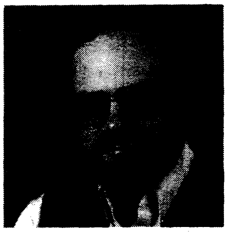
Carlyle Circles and the Lemoine Simplicity of Polygon Constructions

DUANE W. DETEMPLE, *Washington State University*

DUANE W. DETEMPLE: I received my Ph.D. from Stanford University in 1970, where I wrote my dissertation on bounded univalent functions under the supervision of M. M. Schiffer. I have been at Washington State University since then, with the exception of the 1981–82 year when I was a visiting associate professor at Claremont Graduate School. My current research areas include combinatorial geometry and graph theory.



1. Historical Comments and Introduction. Until very late in the eighteenth century the only regular polygons known to have Euclidean straightedge and compass constructions were precisely the ones shown in Book IV of Euclid's *Elements*. This situation changed abruptly on March 30, 1796, when one month before his nineteenth birthday Carl Friedrich Gauss made the first entry in his notebook [7]:

> *Principia quibus innititur sectio circuli, ac divisibilitas geometrica in septemdecim partes etc.*
>
> *Mart.* 30 *Bruns* [*igae*].
>
> *Principle of the circle's division, and how one geometrically divides the circle into seventeen parts, and so forth.*
>
> *March* 30 [*Braunschweig*]

Gauss had discovered that besides the regular polygons of $2^n \cdot 3$, $2^n \cdot 4$, $2^n \cdot 5$ and $2^n \cdot 15$ sides, there were a number of other constructible polygons, including the 17-gon. Gauss secured priority to his discovery by publishing an announcement on June 1, 1796, which appeared in the "Intelligenzblatt der Allgemeinen Literaturzeitung," the first and only time he published in a journal of advance notices. In his short note he wrote that "This discovery is really only a corollary of a theory with greater content, which is not complete yet, but which will be published as soon as it is complete" ([1], [7]). The full meaning of Gauss' pronouncement came in 1801 with the publication of his monumental *Disquisitiones Arithmeticae* [6]. Its final two sections (articles 365 and 366) discuss the issue of polygon constructibility. Recasting the problem in terms of constructing the N vertices of the polygon on a given circle, Gauss stated his result as follows.

> In general therefore in order to be able to divide the circle geometrically into N parts, N must be 2 or a higher power of 2, *or* a prime number of the form $2^m + 1$, or the product of several prime numbers of this form, *or* the product of one or several such primes into 2 or a higher power of 2.

The sufficiency of the condition follows readily from Gauss' analysis. The necessity, however, is not obvious and Gauss never published a proof of this assertion. The first proof is credited to Pierre L. Wantzel (1814–48) [15].

Primes of the form $2^m + 1$, and therefore necessarily of the form $F_k = 2^{2^k} + 1$, are the Fermat primes. Gauss knew that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ were prime, and he knew that Euler had shown F_5 to be composite. Even today no other Fermat primes have been found, although the smallest unsettled cases are F_{22}, F_{24}, and F_{28}. (The primality status of Fermat numbers as of 1983 can be found in Keller [8], and a shorter but more recent table is included in Young and Buell [17]).

Beyond the brilliant theoretical breakthrough of Gauss there is still an intriguing puzzle: how can one devise a sequence of steps with straightedge and compass which constructs a regular N-gon? Gauss expressed interest in this problem, although he did not offer explicit geometric constructions. Throughout the last century, and even into present times, numerous constructions have been contrived for the 17-gon (see [1], [2] for historical comments). J. F. Richelot's construction of the 257-gon required a total of 194 pages, published in four parts in Crelle's journal in 1832. A Professor O. Hermes labored for ten years on the construction and associated algebra of the 65537-gon. The work filled a trunk which was donated to the Mathematical Institute at Göttingen. Nearly a century later it remains stored in an attic there, in all likelihood having never been read.

In what follows we show that a remarkably uniform procedure to construct the regular F_k-gons is afforded by consistent use of an idea attributed to the Scottish historian Thomas Carlyle (1795–1881). Before turning his attention to the literary arts, the young Carlyle taught mathematics, translated Legendre's influential *Elements de Géométrie* into English, and, important for our purposes, devised an elegant geometrical solution to quadratic equations. His idea is based on what we will call the Carlyle circle construction, which we describe in the next section. In the remaining sections we will demonstrate constructions of the 5-, 17- and 257-gon which employ the Carlyle circle method, and, at least in a general way, we also discuss the method's applicability to the 65537-gon.

Our unified approach has two nice features: first, the correctness of the constructions is easy to verify, and second, the constructions are highly efficient. For the pentagon the procedure is similar to the popular construction from antiquity found in Ptolemy's *Almagest*, but with a slight twist at the end. For the 17-gon we rediscover a method of Smith [12] which appeared in 1920, but again we can offer a small improvement. The 257-gon is fairly difficult at the concrete level of actually using the Euclidean tools with sufficient accuracy to produce a convincing construction, but at the conceptual level the procedure is remarkably straightforward in its use of 24 Carlyle circles. Indeed, one becomes convinced that the style of construction needs no change to handle the 65537-gon.

