Cyclotomy and the heptadecagon

PETER SHIU

1. *Introduction*

Cyclotomy is concerned with the division of a circle into a given number of equal segments, amounting to the construction of a regular polygon, say a q-gon, so that we need to deliver the angle $\alpha = 2\pi/q$, or the length $\cos\alpha$. The construction is by Euclidean means, which make use of only ruler and compasses. Now, from given lengths, sums and differences of lengths are easy to obtain and, with the compasses, products and quotients of lengths can be obtained from similar triangles using parallel lines; indeed even the length $\sqrt{a}$ can be obtained by applying the intersecting chord theorem to a circle with diameter $1 + a$. However, there is not much else one can do with the compasses, so that the length $\cos\alpha$ has to come from the real roots of a sequence of quadratic equations with 'suitable' coefficients — the meaning of being suitable will be made clear later.

Gauss made the first significant contribution to the classical theory of cyclotomy in Article 365 of his famous *Disquisitiones Arithmeticae* [1] in 1801. He showed that the construction is possible if $q = p$ is a Fermat prime, that is a prime of the form 2^{2^n+1}; see §7 for a necessary and sufficient condition for q. The only known Fermat primes are $p = 3, 5, 17, 257, 65537$; the cases $p = 3$, 5 and 17 correspond to the construction of the equilateral triangle, the regular pentagon, and the regular heptadecagon, the details for which Gauss gave.

The problem is heavily involved with the pth roots of unity, with particular reference to their algebraic character. Basic to the theory of cyclotomy is a *Gaussian period*, a certain sum of roots of unity; there is also the notion of a *Gauss sum*, which is a linear combination of the periods. The determination of the Gauss sum then enables us to solve the problem, by Euclidean means if p is a Fermat prime.

Besides and beyond the construction of regular polygons, cyclotomy is a pillar of algebraic number theory; see also §10. We consider some of the topics associated with the classical theory; with hindsight, the construction of the regular heptadecagon can be accomplished with only a minimal amount of the theory.

2. *Roots of unity and the cyclotomic polynomial*

Let $p > 3$ be a prime, not necessarily a Fermat prime for the moment. The pth roots of unity are the solutions to $z^p = 1$ and, on writing

$$\zeta = e^{2\pi i/p}, \tag{1}$$

they are given by $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$. The complex roots form conjugate pairs $\{\zeta^n, \zeta^{p-n}\} = \{\zeta^n, \zeta^{-n}\}$, and the construction problem is to use Euclidean means to deliver the length

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

$$2\cos\alpha = \zeta + \zeta^{-1}, \qquad \alpha = \arg\zeta = \frac{2\pi}{p}. \tag{2}$$

It will be convenient to treat the terms *root* and *zero* as synonymous when applied to a polynomial so that, by its roots, we mean the roots of the equation when the polynomial is set to 0. The *cyclotomic polynomial* for p is

$$\Phi_p(z) = z^{p-1} + z^{p-2} + \ldots + z + 1,$$

which comes from the factorisation $z^p - 1 = (z-1)\Phi_p(z)$, so that the roots of $\Phi_p(z)$ are precisely the complex roots of unity. The polynomial is irreducible over the rational field (see Article 341 in [1]), and it then follows from $\zeta^p = 1$, together with $1 + \zeta + \zeta^2 + \ldots + \zeta^{p-1} = 0$, that any polynomial in ζ with integer coefficients can be uniquely written as $A_1\zeta + A_2\zeta^2 + \ldots + A_{p-1}\zeta^{p-1}$, with A_j being integers; we shall make use of this fact in §5.

3. *Primitive roots and indices*

Consider the residue system modulo p under multiplication, with 0 being excluded. The system has a cyclic structure in the sense that there are *primitive roots* g with the property that g generates the system, so that it becomes $\{g, g^2, g^3, \ldots, g^{p-1}\}$. Thus, with g fixed, each $n \in 1, 2, 3, \ldots, p-1$ has an *index* $\nu(n)$ such that $g^{\nu(n)} \equiv n \pmod p$ and, as n runs over the system, $\nu(n)$ runs over the system in another order. The index $\nu(n)$ is also called the discrete logarithm of n with respect to g, because multiplication of residue classes modulo p becomes addition of the corresponding indices modulo $p-1$. For example, if $p = 17$ then $g = 2$ is not a primitive root, because $2^4 \equiv -1 \pmod{17}$, so that $2^{12} \equiv 2^4 \pmod{17}$. However, $g = 3$ is a primitive root modulo 17, which can be verified by the building (see §9 for some remarks) of the following table:

$\nu(n) =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$n =$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Regardless of the choice of g, the indices of 1 and $p-1$ are $p-1$ and $(p-1)/2$, respectively, because, by Fermat's little theorem, $g^{p-1} \equiv 1 \pmod p$ and hence $g^{(p-1)/2} \equiv -1 \equiv p-1 \pmod p$. Indices are particularly useful when we wish to identify sets of residues with certain algebraic properties; for example, quadratic residues modulo p are just numbers with an even index. It will be relevant to mention that if $p \equiv 1 \pmod 4$, so that $(p-1)/2$ is even, then -1 is quadratic residue, and that such residues R come in pairs $\{R, p-R\}$. Thus, from the table, we see that the quadratic residues (mod 17) are 1, 2, 4, 8, 9, 13, 15, 16.

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

4. *Gaussian periods and Gauss sums*

Fix a primitive root g for the prime p, and consider a factorisation of $p - 1$, say

$$p - 1 = ab.$$

With ζ defined by (1), the roots ζ^n of the cyclotomic polynomial $\Phi_p(z)$ can now be separated into a subsets according to the residue classes to which $\nu(n)$ belongs to the modulus a; since $\nu(n)$ takes every value in $1, 2, \ldots, p - 1$ exactly once, there are precisely b roots in each subset. The sum of such roots in a subset is called a Gaussian period, and the a periods are denoted by $\eta_0, \eta_1, \ldots, \eta_{a-1}$, so that

$$\eta_j = \sum_{\substack{1 \leqslant n < p \\ \nu(n) \equiv j \pmod a}} \zeta^n, \qquad j = 0, 1, \ldots, a - 1. \tag{3}$$

The appearance of $\nu(n)$ in the definition shows that these periods depend on the choice of the primitive root g, and if the value of g is changed then the periods may get permuted, except for η_0. Let us first see why η_0 depends only on p and a, and not on g.

The sum $\eta_0 = \sum \zeta^n$ is over n in $1 \leqslant n < p$ with $a \mid \nu(n)$. There are b terms in the sum so that, on writing $\nu(n) = am$, there are b values for m. If we just let m run over $1 \leqslant m < p$ then $\nu(n)$ runs over the same subset a times. Meanwhile, $h = g^m$ runs over the whole interval $1 \leqslant h < p$. Therefore, with $n = g^{\nu(n)} = g^{am} = h^a$, we find that

$$\eta_0 = \frac{1}{a} \sum_{1 \leqslant h < p} \zeta^{h^a}.$$

So, although we use a primitive root and the index to define η_0, its value is uniquely specified by p and a. In particular, if $a = 2$, then $h^a = h^2$ runs twice over the quadratic residues as h runs over $1 \leqslant h < p$; it follows that

$$\eta_0 = \sum \zeta^R, \qquad \eta_1 = \sum \zeta^N, \qquad a = 2, \tag{4}$$

where R and N run over the quadratic residues and non-residues (mod p), respectively; note that $\eta_0 + \eta_1 = -1$.

Our objective is to evaluate η_0, η_1, for which purpose we introduce the Gauss sum:

$$G = \sum_{1 \leqslant m < p} \left(\frac{m}{p}\right) \zeta^m, \tag{5}$$

where $\left(\frac{m}{p}\right)$ is the Legendre symbol, so that $\left(\frac{R}{p}\right) = 1$ and $\left(\frac{N}{p}\right) = -1$. Thus

$$G = \eta_0 - \eta_1,$$

and we have $2\eta_0 + 1 = G$ and $2\eta_1 + 1 = -G$, but we need to determine G.

