Gauss's Theorem on the Regular Polygons which can be constructed by Euclid's Method.

By Professor H. S. Carslaw, Sc.D.

(*Received October 1909, and in revised form 25th April 1910*).

§1. The methods now adopted in the teaching of elementary geometry have made it most important that the teacher should have clear views upon the nature of the problems which are soluble by Euclid's methods: that is, with the aid of the ruler and compass only. With this general question I have dealt in another place.* In this paper I give a short account of the argument by means of which Gauss proved *that the only regular polygons of n sides, which can be constructed by Euclid's methods, are those in which n, when broken up into prime factors, takes the form*

$$2^m\left(2^{2^{m_1}}+1\right)\left(2^{2^{m_2}}+1\right)\ldots\left(2^{2^{m_r}}+1\right),$$

$m_1, m_2, m_3, \ldots m_r$ being all different.†

This discussion is based upon Enriques' article—*Sulle equazioni algebriche risolubili per radicali quadratici e sulla costruibilità dei poligoni regolari*—in his well-known volume on Elementary Geometry.‡ Since sending my paper in its original form to the Society, I have succeeded in obtaining a copy of the scarce booklet§ of Klein's, in which the same question is referred to, and I have also learned that an English translation of that volume is available.‖ I have thus been able in revising my paper to refer

* Cf. *Math. Gazette*, Vol. V., No. 83, p. 170 (1910).

† Gauss: *Werke*, Bd. I. *Disquisitiones arithmeticae*, §365.

‡ Enriques: *Questioni riguardanti la Geometria Elementare* (Bologna 1900). German Translation, *Fragen der Elementargeometrie* (Leipzig, 1908–10).

§ Klein: *Vorträge über ausgewählte Fragen der Elementargeometrie* (Leipzig, 1895).

‖ This translation by W. W. Beman and D. E. Smith is entitled *Famous Problems in Elementary Geometry*, and was published by Ginn & Co. in 1897.

the reader, for the full proof of some of the questions involved, to Klein's pages: although from the condensed form in which Gauss's Theorem is there discussed, the presentation given by Enriques will offer less difficulty to most readers.

§2. If a regular polygon of n sides can be constructed by Euclid's methods, then a similar polygon can be constructed in a circle. We may thus suppose the polygon inscribed in a circle, whose centre is at the origin, and radius the unit of length. Also we take the angular points as A_0, $A_1 \ldots$, A_{n-1} and OA_0 lies along the axis of x.

The coordinates x_r, y_r of A_r will be $\cos\frac{2r\pi}{n}$ and $\sin\frac{2r\pi}{n}$.

Let $z_r = x_r + iy_r$.

Then $z_1, z_2 \ldots, z_{n-1}$ are the roots of the equation

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0.$$

It follows that *if the regular polygon of n sides can be constructed by Euclid's methods, the roots of this equation must be rational or involve quadratic surds only: and that if they are of this nature, the polygon can be constructed.**

The problem is thus reduced to the discussion of this equation.

§3. Now let $f(x) = 0$ be an algebraical equation with rational coefficients, satisfied by an expression x_1, involving ν square roots. By changing the sign of these roots, we obtain 2^ν expressions

$$x_1, x_2, x_3, \ldots x_s$$

all of which satisfy the equations, though all need not be different.

Let $x_1, x_2, \ldots x_r$ be all the *different* values thus obtained.

Also let

$$\phi(x) = (x - x_1)(x - x_2)(x - x_3)\ldots(x - x_s),$$

and

$$\psi(x) = (x - x_1)(x - x_2)\ldots(x - x_r).$$

Then it is not difficult to show† that if any of the factors of $\phi(x)$ occur in repeated form in $\psi(x)$, they are all repeated the same number of times.

---

* Cf. Hardy's *Pure Mathematics* (pp. 64–65), or the paper by the author already referred to.

† Cf. Enriques: loc. cit. Article XI., §3.
Petersen: Théorie des équations algébriques, §91.

Thus we have $\phi(x) = \{\psi(x)\}^m$ where m is some positive integer.

It follows that *the degree of an irreducible equation which can be solved by quadratic surds must be a power of* 2.

§4. We return to the equation

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0.$$

On putting $z = x + 1$, this becomes

$$x^{n-1} + nx^{n-2} + \frac{n \cdot n-1}{1 \cdot 2} x^{n-3} + \ldots + n = 0.$$

It can be shown that *this equation is irreducible, when n is prime.**

It follows from §3 that in this case n must be of the form $2^m + 1$: and that, *when n is a prime number, if the polygon can be constructed by Euclid's methods, n must take the form* $2^m + 1$.

From this result we see that the polygons of

$$7, 11, 13, 19, \ldots$$

sides cannot be constructed with the ruler and compass.

§5. This condition—in the case of n prime—is *sufficient* as well as *necessary*. The argument by means of which this is established depends upon the following theorem which Gauss was the first to prove: *If n is any prime number, there always exists some number g less than n, such that the powers of*

$$g^1, g^2, g^3, \ldots g^{n-1}$$

are congruent with the numbers $1, 2, 3, \ldots n-1$ (*Mod. n*).