A quantitative measure of the simplicity of a geometric construction was devised in 1907 by Émile Lemoine (1840–1912), and is described in Eves [5] this way. Consider the following five operations.

S_1: to make the straightedge pass through one given point.

S_2: to rule a straight line.

C_1: to make one compass leg coincide with any point.

C_2: to make one compass leg coincide with any point of a given locus.

C_3: to describe a circle.

If these operations are performed m_1, m_2, n_1, n_2, n_3 times respectively in a construction then $m_1S_1 + m_2S_2 + n_1C_1 + n_2C_2 + n_3C_3$ is the *symbol* of the construction. The total number of operations $m_1 + m_2 + n_1 + n_2 + n_3$ is called the *simplicity* of the construction, where we note that a low value of simplicity corresponds to an efficient construction. In what follows we will assume that we use a single noncollapsing compass[1]. Simplicity is improved by having circles with a common radius, or a common center, described in succession since the compass would not have to be reset, or one of its legs would not require repositioning.

As an example, the construction of a circle and two lines which cross orthogonally at the circle's center (if we begin with the circle, C_3, then draw a line through the circle's center, $S_1 + S_2$, and finally erect the perpendicular bisector, $2C_1 + 2C_3 + 2S_1 + S_2$) has symbol $3S_1 + 2S_2 + 2C_1 + 0C_2 + 3C_3$ and simplicity 10. If the first two steps in the construction just described are reversed (begin with a line, S_2, and then draw a circle centered on the line, $C_2 + C_3$) then the symbol is $2S_1 + 2S_2 + 2C_1 + C_2 + 3C_3$, but the simplicity is still 10.

The constructions we will describe for regular polygons have lower simplicity measures than their competitors and are perhaps nearly optimal. An interesting, but apparently open, problem is whether or not it can be proved that a given construction has optimal Lemoine simplicity.

2. Carlyle Circles. A variety of methods to construct the roots of a quadratic equation are known, but the one of Carlyle we now describe is especially attractive. It appeared in Leslie's *Elements of Geometry* with the remark "The solution of this important problem now inserted in the text, was suggested to me by Mr. Thomas Carlyle, an ingenious young mathematician, and formerly my pupil" (see **[5]**).

Beginning with the usual Cartesian x, y-axes and a unit distance, our intention is to construct the roots of the quadratic equation $x^2 - sx + p = 0$, where s and p are given signed lengths. To this end, plot the points $A(0,1)$ and $B(s,p)$. The circle which has the segment $\overline{AB}$ as a diameter will be called the *Carlyle circle* $C_{s,p}$ of the given quadratic equation. The center of C_{sp} is at $M(s/2,(1+p)/2)$, which can be constructed as the midpoint of $\overline{AB}$. It will later be found useful to notice that M is also the midpoint of $S(s,0)$ and $Y(0,1+p)$, where the advantage derives from being able to locate S and Y on the x- and y-axes, respectively.

If we suppose $C_{s,p}$ crosses the x-axis at $H_1(x_1,0)$ and $H_2(x_2,0)$, with $x_1 \geqslant x_2$, we have the two cases shown in FIG. 1. For p of either sign we observe that $x_1 + x_2 = s$. For $p \leqslant 0$ the intersecting chords theorem for FIGURE 1(a) shows $OH_1 \cdot OH_2 = OA \cdot OC$; that is, $(x_1)\cdot(-x_2) = (1)\cdot(-p)$. For $p > 0$, the intersecting secants theorem for FIG. 1(b) shows $x_1 \cdot x_2 = p$. In all cases, then,

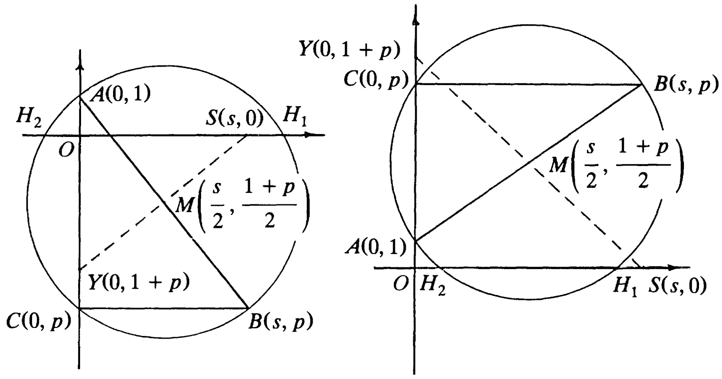
$$(x - x_1)(x - x_2) = x^2 - sx + p, \qquad s = x_1 + x_2, \qquad p = x_1 x_2,$$

and so we conclude the following theorem:

If the Carlyle circle $C_{s,p}$ intersects the x-axis at x_1 and x_2, these are the roots of $x^2 - sx + p = 0$.

