THE MATHEMATICS OF GAUSS

DAVID SAVITT

Introduction

Carl Friedrich Gauss was born on April 30, 1777, in Brunswick, Germany, the son of Gebhard Dietrich Gauss, a bricklayer, and Dorothea Emerenzia Gauss. Carl Friedrich's mathematical talents showed themselves early: when he was three years old, he found an error in his father's payroll calculations. At the age of seven, he entered St. Katharine's Volksschule, where he was taught by J.G. Büttner. The most famous incident from Gauss's youth took place when Büttner assigned to his class the task of summing the numbers from 1 to 100. While the other pupils busied themselves with the task, Gauss almost immediately wrote an answer on his tablet and handed it in. Büttner, at first skeptical, found that Gauss's solution was completely correct. Gauss explained himself: he had noticed that $1 + 100 = 101$, $2 + 99 = 101$, and so on, so that $1 + \cdots + 100 = 50 \cdot 101 = 5050$.

Gauss quickly outpaced what he could be taught at the Katharineum, and began to be tutored privately in mathematics by a neighbor, Johann Bartels, who himself would later become a professor of mathematics. At the age of 14, Gauss came to the attention of the Duke of Brunswick: the Duchess saw Gauss reading in the palace yard one day, and was much impressed that Gauss understood what he was reading. When Gauss entered the Collegium Carolinum in 1792, the Duke paid his tuition.

At the Collegium, Gauss studied the works of Newton, Euler, and Lagrange. His investigations on the distribution of primes in 1792 or 1793 give an early indication of his interest in number theory. He also developed his strong love of languages: he "completed his knowledge of the ancient languages and learned the modern languages" ([Dun04],p. 18).

In 1795, Gauss left Brunswick for Göttingen. He continued to be supplied tuition, a stipend, and a free apartment by his patron, the Duke of Brunswick.

1. The 17-gon

1.1. **Geometry and algebra.** Gauss's first publication appeared in *Allgemeine Literaturzeitung* in April, 1796: ([Dun04], p.28)

> It is known to every beginner in geometry that various regular polygons, viz., the triangle, tetragon, pentagon, 15-gon, and those which arise by the continued doubling of the number of sides of one of them, are geometrically constructible.
>
> One was already that far in the time of Euclid, and, it seems, it has generally been said since then that the field of elementary geometry extends no farther: at least I know of no successful attempt to extend its limits on this side.

> So much the more, methinks, does the discovery deserve attention... that besides those regular polygons a number of others, e.g., the 17-gon, allow of a geometrical construction. This discovery is really only a special supplement to a theory of greater inclusiveness, not yet completed, and is to be presented to the public as soon as it has received its completion.
>
> *Carl Friedrich Gauss*
>
> *Student of Mathematics at Göttingen*

To construct a regular 15-gon with straightedge and compass, first construct a regular pentagon; draw the circle in which this pentagon is inscribed, and inscribe five equilateral triangles inside that circle, each sharing one vertex with the pentagon. The fifteen vertices of these triangles will form the vertices of a regular 15-gon. To construct a regular $2n$-gon from a regular n-gon, simply bisect each of the n central angles of the n-gon. Thus, starting from the triangle, square, and pentagon it is possible to construct regular polygons with 6, 12, 24, etc. sides, with 4, 8, 16 etc. sides, with 5, 10, 20 etc. sides, and even with 15, 30, 60 etc. sides. To this list, which had remained unchanged for nearly 2000 years, Gauss not only added the 17-gon, but gave a nearly-complete solution to the question: for which values of n can the regular n-gon be constructed?

Though the result was announced in 1796, the details appeared in print in 1801, in Section VII ("Equations Defining Sections of a Circle") in Gauss's masterwork *Disquisitiones Arithmeticae* [Gau66]. As we shall explain below, the problem may be translated from geometry into algebra; Gauss's crucial insight, noted on March 30, 1796, in the opening entry of his scientific diary, allowed him to resolve the related algebraic problem:

> The theory of the division of a circle or of a regular polygon treated in Section VII *of itself* does not pertain to Arithmetic but the *principles* involved depend uniquely on Higher Arithmetic. This will perhaps prove unexpected to geometers, but I hope they will be equally pleased with the new results that derive from this treatment. *(*[Gau66]*, Author's Preface)*

According to H.S.M. Coxeter [Cox77], the idea that a complex number $x + iy$ may be viewed as the point (x, y) in the plane should be attributed to the Danish mathematician Caspar Wessel (1745-1818). In this manner, one may study geometry of the plane by studying the arithmetic of complex numbers. View the point (x, y) in polar coordinates: suppose that the point (x, y) has distance r from the origin, and that the line from the origin to (x, y) makes an angle θ from the positive real axis. Then we know, essentially from the definition of the trigonometric functions, that $x = r\cos\theta$ and $y = r\sin\theta$.

From this geometric interpretation, we see that

$$x + iy = r\cos\theta + ir\sin\theta = r(\cos\theta + i\sin\theta)\,,$$

or, writing $\operatorname{cis}\theta = \cos\theta + i\sin\theta$, that $x + iy = r\operatorname{cis}\theta$. This reformulation gives particular insight into the multiplication of complex numbers. If $x + iy = r_1\operatorname{cis}\theta_1$ and $u + iv = r_2\operatorname{cis}\theta_2$, then we can compute the product using the angle-addition

formulas for cos and sin:

$$\begin{aligned}(x+iy)(u+iv) &= (xu-yv)+i(xv+yu)\\ &= r_1r_2((\cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2)+i(\cos\theta_1\sin\theta_2+\cos\theta_2\sin\theta_1))\\ &= r_1r_2(\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2))\\ &= r_1r_2\operatorname{cis}(\theta_1+\theta_2)\,.\end{aligned}$$

That is, when we multiply two complex numbers, the distances from the origin multiply, and the angles add.

Definition 1.1. An nth root of unity is any complex number z such that $z^n = 1$. A primitive nth root of unity is an nth root of unity that is not a kth root of unity for any positive integer $k < n$.

For example, 1 and -1 are both square roots of unity, but only -1 is a primitive square root of unity.

Exercise 1.2. Verify that $\frac{-1\pm\sqrt{-3}}{2}$ are primitive 3rd roots of unity, and that $\pm i$ are the primitive 4th roots of unity. What are the primitive 6th and 8th roots of unity?

Set $\zeta_n = \operatorname{cis}\frac{2\pi}{n}$. Our formula for the multiplication of complex numbers shows immediately that

$$\zeta_n^k = \operatorname{cis}\frac{2\pi k}{n}\,,$$

and in particular that $\zeta_n^n = \operatorname{cis} 2\pi = \cos 2\pi + i\sin 2\pi = 1$. Therefore ζ_n is an nth root of unity.

Exercise 1.3. Prove the formulas

$$\cos\frac{2\pi k}{n} = \frac{1}{2}\left(\zeta_n^k + \zeta_n^{-k}\right)$$

and

$$\sin\frac{2\pi k}{n} = \frac{1}{2i}\left(\zeta_n^k - \zeta_n^{-k}\right)\,.$$

Exercise 1.4. Show that ζ_n is a primitive nth root of unity.

Exercise 1.5. Show that every nth root of unity is of the form ζ_n^k for some k, and moreover that ζ_n^k is a primitive nth root of unity if and only if k is relatively prime to n.

Suppose we have a regular n-gon inscribed in a circle of radius 1 centered at the origin, and with one vertex at the point $(1,0)$. Then the vertices of this n-gon will be at exactly the points corresponding to the complex numbers $\operatorname{cis}\frac{2\pi k}{n}$, that is, to the nth roots of unity. For example, if a square centered at the origin has one vertex at $(1,0)$, then the other vertices will be at $(0,1)$, $(-1,0)$, and $(0,-1)$, and these four vertices correspond to $1, i, -1, -i$ respectively. Therefore, the problem of constructing a regular n-gon is the same as the problem: given points $(0,0)$ and $(1,0)$, construct the number $\zeta_n = \operatorname{cis}\frac{2\pi}{n}$; and any resolution of this problem should make use of the algebraic fact that ζ_n is a root of the polynomial $z^n - 1 = 0$. It was already known (from work of Cotes, of DeMoivre, and of Euler; [Dun04], p. 29) that construction of the n-gon depends on solving the equation $z^n - 1 = 0$; Gauss was the first to succeed at the latter.

Using a straightedge and compass, given a segment of length defined to be 1, it is possible to add, subtract, multiply, and divide known lengths, and it is also possible to extract square roots. We can therefore use a straightedge and compass to solve linear and quadratic equations. (In fact, the reader should try to convince herself or himself that these are essentially the only equations one can solve, when our only operations are intersecting two known lines, two known circles, or a known line and a known circle.) On the other hand, at first glance, it appears that constructing ζ_{17} should involve the solution of an equation of degree 17, since we are trying to find a root of the equation

$$z^{17} - 1 = 0\,.$$

Not so fast! In fact, the polynomial $z^{17} - 1$ has an obvious root, namely 1; and therefore the polynomial has the factor $z - 1$. It follows that ζ_{17} is a root of the polynomial

$$\Phi_{17}(z) = \frac{z^{17} - 1}{z - 1} = z^{16} + z^{15} + \cdots + z + 1\,.$$

Exercise 1.6. If p is a prime number, set $\Phi_p(z) = \frac{z^p-1}{z-1} = z^{p-1} + \cdots + z + 1$. Verify that the roots of $\Phi_p(z) = 0$ are precisely the primitive pth roots of unity.

So we still have some hope: ζ_{17} is actually a root of a polynomial of degree 16, and it is conceivable that a solution of an equation of degree 16 can be found by solving four successive equations of degree 2, which can then be solved by straightedge and compass.

1.2. Φ_p **is irreducible.** A priori, it is possible that ζ_{17} might yet be the root of a polynomial of degree smaller than 16: perhaps there is another, less obvious factor of $\Phi_{17}(z)$ that we have not found. In actuality, no such factor exists. More generally, we will now give Gauss's proof that $\Phi_p(z)$ is an irreducible polynomial, that is, that $\Phi_p(z)$ cannot be factored into two polynomials of lower degree with rational coefficients. The proof may be found in article 341 of [Gau66]. We need the following preliminaries.

Definition 1.7. A polynomial $f(z) = a_n z^n + \cdots + a_0$ with integer coefficients is said to be *monic* if $a_n = 1$.

Lemma 1.8 (Gauss's Lemma)**.** *If $f(z)$ is a monic polynomial with integer coefficients and $f(z)$ can be factored into two polynomials with rational coefficients, then it may be factored into two monic polynomials of lower degree with integer coefficients.*

Gauss proves this important lemma in article 42 in [Gau66].

Exercise 1.9. Prove Gauss's Lemma.

The following lemma is article 338 in [Gau66].

Lemma 1.10. *If the polynomial $f(z) = (z - r_1) \cdots (z - r_d)$ with roots $r_1, \ldots, r_d$ has rational coefficients, then the polynomial $f^{(k)}(z) = (z - r_1^k) \cdots (z - r_d^k)$ also has rational coefficients.*

Exercise 1.11. Prove Lemma 1.10. Hint: If $d = 2$, then $r_1^2 + r_2^2 = (r_1 + r_2)^2 - 2(r_1 r_2)$ and $r_1^2 r_2^2 = (r_1 r_2)^2$ are certainly both rational. The proof for larger d is more complicated, but not more difficult; use Newton's results on symmetric functions.

Lemma 1.12. *If $f(z_1, \ldots, z_d)$ is a polynomial with integer coefficients and if $c_1, \ldots, c_d$ are integers, then the sum*

$$S = \sum_{k=0}^{p-1} f(\zeta_p^{kc_1}, \ldots, \zeta_p^{kc_d})$$

is an integer which is divisible by p.

Proof. Set $g(z) = f(z^{c_1}, \ldots, z^{c_d})$, so that

$$S = \sum_{k=0}^{p-1} g(\zeta_p^k)\,.$$

Using polynomial division, write

$$g(z) = (z^p - 1)q(z) + h(z)$$

with the degree of $h(z)$ strictly less than p; then $g(\zeta_p^k) = h(\zeta_p^k)$, so if $h(z) = h_{p-1}z^{p-1} + \cdots + h_0$ then

$$g(\zeta_p^k) = h_{p-1}\zeta_p^{k(p-1)} + \cdots + h_1\zeta_p^k + h_0\,.$$

Since

$$\sum_{k=0}^{p-1} \zeta_p^{ki} = \begin{cases} 0 & \text{if } 1 < i \leq p-1 \\ p & \text{if } i = 0 \end{cases} \tag{1.13}$$

we find $S = ph_0$, as desired. □

Exercise 1.14. Verify equation (1.13).

Finally, we are ready to give Gauss's proof of:

Theorem 1.15 ([Gau66], art. 341)**.** *$\Phi_p(z)$ is irreducible.*

Suppose, for the purposes of contradiction, that $\Phi_p(z)$ is divisible by a polynomial $f(z)$ with rational coefficients and degree $d < p-1$, and suppose that the roots of $f(z)$ are $\zeta_p^{c_1}, \ldots, \zeta_p^{c_d}$. Let $f^{(k)}(z)$ be the polynomial whose roots are $\zeta_p^{kc_1}, \ldots, \zeta_p^{kc_d}$.

Exercise 1.16. Show that $\prod_{k=1}^{p-1} f^{(k)}(z) = \Phi_p(z)^d$. (Hint: count the number of times each primitive pth root of unity occurs as a root of the product on the left-hand side.)

Exercise 1.17. By Lemma 1.10, each $f^{(k)}(z)$ has rational coefficients. Use Gauss's Lemma (Lemma 1.8) and the preceding exercise to conclude that each $f^{(k)}(z)$ has integer coefficients. In particular, $f^{(k)}(1)$ is an integer for all k.