In other words,

$$g^1, g^2, g^3, \ldots g^{n-1},$$

when divided by n, leave the remainders

$$1, 2, 3, \ldots n-1,$$

in some order or other.†

---

* Cf. Enriques: loc. cit. Article XI., §5.
Klein: loc. cit. Chapter III., §§ 6, 7.
The proof usually given is that of Eisenstein: Crelle's Journal, Bd. XXXIX., p. 167.

† Weber-Wellstein: *Encyklopädie der Elementar-Mathematik*, Bd. I., §78; or, Bachmann, *Die Lehre von der Kreistheilung*, p. 28 (Leipzig, 1872).

This theorem Gauss applied to the roots of the fundamental equation

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0,$$

viz.,

$$\epsilon,\ \epsilon^2,\ \epsilon^3 \ldots \epsilon^{n-1}$$

where

$$\epsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Let g be the number less than n, such that

$$g^1,\ g^2,\ g^3, \ldots g^{n-1},$$

leave the remainders $1, 2, 3, \ldots n-1$, on division by n.

Then

$$\epsilon^g,\ \epsilon^{g^2},\ \epsilon^{g^3}, \ldots \epsilon^{g^{n-1}},$$

become

$$\epsilon^1,\ \epsilon^2,\ \epsilon^3, \ldots \epsilon^{n-1},$$

in some order or other, since $\epsilon^n = 1$.

Now let

$$\left.\begin{aligned} \eta_1 &= \epsilon^g + \epsilon^{g^3} + \epsilon^{g^5} + \ldots \quad \epsilon^{g^{n-2}} \\ \eta_2 &= \epsilon^{g^2} + \epsilon^{g^4} + \epsilon^{g^6} + \ldots + \epsilon^{g^{n-1}} \end{aligned}\right\} \ \eta_1 + \eta_2 = \eta.$$

Dividing each of these groups of $\frac{n-1}{2}$ terms again into two, we put

$$\left.\begin{aligned} \eta_{11} &= \epsilon^g + \epsilon^{g^5} + \ldots + \epsilon^{g^{n-4}}, \\ \eta_{12} &= \epsilon^{g^3} + \epsilon^{g^7} + \ldots + \epsilon^{g^{n-2}}, \end{aligned}\right\} \ \eta_{11} + \eta_{12} = \eta_1;$$

$$\left.\begin{aligned} \eta_{21} &= \epsilon^{g^2} + \epsilon^{g^6} + \ldots + \epsilon^{g^{n-3}}, \\ \eta_{22} &= \epsilon^{g^4} + \epsilon^{g^8} + \ldots + \epsilon^{g^{n-1}}, \end{aligned}\right\} \ \eta_{21} + \eta_{22} = \eta_2;$$

and so on.

In this way we obtain successive sums, containing

$$\frac{n-1}{2},\ \frac{n-1}{2^2},\ \frac{n-1}{2^3},\ \ldots \text{ terms.}$$

All these terms are different roots of the equation; and, since n is of the form $2^m + 1$, we are reduced finally, by this sub-division, to single terms.

The next point in the argument is to show that these sums—usually called *Gauss's Periods*—can all be calculated by successive extractions of square roots.

First of all, we take η_1 and η_2.

https://doi.org/10.1017/S0013091500034866 Published online by Cambridge University Press

We have

$$\begin{aligned}\eta = \eta_1 + \eta_2 &= \epsilon^{\theta} + \epsilon^{\theta^2} + \epsilon^{\theta^3} + \ldots + \epsilon^{\theta^{n-1}} \\ &= \epsilon^1 + \epsilon^2 + \epsilon^3 + \epsilon^{n-1} \\ &= -1.\end{aligned}$$

Also, since the product of any two roots is itself a root,

$$\epsilon^{\theta^r} . \epsilon^{\theta^s} = \epsilon^{\theta^t},$$

r, s, and t being all less than n.

But the product $\eta_1\eta_2$ contains only terms of this type $\epsilon^{\theta^r}\epsilon^{\theta^s}$; and $\eta_1\eta_2$ does not change in value, if in every term we substitute for ϵ the value ϵ^{θ}, since this just interchanges η_1 and η_2.

Hence the sum $\Sigma\epsilon^{\theta^t}$, which we have found for $\eta_1\eta_2$, must contain each root of the equation the same number of times.

Thus $$\eta_1\eta_2 = \nu\eta = -\nu,$$

where ν is some positive integer.

It follows that η_1, η_2 are the roots of the quadratic equation

$$x^2 + x - \nu = 0.$$

From an argument of the same nature—only a little more difficult*—it follows that η_{11}, η_{12} are the roots of the quadratic equation

$$x^2 - \eta_1 x + (\nu_1\eta_1 + \nu_2\eta_2) = 0,$$

where ν_1, ν_2 are certain positive integers.