An alternate proof can be based on the Pythagorean theorem.

[1]The modern noncollapsing compass permits one to draw with ease a circle centered at a given point whose radius is the distance between two other points. If one only has a collapsing compass, the type assumed by Euclid, then it is surprisingly cumbersome to transfer lengths and consequently the simplicity numbers of most constructions is greatly increased.



(a) Case $p \leqslant 0$ (b) Case $p > 0$

FIG. 1

The quadratic equations we will consider later all have real roots, but it should be pointed out that complex roots are also related to the Carlyle circle. Suppose the y-coordinate $(1+p)/2$ of the center of $C_{s,p}$ exceeds the circle's radius

$$r = \left[\left(\frac{s}{2}\right)^2 + \left(\frac{1-p}{2}\right)^2\right]^{1/2},$$

a condition which reduces to having a negative discriminant $\Delta = s^2 - 4p$. The circle $C_{s,p}$ does not intersect the x-axis, which reflects the fact that the quadratic equation has a pair of complex conjugate roots $z_1, z_2 = s/2 \pm \frac{1}{2}i\sqrt{-\Delta}$. We will now verify that any circle centered on the x-axis and orthogonal to $C_{s,p}$ will meet the vertical line through the center of $C_{s,p}$ at

$$\left(\frac{s}{2}, \frac{1}{2}\sqrt{-\Delta}\right) \quad \text{and} \quad \left(\frac{s}{2}, -\frac{1}{2}\sqrt{-\Delta}\right).$$

To see this, consider the circle centered at $(\xi, 0)$ which is orthogonal to $C_{s,p}$. Its equation is

$$(x-\xi)^2 + y^2 = \left(\frac{s}{2} - \xi\right)^2 + \left(\frac{1+p}{2}\right)^2 - r^2,$$

and setting $x = s/2$ we find

$$y^2 = \left(\frac{1+p}{2}\right)^2 - r^2 = -\tfrac{1}{4}\Delta.$$

Therefore any such orthogonal circle can be used to construct z_1, and z_2, with the y-axis now interpreted as the imaginary axis of the complex plane.

3. Construction of the Regular Pentagon. We assume that we have already constructed the unit circle and the x, y-axes. Following Gauss we view the problem as the construction of the roots of $z^5 - 1 = 0$. The root $z_0 = 1$, corresponding to the point $P_0(1,0)$, can be factored out to show that the remaining points P_1, P_2, P_3, P_4 correspond to the roots of the quartic equation $z^4 + z^3 + z^2 +$

$z + 1 = 0$. Letting $\varepsilon = e^{2\pi i/5}$ these roots are $\varepsilon^1, \varepsilon^2, \varepsilon^3, \varepsilon^4$, which we observe sum to -1.

Two other sums of roots are of special interest, namely,

$$\begin{aligned} \eta_0 &= \varepsilon^1 + \varepsilon^4 = 2\cos(2\pi/5) \\ \eta_1 &= \varepsilon^2 + \varepsilon^3 = 2\cos(4\pi/5). \end{aligned} \tag{1}$$

It is simple to check that

$$\eta_0 + \eta_1 = -1, \qquad \eta_0 \cdot \eta_1 = -1, \qquad \eta_0 > 0 > \eta_1. \tag{2}$$

From (2) it follows that η_0 and η_1 are, respectively, the larger and smaller root of the quadratic equation $x^2 + x - 1 = 0$, and therefore they can be constructed by means of the Carlyle circle $C_{-1,-1}$ which has center $M(-1/2, 0)$. M is constructed as the midpoint of $\overline{OQ}$, where $Q(-1, 0)$. The Carlyle circle centered at M and passing through $A(0, 1)$ then intersects the x-axis at $H_0(\eta_0, 0)$ and $H_1(\eta_1, 0)$. In view of (1), circles of unit radius centered at H_0 and H_1 will intersect the original unit circle at P_1, P_2, P_3, P_4, thereby forming the desired pentagon $P_0P_1P_2P_3P_4$ as shown in FIGURE 2.

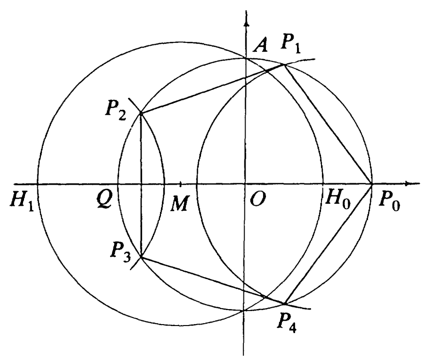


FIG. 2

Beginning with the unit circle and the x, y-axes as given, the construction just described has symbol $2S_1 + S_2 + 8C_1 + 0C_2 + 4C_3$, for a Lemoine simplicity of 15. The popular construction of Ptolemy (see **[4]**, **[15]**) proceeds in the same way through the construction of H_0, but then takes AH_0 as the distance between successive vertices of the pentagon, resulting in a simplicity of 16 to locate all five vertices.