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

Fermat primes $p > 3$ satisfy $p \equiv 1 \pmod 4$, a condition we shall assume henceforth; in particular $\left(\frac{-1}{p}\right) = 1$ in the present evaluation of G^2 by considering

$$G^2 = \sum_{1 \leqslant m_1 < p} \sum_{1 \leqslant m_2 < p} \left(\frac{m_1 m_2}{p}\right) \zeta^{m_1 + m_2}.$$

On changing the variable m_2 to n, where $m_2 \equiv m_1 n \pmod p$, so that $m_1 m_2 \equiv m_1^2 n \pmod p$ and hence $\left(\frac{m_1 m_2}{p}\right) = \left(\frac{m_1^2 n}{p}\right) = \left(\frac{n}{p}\right)$, we get

$$G^2 = \sum_{1 \leqslant m_1 < p} \sum_{1 \leqslant n < p} \left(\frac{n}{p}\right) \zeta^{m_1(n+1)} = \sum_{1 \leqslant n < p} \left(\frac{n}{p}\right) \sum_{1 \leqslant m_1 < p} \zeta^{m_1(n+1)}.$$

Now if $n = p - 1$ then $\zeta^{m_1(n+1)} = \zeta^{m_1 p} = 1$, and if $1 \leqslant n < p - 1$ then $\zeta^{m_1(n+1)} = \zeta^{\ell}$, and as m_1 runs over $1 \leqslant m_1 < p$, so does ℓ. Therefore

$$\sum_{1 \leqslant m_1 < p} \zeta^{m_1(n+1)} = \begin{cases} p - 1 & \text{if } n = p - 1, \\ -1 & \text{if } 1 \leqslant n < -1, \end{cases}$$

and we arrive at

$$G^2 = \left(\frac{-1}{p}\right)(p - 1) - \sum_{1 \leqslant n < p} \left(\frac{n}{p}\right) + 1 = p, \qquad p \equiv 1 \pmod 4,$$

so that $G = \pm\sqrt{p}$, when $p \equiv 1 \pmod 4$.

However, it took Gauss four years, during which time he made many and varied unsuccessful attempts, to determine the correct sign for G, that is

$$G = \sqrt{p}, \qquad \text{if } p \equiv 1 \pmod 4.$$

It is not surprising then that, although there are many different methods to determine G, none of them can be described as straightforward. In §8 we give a sketch of probably the simplest solution by T. Estermann [2].

For a given $p \equiv 1 \pmod 4$ of modest size it is, of course, possible to verify that $\eta_0 > 0$, which implies $G = \sqrt{p}$. Take, for example, $p = 17$, so that

$$\begin{aligned} \eta_0 &= \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} \\ &= 2\left(\cos\alpha + \cos 2\alpha + \cos 4\alpha + \cos 8\alpha\right), \qquad \alpha = \frac{2\pi}{17}. \end{aligned}$$

From $0 < \alpha < 2\alpha < \frac{\pi}{4} < 4\alpha < \frac{\pi}{2} < 8\alpha < \pi$, we have

$$1 > \cos\alpha > \cos 2\alpha > \frac{1}{\sqrt{2}} > \cos 4\alpha > 0 > \cos 8\alpha > -1,$$

so that $\eta_0 > 2\left(\sqrt{2} - 1\right) > 0$.

Anyway, with $G = \sqrt{p}$, the two periods for $a = 2$ are given by

$$\eta_0 = \frac{-1 + \sqrt{p}}{2}, \qquad \eta_1 = \frac{-1 - \sqrt{p}}{2}, \qquad p \equiv 1 \pmod 4. \tag{6}$$

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

The case $p = 3$ is excluded from the discussion here, but the construction of the equilateral triangle is easy. For $p = 5$, we have $\eta_0 = \zeta + \zeta^4 = 2\cos\alpha$, and hence $4\cos 2\pi/5 = \sqrt{5} - 1$, so that the regular pentagon can be constructed by Euclidean means.

5. *Gaussian periods for a Fermat prime*

For a Fermat prime $p = 2^k + 1 > 5$, the proper divisors a of $p - 1 = 2^k$ are $a = 2^r$, with $1 \leqslant r < k$. For $a = 2$, we have (6) for the periods.

With the primitive root g chosen, the periods for $a = 2^r$ can now be evaluated successively—the results are given as solutions to quadratic equations, with the results for $a = 2^{r-1}$ as coefficients. We need the following lemma.