And a similar remark holds for η_{21}, η_{22}.

Proceeding in this way we reach finally the periods of one term only, and thus show that these involve quadratic surds only.

Therefore *when n is a prime number of the form $2^m + 1$, the* equation

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0$$

can be solved by successive extractions of square roots, and the regular polygons of n sides can be constructed by Euclid's methods.

§6. Further, if n is a prime number of the form $2^m + 1$, the index m cannot contain any odd factor. This follows at once from the fact that $(x^{2r+1} + 1)$ is divisible by $(x + 1)$.

* Cf. Enriques: loc. cit. Article XI., §7.

https://doi.org/10.1017/S0013091500034866 Published online by Cambridge University Press

Therefore *the only regular polygons of n sides (n being a prime number) which can be constructed by Euclid's methods are those for which n takes the form* $2^{2^{m_1}}+1$.

If we put $m_1 = 0$, 1, 2, 3 and 4, we obtain numbers 3, 5, 17, 257 and 65537 ; and all these polygons can be constructed.

But $m_1 = 5$, 6 and 7 do not give prime numbers, while the nature of those given by higher values of m_1 is not yet known. Still these results are sufficient to show that *among the prime numbers with less than 75 digits there are only five giving regular polygons which can be constructed by Euclid's methods.*

§7. There remains the case when n is not a prime number.

If a polygon of (p, q) sides can be constructed, then the angle $\frac{2\pi}{pq}$ can be obtained.

Hence the angles $\frac{2\pi}{p}$ and $\frac{2\pi}{q}$ can be found.

It follows that if a polygon of (p, q) sides can be constructed, then the polygons of p sides and q sides can also be constructed.

Let the composite number n, with which we are concerned, be broken up into its prime factors

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Then *if this polygon can be constructed, the polygon of* $p_1^{\alpha_1}$, $p_2^{\alpha_2}, \ldots p_r^{\alpha_r}$ sides can also be constructed.

§8. The construction of the polygon of p^α sides reduces to the solution of the equation

$$\frac{z^{p^\alpha}-1}{z-1}=0.$$

Also the expression $z^{p^\alpha}-1$ obviously contains $z^{p^{\alpha-1}}-1$ as a factor.

Further, it can be shown that

$$\frac{z^{p^\alpha}-1}{z^{p^{\alpha-1}}-1}$$

is irreducible when p is prime.*

* Cf. Enriques: loc. cit. Article XI., §10.
Bachmann: loc. cit. p. 32.

https://doi.org/10.1017/S0013091500034866 Published online by Cambridge University Press

Hence the roots of this equation must involve quadratic surds only.

It follows from §3 that $p^{\alpha-1}(p-1)$ must be a power of 2, and that therefore $p^{\alpha-1}$ and $(p-1)$ must both be powers of 2.

But if $\alpha > 1$ and p is a prime number other than 2, $p^{\alpha-1}$ cannot be a power of 2: so that the only possible case of repeated factors is that for which $p = 2$.

As to the non-repeated factors, we have already seen that they must take the form

$$2^{2^{m_1}} + 1.$$

Thus *a necessary condition for the possibility of the construction of a polygon of n sides by Euclid's methods, when n is not prime, is that it must take the form*

$$2^m\left(2^{2^{m_1}}+1\right)\left(2^{2^{m_2}}+1\right)\ldots\left(2^{2^{m_r}}+1\right)$$

where $m_1, m_2, \ldots m_r$ *are all different.*

From this result it is clear that the polygons of 9, 14, 18, 21, 22, 25, ... sides cannot be constructed in this way.

§9. *Finally, we must show that this condition is also sufficient.*

To prove this, we need only show that if the polygons of r and s sides can be constructed (r, s being different primes), then the polygon of $(r \,.\, s)$ sides can be constructed.

But if we are given the polygons of r and s sides, we have the angles $\frac{2\pi}{r}(\alpha)$ and $\frac{2\pi}{s}(\beta)$.

Also we can always find integers x, y, which satisfy the equation

$$sx - ry = 1,$$

if r and s are prime to each other.*

Thus we have

$$\alpha x - \beta y = \frac{2\pi}{rs}(sx - ry)$$

$$= \frac{2\pi}{rs}$$

if x, y are these two integers.

* Cf. C. Smith's Algebra, ch. XXIX., §399.

https://doi.org/10.1017/S0013091500034866 Published online by Cambridge University Press

Hence the angle $\frac{2\pi}{rs}$ can be found, and the polygon of rs sides constructed.

This completes the argument, and is the final step in proving Gauss's Theorem *the necessary and sufficient condition that a regular polygon of n sides can be constructed by Euclid's methods is that, when n is broken up into its prime factors, it must take the form*

$$2^m\left(2^{2^{m_1}}+1\right)\left(2^{2^{m_2}}+1\right)\ldots\left(2^{2^{m_r}}+1\right),$$

where $m_1, m_2, \ldots m_r$ *are all different.*

https://doi.org/10.1017/S0013091500034866 Published online by Cambridge University Press