4. Construction of the Regular Heptadecagon (17-gon). Letting $\varepsilon = e^{2\pi i/17}$, our task here is to construct the roots $\varepsilon^1, \varepsilon^2, \dots, \varepsilon^{16}$ of the equation $z^{16} + z^{15} + \cdots + z + 1 = 0$. Gauss' idea was to arrange these roots in a cycle in which each root is a gth power of its predecessor:

$$\varepsilon^1, \varepsilon^g, \varepsilon^{g^2}, \dots, \varepsilon^{g^{15}}, \varepsilon^{g^{16}} = \varepsilon^1. \tag{3}$$

Since $\varepsilon^m = \varepsilon^{m \pmod{17}}$, we can see that corresponding to the prime $p = 17$ there must be found a g for which

$$g^r \not\equiv 1 \pmod{p}, \qquad 1 \leqslant r \leqslant p-2 \quad \text{and} \quad g^{p-1} \equiv 1 \pmod{p}. \tag{4}$$

A positive integer g which satisfies the conditions of (4) for p is said to be a primitive root of the prime p. For any Fermat prime $p > 3$, $g = 3$ is always a primitive root. This follows from the fact that 3 is a quadratic nonresidue by the quadratic reciprocity theorem, and any nonresidue is a primitive root because the size of the multiplicative group is a power of 2. With this choice the cycle (3) becomes

$$\varepsilon^1, \varepsilon^3, \varepsilon^9, \varepsilon^{10}, \varepsilon^{13}, \varepsilon^5, \varepsilon^{15}, \varepsilon^{11}, \varepsilon^{16}, \varepsilon^{14}, \varepsilon^8, \varepsilon^7, \varepsilon^4, \varepsilon^{12}, \varepsilon^2, \varepsilon^6. \tag{5}$$

Next, Gauss considered the sums of the terms of various subcycles of (5), which are called periods. A typical example is the period $\eta_{0,2} = \varepsilon^1 + \varepsilon^9 + \varepsilon^{13} + \cdots + \varepsilon^2$. For notational convenience a period will be represented by an l-tuple of the exponents of ε which occur in the sum, and so the two periods of length eight are expressed as

$$\begin{aligned} \eta_{0,2} &= (1, 9, 13, 15, 16, 8, 4, 2) \\ \eta_{1,2} &= (3, 10, 5, 11, 14, 7, 12, 6). \end{aligned} \tag{6}$$

There are four periods of length four, namely,

$$\begin{aligned} \eta_{0,4} &= (1, 13, 16, 4), \qquad & \eta_{2,4} &= (9, 15, 8, 2) \\ \eta_{1,4} &= (3, 5, 14, 12), \qquad & \eta_{3,4} &= (10, 11, 7, 6). \end{aligned} \tag{7}$$

There are eight periods of length two, but only two are needed for the construction,

$$\begin{aligned} \eta_{0,8} &= (1, 16) = 2\cos(2\pi/17) \\ \eta_{4,8} &= (13, 4) = 2\cos(8\pi/17). \end{aligned} \tag{8}$$

From (8), and using (7), we easily see that

$$\eta_{0,8} + \eta_{4,8} = \eta_{0,4}, \qquad \eta_{0,8} \cdot \eta_{4,8} = \eta_{1,4}, \qquad \eta_{0,8} > \eta_{4,8}. \tag{9}$$

Similarly it is straightforward to calculate that

$$\eta_{0,4} + \eta_{2,4} = \eta_{0,2}, \qquad \eta_{0,4} \cdot \eta_{2,4} = -1, \qquad \eta_{0,4} > \eta_{2,4} \tag{10}$$

$$\eta_{1,4} + \eta_{3,4} = \eta_{1,2}, \qquad \eta_{1,4} \cdot \eta_{3,4} = -1, \qquad \eta_{1,4} > \eta_{3,4} \tag{11}$$

$$\eta_{0,2} + \eta_{1,2} = -1, \qquad \eta_{0,2} \cdot \eta_{1,2} = -4, \qquad \eta_{0,2} > \eta_{1,2}. \tag{12}$$

The inequalities in (10) and (11) are geometrically obvious, and since a calculation shows that $(\eta_{0,4} - \eta_{2,4}) \cdot (\eta_{1,4} - \eta_{3,4}) = 2(\eta_{0,2} - \eta_{1,2})$ it then follows that $\eta_{0,2} > \eta_{1,2}$ as claimed in (12).

