15.A3 The constructability of the regular 17-gon

(a) The discovery of the constructability

It is well known to every beginner in Geometry that various regular polygons can be constructed geometrically, namely the triangle, pentagon, 15-gon, and those which arise from these by repeatedly doubling the number of sides. One had already got this far in Euclid's time, and it seems that one has persuaded oneself ever since that the domain of elementary geometry could not be extended; at least I do not know of any successful attempts to enlarge its boundaries on this side.

It seems to me then to be all the more remarkable that *besides the usual polygons there is a collection of others which are constructable geometrically, e.g. the 17-gon.* This discovery is properly only a corollary of a not quite completed discovery of greater extent which will be laid before the public as soon as it is completed.

(b) The theory underlying the constructability

Nevertheless none of these equations is so tractable and so suitable for our purposes as $x^n - 1 = 0$. Its roots are intimately connected with the roots of the above. That is, if for brevity we write i for the imaginary quantity $\sqrt{-1}$, the roots of the equation $x^n - 1 = 0$ will be

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r$$

where for k we should take all the numbers $0, 1, 2, \ldots, n-1$. Therefore since $1/r = \cos kP/n - i\sin kP/n$ the roots of equation I will be $[r - (1/r)]/2i$ or $i(1 - r^2)/2r$; the roots of equation II, $[r + (1/r)]/2 = (1 + r^2)/2r$; finally the roots of equation III, $i(1 - r^2)/(1 + r^2)$. For this reason we build our investigation on a consideration of the equation $x^n - 1 = 0$, and presume that n is an odd prime number.

[When Gauss considered the 17-gon, whose vertices are the complex roots of $x^{17} - 1$, he labelled the 16 roots other than $x = 1$ [1], [2], ..., [16], and then calculated them by working through a chain of four quadratics. His results, expressed numerically, are as follows.]

If we then compute the remaining roots we will obtain the following numerical values, where the upper sign is to be taken for the first root, the lower sign for the second:

[1], [16] ...	$0.9324722294 \pm 0.3612416662i$
[2], [15] ...	$0.7390089172 \pm 0.6736956436i$
[3], [14] ...	$0.4457383558 \pm 0.8951632914i$
[4], [13] ...	$0.0922683595 \pm 0.9957341763i$
[5], [12] ...	$-0.2736629901 \pm 0.9618256432i$
[6], [11] ...	$-0.6026346364 \pm 0.7980172273i$
[7], [10] ...	$-0.8502171357 \pm 0.5264321629i$
[8], [9] ...	$-0.9829730997 \pm 0.1837495178i$

[...]

Thus by the preceding discussions we have reduced the division of the circle into n parts, if n is a prime number, to the solution of as many equations as there are factors in the number $n - 1$. The degree of the equations is determined by the size of the factors. Whenever therefore $n - 1$ is a power of the number 2, which happens when the value of n is 3, 5, 17, 257, 65537, etc. the sectioning of the circle is reduced to quadratic equations only, and the trigonometric functions of the angles P/n, $2P/n$, etc. can be expressed by square roots which are more or less complicated (according to the size of n). Thus in these cases the division of the circle into n parts or the inscription of a regular polygon of n sides can be accomplished by geometric constructions. Thus, e.g., for $n = 17$, by articles 354, 361 we get the following expression for the cosine of the angle $P/17$:

$$-\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{[34 - 2\sqrt{17}]} + \tfrac{1}{8}\sqrt{[17 + 3\sqrt{17} - \sqrt{(34 - 2\sqrt{17})} - 2\sqrt{(34 + 2\sqrt{17})}]}$$

The cosine of multiples of this angle will have a similar form, but the sine will have one more radical sign. It is certainly astonishing that although the geometric divisibility of the circle into three and five parts was already known in Euclid's time, nothing was added to this discovery for 2000 years. And all geometers had asserted that, except for those sections and the ones that derive directly from them (that is, division into 15, $3 \cdot 2^\mu$, $5 \cdot 2^\mu$, and 2^μ parts), there are no others that can be effected by geometric constructions. But it is easy to show that if the prime number $n = 2^m + 1$, the exponent m can have no other prime factors except 2, and so it is equal to 1 or 2 or a higher power of the number 2. For if m were divisible by any odd number ζ (greater than unity) so that $m = \zeta\eta$, then $2^m + 1$ would be divisible by $2^\eta + 1$ and so necessarily composite. All values of n, therefore, that can be reduced to quadratic equations, are contained in the form $2^{2^v} + 1$. Thus the five numbers 3, 5, 17, 257, 65537 result from letting $v = 0, 1, 2, 3, 4$ or $m = 1, 2, 4, 8, 16$. But the geometric division of the circle cannot be accomplished for *all* numbers contained in the formula but only for those that are prime. Fermat was misled by his induction and affirmed that all numbers contained in this form are necessarily prime, but the distinguished Euler first noticed that this rule is erroneous for $v = 5$ or $m = 32$, since the number $2^{32} + 1 = 4294967297$ involves the factor 641.

Whenever $n - 1$ implies prime factors other than 2, we are always led to equations of higher degree, namely, to one or more cubic equations when 3 appears once or several times among the prime factors of $n - 1$, to equations of the fifth degree when $n - 1$ is divisible by 5, etc. *We can show with all rigour that these higher-degree equations cannot be avoided in any way nor can they be reduced to lower-degree equations.* The limits of the present work exclude this demonstration here, but we issue this warning lest anyone attempt to achieve geometric constructions for sections other than the ones suggested by our theory (e.g. sections into 7, 11, 13, 19, etc. parts) and so spend his time uselessly.

15.A4 The charms of number theory

The fundamental theorem on quadratic residues is one of the most beautiful truths of higher Arithmetic, [and] was indeed easily found by induction [inspection from