Exercise 1.18. Use Lemma 1.12 and the fact that $f^{(0)}(1) = 0$ to show that $p \,|\, \sum_{k=1}^{p-1} f^{(k)}(1)$. Also verify that $\prod_{k=1}^{p-1} f^{(g)}(1) = p^d$.

Exercise 1.19. Finally, prove that $f^{(k)}(1)$ is positive for all k. (Hint: how many real roots does $f^{(k)}$ have?) It follows that $f^{(k)}(1)$ is either 1 or a multiple of p; use the results of Exercise 1.18 to deduce a contradiction to the hypothesis that $d < p-1$. Conclude that $\Phi_p(z)$ is irreducible.

Finally, we note that this is not at all equivalent to the more standard proof that Φ_p is irreducible using Eisenstein's irreducibility criterion:

Theorem 1.20 (Eisenstein's Criterion)**.** *Let $f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$ be a monic polynomial with integer coefficients. Suppose that all the coefficients $a_0, \ldots, a_{n-1}$ are divisible by p and the constant coefficient a_0 is not divisible by p^2. Then $f(z)$ is irreducible.*

A polynomial satisfying the hypotheses of this theorem is said to be "Eisenstein at p".

Exercise 1.21. Fill in the details in the following sketch of a proof of Eisenstein's criterion: suppose $f(z)$ factors as $f(z) = g(z)h(z)$, with $g(z), h(z)$ monic of degree $d, n-d$ respectively. Show that $g(z) \equiv z^d \pmod{p}$ and $h(z) \equiv z^{n-d} \pmod{p}$, so that $g(0)$ and $h(0)$ are both divisible by p. Deduce a contradiction.

Exercise 1.22. Show that the polynomial $\Phi_p(z+1)$ is Eisenstein at p, so that it is irreducible. Conclude that $\Phi_p(z)$ is also irreducible.

Eisenstein's criterion is essentially a p-adic irreducibility criterion. On the other hand, Gauss's proof makes definite use of properties of the integers.

1.3. **The algebraic construction.** At the heart of Gauss's deduction of the constructibility of the 17-gon is the following observation, which we will study more systematically in Section 4.1. If we begin with ζ_{17} and repeatedly square this number, we get a cycle of length 8:

$$\zeta_{17} \rightsquigarrow \zeta_{17}^2 \rightsquigarrow \zeta_{17}^4 \rightsquigarrow \zeta_{17}^8 \rightsquigarrow \zeta_{17}^{16} \rightsquigarrow \zeta_{17}^{15} \rightsquigarrow \zeta_{17}^{13} \rightsquigarrow \zeta_{17}^9 \rightsquigarrow \zeta_{17} \cdots$$

where we use, for example, that $\zeta_{17}^{32} = \zeta_{17}^{15}$. Choosing any primitive 17th root of unity not in the above cycle and repeatedly squaring yields another cycle containing all of the remaining primitive 17th roots of unity:

$$\zeta_{17}^3 \rightsquigarrow \zeta_{17}^6 \rightsquigarrow \zeta_{17}^{12} \rightsquigarrow \zeta_{17}^7 \rightsquigarrow \zeta_{17}^{14} \rightsquigarrow \zeta_{17}^{11} \rightsquigarrow \zeta_{17}^5 \rightsquigarrow \zeta_{17}^{10} \rightsquigarrow \zeta_{17}^3 \rightsquigarrow \cdots .$$

Define

$$(8, \zeta_{17}) = \zeta_{17} + \zeta_{17}^2 + \zeta_{17}^4 + \zeta_{17}^8 + \zeta_{17}^{16} + \zeta_{17}^{15} + \zeta_{17}^{13} + \zeta_{17}^9$$

and

$$(8, \zeta_{17}^3) = \zeta_{17}^3 + \zeta_{17}^6 + \zeta_{17}^{12} + \zeta_{17}^7 + \zeta_{17}^{14} + \zeta_{17}^{11} + \zeta_{17}^5 + \zeta_{17}^{10},$$

the sums of the roots contained in the two cycles; we will call these two numbers the *periods of length* 8 for ζ_{17}.

Then

$$(8, \zeta_{17}) + (8, \zeta_{17}^3) = \zeta_{17} + \zeta_{17}^2 + \cdots + \zeta_{17}^{16} = -1$$

since $\zeta_{17}^{16} + \cdots + \zeta_{17} + 1 = 0$. We can also evaluate the product $(8, \zeta_{17}) \cdot (8, \zeta_{17}^3)$. Since the two periods each are defined as a sum of eight terms, the product contains 64 terms, and one can see by direct (if exhausting) calculation that the product is simply

$$4\zeta_{17} + 4\zeta_{17}^2 + \cdots + 4\zeta_{17}^{16} = -4.$$

On the other hand, one can also see this by "pure thought".

Exercise 1.23. Verify that each of the primitive 17th roots of unity appearing in $(8, \zeta_{17})$ are of the form ζ_{17}^k where k is a square (mod 17), and that each of the primitive 17th roots of unity appearing in $(8, \zeta_{17})$ are of the form ζ_{17}^k where k is a non-square (mod 17). Use this, together with the fact that -1 is a square (mod 17), to check that none of the 64 terms in the product $(8, \zeta_{17}) \cdot (8, \zeta_{17}^3)$ are equal to 1. to Conclude that

$$(8, \zeta_{17}) \cdot (8, \zeta_{17}^3) = a_1\zeta_{17}^1 + \cdots + a_{16}\zeta_{17}^{16}$$

with $a_1 + \cdots + a_{16} = 64$.

Let

$$f(x) = (x + x^2 + x^4 + \cdots + x^9)(x^3 + x^6 + \cdots + x^{10}),$$

where the exponents in the first factor are the eight squares (mod 17) and the exponents in the second factor are the eight non-squares (mod 17). Divide

$$f(x) = (x^{17} - 1)q(x) + h(x)$$

so that the degree of $h(x)$ is smaller than 17.

Exercise 1.24. Prove that $h(x) = a_1x^1 + \cdots + a_{16}x^{16}$. Verify from the definition of $f(x)$ that both $h(\zeta_{17})$ and $h(\zeta_{17}^3)$ are equal to $(8, \zeta_{17}) \cdot (8, \zeta_{17}^3)$. It follows that

$$a_1\zeta_{17} + a_2\zeta_{17}^2 + \cdots + a_{16}\zeta_{17}^{16} = a_1\zeta_{17}^3 + a_2\zeta_{17}^{2\cdot 3} + \cdots + a_{16}\zeta_{17}^{16\cdot 3}.$$

Finally, use the irreducibility of $\Phi_{17}(z)$ to conclude that $a_{3\cdot k} = a_k$ for all k (with the subscripts considered modulo 17), and therefore that all of the a_k are equal (and hence all equal to 4).

In any case, we have shown that

$$(8, \zeta_{17}) + (8, \zeta_{17}^3) = -1$$

and

$$(8, \zeta_{17}) \cdot (8, \zeta_{17}^3) = -4$$

If follows that $(8, \zeta_{17})$ and $(8, \zeta_{17}^3)$ are the two roots of the quadratic equation

$$z^2 + z - 4.$$

This equation has roots $\frac{-1\pm\sqrt{17}}{2}$, and it is natural to ask which of these is $(8, \zeta_{17})$ and which is $(8, \zeta_{17}^3)$. We shall see in Section 4.3 how to determine this theoretically; for now, note that using a hand-held calculator to perform an approximate computation of the sum

$$\cos\frac{2\pi}{17} + \cos\frac{2\pi\cdot 2}{17} + \cos\frac{2\pi\cdot 4}{17} + \cdots + \cos\frac{2\pi\cdot 9}{17} \approx 1.5615528\cdots$$

is enough to prove that $(8, \zeta_{17}) = \frac{-1+\sqrt{17}}{2}$ and $(8, \zeta_{17}^3) = \frac{-1-\sqrt{17}}{2}$.

So we have seen how to write the two periods of length 8 as the roots of a quadratic equation with integer coefficients. The next step is to see that there are periods of length 4 for ζ_{17} which may be written as roots of a quadratic equation whose coefficients are not necessarily integers, but may be computed from the periods of length 8.

To this end, observe that each period of length 8 breaks naturally into two cycles of length 4, obtained by successively squaring twice (i.e., by successively taking fourth powers). That is, the cycles are

$$\begin{aligned}
&\zeta_{17} \rightsquigarrow \zeta_{17}^4 \rightsquigarrow \zeta_{17}^{16} \rightsquigarrow \zeta_{17}^{13} \rightsquigarrow \zeta_{17} \rightsquigarrow \cdots \\
&\zeta_{17}^2 \rightsquigarrow \zeta_{17}^8 \rightsquigarrow \zeta_{17}^{15} \rightsquigarrow \zeta_{17}^9 \rightsquigarrow \zeta_{17}^2 \rightsquigarrow \cdots \\
&\zeta_{17}^3 \rightsquigarrow \zeta_{17}^{12} \rightsquigarrow \zeta_{17}^{14} \rightsquigarrow \zeta_{17}^5 \rightsquigarrow \zeta_{17}^3 \rightsquigarrow \cdots \\
&\zeta_{17}^6 \rightsquigarrow \zeta_{17}^7 \rightsquigarrow \zeta_{17}^{11} \rightsquigarrow \zeta_{17}^{10} \rightsquigarrow \zeta_{17}^6 \rightsquigarrow \cdots
\end{aligned}$$

and the corresponding periods (i.e., the sums of the numbers in the cycle) will be denoted $(4, \zeta_{17})$, $(4, \zeta_{17}^2)$, $(4, \zeta_{17}^3)$ and $(4, \zeta_{17}^6)$ respectively. One verifies immediately that

$$(4, \zeta_{17}) + (4, \zeta_{17}^2) = (8, \zeta_{17})$$

and

$$(4, \zeta_{17}^3) + (4, \zeta_{17}^6) = (8, \zeta_{17}^3)\,.$$

We can also directly compute the products

$$(4, \zeta_{17}) \cdot (4, \zeta_{17}^2) = \zeta_{17} + \cdots + \zeta_{17}^{16} = -1$$

and

$$(4, \zeta_{17}^3) \cdot (4, \zeta_{17}^6) = \zeta_{17} + \cdots + \zeta_{17}^{16} = -1\,,$$

so that these periods may be found as the four roots of the two quadratic equations

$$z^2 - (8, \zeta_{17})z - 1$$

and

$$z^2 - (8, \zeta_{17}^3)z - 1\,.$$

Exercise 1.25. Show by "pure thought" (as in Exercise 1.24, but using an identity of the form $h(\zeta_{17}) = h(\zeta_{17}^4)$ instead) that the product of any two of the periods of length 4 will be an integer plus a sum of periods of length 4. Similarly, show by pure thought that $(4, \zeta_{17}) \cdot (4, \zeta_{17}^2)$ is a sum of periods of length 8.

Finally, the four cycles of length 4 break into eight cycles of length 2:

$$\zeta_{17} \leftrightarrow \zeta_{17}^{16},\ \zeta_{17}^4 \leftrightarrow \zeta_{17}^{13},\ \ldots$$

yielding eight periods $(2, \zeta_{17}), (2, \zeta_{17}^4), \ldots$ of length 2. Check that $(2, \zeta_{17}) + (2, \zeta_{17}^4) = (4, \zeta_{17})$ and $(2, \zeta_{17}) \cdot (2, \zeta_{17}^4) = (4, \zeta_{17}^3)$, so that $(2, \zeta_{17})$ and $(2, \zeta_{17}^4)$ are roots of

$$z^2 - (4, \zeta_{17})z + (4, \zeta_{17}^3) = 0\,.$$

Finally, ζ_{17} and ζ_{17}^{16} are the roots of

$$z^2 - (2, \zeta_{17})z + 1 = 0\,.$$

In this manner, ζ_{17} may be computed by solving a succession of four quadratic equations, the coefficients of the next equation involving only the roots of the former. We conclude that the 17-gon is constructible.

Gauss was so fond of this result that he requested that a 17-gon be engraved on his tombstone; in fact this request was not honored, as the engraver felt that visitors would mistake the 17-gon for a circle, but there is a 17-pointed star on the base of the monument.

We close this section with two notes. First, one can solve the above quadratic equations to obtain an explicit expression for ζ_{17}. For example, $\cos \frac{2\pi}{17}$ is equal to

$$\frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right)\,.$$

Second, we shall see in Section 4.1 that the same method as the above can be used to show that the $(2^{2^m} + 1)$-gon is constructible whenever $2^{2^m} + 1$ is prime. (Note that $2^k + 1$ may be prime only if k is a power of 2.) Moreover, the p-gon is *not* constructible if $p - 1$ is not a power of 2: if $p - 1$ has a prime factor $q > 2$, one cannot avoid having to solve an equation of degree q in an attempted construction of ζ_p. Similarly, the p^2-gon is never constructible for $p > 2$. Hence the n-gon is constructible if and only if n is a product of primes of the form $2^{2^m} + 1$ (at most once each) times a power of 2. This is not quite a complete description of the constructible n-gons, since it is still an open problem to determine whether $3, 5, 17, 257, 65537$ is a complete list of the primes of the form $2^{2^m} + 1$.