Equations (8)–(12) readily lead to the construction of the regular 17-gon as shown in FIGURE 3. It is assumed that we are given the unit circle centered at O and the x, y-axes. From (12) we see that $\eta_{0,2}$ and $\eta_{1,2}$ are, respectively, the larger and smaller roots of the quadratic equation $x^2 + x - 4 = 0$ whose corresponding Carlyle circle $C_{-1,-4}$ is centered at $M_0(-1/2, -3/2)$. Therefore:

(i) Draw the perpendicular bisector of $\overline{QO}$, using a circle at Q through O and the existing circle. This construction has Lemoine symbol $2S_1 + S_2 + 2C_1 + C_3$ and locates Q'.
(ii) Draw a circle at Q' through P_0 (symbol $2C_1 + C_3$) to locate M_0.
(iii) Draw the Carlyle circle at M_0 (symbol $2C_1 + C_3$) to locate $H_{0,2}(\eta_{0,2}, 0)$ and $H_{1,2}(\eta_{1,2}, 0)$.

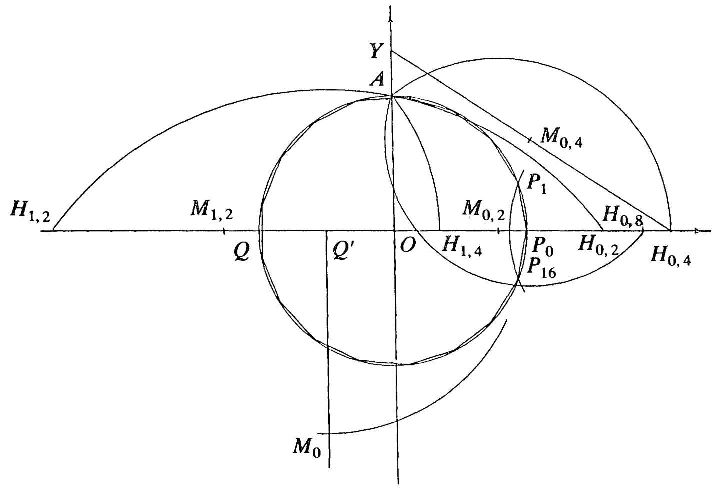


FIG. 3

From equations (10) and (11) we see that Carlyle circles centered at $M_{0,2}(\frac{1}{2}\eta_{0,2}, 0)$ and $M_{1,2}(\frac{1}{2}\eta_{1,2}, 0)$ will locate $H_{0,4}(\eta_{0,4}, 0)$ and $H_{1,4}(\eta_{1,4}, 0)$. Therefore:

(iv) Draw the perpendicular bisectors of $\overline{OH_{0,2}}$ and $\overline{OH_{1,2}}$, using the same circle at O (symbol $4S_1 + 2S_2 + 3C_1 + 3C_3$). This locates $M_{0,2}$ and $M_{1,2}$.

(v) Draw the Carlyle circles at $M_{0,2}$ and $M_{1,2}$ (symbol $4C_1 + 2C_3$) to locate $H_{0,4}$ and $H_{1,4}$.

Turning next to Equation (9), we see that $H_{0,8}(\eta_{0,8}, 0)$ requires a Carlyle circle at $M_{0,4}$. Therefore:

(vi) Set the compass to radius $QH_{1,4}$ and draw a circle at O (symbol $3C_1 + C_3$) to locate $Y(0, 1 + \eta_{1,4})$.

(vii) Draw the line $\overline{YH_{0,4}}$ (symbol $2S_1 + S_2$).

(viii) Draw the perpendicular bisector to $\overline{YH_{0,4}}$ (symbol $2S_1 + S_2 + 2C_1 + 2C_3$) to locate $M_{0,4}$.

(ix) Draw the Carlyle circle at $M_{0,4}$ (symbol $2C_1 + C_3$) to locate $H_{0,8}$.

In view of equation (8), the following step locates P_1 and P_{16}, which correspond to ε^1 and ε^{16}, respectively. Except for laying off the distance P_0P_1, this completes the construction.

(x) Set the compass to unit radius and draw a circle at $H_{0,8}$ (symbol $3C_1 + C_3$) to locate P_1 and P_{16}.

The ten steps described above have total symbol $10S_1 + 5S_2 + 23C_1 + 0C_2 + 13C_3$, for a simplicity of 51. However, two simple modifications can reduce the simplicity of the construction to 45.* First, the costly double bisection of step (iv) can be avoided by using half-scaled Carlyle circles to locate $M_{0,2}$ and $M_{1,2}$. This requires a perpendicular bisector of $\overline{Q'O}$, but since the compass is already set at

*Our thanks to the referee for suggesting these modifications.

unit radius the symbol is $2S_1 + S_2 + C_1 + C_3$. We also need a circle of radius OQ' at O (symbol $2C_1 + C_3$). Since there is no more need for step (iv) the simplicity is reduced by four. Step (viii) can also be replaced by a less costly procedure. Following step (vi) the perpendicular bisector of OY can be constructed with symbol $2S_1 + S_2 + C_1 + C_3$, since the compass need not be reset for the circle at Y. Step (vii) now locates $M_{0,4}$ and so we have further reduced the simplicity by two. Altogether the modified Carlyle construction has symbol $8S_1 + 4S_2 + 22C_1 + 11C_3$, for a simplicity of 45.