Lemma: Let $f(\zeta) = A_1\zeta + A_2\zeta^2 + \ldots + A_{p-1}\zeta^{p-1}$, with integers A_j. Suppose that $f(\zeta^m) = f(\zeta)$ whenever m is a quadratic residue. Then $f(\zeta) = A_1\eta_0 + A_g\eta_1$.

Proof: Let m be a quadratic residue, and j run over the reduced residue system (mod p), so that jm also runs over the system. It then follows from $f(\zeta) = f(\zeta^m)$ that

$$A_m\zeta^m + \sum_{j \neq m} A_j\zeta^j = A_1\zeta^m + \sum_{j \neq 1} A_j\zeta^{jm}.$$

If m is a quadratic non-residue, then let $m\overline{m} \equiv 1 \pmod p$, and set $n \equiv g\overline{m} \pmod p$, so that $mn \equiv g \pmod p$, and jn runs over the system as j does. Since n is now a quadratic residue we have $f(\zeta) = f(\zeta^n)$, so that

$$A_g\zeta^g + \sum_{j \neq q} A_j\zeta^j = A_m\zeta^g + \sum_{j \neq m} A_j\zeta^{jn}.$$

The unique representation of $f(\zeta)$ implies that $A_m = A_1$, or A_g, depending on whether m is a quadratic residue, or not. The required result follows from (4).

The lemma still applies when the coefficients A_m are themselves quadratics in a variable x with integer coefficients, because the equation is then valid for every integer value of x, and is therefore valid identically in x. Now let $a = 2^2$, and use η' to denote the four periods. Let m be a quadratic residue, and suppose that we replace ζ by ζ^m in the definition for η'_1, η'_3 in (3). We find that, depending on $\nu(m) \equiv 0$ or $2 \pmod 4$, the effect of the replacement is either to leave η'_1, η'_3 unchanged, or to interchange them. Thus, as a polynomial in ζ, the expression $(x - \eta'_1)(x - \eta'_3)$ is unaltered under such a replacement. We may therefore apply the lemma to deliver

$$(x - \eta'_1)(x - \eta'_3) = A(x)\eta_0 + b(x)\eta_1,$$

where $A(x)$ and $B(x)$ are quadratics with integer coefficients, so that η'_1, η'_3

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

are roots of a quadratic with η_0, η_1 as coefficients, and the same applies to the pair η_0', η_2'. Therefore each of the four periods η' can be expressed in two layers of square-root signs involving only rational numbers, and they themselves are suitable numbers to be coefficients of quadratic equations in the next step.

For $a = 2^3$, each $\eta^{(3)}$ is a sum of 2^{k-3} roots; they form four pairs:

$$\eta_1^{(3)}, \eta_5^{(3)}; \qquad \eta_2^{(3)}, \eta_6^{(3)}; \qquad \eta_3^{(3)}, \eta_7^{(3)}; \qquad \eta_4^{(3)}, \eta_0^{(3)}.$$

This time $(x - \eta_1^{(3)})(x - \eta_5^{(3)})$ is unaltered if ζ is replaced by ζ^m, provided that $4 \mid \nu(m)$. By considering $\nu(m) \equiv 0, 1, 2, 3 \pmod 4$, the argument used in the proof of the lemma can be extended to show that

$$(x - \eta_1^{(3)})(x - \eta_5^{(3)}) = A_0(x)\eta_0' + A_1(x)\eta_1' + A_2(x)\eta_2' + A_3(x)\eta_3',$$

where $A_j(x)$ are quadratics with integer coefficients, so that $\eta_1^{(3)}$, $\eta_5^{(3)}$ are solutions to a quadratic equation with coefficients $\eta^{(2)} = \eta'$, and can thus be expressed in another layer of square-root signs involving only rational numbers. The same applies to each of the remaining of periods $\eta^{(3)}$.

The process can be continued until the final step when there are 2^{k-1} periods: $\eta_{m-1}^{(k-1)} = \zeta^m + \zeta^{p-m}$ for $1 \leqslant m \leqslant 2^{k-1}$. In particular, $\eta_0^{(k-1)} = \zeta + \zeta^{-1} = 2\cos\alpha$ in (2) can be expressed in $k-1$ nested square root signs involving only rational numbers, so that the regular p-gon can be constructed by Euclidean means.