2. An Extraordinary Arithmetic Truth

2.1. ***Disquisitiones Arithmeticae.*** In 1795, Gauss happened upon the following theorem:

Theorem 2.1 ([Gau66], article 108)**.** *There exists x such that $x^2 \equiv -1 \pmod{p}$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

In fact, this result was long-known when Gauss discovered it; Euler and Lagrange certainly both knew how to prove it. In the Author's Preface to *Disquisitiones Arithmeticae* [Gau66], published in 1801, Gauss explains the significance of the result to him:

> The purpose of this volume whose publication I promised five years ago is to present my investigations into the field of Higher Arithmetic. Lest anyone be surprised that the contents here go back over many first principles and that many results had been given energetic attention by other authors, I must explain to the reader that when I first turned to this type of inquiry in the beginning of 1795 I was unaware of the more recent discoveries in the field and was without the means of discovering them. What happened was this. Engaged in other work I chanced upon an extraordinary arithmetic truth (if I am not mistaken, it was the theorem of art. 108). Since I considered it so beautiful in itself and since I suspected its connection with even more profound results, I concentrated all my efforts in order to understand the principles on which it depended and to obtain a rigorous proof. When I succeeded in this I was so attracted by these questions that I could not let them be.

Thus Gauss, in the first four sections of *Disquisitiones*, gives a systematic introduction to modular arithmetic, building to his first proof of quadratic reciprocity; as Gauss explains above, many (perhaps most) of the results therein are not original to him, though to some extent he discovered them independently. In fact, Legendre's *Essai sur la théorie des nombres* [Leg98] was published during the writing of *Disquisitiones*, and contained many of the same introductory results. However, although Euler and Lagrange knew the statement of quadratic reciprocity and Lagrange (as we shall see in Sections 3.1) had been able to prove a few special cases, the first complete proof of quadratic reciprocity was due to Gauss.

The final three sections contain wholly novel contributions to the field: Gauss's theory of quadratic forms and applications, and his study of roots of unity (motivated, as we have seen, by the constructibility of the 17-gon). An eighth section, omitted due to the length of the rest of the volume, was published posthumously and contains "a general treatment of algebraic congruences of indeterminate rank" ([Gau66], Author's Preface)—in modern terminology, a theory of function fields over finite fields.

Lagrange wrote to Gauss with effusive praise: "Your *Disquisitiones* have with one stroke elevated you to the rank of the foremost mathematicians, and contest of the last section [on roots of unity and the 17-gon] I look on as the most beautiful analytical discovery which has been made for a long time." ([Dun04], p. 44)

The *Disquisitiones* were dedicated to Gauss's patron the Duke of Brunswick, who financed its publication and had already financed Gauss's education, and to whom Gauss felt deeply endebted. Gauss writes:

> I consider it my greatest good fortune that you allow me to adorn this work of mine with your most honorable name. I offer it to you as a sacred token of my filial devotion. Were it not for your favor, most serene Prince, I would not have had my first introduction to the sciences. Were it not for your unceasing benefits in support of my studies, I would not have been able to devote myself totally to my passionate love, the study of mathematics. It has been your generosity alone which freed me from other cares, allowed me to give myself to so many years of fruitful contemplation and study, and finally provided me the opportunity to set down in this volume some partial results of my investigations. And when at length I was ready to present my work to the world, it was your munificence alone which removed all the obstacles which threatened to delay its publication. *(*[Gau66]*)*

2.2. **Quadratic residues.** We will shortly give three proofs of Theorem 2.1, all of which can be found in *Disquisitiones*. The first and third proofs are due to Euler; the second is Gauss's modification of the first proof. We will see two more proofs of this theorem in Section 3.4 (Exercises 3.28 and 3.31) and a sixth proof in Section 4.2. We take as a starting point the following fact, which follows from the Euclidean division algorithm:

Proposition 2.2. *If a and b are integers, then there exist integers x and y such that*

$$(a, b) = ax + by\,,$$

where (a, b) denotes the greatest common divisor of a and b.

This has the following important consequence:

Proposition 2.3 ([Gau66], art. 14)**.** *Let p be a prime number (i.e., a number with exactly two positive divisors, namely 1 and p). If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Recall that the notation $x \mid y$ indicates that x divides y, that is, that y/x is an integer; if x does not divide y, we write $x \nmid y$.

Proof. Assume that $p \nmid a$. Since the only positive divisors of p are 1 and p, and since p does not divide a, it follows that $(a, p) = 1$. By Proposition 2.2, there exist x and y such that

$$1 = ax + py\,.$$

Multiplying this equation by b, we obtain

$$b = (ab)x + p(by)\,.$$

Since ab and p are both divisible by p, so is b. □

Of this result, Gauss notes: "Euclid had already proved this theorem in this *Elements* (Book VII, No. 32). However, we did not wish to omit it because many modern authors have employed vague computations in place of proof or have neglected the theorem completely" ([Gau66], art. 14). The above proof is now standard, but it is not the proof given by Gauss. Gauss notes that (if we are to find a contradiction) we may suppose that a and b are positive and less than p. But given $a < p$, suppose $b > 1$ is the smallest positive integer such that $p \mid ab$. Now p, being prime, is not a multiple of b, so suppose $mb < p < (m + 1)b$. Then $0 < p - mb < b$,

but $a(p-mb) = p(a-\frac{ab}{p})$ is a multiple of p, contradicting the minimality of b. This result is at the heart of Gauss's proof of the fundamental theorem of algebra.

Proposition 2.4 (The fundamental theorem of algebra; [Gau66], art. 16)**.** *Every integer can be factored as a product of primes in exactly one way.*

Here Gauss notes "It is clear from elementary considerations that any composite number can be resolved into prime factors, but it is tacitly supposed and generally without proof that this cannot be done in various ways." Thus Gauss departs from his contemporaries by providing a rigorous proof of unique factorization of the integers.

Exercise 2.5. Prove the fundamental theorem of algebra.

We now continue towards our goal of proving Theorem 2.1.

Proposition 2.6. *Suppose that $p \nmid k$. Then there exists x such that $kx \equiv 1 \pmod{p}$.*

Proof. As before, we may write $1 = kx + py$. Reducing this equation modulo p yields $1 \equiv kx \pmod{p}$. □

In fact, such x is unique, at least considered modulo p. This follows directly from:

Proposition 2.7. *Suppose that $p \nmid k$ and $kx \equiv ky \pmod{p}$. Then $x \equiv y \pmod{p}$.*

Proof. The hypotheses tell us that $p \mid k(x-y)$ and that $p \nmid k$; by Proposition 2.3 we must have $p \mid x-y$, so that $x \equiv y \pmod{p}$. □

If $p \nmid k$, we shall let k^{-1} denote the unique residue $x \pmod{p}$ such that $kx \equiv 1 \pmod{p}$; we call k^{-1} the inverse of $k \pmod{p}$. Evidently $(k^{-1})^{-1}$ is equal to k. In this manner, we see that the $p-1$ non-zero residues modulo p may be paired off by pairing k with k^{-1}, with the exception of any cases where k is actually equal to $k^{-1} \pmod{p}$. But in fact, we have:

Proposition 2.8. *If $k^2 \equiv 1 \pmod{p}$, then $k \equiv \pm 1 \pmod{p}$. In fact, if $x^2 \equiv y^2 \pmod{p}$, then $x \equiv \pm y \pmod{p}$.*

Proof. The first statement is a special case of the second. If $x^2 \equiv y^2 \pmod{p}$, then

$$p \mid (x^2 - y^2) = (x-y)(x+y)\,.$$

By Proposition 2.3 we have either $p \mid x-y$ or $p \mid x+y$; in the former case $x \equiv y \pmod{p}$, and in the latter case $x \equiv -y \pmod{p}$. □

Exercise 2.9 (Wilson's Theorem)**.** Prove that $(p-1)! \equiv -1 \pmod{p}$. (Hint: use the fact that k, k^{-1} form a pair unless $k \equiv \pm 1 \pmod{p}$.)

Definition 2.10. We say that an integer k which is not divisible by p is a *quadratic residue* modulo p if there exists x such that $x^2 \equiv k \pmod{p}$; we say that k is a *quadratic non-residue* if no such x exists. This definition is encapsulated in the *Legendre symbol*: we write

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \text{if } k \text{ is a quadratic residue modulo } p \\ -1 & \text{if } k \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } k \equiv 0 \pmod{p} \end{cases}$$

Remark 2.11. This notation is the modern notation, and was not used by Gauss. He wrote $k\,R\,p$ to denote that k is a quadratic residue (mod p) and $k\,N\,p$ to denote that k is a quadratic non-residue.

Corollary 2.12 ([Gau66], art. 96)**.** *Let p be an odd prime. There are exactly $(p-1)/2$ quadratic residues modulo p, and exactly $(p-1)/2$ quadratic non-residues.*

Proof. By Proposition 2.8, the numbers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are distinct modulo p; moreover the numbers in this list are the same modulo p as the numbers in the list $\left(\frac{p+1}{2}\right)^2 \equiv \left(-\frac{p-1}{2}\right)^2, \ldots, (p-1)^2 \equiv (-1)^2$. □

Proposition 2.13 ([Gau66], art. 99)**.** *We have the formula $\left(\frac{k}{p}\right)\left(\frac{l}{p}\right) = \left(\frac{kl}{p}\right)$. That is, (a) the product of two quadratic residues is a quadratic residue; (b) the product of a quadratic residue and a non-residue is a non-residue; and (c) the product of two non-residues is a non-residue.*

Proof. The proof is in three parts. To see (a), suppose that $x^2 \equiv k$ and $y^2 \equiv l \pmod{p}$. Then $(xy)^2 \equiv kl \pmod{p}$, so kl is a quadratic residue.

For (b), suppose that $x^2 \equiv k \pmod{p}$, and assume that kl is a quadratic residue; let $y^2 \equiv kl \pmod{p}$. Then $(yx^{-1})^2 \equiv l \pmod{p}$, and l is a quadratic residue. This establishes the contrapositive of (b).

To establish (c), suppose that k and l are quadratic non-residues modulo p. Observe from part (b) that $x^2 l$ is a quadratic non-residue for any x. By Proposition 2.7 and the proof of Corollary 2.12, the numbers $1^2 l, \ldots, \left(\frac{p-1}{2}\right)^2 l$ are distinct modulo p and so form a complete list of the quadratic non-residues modulo p. Since kl is not in this list, again by Proposition 2.7, it follows that kl must be a quadratic residue. □

2.3. **Two proofs of Theorem 2.1.** We are now ready to give our first two proofs of Theorem 2.1. We suppose throughout that p is an odd prime.

Proof 1 of Theorem 2.1. (Euler; also [Gau66]*, art. 109).* Since $k \cdot k^{-1} \equiv 1 \pmod{p}$ is always a quadratic residue, it follows from Proposition 2.13 that k and k^{-1} are either both quadratic residues or both quadratic non-residues modulo p. As we observed before the proof of Proposition 2.8, the residues modulo p may be paired off by pairing k with k^{-1}, with the exception of 1 and -1, which would pair with themselves. In this manner, the quadratic residues themselves can be paired off, with the exception of 1 and possibly -1. But 1 is always a quadratic residue, and so the total number of quadratic residues modulo p is even if -1 is a quadratic residue, and odd otherwise.

However, the number of quadratic residues modulo p is $(p-1)/2$, which is even if $p \equiv 1 \pmod{4}$ and odd if $p \equiv 3 \pmod{4}$. We conclude that $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod{4}$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \pmod{4}$. □

Our second proof is Gauss's variant of the above:

Proof 2 of Theorem 2.1. ([Gau66]*, art. 110).* Observe that $(p-1)!$ is a product of $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues. By Proposition 2.13, whether or not this is a quadratic residue depends only on the number of quadratic non-residues in the product: namely, a non-zero product is a quadratic

residue if the number of quadratic non-residues in the product is even, and a non-residue if the number of quadratic non-residues in the product is odd.

The number of quadratic residues in the product is $(p-1)/2$, which is even if $p \equiv 1 \pmod 4$ and odd if $p \equiv 3 \pmod 4$; so $(p-1)!$ is a quadratic residue if $p \equiv 1 \pmod 4$ and a non-residue of $p \equiv 3 \pmod 4$. But by Wilson's Theorem (Exercise 2.9), $(p-1)! \equiv -1 \pmod p$. The result follows. □

Exercise 2.14. If $p \equiv 1 \pmod 4$, verify that $\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod p$.

2.4. **Primitive roots.** Our third proof of Theorem 2.1 depends on a more careful analysis of the multiplicative structure of the integers modulo p. Since the extra generality does not add much difficulty, we will begin by working modulo an arbitrary integer n, and later specialize back to the case where the modulus is a prime. Gauss's treatment of the subject may be found at the beginning of Section III of [Gau66], in articles 45 through 55. The arguments are somewhat dry, but we will use the main result (Theorem 2.29) repeatedly.

Definition 2.15. If $(a,n) = 1$, then the order of $a \pmod n$, denoted $\mathrm{ord}_n(a)$, is defined to be the smallest positive integer k such that $a^k \equiv 1 \pmod n$.

This definition makes sense, because we certainly know that $a^{\phi(n)} \equiv 1 \pmod n$, where ϕ denotes the Euler ϕ-function.

Example 2.16. For any n, $\mathrm{ord}_n(1) = 1$. Modulo 7, we have the following table of powers:

a^k	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

From the table, we observe that $\mathrm{ord}_7(6) = 2$, $\mathrm{ord}_7(2) = \mathrm{ord}_7(4) = 2$, and $\mathrm{ord}_7(3) = \mathrm{ord}_7(5) = 6$.