The Smith construction **[12]** is similar to that described in (i)–(x), but it requires a perpendicular bisector at $H_{0,4}$, which increases the simplicity to 58. The construction of Richmond **[11]** (also shown in **[13]**, **[16]**, and elsewhere) seems to appear more often than its efficiency warrants. Even arranging for several circles to do double duty, as in the modified Carlyle construction, the simplicity is 53 (which constructs P_3; the simplicity increases to 60 to locate P_1.) The comparatively recent construction of Tietze **[14]**, also described in Hall **[7]**, can be done with simplicity 50. Neither reference provides a proof of the construction, and indeed Hall remarks that "the proof that it is correct requires extensive calculation." His assessment applies equally well to the method of Richmond.

5. Construction of the Regular 257-gon. Since $g = 3$ is also a primitive root of 257, the roots of $z^{256} + z^{255} + \cdots + 1 = 0$ are ordered in the cycle

$$\varepsilon^1, \varepsilon^3, \varepsilon^9, \varepsilon^{27}, \varepsilon^{81}, \varepsilon^{243}, \varepsilon^{215}, \ldots, \varepsilon^{165}, \varepsilon^{238}, \varepsilon^{200}, \varepsilon^{86},$$

where $\varepsilon = e^{2\pi i/257}$. The period of length $l = (p-1)/2^r$ which contains the term ε^{g^j} is denoted by

$$\eta_{j,k} = \sum_{n=0}^{l-1} \varepsilon^{g^{j+nk}}, \qquad k = 2^r.$$

In particular, $\eta_{0,1} = -1$ and we also observe that $\eta_{j,k} = \eta_{i,k}$ when $j \equiv i \pmod{k}$.

To set up the hierarchy of quadratic equations to be solved in succession, it is necessary to know the sum, product, and relative size of pairs of periods. This allows the construction of the periods by means of the appropriate Carlyle circles.

The addition formulas

$$\eta_{j,2k} + \eta_{j+k,2k} = \eta_{j,k} \tag{13}$$

are obvious. Formulas for products require effort but perhaps less than expected. The following sample calculation of $\eta_{0,64} \cdot \eta_{32,64}$ illustrates some useful principles of computation. Since $\eta_{0,64} = (1, 241, 256, 16)$ and $\eta_{32,64} = (64, 4, 193, 253)$ are represented by quadruples of exponents, the product we seek corresponds to a modulo 257 addition table.

		$\eta_{32,64}$			
		64	4	193	253
$\eta_{0,64}$	1	65	5	194	254
	241	48	245	177	237
	256	63	3	192	252
	16	80	20	209	12

The main diagonal, it can be checked, is $\eta_{33,64} = (65, 245, 192, 12)$, and the "diagonal" just below it is $\eta_{55,64} = (48, 3, 209, 254)$. Altogether we find that

$$\eta_{0,64} \cdot \eta_{32,64} = \eta_{33,64} + \eta_{55,64} + \eta_{23,64} + \eta_{1,64}. \tag{14}$$

Thus products can be computed by knowing which periods of the same length contain the terms in the first column.

The right side of (14) can be simplified by use of the addition formulas (13), giving

$$\eta_{0,64} \cdot \eta_{32,64} = \eta_{1,32} + \eta_{23,32}. \tag{15}$$

The derivation of (15) is actually enough from which to deduce the general formula obtained by increasing the first subscripts by j. That is,

$$\eta_{j,64} \cdot \eta_{j+32,64} = \eta_{j+1,32} + \eta_{j+23,32}. \tag{16}$$

Additional discussion of these computational details can be found in Rademacher **[10]**.

The last algebraic difficulty is the ordering of $\eta_{j,2k}$ and $\eta_{j+k,2k}$. It is obvious that $\eta_{0,64} > \eta_{32,64}$ but showing that $\eta_{4,16} > \eta_{12,16}$ is somewhat delicate. The methods described in Klein [9] and Rademacher **[10]** for the 17-gon can be extended to the present case however, thus allowing the identification of the larger and smaller root of a pair.

The results of the calculations are shown in TABLE 1. The same information is contained in Bishop **[3]**, but in a different form, since we have used formula (13) to simplify the expressions for the period products. Since it will be sufficient to construct the point P_1 on the unit circle whose x-coordinate is $\cos(2\pi/257) = (1/2)\eta_{0,128}$, we observe that we need only construct two of the period pairs of length 4 and six of length 8.