To complete the argument we still have to show that all the periods η are real numbers, so that all the roots of the quadratics concerned are real numbers. Recall that the index of $p-1$ is $(p-1)/2$, that is $\nu(-1) = 2^{k-1}$, so that $\nu(-n) \equiv \nu(n) \pmod{2^r}$, for $1 \leqslant r < k$. Consequently the summation condition for the sum η in (3) is unaltered if n is replaced by $-n$. Since $\zeta^n\zeta^{-n} = 1$, it follows that $\eta = \overline{\eta}$ is indeed a real number.

6. *The case* $p = 17$

For $p = 17$, we have $\zeta = e^{i\alpha}$, $\alpha = 2\pi/17$, and we take $g = 3$, so that $\nu(n)$ is given in the table in §3. The proper divisors of $p - 1 = 16$ are $a = 2, 4, 8$, and we already know that η_0, η_1 are solutions of $x^2 + x + 4 = 0$ when $a = 2$.

For $a = 4$, the periods η' from (3) are sums of four ζ^n:

$$\eta_0' = \zeta + \zeta^4 + \zeta^{13} + \zeta^{16}, \qquad \eta_1' = \zeta^3 + \zeta^5 + \zeta^{12} + \zeta^{14},$$
$$\eta_2' = \zeta^2 + \zeta^8 + \zeta^9 + \zeta^{15}, \qquad \eta_3' = \zeta^6 + \zeta^7 + \zeta^{10} + \zeta^{11};$$

and we note that $\eta_0' + \eta_2' = \eta_0$, $\eta_1' + \eta_3' = \eta_1$, and $\eta_0'\eta_2' = \eta_1'\eta_3' = -1$. Therefore η_0', η_2' and η_1', η_3' are the roots of the quadratic equations $x^2 - \eta_0 x - 1 = 0$ and $x^2 - \eta_1 x - 1 = 0$, respectively, so that

$$\eta_0', \eta_2' = \frac{\eta_0 \pm \sqrt{8 - \eta_0}}{2}, \qquad \eta_1', \eta_3' = \frac{\eta_1 \pm \sqrt{8 - \eta_1}}{2}; \tag{7}$$

trigonometric inequalities show that $\eta_0' > \eta_2'$ and $\eta_1' > \eta_3'$.

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

Finally, for $a = 8$, each period in (3) is the sum of two ζ^n:

$$\eta_0^{(3)} = \zeta + \zeta^{16}, \qquad \eta_1^{(3)} = \zeta^3 + \zeta^{14}, \qquad \eta_2^{(3)} = \zeta^8 + \zeta^9, \qquad \eta_3^{(3)} = \zeta^7 + \zeta^{10},$$

$$\eta_4^{(3)} = \zeta^4 + \zeta^{13}, \qquad \eta_5^{(3)} = \zeta^5 + \zeta^{12}, \qquad \eta_6^{(3)} = \zeta^2 + \zeta^{17}, \qquad \eta_7^{(3)} = \zeta^6 + \zeta^{11}.$$

Note that

$$\eta_0^{(3)} + \eta_4^{(3)} = \eta_0', \qquad \eta_1^{(3)} + \eta_5^{(3)} = \eta_1', \qquad \eta_2^{(3)} + \eta_6^{(3)} = \eta_2', \qquad \eta_3^{(3)} + \eta_7^{(3)} = \eta_3',$$

and we find that $\eta_0^{(3)}\eta_4^{(3)} = \eta_1'$, so that $\eta_0^{(3)}$ and $\eta_4^{(3)}$ are the roots of the quadratic equation $x^2 - \eta_0' x + \eta_1' = 0$, with $\eta_0^{(3)} > \eta_4^{(3)}$. It follows that $\eta_0^{(3)} = 2\cos\alpha$ can be expressed in terms of rational numbers with the application of three nested square root operations. More specifically, we have

$$4\cos\alpha = \eta_0' + \sqrt{(\eta_0')^2 - 4\eta_1'},$$

and, by (7) together with $\eta_0,\ \eta_1 = \left(1 \pm \sqrt{17}\right)/2$, we find that

$$16\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} +$$

$$+ \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2\left(1 - \sqrt{17}\right)\sqrt{34 - 2\sqrt{17}}}.$$