We begin with:

Proposition 2.17. *If $a^k \equiv 1 \pmod n$, then $ord_n(a)$ divides k.*

Proof. Using the Euclidean algorithm, write $k = q \cdot \mathrm{ord}_n(a) + r$, where r is a nonnegative integer smaller than $\mathrm{ord}_n(a)$. Then

$$a^k = a^{q\cdot \mathrm{ord}_n(a)+r} = a^r (a^{\mathrm{ord}_n(a)})^q \equiv a^r \cdot 1^q \equiv a^r \pmod n.$$

Since $a^k \equiv 1 \pmod n$, we have $a^r \equiv 1 \pmod n$. Since $\mathrm{ord}_n(a)$ is the smallest *positive* integer power of a which is $1 \pmod n$, and since $r < \mathrm{ord}_n(a)$, it is therefore impossible for r to be positive. Consequently, $r = 0$ and $\mathrm{ord}_n(a)$ divides k. □

The converse is evident, i.e. if $\mathrm{ord}_n(a)$ divides k then certainly $a^k \equiv 1 \pmod n$, so we can in fact say that $a^k \equiv 1 \pmod n$ if and only if $\mathrm{ord}_n(a)$ divides k. As a corollary, we obtain:

Corollary 2.18. *If $(a,n) = 1$, then $ord_n(a)$ divides $\phi(n)$.*

Proof. By Euler's generalization of Fermat's Little Theorem, we know that $a^{\phi(n)} \equiv 1 \pmod{n}$. The result then follows directly from the preceding theorem. □

There is a useful result which allows us to calculate the order of a^k once we know the order of a.

Proposition 2.19. *If $(a, n) = 1$, then $ord_n(a^k) = ord_n(a)/(k, ord_n(a))$.*

Proof. We are trying to answer the question: for what l does $(a^k)^l \equiv 1 \pmod{n}$? By Proposition 2.17, this congruence holds if and only if $\mathrm{ord}_n(a) \mid kl$. This is the case if and only if $\mathrm{ord}_n(a)/(k, \mathrm{ord}_n(a))$ divides l: see the Lemma following this proof. Thus, the smallest positive value of l which makes $(a^k)^l \equiv 1 \pmod{n}$ is $\mathrm{ord}_n(a)/(k, \mathrm{ord}_n(a))$, and so $\mathrm{ord}_n(a^k) = \mathrm{ord}_n(a)/(k, \mathrm{ord}_n(a))$. □

Lemma 2.20. *We have $a \mid bc$ if and only if $\frac{a}{(a,b)} \mid c$.*

Exercise 2.21. Use Proposition 2.2 to prove Lemma 2.20.

Example 2.22. Using $\mathrm{ord}_7(3) = 6$, we obtain $\mathrm{ord}_7(3^5) = 6/(6, 5) = 6/1 = 6$. Since $3^5 \equiv 5 \pmod{7}$, we conclude that $\mathrm{ord}_7(5) = 6$ as well.

Finally, we use the above result to prove a lemma which will be useful to us in the next section. The lemma states that if the orders of two elements are relatively prime, then the order of their product is the product of their orders, which allows us to construct elements of larger order from elements of smaller order.

Lemma 2.23. *If $ord_n(a)$ and $ord_n(b)$ are relatively prime, then $ord_n(ab) = ord_n(a) \cdot ord_n(b)$.*

Proof. If $(ab)^k \equiv 1 \pmod{n}$, then $a^k \equiv b^{-k} \pmod{n}$, so $\mathrm{ord}_n(a^k) = \mathrm{ord}_n(b^{-k})$. By Proposition 2.19, we therefore have

$$\mathrm{ord}_n(a)/(k, \mathrm{ord}_n(a)) = \mathrm{ord}_n(b)/(-k, \mathrm{ord}_n(b)).$$

Rewriting this as

$$\mathrm{ord}_n(a) \cdot (-k, \mathrm{ord}_n(b)) = \mathrm{ord}_n(b) \cdot (k, \mathrm{ord}_n(a)),$$

it follows that

$$\mathrm{ord}_n(a) \mid \mathrm{ord}_n(b) \cdot (k, \mathrm{ord}_n(a)).$$

By another application of Lemma 2.20 using the fact that $(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1$ we conclude that $\mathrm{ord}_n(a)$ divides $(k, \mathrm{ord}_n(a))$, and so $\mathrm{ord}_n(a)$ is a divisor of k. Similarly, $\mathrm{ord}_n(b)$ divides k, and so in fact $\mathrm{ord}_n(a) \cdot \mathrm{ord}_n(b)$ divides k. But certainly $(ab)^{\mathrm{ord}_n(a) \cdot \mathrm{ord}_n(b)} \equiv 1 \pmod{n}$, so as desired we obtain $\mathrm{ord}_n(ab) = \mathrm{ord}_n(a) \cdot \mathrm{ord}_n(b)$. □

Definition 2.24. An integer a, relatively prime to n, is called a primitive root (mod n) if the powers $a^1, a^2, \ldots, a^{\phi(n)}$ are all different (mod n). Since adding a multiple of n to a doesn't change whether or not it's a primitive root (mod n), we consider any two primitive roots (mod n) which differ by a multiple of n to be the same primitive root.

Since there are exactly $\phi(n)$ different residues (mod n) which are relatively prime to n, and since if $(a, n) = 1$ then the powers a^k are all also relatively prime to n, it follows that if a is a primitive root (mod n), then the residues of $a^1, a^2, \ldots, a^{\phi(n)}$ must be *all* of the different residues (mod n) which are relatively prime to n. So,

the row corresponding to a in the table of powers (mod n) is a row containing every possible residue.

Exercise 2.25. Show that 3 and 5 are the two primitive roots (mod 7). Show that there are no primitive roots (mod 8).

Proposition 2.26. *An integer a is a primitive root (mod n) if and only if $ord_n(a) = \phi(n)$.*

Proof. If $\mathrm{ord}_n(a) < \phi(n)$, then 1 appears at least twice in the list of powers $a^1, a^2, \ldots, a^{\phi(n)}$: in particular, $a^{\mathrm{ord}_n(a)} \equiv a^{\phi(n)} \equiv 1 \pmod{n}$. So, these residue classes are not all different, and a cannot be a primitive root. On the other hand, if $\mathrm{ord}_n(a) = \phi(n)$, could we have $a^i \equiv a^j \pmod{n}$ with $1 \leq i < j \leq \phi(n)$? No, because then we would find that $a^{j-i} \equiv 1 \pmod{n}$, contradicting the assumption that $a^{\phi(n)}$ is the smallest power of a to be congruent to 1 (mod n). Thus, a is indeed a primitive root (mod n). □

Exercise 2.27. Verify that 2 and 5 are the only primitive roots (mod 9).

Suppose a and b are primitive roots (mod n). Then $b \equiv a^k \pmod{n}$ for some k, by the definition of a primitive root and the fact that b must be relatively prime to n. What, then, is $\mathrm{ord}_n(b)$? By Theorem 2.19,

$$\mathrm{ord}_n(b) = \mathrm{ord}_n(a^k) = \mathrm{ord}_n(a)/(k, \mathrm{ord}_n(a)).$$

But since we've assumed that b and a are both primitive roots, we need $\mathrm{ord}_n(b) = \mathrm{ord}_n(a) = \phi(n)$, and $(k, \mathrm{ord}_n(a)) = (k, \phi(n)) = 1$. Thus, k must be relatively prime to $\phi(n)$. On the other hand, if we start with a primitive root a and an integer k that is relatively prime to n, then reversing the preceeding argument shows that $\mathrm{ord}_n(a^k) = \phi(n)$, and so a^k is a primitive root as well. Therefore, we get a primitive root (mod n) exactly for each integer between 1 and $\phi(n)$ which is relatively prime to $\phi(n)$, and we have proved:

Proposition 2.28. *If there are any primitive roots (mod n), then there are exactly $\phi(\phi(n))$ of them. Given one primitive root, a, the others can be obtained by taking powers a^k with $(k, \phi(n)) = 1$.*

Notice that this argument *assumed* the existence of at least one primitive root (mod n), and proceeded to count exactly the number of different primitive roots (mod n). However, this argument does *not* say anything about whether or not any primitive roots exist (mod n).

Finally, we come to:

Theorem 2.29 ([Gau66], art. 55)**.** *If p is a prime, then there exist primitive roots (mod p).*

In the proof of this Theorem, we will need to use the fact that for any divisor k of $p-1$, there exists a such that $a^{(p-1)/k} \not\equiv 1 \pmod{p}$. To establish this fact, we will use:

Proposition 2.30. *Let $f(x)$ be a polynomial of degree d. Then $f(x)$ has at most d roots (mod p).*

Proof. We prove the following stronger result: there exist $r_1, \ldots, r_e$ and a polynomial $g(x)$ of degree $d - e$ such that $f(x) \equiv (x - r_1) \cdots (x - r_e) g(x) \pmod{p}$ and

$g(x)$ has no roots (mod p). (We say that two polynomials are congruent modulo p if they are congruent coefficient by coefficient: that is, their constant terms are congruent modulo p, the coefficients of their linear terms are congruent modulo p, and so on.)

The proof proceeds by induction on d; the case $d = 1$ is clear. Suppose the result is established for degree $d-1$, and let $f(x)$ have degree d. If $f(x)$ has no roots modulo p, then we are done; assume, then, that $f(x)$ has a root r_1. Divide the polynomial $f(x)$ by $(x-r_1)$ using the usual polynomial division, so that $f(x) = (x-r_1)g(x)+f(r_1)$ and $g(x)$ has degree $d-1$. Since $f(r_1) \equiv 0 \pmod{p}$, we have $f(x) \equiv (x-r_1)g(x) \pmod{p}$. Applying the induction hypothesis, the result follows.

Finally, note (e.g. by Proposition 2.3) that $r_1, \dots, r_e$ are all of the roots of $f(x)$ modulo p, and $e \leq d$. □

Proof of Theorem 2.29. Write the prime factorization

$$p - 1 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$$

with $q_1, \dots, q_s$ distinct primes. By Proposition 2.30, the polynomial $x^{(p-1)/q_i} - 1$ has at most $(p-1)/q_i$ roots modulo p. In particular, there exists b_i that is *not* a root of this polynomial.

Set $a_i = b_i^{(p-1)/q_i^{\alpha_i}}$. Then

$$a_i^{q_i^{\alpha_i}} \equiv b_i^{p-1} \equiv 1 \pmod{p},$$

so that $\mathrm{ord}_p(a_i) \mid q_i^{\alpha_i}$. On the other hand,

$$a_i^{q_i^{\alpha_i - 1}} \equiv b_i^{(p-1)/q_i} \not\equiv 1 \pmod{p},,$$

and therefore $\mathrm{ord}_p(a_i)$ is exactly $q_i^{\alpha_i}$.

Then, by repeated application of Lemma 2.23, we see that $\mathrm{ord}_p(a_1 \cdots a_s) = q_1^{\alpha_1} \cdots q_s^{\alpha_s} = p - 1$, and $a_1 \cdots a_s$ is a primitive root modulo p. □

We can now give:

Proof 3 of Theorem 2.1. (Euler; also [Gau66]*, art. 64).* Since the case $p = 2$ is clear, let p be an odd prime. Suppose that $x^2 \equiv -1 \pmod{p}$. Then $x^4 \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(x) = 4$. It follows that $4 \mid p-1$, and we must have $p \equiv 1 \pmod{4}$.

On the other hand, if $p \equiv 1 \pmod{4}$, choose a primitive root a modulo p, and let $x = a^{(p-1)/4}$. Then $x^2 \not\equiv 1 \pmod{p}$ but $(x^2)^2 \equiv 1 \pmod{p}$, and so by Proposition 2.8 we have $x^2 \equiv -1 \pmod{p}$. □

3. Two Elementary Proofs of Quadratic Reciprocity

3.1. **When are $2, 3, 5, \dots$ squares modulo p?** Now that we have determined the primes p such that -1 is a square modulo p, it is natural to turn to similar questions: when is 2 a square modulo p? 3? An arbitrary number k? In articles 112 to 124 of [Gau66], Gauss discusses the work of Fermat, Euler, and Lagrange on these problems when $k \leq 7$. We begin with:

Proposition 3.1. *If $p \equiv 3$ or $5 \pmod{8}$ then $\left(\frac{2}{p}\right) = -1$.*

Proof. Suppose not. Then there exists a smallest prime p which is congruent to 3 or 5 (mod 8) and such that $\left(\frac{2}{p}\right) = 1$; say $a^2 \equiv 2 \pmod{p}$. Replacing a by its smallest residue (mod p), and then replacing a by $p-a$ if necessary, we may suppose without loss of generality that a is odd and less than p. Write

$$a^2 - 2 = pt\,.$$

Now any prime q dividing t has $a^2 \equiv 2 \pmod{q}$ as well, and moreover

$$t = \frac{a^2-2}{p} < \frac{p^2}{p} = p\,,$$

so $q \leq t < p$. Therefore, to obtain a contradiction to the minimality of p, it suffices to prove that t is divisible by a prime which is congruent to 3 or 5 (mod 8).

But the square of any odd number is congruent to 1 (mod 8). Hence $pt = a^2 - 2 \equiv -1 \pmod{8}$, and since $p \equiv 3$ or 5 (mod 8), we find $t \equiv 3$ or 5 (mod 8) as well. But a product of primes which are congruent to ± 1 (mod 8) must again be ± 1 (mod 8); it follows that t cannot be a product of only such primes, and so must be divisible by a prime which is congruent to 3 or 5 (mod 8). □

Exercise 3.2. Use an essentially identical argument to prove that if $p \equiv 5$ or 7 (mod 8), then $\left(\frac{-2}{p}\right) = -1$.

Proposition 3.3. $\left(\frac{2}{p}\right) = 1$ *if and only if* $p \equiv 1$ *or* 7 (mod 8).

Proof. In Proposition 3.1, we have proved the negative portion of this statement: that if $p \equiv 3$ or 5 (mod 8), then 2 is not a square (mod p). We will have to show that if $p \equiv 1$ or 7 (mod 8), then 2 is a square (mod p). We use a different trick for each of the two cases.

If $p \equiv 7$ (mod 8), then -2 and -1 are both non-squares mod p: the former by Exercise 3.3, the latter by Theorem 2.1. The product of two non-squares is a square (Proposition 2.13), and so 2 is a square mod p.