TABLE 1

Products of Required Period Pairs	Order of Period Pairs
$\eta_{0,2} \cdot \eta_{1,2} = -64$	$\eta_{0,2} > \eta_{1,2}$
$\eta_{j,4} \cdot \eta_{j+2,4} = -16, \quad j = 0, 1$	$\eta_{0,4} > \eta_{2,4}, \eta_{1,4} > \eta_{3,4}$
$\eta_{j,8} \cdot \eta_{j+4,8} = -2 + 3\eta_{j+1,2} + 2\eta_{j+2,4}$, $j = 0, 1, 2, 3$	$\eta_{0,8} > \eta_{4,8}, \eta_{2,8} > \eta_{6,8}, \eta_{1,8} < \eta_{5,8}, \eta_{3,8} < \eta_{7,8}$
$\eta_{j,16} \cdot \eta_{j+8,16} = \eta_{j,2} + \eta_{j,8} + \eta_{j+2,8} + 2\eta_{j+5,8}$, $j = 0, \ldots, 7$	$\eta_{0,16} > \eta_{8,16}, \eta_{4,16} > \eta_{12,16}, \eta_{2,16} > \eta_{10,16}, \eta_{6,16} < \eta_{14,16}, \eta_{1,16} > \eta_{9,16}, \eta_{5,16} > \eta_{13,16}, \eta_{3,16} > \eta_{11,16}, \eta_{7,16} > \eta_{15,16}$
$\eta_{j,32} \cdot \eta_{j+16,32} = \eta_{j,16} + \eta_{j+1,16} + \eta_{j+2,16} + \eta_{j+5,16}$, $j = 0, 1, 7, 8, 9, 15$	$\eta_{0,32} > \eta_{16,32}, \eta_{8,32} < \eta_{24,32}, \eta_{1,32} > \eta_{17,32}, \eta_{9,32} < \eta_{25,32}, \eta_{7,32} < \eta_{23,32}, \eta_{15,32} > \eta_{31,32}$
$\eta_{j,64} \cdot \eta_{j+32,64} = \eta_{j+1,32} + \eta_{j+23,32}$, $j = 0, 24$	$\eta_{0,64} > \eta_{32,64}, \eta_{24,64} < \eta_{56,64}$
$\eta_{0,128} \cdot \eta_{64,128} = \eta_{56,64}$	$\eta_{0,128} > \eta_{64,128}$

Translating the results of the table into an explicit construction is straight-forward, although we must be alert to carrying out the required procedure in an efficient manner. Beginning with the first row of information in TABLE 1 we see that $\eta_{0,2}$ and $\eta_{1,2}$ are the larger and smaller roots, respectively, of $x^2 + x - 64 = 0$, and so the first step is to construct the center $M_0(-1/2, -63/2)$ of the Carlyle circle $C_{-1,-64}$. Successive distance doublings along the positive x-axis will locate $T(31, 0)$, and then swinging an arc from $Q'(-1/2, 0)$ of radius $Q'T$, will locate M_0 on the perpendicular bisector $x = -1/2$ of O and $Q(-1, 0)$. As shown in FIGURE 4, the Carlyle circle $C_{-1,-64}$ then locates $H_{0,2}(\eta_{0,2}, 0)$ and $H_{1,2}(\eta_{1,2}, 0)$.

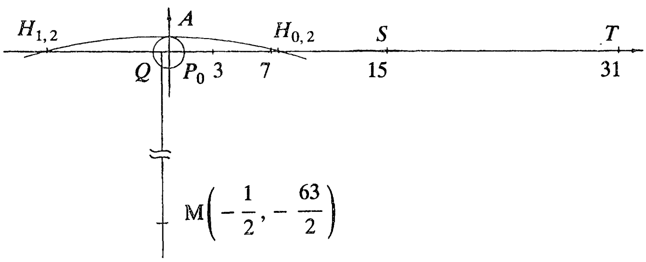


FIG. 4

The construction of the four periods of length 64 is depicted in FIGURE 5. The point $Y(0, -15)$ is located by swinging an arc from O of radius OS, where $S(15, 0)$ was constructed in the previous step. The midpoint $M_{0,2}$ of $\overline{YH_{0,2}}$ is the center of the Carlyle circle which determines $H_{0,4}(\eta_{0,4}, 0)$ and $H_{2,4}(\eta_{2,4}, 0)$. Similarly the points at $x = \eta_{1,4}$ and $x = \eta_{3,4}$ are found by the Carlyle circle centered at the midpoint $M_{1,2}$ of $\overline{YH_{1,2}}$.

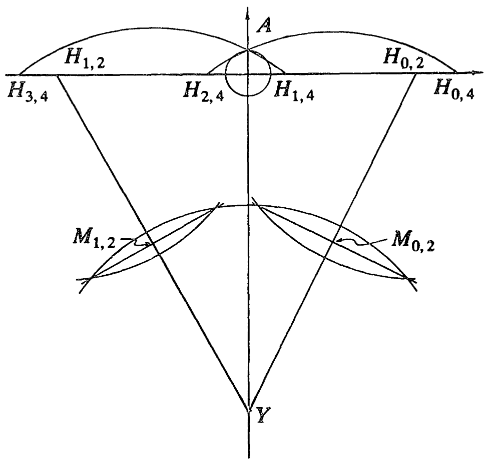


FIG. 5

The remaining pairs of periods are constructed in an analogous way, although extra distance transfers are required because of the more complicated product expressions shown in TABLE 1. A circle of unit radius centered at $H_{0,128}$ will cross the unit circle at P_1 and P_{256}, which completes the construction up to laying off the distance P_0P_1 to locate all of the vertices of the 257-gon.