7. *The condition for q*

Suppose that the construction is possible for $q = n_1$ and for $q = n_2$, where n_1 and n_2 are coprime, so that the angles $\alpha_1 = 2\pi/n_1$ and $\alpha_2 = 2\pi/n_2$ can be delivered. There are integers r_1, r_2 such that $r_1 n_1 + r_2 n_2 = 1$, so that

$$\frac{r_1}{n_2} + \frac{r_2}{n_1} = \frac{1}{n_1 n_2},$$

and hence the angle $2\pi/n_1 n_2$ is just the linear combination $r_1\alpha_2 + r_2\alpha_1$, which shows that the construction is possible also for $q = n_1 n_2$. For example, if $n_1 = 5$ and $n_2 = 17$, we take $r_1 = 7, r_2 = -2$, so that $q = 85$ is admissible. The bisection of an angle is easy, so that a sufficient condition for the possible construction of a regular q-gon is that $q = 2^a P$, where P is a (possibly empty) product of distinct Fermat primes. Euler's totient function $\phi(n)$ counts the numbers $m \leqslant n$ that are coprime with n, so that another way of stating the condition for q is that $\phi(q) = 2^k$ for some $k \geqslant 1$.

Gauss claimed that the construction is impossible for other values of q, so that the sufficient condition is also necessary. He did not attach much importance to the claim, saying only that, for other q, an equation with degree not being a power of 2 is unavoidable, adding that his reason for including the claim at all was to prevent people from wasting their effort trying to do the impossible.

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

The cyclotomic polynomial $\Phi_q(z)$ for q is the irreducible polynomial with integer coefficients which is a divisor of $z^q - 1$ and is not a divisor of $z^k - 1$ for any $k < q$. Thus, for $q = 9$, with $\zeta = e^{2\pi/9}$, we find that $1, \zeta^3, \zeta^6$ are also third roots of unity, and we have the factorisation $z^9 - 1 = (z^3 - 1)(z^6 + z^3 + 1)$. The cyclotomic polynomial for 9 is given by

$$\Phi_9(z) = (z-\zeta)(z-\zeta^2)(z-\zeta^4)(z-\zeta^5)(z-\zeta^7)(z-\zeta^8) = z^6 + z^3 + 1;$$

the corresponding 'unavoidable' equation has degree $\phi(9) = 6 = 2 \times 3$, so that the construction of a 9-gon is impossible. Incidentally, as a corollary, the angle $2\pi/3$ cannot be trisected by Euclidean means.

Perhaps, back then, such a negative result would be considered more in the area of metamathematics rather than mathematics itself. The interested reader can find out more on the history of the impossibility result in [3], in which the proof of Gauss' claim is attributed mainly to P. L. Wantzel.

8. *Estermann's evaluation of the Gauss sum*

The Gauss sum in (5) satisfies

$$G = \eta_0 - \eta_1 = \sum \zeta^R - \sum \zeta^N = 1 + 2\sum \zeta^R,$$

and the observation that, as m runs over $1 \leqslant m < p$, m^2 runs twice over the quadratic residues, shows that

$$G = \sum_{m=0}^{p-1} e^{2\pi i m^2/p};$$

written in this form, G is sometimes called the quadratic Gauss sum.

Let $p \equiv 1 \pmod 4$, so that $G = \pm\sqrt{p}$ by §4, and we need to show that $G = \sqrt{p}$. Various sophisticated methods deliver G directly, while the more elementary ones show that $G > -\sqrt{p}$, which implies the desired result.

As θ varies in $0 \leqslant \theta < 2p\pi$, the point $e^{i\theta}$ goes round the unit circle p times. Thus, for $0 \leqslant m < p$, the p points $e^{2\pi i m^2/p}$ are dotted along the circle accordingly. With $|G| = \sqrt{p}$, there has to be much cancellation in the formation of the quadratic Gauss sum. However, for $0 \leqslant m < \sqrt{p}$, the $[\sqrt{p}] + 1$ points $e^{2\pi i m^2/p}$ take the 'first round' of the circle, and the cancellation effect has hardly begun. To adapt such an idea effectively, Estermann [2] first applied the identity