On the other hand, if $p \equiv 1$ (mod 8), let g be a primitive root modulo p, so that g has order $p - 1 = 8k$ for some k. Then $g^{4k} \equiv -1 \pmod{p}$, so

$$\begin{aligned}(g^k + g^{-k})^2 &\equiv g^{2k} + 2 + g^{-2k} \pmod{p} \\ &\equiv g^{-2k}(g^{4k}+1) + 2 \pmod{p} \\ &\equiv 2 \pmod{p}\,,\end{aligned}$$

as desired. □

Amusingly, although it appears the above proof is constructive in the case $p \equiv 1$ (mod 8) and non-constructive when $p \equiv 7$ (mod 8), from an algorithmic point of view this is not the case! The above construction of a square root of 2 (mod p) when $p \equiv 1$ (mod 8) depends on finding a primitive root mod p, for which fast algorithms are only known conditionally on the Extended Riemann Hypothesis. On the other hand, now that we know $\left(\frac{2}{p}\right) = 1$ if $p \equiv 7$ (mod 8), we can show:

Exercise 3.4. If $p = 8k + 7$, then 2^{2k+2} is a square root of 2 modulo p.

The above propositions are due to Lagrange [Lag75]. Fermat had correctly determined the primes p for which 2 is a square modulo p (as well as those for which 3 is a square modulo p), but never wrote down a proof. The arguments for $\left(\frac{\pm 3}{p}\right)$

below are due to Euler [Eul63]; Gauss notes that it is "astonishing that proof of the propositions relative to the residues +2 and −2 kept eluding Euler, since they depend on similar devices." We will see another proof of these results in Exercises 3.32 and refthree-again. The arguments for $\left(\frac{\pm 5}{p}\right)$ and $\left(\frac{\pm 7}{p}\right)$ are due to Lagrange [Lag75].

Exercise 3.5. Use methods similar to those of Proposition 3.1 to show that $\left(\frac{3}{p}\right) = -1$ if $p \equiv 5, 7 \pmod{12}$; and that $\left(\frac{-3}{p}\right) = -1$ if $p \equiv 5, 11 \pmod{12}$.

Exercise 3.6. Conclude that $\left(\frac{3}{p}\right) = 1$ if $p \equiv 11 \pmod{12}$ and $\left(\frac{-3}{p}\right) = -1$ if $p \equiv 7 \pmod{12}$.

Exercise 3.7. Suppose $p = 3k + 1$, and let g be a primitive root mod p. Prove that $2g^k + 1$ is a square root of $-3 \pmod{p}$. Conclude in particular that $\left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right) = 1$ if $p \equiv 1 \pmod{12}$.

Exercise 3.8. Prove that $\left(\frac{5}{p}\right) = -1$ if $p \equiv 2, 3 \pmod{5}$, by proving more generally that there is no odd integer t such that 5 is square mod t but $\left(\frac{t}{5}\right) = -1$.

Exercise 3.9. Suppose $p = 5k + 1$, and let g be a primitive root mod p. Prove that $2g^k + 1 + 2g^{-k}$ is a square root of 5 mod p.

We will see later (Propositions 4.26 and 4.29) how to generalize this argument to determine $\left(\frac{q}{p}\right)$ for primes $p \equiv 1 \pmod{q}$.

Exercise 3.10. Let p be a prime, and b a quadratic non-residue modulo p. Prove that

$$\frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}$$

is divisible by p for all integers x.

Exercise 3.11. Use the preceding exercise to prove that if e divides $p + 1$, then the polynomial

$$\frac{(x + \sqrt{b})^{e} - (x - \sqrt{b})^{e}}{\sqrt{b}}$$

has at least $e - 1$ roots modulo p.

Exercise 3.12. Suppose $p = 5k + 4$, let b be a quadratic non-residue modulo p, and choose a such that

$$\frac{(a + \sqrt{b})^{5} - (a - \sqrt{b})^{5}}{\sqrt{b}}$$

is divisible by p. Show that

$$(b + 5a^2)^2 \equiv 20a^2 \pmod{p}$$

and conclude that 5 is a square modulo p.

Exercise 3.13. Conclude that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ for all odd primes $p \neq 5$.

Gauss notes that the arguments for $\left(\frac{\pm 7}{p}\right)$ are largely similar, but that the cases $p = 7k + 2$ and $p = 7k + 4$ must be handled differently.

3.2. **Quadratic Reciprocity.** In an appendix to *Disquisitiones*, Gauss includes a table of $\left(\frac{p}{q}\right)$ for primes $p, q < 100$. We have already seen that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ for all odd primes $p \neq 5$; investigating the table, one observes that the same pattern appears to hold when 5 is replaced by any prime $q \equiv 1 \pmod 4$.

On the other hand, it is certainly not the case that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ for all odd primes p, q: for example, $\left(\frac{3}{7}\right) = -1$ whereas $\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Exercise 3.14. Use the results of Exercises 3.5,3.6,3.7 to show that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p \equiv 1 \pmod 4$, whereas $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ if $p \equiv 3 \pmod 4$.

An identical pattern emerges upon replacing 3 by any prime $q \equiv 3 \mod 4$. One is led to the following conjecture:

Theorem 3.15 (Quadratic Reciprocity)**.** *Let p, q be odd primes. If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. If $p, q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

Exercise 3.16. Show that quadratic reciprocity may be reformulated as follows: if p, q are odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Gauss found six proofs of quadratic reciprocity; as of 2004, there are more than 200 known proofs of quadratic reciprocity . In the introduction to his third proof of quadratic reciprocity, Gauss describes the history of the result:

> We must consider Legendre as the discoverer of this very elegant theorem, although special cases of it had previously been discovered by the celebrated geometers Euler and Lagrange. [...] I discovered this theorem independently in 1795 at a time when I was totally ignorant of what had been achieved in higher arithmetic, and consequently had not the slightest aid from the literature on the subject. For a whole year this theorem tormented me and absorbed my greatest efforts until at last I obtained a proof given in the fourth section of [*Disquisitiones*]. Later I ran across three other proofs which were built on entirely different principles. One of these I have already given in the fifth section [of *Disquisitiones*], the others, which do not compare with it in elegance, I have reserved for future publication. Although these proofs leave nothing to be desired as regards rigor, they are derived from sources much too remote, except perhaps the first, which however proceeds with laborious arguments and is overloaded with extended operations. I do not hesitate to say that till now a *natural* proof has not been produced. I leave it to the authorities to judge whether the following proof which I have recently been fortunate enough to discover deserves this description. [Gau08]*; translated in* [Smi59] *by D.H. Lehmer*

Gauss's first proof, completed in April 1796, and his third proof, completed in May 1807, use essentially only elementary principles; it is these two proofs that we will give in the next two sections. As Gauss notes, his other proofs rely on

machinery ("sources much too remote"): for example, Gauss's second proof uses his genus theory of quadratic forms, while his fourth proof (completed in May 1801, but not published until 1811) follows from his evaluation of the Gauss sum. From a 21st century vantage point, these proofs (which we will see later) may seem more natural than the elementary proofs! Gauss understood this: indeed, he continued to seek more proofs of quadratic reciprocity, in the hope of finding techniques that would generalize to the cubic and biquadratic situations. (When do $x^3 \equiv q \pmod{p}$ or $x^4 \equiv q \pmod{p}$ have solutions?) Though it was Eisenstein and Jacobi, not Gauss, who eventually proved the laws of cubic and biquadratic reciprocity, the ideas in Gauss's later proofs of quadratic reciprocity would play important roles.

3.3. **The First Proof of Quadratic Reciprocity.** Gauss's first proof of quadratic reciprocity proceeds by induction. (One should be aware that when Gauss says he is obtaining a result "by induction", he means that he is producing the statement of a result by generalizing from examples, not that he is proving the result. When we write "induction", we will always mean mathematical induction.) Our proof is essentially the one given by Gauss in articles of [Gau66], but we an elucidation of a simplification due to L. Carlitz [Car60].

Before giving the proof, we sketch an outline of it. Suppose p and q are positive, odd primes with $p < q$; we wish to relate $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$. The first step is to produce a number $r < q$ such that

$$e^2 = pr + qf$$

for some even e and odd $f < q$. Reducing this equation modulo p, we see that $\left(\frac{q}{p}\right)$ depends only on $\left(\frac{f}{p}\right)$; since $f < q$ we may use an inductive hypothesis to determine $\left(\frac{f}{p}\right)$ in terms of whether p is a square (mod f). But pr is known to be a square (mod f), so it suffices to determine whether r is a square (mod f); by another use of the inductive hypothesis, this is determined by whether f is a square (mod r). But the latter is known, by our assumption that $\left(\frac{r}{q}\right)$ is understood, and our proof will go through.

There are, of course, many details to be added. To begin with, note that f may be composite, and yet in our induction step we wish to consider whether p and r are squares modulo f. To that end, we require the following generalization of the Legendre symbol:

Definition 3.17. If m and n are odd numbers, with $n = p_1^{a_1} \cdots p_k^{a_k}$ and positive, the Jacobi symbol is defined to be

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{a_1} \cdots \left(\frac{m}{p_k}\right)^{a_k}$$

where the terms in the product on the right-hand side are the Legendre symbol. In particular, if m and n are primes, the Jacobi symbol is equal to the Legendre symbol.

Exercise 3.18. If m is congruent to a square modulo n, prove that $\left(\frac{m}{n}\right) = 1$. Prove that $\left(\frac{m}{n}\right)\left(\frac{m'}{n}\right) = \left(\frac{mm'}{n}\right)$.

Exercise 3.19. If x, y are odd integers, set $\mu(x,y) = (-1)^{(x-1)(y-1)/4}$. If m is another odd integer, show that $\mu(x,m)\mu(y,m) = \mu(xy,m)$.

Exercise 3.20. Show that quadratic reciprocity implies the following reciprocity law for the Jacobi symbol:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}.$$

Note that to prove the above reciprocity law, one needs quadratic reciprocity only for primes up to m and n.

Exercise 3.21. Extend the definition of the Jacobi symbol to negative odd integers by defining $\left(\frac{m}{n}\right) = \left(\frac{m}{-n}\right)$. Show that the reciprocity law of Exercise 3.20 still holds if one (but not both) of m, n are negative.

To produce our auxiliary r, we use the following lemma:

Lemma 3.22. *If $q \equiv 1 \pmod 4$, there exists a prime $p' < 2\lfloor\sqrt{q}\rfloor + 1$ such that $\left(\frac{q}{p'}\right) = -1$.*

Proof. We argue as in articles 124 through 129 of [Gau66]; for the case $q \equiv 1 \pmod 8$, we follow the exposition of [Lem00]. If $q \equiv 5 \pmod 8$, take any $a < \sqrt{q/2}$. Then $q - 2a^2$ is positive and congruent either to 3 or 5 (mod 8), so must have some prime divisor $p' \equiv 3, 5 \pmod 8$. Certainly $q \equiv 2a^2 \pmod{p'}$. But by Proposition 3.3 we know that 2 is not a square modulo p', and so q is also not a square modulo p'.

Suppose that $q \equiv 1 \pmod 8$, and set $m = \lfloor\sqrt{q}\rfloor$. Assume that $\left(\frac{q}{p'}\right) = 1$ for all $p' \leq 2m+1$. By the exercise following this proof, the congruence $x^2 \equiv q \pmod{(p')^s}$ has solutions for all $p' \leq 2m+1$ and all $s > 0$. By the Chinese Remainder Theorem, there is an integer x such that $x^2 \equiv q \pmod{(2m+1)!}$.

But $\binom{x+m}{2m+1}$ is an integer, which implies

$$\begin{aligned} 0 &\equiv x(x-1)(x+1)\cdots(x-m)(x+m) \pmod{(2m+1)!} \\ &\equiv x(x^2-1^2)\cdots(x^2-m^2) \pmod{(2m+1)!} \\ &\equiv x(q-1^2)\cdots(q-m^2) \pmod{(2m+1)!} \end{aligned}$$

Since x and $(2m+1)!$ are relatively prime, it follows that $(2m+1)!$ divides $(q-1^2)\cdots(q-m^2)$. But in fact

$$\begin{aligned} (2m+1)! &= (m+1+m)\cdots(m+1)\cdots(m+1-m) \\ &= ((m+1)^2-1)\cdots((m+1)^2-m^2)(m+1) \\ &> (q-1^2)\cdots(q-m^2) \end{aligned}$$

a contradiction. □

Exercise 3.23. If p' is odd and $x^2 \equiv q \pmod{p'}$ has a solution, prove by induction that $x^2 \equiv q \pmod{(p')^s}$ has a solution for all $s \geq 1$. Similarly, if $x^2 \equiv q \pmod 8$ has a solution, prove that $x^2 \equiv q \pmod{2^s}$ has a solution for all $s \geq 3$.

Finally, we are ready to prove quadratic reciprocity by induction. Our induction is on the maximum $\max(p, q)$, where p and q are distinct odd primes. Assume without loss of generality that $p < q$, so that in the induction step we fix q and we wish to prove $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \mu(p, q)$ for all $p < q$. In fact, we need to proceed by proving this statement first for all p such that $\left(\frac{p}{q}\right) = 1$, and then for all p such

that $\left(\frac{p}{q}\right) = -1$; that is, if $\left(\frac{p}{q}\right) = -1$ then quadratic reciprocity for all pairs (p', q) with $\left(\frac{p'}{q}\right) = 1$ will already be available to us as part of the induction hypothesis.