To optimize the simplicity of the construction it is essential to transfer distances efficiently. For example some useful savings in constructing $\eta_{0,16}, \eta_{4,16}, \eta_{8,16}, \eta_{12,16}$ are possible when advantage is taken of the relation $\eta_{0,16} \cdot \eta_{8,16} + \eta_{4,16} \cdot \eta_{12,16} = 3\eta_{0,2} + 2\eta_{1,4}$. The construction of the three other quadruples of periods of length sixteen are aided by the corresponding algebraic relations.

Beginning with the unit circle and the x, y-axes, the construction of $P_1(\cos(2\pi/257), \sin(2\pi/257))$ has symbol

$$94S_1 + 47S_2 + 275C_1 + 0C_2 + 150C_3$$

for a Lemoine simplicity of 566. Among the 150 circles are 24 Carlyle circles.

6. Remarks on the Construction of the Regular 65537-gon. We have already observed that $g = 3$ is a primitive root of $p = 65537$. The sum, product, and relative order of period pairs must then be computed (one feels sorry for the computerless Hermes!). The first line of the required table of information is

$$\eta_{0,2} + \eta_{1,2} = -1, \qquad \eta_{0,2} \cdot \eta_{1,2} = -2^{14}, \qquad \eta_{0,2} > \eta_{1,2}. \tag{17}$$

The product formula derives from the fact that the exponent sums evenly divide into quadratic residues and nonresidues. Drawing the Carlyle circle $C_{-1,-2^{14}}$ may place impossible demands on any compass we own, but at the conceptual level there is no problem.

Successive levels in the hierarchy of quadratic equations require $2, 4, 8, \ldots$ Carlyle circles. Working upwards however, and assuming the worst case possibility that the product formulas and sums involve all distinct periods, the largest possible number of Carlyle circles required is $1, 2, 6, 30, 270, 4590, \ldots$. Actually the 4590 is spurious, since there are only 2^{10} periods with 2^6 terms and so these can all be computed with $2^9 = 512$ Carlyle circles. Even though we know little about the details of the construction, we can conclude that the construction we seek requires $1 + 2 + 4 + 8 + \cdots + 512 + 270 + 30 + 6 + 2 + 1 = 1332$ or fewer Carlyle circles.

REFERENCES

1. R. C. Archibald, The history of the construction of the regular polygon of seventeen sides, *Bull. Amer. Math. Soc.*, 22 (1916) 239–246.
2. ______, Gauss and the regular polygon of seventeen sides, *Amer. Math. Monthly*, 27 (1920) 323–326.
3. Wayne Bishop, How to construct a regular polygon, *Amer. Math Monthly*, 85 (1978) 186–188.
4. H. S. M. Coxeter, Introduction to Geometry, Wiley, New York, 1961.
5. Howard Eves, An Introduction to the History of Mathematics, fourth edition, Holt, Rinehart, and Winston, New York, 1976.
6. C. F. Gauss, Disquisitiones Arithmeticae, Leipzig 1801, translated from the Latin by A. A. Clarke, Yale University Press, 1965.
7. Tord Hall, Carl Friedrich Gauss: A Biography, MIT Press, 1970.
8. Wilfred Keller, Factors of Fermat numbers and large primes of the form $k \times 2^n + 1$, *Math. Comp.* 41 (1983) 661–673.
9. Felix Klein, Famous Problems of Elementary Geometry, Dover, 1956 (original German edition in 1895).
10. Hans Rademacher, Lectures on Elementary Number Theory. Blaisdell, New York, 1964.
11. H. W. Richmond, *Quart. J. Math.*, 26 (1893) 296–297.

12. L. Linn Smith, A construction of the regular polygon of seventeen sides, *Amer. Math. Monthly*, 27 (1920) 322–323.
13. Ian Stewart, Gauss, *Sci. Amer.*, 237 (1977) 122–131.
14. Heinrich Tietze, Famous Problems of Mathematics, Graylock Press, New York, 1965 (original German edition in 1949).
15. P. L. Wantzel, *Journal de Mathematiques pures et appliquées*, 2 (1837) 366–372.
16. R. C. Yates, Geometrical Tools, Educational Publishers, St. Louis, 1949.
17. Jeff Young and Duncan A. Buell, The twentieth Fermat number is composite, *Math. Comp.*, 50 (1988) 261–263.

Notice to authors: Recently the MONTHLY has not been processing papers because of a very high backlog. This situation has now eased somewhat and we are once again considering new manuscripts for possible publication. Thank you for your patience. —The Editors.