$$\sum_{m=1}^{\frac{1}{2}(p-1)} \left(f(m) + f\left(\tfrac{p}{2} - m\right)\right) = \sum_{m=1}^{p-1} f\left(\tfrac{m}{2}\right)$$

with $f(m) = e^{2\pi i m^2/p}$, so that $f\left(\frac{p}{2} - m\right) = if(m)$, in order to arrive at

$$\tfrac{1}{2}(1+i)(G-1) = \sum_{m=1}^{p-1} e^{\pi i m^2/2p}.$$

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

Considering the sum here as $A + B$, where A and B are sums corresponding to $1 \leqslant m < \sqrt{p}$ and $\sqrt{p} < m < p$, we then have $G - 1 = (1 - i)(A + B)$. Now, for $0 \leqslant \theta \leqslant \pi/2$, the real part of $(1 - i)e^{i\theta}$ is $\cos\theta + \sin\theta \geqslant 1$ (the triangle inequality!) so that the real part of $(1 - i)A$ exceeds $\sqrt{p} - 1$. Estermann then applied partial summation to the sum B in an ingenious way to show that $|B| < \sqrt{p}$, so that

$$G - 1 = \mathrm{Re}(1 - i)A + \mathrm{Re}(1 - i)B > \sqrt{p} - 1 - |1 - i||B|$$
$$> \sqrt{p} - 1 - \sqrt{2}\sqrt{p},$$

and thus $G > \sqrt{p} - \sqrt{2}\sqrt{p} > -\sqrt{p}$.

9. *Computing the discrete logarithm*

Although it is not relevant to our construction problem here, an alert reader may have noticed the following: For a given prime p and a primitive root g, in the construction of a table for the discrete logarithm $\nu(n)$ we start by taking $m = 1, 2, \ldots, p - 1$ and compute $n \equiv g^m \pmod{p}$ successively, and then set $\nu(n) = m$. The task of starting with $n = 1, 2, \ldots, p - 1$ and trying to compute $\nu(n)$ directly is onerous, especially if p is no longer small.

Thus, for computation, the mapping $\nu(n) \to n$ is easy, but the inverse mapping $n \to \nu(n)$ is difficult; in other words, whereas it is easy to exponentiate in modular arithmetic, the computation of the discrete logarithm is difficult. The phenomenon is useful in computational number theory, particularly for the construction of cryptographic schemes. Thus $\nu(n) \to n$ is a *one-way-function*, in the sense that it is difficult to recover $\nu(n)$ from an input n, and indeed the discrete logarithm is widely used in key-exchange protocols, for example.

10. *A wish unfulfilled, half a dream came true*

Gauss was in his teens when (on 30 March 1796) he solved the problem of the constructing of the regular heptadecagon. So proud of the achievement was he that apparently his unfulfilled wish was to have, instead of an epitaph, a regular heptadecagon inscribed on his tombstone.

The young Gauss was also interested in what is now known as his dream: efficient primality tests and factorisation algorithms. Thus, in Article 329 [1] he wrote passionately: 'The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. ... [T]he dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.'

Almost exactly two centuries later, the first part of his dream came true when three Indian computer scientists – Manindra Agrawal, Neeraj Kayal and Nitin Saxena – constructed a deterministic polynomial-time primality

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press

test (AKS test), a much sought-after goal of researchers in the algorithmic number theory world. Moreover, cyclotomy, Gaussian periods and Gauss sums are often at the centre of various algorithms for primality tests and factorisation, including innovations associated with the efficient AKS test (see [4]).

References

1. Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, translated by Arthur A. Clarke, Yale University Press (1966).
2. T. Estermann, On the sign of the Gaussian sum, *J. London Math. Soc.* **20** (1945) pp. 66-67.
3. Jesper Lützen, Why was Wantzel overlooked for a century? The changing importance of an impossibility result, *Historia Mathematica*, **36** (2009) pp. 374-394.
4. Andrew Granville, It is easy to determine whether a given integer is prime, *Bull. Amer. Math. Soc.* **42** (2005) pp. 3-38.

10.1017/mag.2016.66

PETER SHIU
353 Fulwood Road, Sheffield S10 3BQ
e-mail: *p.shiu@yahoo.co.uk*

https://doi.org/10.1017/mag.2016.66 Published online by Cambridge University Press