Define

$$r = \begin{cases} 1 & \text{if } \left(\frac{p}{q}\right) = 1 \\ -1 & \text{if } \left(\frac{p}{q}\right) = -1 \text{ and } q \equiv 3 \pmod 4 \\ p' & \text{if } \left(\frac{p}{q}\right) = -1 \text{ and } q \equiv 1 \pmod 4 \end{cases}$$

where in the last case we use Lemma 3.22 to obtain $p' < q$ such that $\left(\frac{q}{p'}\right) = -1$.

In this last case, if we had $\left(\frac{p'}{q}\right) = 1$ then the induction hypothesis would imply $\left(\frac{q}{p'}\right) = 1$, a contradiction; so $\left(\frac{r}{q}\right) = \left(\frac{p'}{q}\right) = -1$ as well. Observe then that in all cases $\left(\frac{pr}{q}\right) = 1$, so we may write

$$e^2 = pr + qf \tag{3.24}$$

for some even $e < q$, and it is easy to see (since $p, r < q$ and $r \geq -1$) that $|f| < q$. The proof now breaks into several cases depending on the greatest common divisor of f and pr. Carlitz [Car60] notes that these cases can be unified with judicious notation, but since this obfuscates the proof somewhat, we precede the general case with the case $(f, pr) = 1$. We may compute

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{f}{p}\right) && \text{reducing equation (3.24) mod } p \\ &= \mu(p, f)\left(\frac{p}{f}\right) && \text{by the induction hypothesis} \\ &= \mu(p, f)\left(\frac{r}{f}\right) && \text{reducing equation (3.24) mod } f \\ &= \mu(p, f)\mu(r, f)\left(\frac{f}{r}\right) && \text{by the induction hypothesis} \\ &= \mu(p, f)\mu(r, f)\left(\frac{q}{r}\right) && \text{reducing equation (3.24) mod } r \\ &= \mu(p, f)\mu(r, f)\mu(r, q)\left(\frac{r}{q}\right) \end{aligned}$$

where the last step uses either the induction hypothesis (if $r = p'$) or is obvious if $r = \pm 1$. Note that in the fourth step, we are using the extended version of quadratic reciprocity of Exercise 3.21 (whose proof for $\left(\frac{f}{r}\right)$ only entails quadratic reciprocity for primes dividing f and r, so is obtainable from the induction hypothesis). Now, we know $\left(\frac{r}{q}\right) = \left(\frac{p}{q}\right)$; moreover, by Exercise 3.19 we have $\mu(p, f)\mu(r, f)\mu(r, q) = \mu(pr, qf)\mu(p, q)$, so that

$$\left(\frac{q}{p}\right) = \mu(pr, qf)\mu(p, q)\left(\frac{p}{q}\right).$$

But pr and qf are odd and $pr + qf = e^2$ is divisible by 4, so exactly one of pr and qf is congruent to 1 (mod 4). Therefore $\mu(pr, qf) = 1$, and the result follows.

We now prove the general case, which uses the same ideas but is somewhat more complicated. Note that if $r = p$ then we are already done, so we may assume $r \neq p$. Write $(f, pr) = d$, set $s = pr/d$, and write

$$d(e')^2 = s + qf' \tag{3.25}$$

with $e' = e/d$, $f' = f/d$, and s relatively prime to d. Now

$$\begin{aligned}
\left(\frac{q}{p}\right) &= \left(\frac{q}{s}\right)\left(\frac{q}{d}\right)\left(\frac{q}{r}\right) && \text{since } sd = pr \\
&= \left(\frac{df'}{s}\right)\left(\frac{q}{d}\right)\left(\frac{q}{r}\right) && \text{since } d(e')^2 \equiv qf' \pmod{s} \\
&= \mu(s, df')\left(\frac{s}{d}\right)\left(\frac{s}{f'}\right)\left(\frac{q}{d}\right)\left(\frac{q}{r}\right) && \text{by the induction hypothesis} \\
&= \mu(s, df')\left(\frac{-qf'}{d}\right)\left(\frac{d}{f'}\right)\left(\frac{q}{d}\right)\left(\frac{q}{r}\right) && \text{reducing (3.25) modulo } d \\
&= \mu(s, df')\mu(d, f')\left(\frac{-1}{d}\right)\left(\frac{q}{r}\right) \\
&= \mu(s, df')\mu(d, f')\mu(-1, d)\mu(r, q)\left(\frac{r}{q}\right) \\
&= \mu(s, df')\mu(d, f')\mu(-1, d)\mu(r, q)\left(\frac{p}{q}\right)
\end{aligned}$$

and so it remains to prove that

$$\mu(p, q) = \mu(s, df')\mu(d, -f')\mu(r, q)\,.$$

But

$$\mu(s, df')\mu(s, q) = \mu(s, df'q) = \mu(s, -sd) = \mu(s, d) = \mu(d, -qf') \tag{3.26}$$

where the first equality uses Exercise 3.19, the second uses the congruence $sd + df'q = (de')^2 \equiv 0 \pmod 4$, the third uses $\mu(s, -s) = 1$, and the fourth uses the congruence $s + qf' \equiv 0 \pmod 4$. Multiplying the leftmost and rightmost sides of (3.26) by $\mu(d, -f')\mu(rs, q)$ yields

$$\mu(s, df')\mu(d, -f')\mu(r, q) = \mu(d, -qf')\mu(d, -f')\mu(rs, q)$$

and, as desired, the right-hand side simplifies to

$$\mu(d, q)\mu(rs, q) = \mu(p, q)$$

since $pr = sd$. This completes the proof.

3.4. **Gauss's third proof of quadratic reciprocity.** Let p be an odd prime. We recall the following result due to Euler:

Proposition 3.27 (Euler's criterion)**.** $\left(\frac{k}{p}\right) \equiv k^{\frac{p-1}{2}} \pmod p$.

Proof. If $\left(\frac{k}{p}\right) = 1$, write $k \equiv x^2 \pmod p$. Then

$$k^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

as well.

Conversely, suppose that $k^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Let g be a primitive root modulo p (Theorem 2.29) and suppose $k \equiv g^r \pmod{p}$. Then

$$k^{\frac{p-1}{2}} \equiv g^{r\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p},$$

which implies that $p-1 \mid r\left(\frac{p-1}{2}\right)$ and r is even. Therefore $k \equiv (g^{r/2})^2$ is a square modulo p.

Thus $\left(\frac{k}{p}\right) = 1$ if and only if $k^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Certainly $\left(\frac{k}{p}\right) = 0$ if and only if $k^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. The only other possibility for each quantity is $-1 \pmod{p}$, and the result follows. □

Exercise 3.28. Prove Theorem 2.1 using Euler's criterion.

Gauss's third proof of quadratic reciprocity relies on a clever application of Euler's criterion:

Proposition 3.29 (Gauss's Lemma)**.** *Let p be an odd prime, and set*

$$A = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, \ B = \left\{\frac{p+1}{2}, \ldots, p-1\right\}.$$

Let k be an integer not divisible by p, and let $b(k,p)$ be the number of integers in the list

$$k \cdot 1, k \cdot 2, \ldots, k \cdot \frac{p-1}{2}$$

whose least residue (mod p) lies in B. Then $\left(\frac{k}{p}\right) = (-1)^{b(k,p)}$.

Proof. The least residues (mod p) of the integers in the list $k \cdot 1, k \cdot 2, \ldots, k \cdot \frac{p-1}{2}$ are evidently distinct (by Proposition 2.7). Note that if the least residue of i lies in B, then the least residue of $-i$ lies in A. Moreover, if the least residue of ki lies in B, then the least residue of $-ki$ is not equal to the least residue of $\pm kj$ for any other j in $1, 2, \ldots, \frac{p-1}{2}$. Indeed, if this were not so, we would have $-ki \equiv \pm kj \pmod{p}$, so that $i \pm j \equiv 0 \pmod{p}$; this is an impossibility if i and j are distinct integers between 1 and $\frac{p-1}{2}$.

Consider the list

$$\pm k \cdot 1, \pm k \cdot 2, \ldots, \pm k \cdot \frac{p-1}{2},$$

where the term ki is given the sign $+$ if the least residue of ki lies in A, and the sign $-$ if the least residue of ki lies in B. Note that there are exactly $b(k,p)$ minus signs. It follows from the previous paragraph that the least residues of the numbers in this list are distinct and lie in A; since there are $\frac{p-1}{2}$ of them, they are simply a permutation of the numbers in A.

We conclude that if we multiply the numbers in the list $k \cdot 1, k \cdot 2, \ldots, k \cdot \frac{p-1}{2}$, then the product is congruent to $(-1)^{b(k,p)}\left(\frac{p-1}{2}\right)! \pmod{p}$. On the other hand, the product is exactly $k^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$ and obtain

$$k^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv (-1)^{b(k,p)}\left(\frac{p-1}{2}\right)! \pmod{p}.$$

By Euler's criterion, it follows (cancelling the $\left(\frac{p-1}{2}\right)!$ terms) that $\left(\frac{k}{p}\right) = (-1)^{b(k,p)}$. □

This argument is best illustrated by an example. Let $p = 11$ and $k = 7$. Then $\frac{11-1}{2} = 5$, and the least residues of $7 \cdot 1, \ldots, 7 \cdot 5$ modulo 11 are, in order,

$$7, 3, 10, 6, 2\,.$$

Modulo 11, these are the same as

$$-4, 3, -1, -5, 2\,.$$

Therefore $b(7, 11) = 3$,

$$(7 \cdot 1) \cdots (7 \cdot 5) \equiv (-4) \cdot 3 \cdot (-1) \cdot (-5) \cdot 2 \pmod{11}\,,$$

and

$$7^5 5! \equiv (-1)^3 5! \pmod{11}\,.$$

We conclude $\left(\frac{7}{11}\right) \equiv 7^5 = -1 \pmod{11}$.

We can now give Gauss's third proof of quadratic reciprocity, following the treatment of [Gau08]. Let p and q be distinct odd primes. By Gauss's Lemma (Proposition 3.29) and the reformulation of quadratic reciprocity in Exercise 3.16, we want to prove

$$(-1)^{b(p,q)+b(q,p)} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\,,$$

or equivalently that

$$b(p, q) + b(q, p) \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod{2}\,. \tag{3.30}$$

Exercise 3.31. Prove Theorem 2.1 using Gauss's Lemma.

Exercise 3.32. Use Gauss's lemma to give another proof that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$.

Exercise 3.33. Use Gauss's lemma to give another proof that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

Recall that $\lfloor x \rfloor$ is defined to be the greatest integer less than or equal to x. The fractional part of x is defined to be $x - \lfloor x \rfloor$. We use this to give this an algebraic formula for $b(k, p)$. Indeed, note that if i is not divisible by p, then the least residue of $ki \pmod p$ lies in A if and only if the fractional part of ki/p is less than $1/2$, and lies in B if and only if the fractional part of ki/p is greater than $1/2$.

Exercise 3.34. Verify that $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0 & \text{if the fractional part of } x \text{ is } < 1/2 \\ 1 & \text{if the fractional part of } x \text{ is } > 1/2 \end{cases}$.

Exercise 3.35. Use the result of the previous Exercise to show that

$$b(k, p) = \sum_{i=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{2ik}{p} \right\rfloor - 2 \left\lfloor \frac{ik}{p} \right\rfloor \right)\,.$$

We now depart slightly from Gauss's original presentation of his proof. According to (3.30), we are concerned only with whether $b(q, p)$ and $b(p, q)$ are even or odd. Gauss continues to work with exactly formulae for $b(k, p)$ as long as possible and

later reduces mod 2. For simplicity, we will reduce mod 2 immediately; in particular we have

$$\begin{aligned} b(k,p) &\equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ik}{p} \right\rfloor \pmod 2 \\ &= \left\lfloor \frac{2k}{p} \right\rfloor + \left\lfloor \frac{4k}{p} \right\rfloor + \cdots + \left\lfloor \frac{(p-1)k}{p} \right\rfloor \pmod 2 . \end{aligned} \tag{3.36}$$

Exercise 3.37. If a is an integer and x is not, show that $\lfloor x \rfloor + \lfloor a - x \rfloor = a - 1$.

We apply the previous exercise to obtain

$$\left\lfloor \frac{ik}{p} \right\rfloor + \left\lfloor \frac{(p-i)k}{p} \right\rfloor = k - 1 .$$

For k odd, this implies

$$\left\lfloor \frac{ik}{p} \right\rfloor \equiv \left\lfloor \frac{(p-i)k}{p} \right\rfloor \pmod 2 . \tag{3.38}$$

Note that i is even and greater than $p/2$ if and only if $p - i$ is odd and less than $p/2$; substituting (3.38) for all terms $\left\lfloor \frac{2ik}{p} \right\rfloor$ of (3.36) with $2i > p/2$, we get

$$b(k,p) \equiv \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{2k}{p} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{p-1}{2}\right) k}{p} \right\rfloor \pmod 2$$

when k is odd. We therefore obtain

$$\begin{aligned} b(p,q) + b(q,p) \equiv &\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{p-1}{2}\right) q}{p} \right\rfloor \\ &+ \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{q-1}{2}\right) p}{q} \right\rfloor \pmod 2 . \end{aligned} \tag{3.39}$$

Now the proof of quadratic reciprocity is completed by the following exercise:

Exercise 3.40. Prove that

$$\left(\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{p-1}{2}\right) q}{p} \right\rfloor \right) + \left(\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{\left(\frac{q-1}{2}\right) p}{q} \right\rfloor \right) \tag{3.41}$$

is exactly equal to $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$, as follows. Consider the rectangle of lattice points (x, y) in the plane, with $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{q-1}{2}$. Show that $\left\lfloor \frac{iq}{p} \right\rfloor$ counts the number of lattice points of the form (i, y) lying below the line $py = qx$. Show that $\left\lfloor \frac{ip}{q} \right\rfloor$ counts the number of lattice points of the form (x, i) lying to the left of the line $py = qx$. Conclude that the sum (3.41) counts the number of lattice points in the full rectangle. How many lattice points are in the rectangle?

