this equation are

$$2\tan 2C, \qquad -2\cot 2C.$$

Since $x_1 > x_2$, this gives

$$x_1 = 2\tan 2C, \qquad x_2 = -2\cot 2C.$$

Substituting in (5.8.7) and (5.8.9) and solving, we obtain

$$y_1 = \tan(C+\tfrac{1}{4}\pi), \qquad y_3 = \tan C,$$
$$y_2 = \tan(C-\tfrac{1}{4}\pi), \qquad y_4 = -\cot C.$$

Hence

$$(5.8.13) \quad \begin{cases} 2\cos 3\alpha+2\cos 5\alpha = y_3 = \tan C, \\ 2\cos 3\alpha . 2\cos 5\alpha = 2\cos 2\alpha+2\cos 8\alpha = y_2 = \tan(C-\tfrac{1}{4}\pi). \end{cases}$$

Now let OA, OB (Fig. 6) be two perpendicular radii of a circle. Make OI one-fourth of OB and the angle OIE (with E in OA) one-fourth of the angle OIA. Find on AO produced a point F such that $EIF = \frac{1}{4}\pi$. Let the circle on AF as diameter cut OB in K, and let the circle whose centre is E and radius EK cut OA in N_3 and N_5 (N_3 on OA, N_5 on AO produced). Draw N_3P_3, N_5P_5 perpendicular to OA to cut the circumference of the original circle in P_3 and P_5.

Then $OIA = 4C$ and $OIE = C$. Also

$$2\cos AOP_3 + 2\cos AOP_5 = 2\frac{ON_3 - ON_5}{OA} = \frac{4OE}{OA} = \frac{OE}{OI} = \tan C,$$

$$2\cos AOP_3 . 2\cos AOP_5 = -4\frac{ON_3\,ON_5}{OA^2} = -4\frac{OK^2}{OA^2}$$

$$= -4\frac{OF}{OA} = -\frac{OF}{OI} = \tan(C - \tfrac{1}{4}\pi).$$

Comparing these equations with (5.8.13), we see that $AOP_3 = 3\alpha$ and $AOP_5 = 5\alpha$.

It follows that A, P_3, P_5 are the first, fourth, and sixth vertices of a regular polygon of 17 sides inscribed in the circle; and it is obvious how the polygon may be completed.

NOTES ON CHAPTER V

§ 5.1. The contents of this chapter are all 'classical' (except the properties of Ramanujan's and Kloosterman's sums proved in § 5.6), and will be found in text-books. The theory of congruences was first developed scientifically by Gauss, *D.A.*, though the main results must have been familiar to earlier mathematicians such as Fermat and Euler. We give occasional references, especially when some famous function or theorem is habitually associated with the name of a particular mathematician, but make no attempt to be systematic.

§ 5.5. Euler, *Novi Comm. Acad. Petrop.* 8 (1760–1), 74–104 [*Opera* (1), ii. 531–44].

It might seem more natural to say that $f(m)$ is multiplicative if

$$f(mm') = f(m)f(m')$$

for *all* m, m'. This definition would be too restrictive, and the less exacting definition of the text is much more useful.

§ 5.6. The sums of this section occur in Gauss, 'Summatio quarumdam serierum singularium' (1808), *Werke*, ii. 11–45; Ramanujan, *Trans. Camb. Phil. Soc.* 22 (1918), 259–76 (*Collected Papers*, 179–99); Kloosterman, *Acta Math.* 49 (1926), 407–64. 'Ramanujan's sum' may be found in earlier writings; see, for example, Jensen, *Beretning d. tredje Skand. Matematikercongres* (1913), 145, and Landau, *Handbuch*, 572: but Ramanujan was the first mathematician to see its full importance and use it systematically. It is particularly important in the theory of the representation of numbers by sums of squares.

§ 5.8. The general theory was developed by Gauss, *D.A.*, §§ 335–66. The first explicit geometrical construction of the 17-agon was made by Erchinger (see Gauss, *Werke*, ii. 186–7). That in the text is due to Richmond, *Quarterly Journal of Math.* 26 (1893), 206–7, and *Math. Annalen*, 67 (1909), 459–61. Our figure is copied from Richmond's.

Gauss (*D.A.*, § 341) proved that the equation (5.8.1) is irreducible, i.e. that its left-hand side cannot be resolved into factors of lower degree with rational coefficients, when n is prime. Kronecker and Eisenstein proved, more generally, that the equation satisfied by the $\phi(n)$ primitive nth roots of unity is irreducible; see, for example, Mathews, 186–8. Grandjot has shown that the theorem can be deduced very simply from Dirichlet's Theorem 15: see Landau, *Vorlesungen*, iii. 219.