We remark that Gauss evaluated (3.41) in a somewhat laborious manner, rather than as above; but the above counting proof is too pretty to omit!

4. Roots of Unity and Gauss sums

We return now to the ideas of Section 1, in which we saw that Gauss used algebraic properties of the 17th roots of unity to prove that the regular 17-gon is constructible. In Section VII of *Disquisitiones*, Gauss gives a systematic treatment of these arguments.

4.1. **Periods.** In Section 1.3, we saw how the set of primitive 17th roots of unity could be partitioned into cycles, whose sums (*periods*) satisfied polynomials whose coefficients were periods of longer cycles. We will now generalize these ideas to the case an arbitrary prime p.

Fix a primitive root g modulo p. Starting from ζ_p and repeatedly raising to the gth power, we obtain a cycle

$$\zeta_p \rightsquigarrow \zeta_p^g \rightsquigarrow \zeta_p^{g^2} \rightsquigarrow \cdots \rightsquigarrow \zeta_p^{g^{p-2}} \rightsquigarrow \zeta_p^{g^{p-1}} = \zeta_p \rightsquigarrow \cdots$$

of length $p-1$ containing all of the primitive pth roots of unity. If f is any divisor of $p-1$, the cycle of length $p-1$ breaks up into $e = \frac{p-1}{f}$ cycles of length f (obtained by repeatedly raising to the g^eth power):

$$\zeta_p^{g^i} \rightsquigarrow \zeta_p^{g^{i+e}} \rightsquigarrow \zeta_p^{g^{i+2e}} \rightsquigarrow \cdots \rightsquigarrow \zeta_p^{g^{i+fe}} = \zeta_p^{g^i} \rightsquigarrow \cdots$$

for each $0 \leq i < e$.

Definition 4.1. If $f \mid p-1$, then the period (f, ζ_p^k) is defined to be the sum of the roots of unity in the cycle of length f containing ζ_p^k; that is,

$$(f, \zeta_p^k) = \zeta_p^k + \zeta_p^{kg^e} + \cdots + \zeta_p^{kg^{(f-1)e}}.$$

By analogy, we define $(f, 1) = f$. We will say that (f, ζ_p^k) is a period of length f, and that $\zeta_p^k, \zeta_p^{kg^e}, \ldots, \zeta_p^{kg^{(f-1)e}}$ are the roots contained in (f, ζ_p^k).

Exercise 4.2. Prove that the period (f, ζ_p^k) does not depend on the choice of primitive root g.

Exercise 4.3. Show that $(p-1, \zeta_p) = -1$.

Proposition 4.4 ([Gau66], art. 345)**.** *If λ, μ are pth roots of unity, then the product $(f, \lambda)(f, \mu)$ is a sum of periods of length f.*

Proof. Suppose $\lambda = \zeta_p^j$ and $\mu = \zeta_p^k$. One checks explicitly that terms in the product

$$(f, \lambda)(f, \mu) = (\zeta_p^j + \zeta_p^{jg^e} + \cdots + \zeta_p^{jg^{(f-1)e}})(\zeta_p^k + \zeta_p^{kg^e} + \cdots + \zeta_p^{kg^{(f-1)e}})$$

may be rearranged into the sum

$$\begin{aligned}(\zeta_p^{j+k} + \zeta_p^{(j+k)g^e} + \cdots + \zeta_p^{(j+k)g^{(f-1)e}}) + (\zeta_p^{j+g^e k} + \zeta_p^{(j+g^e k)g^e} + \cdots + \zeta_p^{(j+g^e k)g^{(f-1)e}}) \\ + \cdots + (\zeta_p^{j+g^{(f-1)e}k} + \zeta_p^{(j+g^{(f-1)e}k)g^e} + \cdots + \zeta_p^{(j+g^{(f-1)e}k)g^{(f-1)e}}),\end{aligned}$$

which is equal to the sum of periods

$$(f, \lambda\mu) + (f, \lambda\mu^{g^e}) + \cdots + (f, \lambda\mu^{g^{(f-1)e}}).$$

Note that by symmetry, this must also be equal to the sum

$$(f, \lambda\mu) + (f, \lambda^{g^e}\mu) + \cdots + (f, \lambda^{g^{(f-1)e}}\mu).$$

Also note that some of these periods may be $(f, 1) = f$. □

Recall that the roots of the pth *cyclotomic polynomial*

$$\Phi_p(z) = \frac{z^p - 1}{z - 1} = z^{p-1} + \cdots + z + 1$$

are the primitive pth roots of unity $\zeta_p, \zeta_p^2, \ldots, \zeta^{p-1}$. We saw in Theorem 1.15 that $\Phi_p(z)$ is irreducible; this has the following consequences:

Corollary 4.5. *If $a_1, \ldots, a_{p-1}$ and $b_1, \ldots, b_{p-1}$ are rational numbers and*

$$a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} = b_1\zeta_p + b_2\zeta_p^2 + \cdots + b_{p-1}\zeta_p^{p-1} \tag{4.6}$$

then $a_i = b_i$ for $i = 1, 2, \ldots, p-1$.

Proof. The identity (4.6) implies that ζ_p is a root of the polynomial

$$h(z) = (b_{p-1} - a_{p-1})z^{p-2} + \cdots + (b_2 - a_2)z + (b_1 - a_1)\,.$$

By the exercise following this proof, $h(z)$ must be divisible by $\Phi_p(z)$; since the degree of $h(z)$ is smaller than that of $\Phi_p(z)$, we must have $h(z) = 0$. □

Exercise 4.7. If $g(z), h(z)$ are polynomial with rational coefficients such that $g(r) = h(r) = 0$, and if $g(z)$ is irreducible, then $g(z)$ divides $h(z)$. (Consider the GCD of $g(z)$ and $h(z)$.)

Corollary 4.8. *If $g(z)$ and $h(z)$ are two polynomials with rational coefficients such that $g(\zeta_p) = h(\zeta_p)$, then $g(\zeta_p^l) = h(\zeta_p^l)$ for any $1 \leq l \leq p-1$.*

Proof. The difference $g(z) - h(z)$ has ζ_p as a root. Applying Exercise 4.7 again, we see that $g(z) - h(z)$ must be divisible by $\Phi_p(z)$. Therefore $g(z) - h(z)$ has each ζ_p^l as a root as well. □

Proposition 4.9 ([Gau66], art. 347)**.** *Suppose that $g(x_1, \ldots, x_f)$ is a symmetric polynomial in the variables $x_1, \ldots, x_f$, with integer coefficients. If we substitute for $x_1, \ldots, x_f$ the f roots contained in the period (f, ζ_p^k), then the resulting value $g(\zeta_p^k, \zeta_p^{kg^e}, \ldots, \zeta_p^{kg^{(f-1)e}})$ may be written as a sum of periods*

$$A + A_0(f, \zeta_p) + A_1(f, \zeta_p^g) + \cdots + A_{e-1}(f, \zeta^{g^{e-1}})$$

for integers $A, A_0, \ldots, A_{e-1}$.

Proof. Write

$$g(\zeta_p^k, \zeta_p^{kg^e}, \ldots, \zeta_p^{kg^{(f-1)e}}) = a + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}\,.$$

We need to prove that $a_i = a_{g^e i}$ for all i, where the subscripts are considered modulo p. By Corollary 4.8 applied with $l = g^e$, we have

$$g(\zeta_p^{kg^e}, \zeta_p^{kg^{2e}}, \ldots, \zeta_p^{kg^{fe}}) = a + a_1\zeta_p^{g^e} + \cdots + a_{p-1}\zeta_p^{(p-1)g^e}\,.$$

Since g is symmetric, the order of the arguments does not affect the value of the polynomial, and so

$$a + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1} = a + a_1\zeta_p^{g^e} + \cdots + a_{p-1}\zeta_p^{(p-1)g^e}\,.$$

By Corollary 4.5, the result follows. □

Corollary 4.10. *Retaining the hypotheses of Proposition 4.9, if we substitute for $x_1, \ldots, x_f$ the f roots contained in the period (f, ζ_p^{kl}) then the resulting value of g is equal to*

$$A + A_0(f, \zeta_p^l) + A_1(f, \zeta_p^{gl}) + \cdots + A_{e-1}(f, \zeta^{g^{e-1}l})$$

Proof. Immediate from Corollary 4.8. □

Corollary 4.11 ([Gau66], art. 348)**.** *Let $g(z)$ be the polynomial whose roots are the roots contained in the period (f, ζ_p^k). Then the coefficients of $g(z)$ are sums of periods of length f (plus an integer).*

Proof. Immediate from Proposition 4.9, since the coefficients of $g(z)$ are symmetric polynomials in the roots. □

Example 4.12. Let $g(z)$ be the polynomial whose roots are the roots contained in $((p-1)/2, \zeta_p)$. By Corollary 4.11, we can write

$$g(z) = R(z) + ((p-1)/2, \zeta_p)S(z) + ((p-1)/2, \zeta_p^g)T(z)$$

for polynomials R, S, T with integer coefficients. By Corollary 4.10, the polynomial $g'(z)$ whose roots are the roots contained in $((p-1)/2, \zeta_p^g)$ must be

$$g'(z) = R(z) + ((p-1)/2, \zeta_p^g)S(z) + ((p-1)/2, \zeta_p)T(z)\,.$$

Using the same proof as that of Proposition 4.9, we can prove a generalization:

Proposition 4.13 ([Gau66], art. 350)**.** *Suppose $f' \mid f$, and that the period (f, ζ_p^k) of length f breaks up into the periods*

$$(f', \zeta_p^k), (f', \zeta_p^{kg^e}), \ldots, (f', \zeta_p^{kg^{(d-1)e}})$$

where $df' = f$. If $g(x_1, \ldots, x_d)$ is a symmetric polynomial and we substitute for $x_1, \ldots, x_d$ the periods $(f', \zeta_p^k), \ldots, (f', \zeta_p^{kg^{(d-1)e}})$, then the resulting value may be written as a sum of periods

$$A + A_0(f, \zeta_p) + A_1(f, \zeta_p^g) + \cdots + A_{e-1}(f, \zeta^{g^{e-1}})\,.$$

We remark that Proposition 4.9 is precisely the case $f' = 1$ of Proposition 4.13.

Proof. The proof is precisely the same as that of Proposition 4.9, noting that if we replace ζ_p by $\zeta_p^{g^e}$ in the period $(f', \zeta_p^{kg^{ie}})$, it becomes $(f', \zeta_p^{kg^{(i+1)e}})$. □

Corollary 4.14 ([Gau66], art. 351)**.** *Suppose $f' \mid f$, and that the period (f, ζ_p^k) of length f breaks up into the periods*

$$(f', \zeta_p^k), (f', \zeta_p^{kg^e}), \ldots, (f', \zeta_p^{kg^{(d-1)e}})$$

where $df' = f$. Then the polynomial whose roots are $(f', \zeta_p^k), \ldots, (f', \zeta_p^{kg^{(d-1)e}})$ has coefficients which are sums of periods of length f (plus an integer).

Proof. As with Corollary 4.11, the proof is immediate from Proposition 4.13, since the coefficients of the polynomial are symmetric polynomials in the roots. □

Corollary 4.14 is the general analogue of the computations in Section 1.3. This enables us to prove:

Theorem 4.15 ([Gau66], art. 365)**.** *If p is a Fermat prime (a prime of the form $2^{2^m} + 1$), then the regular p-gon is constructible with straightedge and compass.*

Proof. Corollary 4.14 shows that each period $(2^n, \zeta_p^k)$ is the root of a quadratic polynomial whose coefficients are sums of periods of length 2^{n+1}. Since quadratics can be solved by straightedge and compass, and since the period $(2^{2^m}, \zeta_p) = -1$ is constructible, it follows recursively that all shorter periods $(2^n, \zeta_p^k)$ are constructible by straightedge and compass. In particular, the period $(1, \zeta_p) = \zeta_p$ is constructible, and therefore so is the regular p-gon. □

Gauss remarks that when p is not a Fermat prime, so that $p-1$ is divisible by a prime other than 2, then

> we can show with all rigor 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 time uselessly. [Gau66], *art. 365*

However, Gauss never published a proof of this claim; the first proof is now attributed to Pierre Wantzel, and may be found in almost any algebra textbook.

4.2. **Gauss Sums.** We saw in the previous section that the periods $((p-1)/2, \zeta_p)$ and $((p-1)/2, \zeta_p^g)$ will be the roots of a quadratic polynomial with integer coefficients. In this section, we will give Gauss's determination of this polynomial, and some of its implications. These arguments can be found in articles 356 and 357 of *Disquisitiones*.

We know that

$$((p-1)/2, \zeta_p) + ((p-1)/2, \zeta_p^g) = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1\,,$$

and so it remains to determine the product

$$((p-1)/2, \zeta_p) \cdot ((p-1)/2, \zeta_p^g)\,.$$

We follow the strategy sketched in Exercise 1.2 in the case $p = 17$. By Proposition 4.4, we have

$$((p-1)/2, \zeta_p) \cdot ((p-1)/2, \zeta_p^g) = a((p-1)/2, 1) + a_0((p-1)/2, \zeta_p) + a_1((p-1)/2, \zeta_p^g)$$

for integers a, a_0, a_1 satisfying $a + a_0 + a_1 = (p-1)/2$. By Corollary 4.8 applied with $l = g$, we have

$$((p-1)/2, \zeta_p^g) \cdot ((p-1)/2, \zeta_p^{g^2}) = a((p-1)/2, 1) + a_0((p-1)/2, \zeta_p^g) + a_1((p-1)/2, \zeta_p^{g^2})$$

and since $((p-1)/2, \zeta_p^{g^2}) = ((p-1)/2, \zeta_p)$ we get $a_0 = a_1$.

As noted in Exercise 1.2, the roots contained in $((p-1)/2, \zeta_p^g)$ are those of the form $\zeta_p^{g^i}$ for i odd, that is, they are of the form ζ_p^k for quadratic non-residues $k \pmod{17}$. Therefore

$$((p-1)/2, \zeta_p) \cdot ((p-1)/2, \zeta_p^g) = \sum_{(k/p)=-1} ((p-1)/2, \zeta_p^{k+1})$$

where the sum on the right-hand side is taken over quadratic non-residues k modulo p. It follows that at most one of the periods on the right-hand side can be $((p-1/2), 1)$; indeed, $a \leq 1$, and $a = 1$ and only if -1 is a quadratic non-residue $(\mathrm{mod}\ p)$.

Since $a_0 = a_1$ and $a + a_0 + a_1 = (p-1)/2$, it follows that $a \equiv (p-1)/2 \pmod 2$; we conclude that -1 is a quadratic non-reside (mod p) if and only if $a = 1$ if and only if $(p-1)/2$ is odd if and only if $p \equiv 3 \pmod 4$. This yields a sixth proof of Theorem 2.1. Moreover, we have

$$(a, a_0, a_1) = \begin{cases} (0, (p-1)/4, (p-1)/4) & \text{if } p \equiv 1 \pmod 4 \\ (1, (p-3)/4, (p-3)/4) & \text{if } p \equiv 3 \pmod 4 \end{cases}.$$

Since $((p-1)/2, 1) = (p-1)/2$ and $((p-1)/2, \zeta_p) + ((p-1)/2, \zeta_p^g) = -1$, we obtain

$$((p-1)/2, \zeta_p) \cdot ((p-1)/2, \zeta_p^g) = \begin{cases} -(p-1)/4 & \text{if } p \equiv 1 \pmod 4 \\ (p+1)/4 & \text{if } p \equiv 3 \pmod 4 \end{cases}.$$

We conclude that the two periods $((p-1)/2, \zeta_p), ((p-1)/2, \zeta_p^g)$ are roots of the quadratic equation

$$\begin{cases} x^2 + x - (p-1)/4 & \text{if } p \equiv 1 \pmod 4 \\ x^2 + x + (p+1)/4 & \text{if } p \equiv 3 \pmod 4 \,. \end{cases} \tag{4.16}$$

The roots of these equations are $\frac{-1 \pm \sqrt{p}}{2}$ if $p \equiv 1 \pmod 4$ and $\frac{-1 \pm i\sqrt{p}}{2}$ if $p \equiv 3 \pmod 4$, and so the difference

$$((p-1)/2, \zeta_p) - ((p-1)/2, \zeta_p^g) = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \,. \end{cases} \tag{4.17}$$

Exercise 4.18. Reformulate (4.17) as follows:

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \,. \end{cases}.$$

The sum on the left-hand side is called a *quadratic Gauss sum*.

Exercise 4.19. Prove that the quadratic Gauss sum $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k$ is equal to the exponential sum

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} \,.$$

(Hint: show that both sums are equal to $1 + 2((p-1)/2, \zeta_p)$.)

Exercise 4.20. Define the exponential sum

$$\tau_p(a) = \sum_{k=0}^{p-1} \zeta_p^{ak^2} \,. \tag{4.21}$$

If a is a quadratic residue mod p, show that $\tau_p(a) = \tau_p(1)$. If a is a quadratic non-residue mod p, show that

$$\sum_{k=0}^{p-1} \zeta_p^{ak^2}$$

is equal to $1 + 2((p-1)/2, \zeta_p^g) = -(1 + 2((p-1)/2, \zeta_p^g))$. Conclude that

$$\tau_p(a) = \left(\frac{a}{p}\right) \tau_p(1) \,. \tag{4.22}$$

It is natural to ask which sign holds in (4.17); for example, we saw in Section 1.3 that when $p = 17$, $(8, \zeta_{17}) - (8, \zeta_{17}^3) = +\sqrt{17}$. Gauss perceptively writes that "these matters are on a higher level of investigation"; indeed, as we will see in Section 4.4, the knowing the sign of the Gauss sum is essentially equivalent to quadratic reciprocity. We will give Gauss's determination of the sign of the Gauss sum in the next section.

For now, we give an interesting application of (4.17).

Definition 4.23. Let p^* denote $+p$ if $p \equiv 1 \pmod 4$ and $-p$ if $p \equiv 3 \pmod 4$, so that $((p-1)/2, \zeta_p) - ((p-1)/2, \zeta_p^g) = \sqrt{p^*}$ for all p. This notation is common, if not standard.

Exercise 4.24. In the notation of Example 4.12, show that

$$2g(z) = (2R(z) - S(z) - T(z)) \pm \sqrt{p^*}(S(z) - T(z))$$

and

$$2g'(z) = (2R(z) - S(z) - T(z)) \mp \sqrt{p^*}(S(z) - T(z)) \,.$$

Exercise 4.25. Conclude that

$$4\Phi_p(z) = (2R(z) - S(z) - T(z))^2 - p^*(S(z) - T(z))^2 \,.$$

In particular, this proves:

Proposition 4.26. *If $p \equiv 1 \pmod 4$, there exist polynomials $G(z)$ and $H(z)$ with integer coefficients such that*

$$4\Phi_p(z) = G(z)^2 - pH(z)^2 \,,$$

while if $p \equiv 3 \pmod 4$, there exist polynomials $G(z)$ and $H(z)$ with integer coefficients such that

$$4\Phi_p(z) = G(z)^2 + pH(z)^2 \,,$$

Exercise 4.27. What are the polynomials $G(z), H(z)$ for $p = 3, 5, 7, 11$?

Exercise 4.28. Prove that the two highest terms of $G(z)$ are $2z^{(p-1)/2} + z^{(p-3)/2}$, and that the highest term of $H(z)$ is $z^{(p-3)/2}$.

As promised in Section 3.1, we can use these ideas to prove quadratic reciprocity in the special case where $p \equiv 1 \pmod q$:

Proposition 4.29. *If p and q are primes and $p \equiv 1 \pmod q$, then $\left(\frac{q^*}{p}\right) = 1$. It follows that $\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$.*

Proof. Write $4\Phi_q(z) = G(z)^2 - q^*H(z)^2$. Since $q \mid p-1$, there exist $q-1$ elements of order $q \pmod p$. Since $H(z)$ has degree $(q-3)/2$, by Proposition 2.30 we can find an element a of order $q \pmod p$ such that $H(a) \not\equiv 0 \pmod p$. But $\Phi_q(a) = (a^q - 1)(a-1)^{-1} \equiv 0 \pmod p$, and so

$$G(a)^2 - q^*H(a)^2 \equiv 0 \pmod p \,,$$

or equivalently

$$(G(a)H(a)^{-1})^2 \equiv q^* \pmod p \,.$$

Hence $\left(\frac{q^*}{p}\right) = 1$ for all primes $q \mid p-1$. Since $q^* = (-1)^{\frac{q-1}{2}} q$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, the second statement of the Proposition follows from the first. □

4.3. **The sign of the Gauss sum.** In this section, we will prove:

Theorem 4.30.

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} = \begin{cases} +\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ +i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \,. \end{cases}$$

By Exercise 4.19, this immediately implies:

Corollary 4.31.

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k = \begin{cases} +\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ +i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \,. \end{cases}$$

Gauss conjectured this result in May 1801; he finally found a proof in August 1805, as noted in his mathematical diary:

> At length, we achieved a demonstration of the very elegant theorem mentioned before in May, 1801, which we had sought for more than four years with all efforts.

Gauss's proof was published in 1811 ([Gau11]). We provide a series of exercises which follow Berndt and Evans's treatment of the proof in [BE81]. The proof uses the so-called *q-binomial coefficients* (or *Gaussian polynomials*) to establish a product formula for the Gauss sum.

Definition 4.32. Set $(q)_n = (1-q)(1-q^2)\cdots(1-q^n)$, and define the Gaussian polynomial

$$\begin{bmatrix} n \\ m \end{bmatrix} = \frac{(q)_n}{(q)_m (q)_{n-m}} \,.$$

Exercise 4.33. Prove that $\begin{bmatrix} n \\ m \end{bmatrix}$ is a polynomial in the variable q.

Exercise 4.34. Prove the formula

$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} n-1 \\ m-1 \end{bmatrix} + q^m \begin{bmatrix} n-1 \\ m \end{bmatrix}$$

for $1 \le m < n$.

For a nonnegative integer n, define $f_n(q) = \sum_{k=0}^{n} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}$.

Exercise 4.35. Use Exercise 4.34 to prove the recursion formula $f_n(q) = (1 - q^{n-1}) f_{n-2}(q)$ for $n \ge 2$. Deduce that

$$f_{2n}(q) = \prod_{j=1}^{n} (1 - q^{2j-1}) \,. \tag{4.36}$$

Our product formula for the Gauss sum rests on evaluating $f_{p-1}(\zeta_p)$ in two different ways. First:

Exercise 4.37. Use the identity $2j - 1 = p - 1 - 2(p - j)$ in (4.36) to prove

$$f_{p-1}(\zeta_p) = \prod_{r=1}^{(p-1)/2} \zeta_p^{-r} (\zeta_p^r - \zeta_p^{-r}) \,.$$

Conclude, using Exercise 1.3, that

$$f_{p-1}(\zeta_p) = \zeta_p^{-(p^2-1)/8} (2i)^{(p-1)/2} \prod_{r=1}^{(p-1)/2} \sin(2\pi r/p) \,. \tag{4.38}$$

On the other hand, we have

Exercise 4.39. Prove directly from the definition that

$$\begin{bmatrix} p-1 \\ m \end{bmatrix}(\zeta_p) = (-1)^m \zeta_p^{-m(m+1)/2}\,.$$

Exercise 4.40. Use Exercise 4.39 to show

$$f_{p-1}(\zeta_p) = \sum_{k=0}^{p-1} \zeta_p^{-k(k+1)/2}\,. \tag{4.41}$$

Exercise 4.42. Manipulate (4.41) by noting that

$$-k(k+1)/2 \equiv \frac{(p-1)}{2} k(k+1) \pmod p\,,$$

completing the square in the exponent, and using (4.22) to prove that

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} = \zeta_p^{(p^2-1)/8} \left(\frac{(p-1)/2}{p}\right) f_{p-1}(\zeta_p)\,. \tag{4.43}$$

Exercise 4.44. Combine (4.38), (4.43), and a calculation of $\left(\frac{(p-1)/2}{p}\right) = \left(\frac{-2}{p}\right)$ to prove that

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} = (-1)^{(p-1)(p-3)/8} (2i)^{(p-1)/2} \prod_{r=1}^{(p-1)/2} \sin(2\pi r/p)\,. \tag{4.45}$$

Exercise 4.46. Finally, note that the product of sines in (4.45) is positive; use (4.45) to prove that $\sum_{k=0}^{p-1} \zeta_p^{k^2}$ is positive if $p \equiv 1 \pmod 4$, and is i times a positive real if $p \equiv 3 \pmod 4$. Use Exercises 4.18 and 4.19 to conclude that

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \end{cases}\,.$$

This completes the proof of Theorem 4.30.

Exercise 4.47. Note that we have also shown

$$\prod_{r=1}^{(p-1)/2} \sin(2\pi r/p) = \sqrt{p}$$

for all primes p.

4.4. **Gauss sums for Composite Moduli and Quadratic Reciprocity.** In his article [Gau11], Gauss considered the exponential sum

$$\tau_n(a) = \sum_{k=0}^{n-1} \zeta_n^{ak^2}$$

for composite n as well as prime n; this is necessary for Gauss's fourth proof of quadratic reciprocity via Gauss sums. We will prove:

Theorem 4.48. *If n is an odd positive integer, then*

$$\tau_n(1) = \sum_{k=0}^{n-1} \zeta_n^{k^2} = \begin{cases} \sqrt{n} & \text{if } n \equiv 1 \pmod 4 \\ i\sqrt{n} & \text{if } n \equiv 3 \pmod 4\,. \end{cases}$$

Gauss's proof, which we follow from [BEW98], follows the same outline for composite n as it does in the prime case: prove a product formula for a value of f_{n-1}; relate this value of f_{n-1} to the desired exponential sum, to determine its sign; and separately compute the magnitude of the exponential sum, thereby pinning down its exact value. It turns out that we want to use $f_{n-1}(\zeta_n^{-2})$ rather than $f_{n-1}(\zeta_n)$: this erases the $-1/2$ in the exponent $-k(k+1)/2$ of Exercise 4.40, which would be difficult to deal with because we do not have an analogue of (4.22) in the composite case. It is in this step, and in determining the magnitude of the exponential sum, that we used the primality of p.

We first note that the product formula is essentially unchanged in the composite case:

Exercise 4.49. Observe that the argument in Exercise 4.37 did not make use of the primality of p; show that

$$f_{n-1}(\zeta_n^{-2}) = \zeta_n^{(n^2-1)/4}(-2i)^{(n-1)/2} \prod_{r=1}^{(n-1)/2} \sin(4\pi r/n)\,. \tag{4.50}$$

Now we relate the product formula to the exponential sum:

Exercise 4.51. Verify, as in Exercise 4.40, that

$$f_{n-1}(\zeta_n^{-2}) = \sum_{k=0}^{n-1} \zeta_n^{k(k+1)}\,.$$

Note that $k(k+1) \equiv (k+(n+1)/2)^2 - (n+1)^2/4 \pmod n$, and show that

$$f_{n-1}(\zeta_n^{-2}) = \zeta_n^{-(n+1)^2/4} \sum_{k=0}^{n-1} \zeta_n^{k^2}\,. \tag{4.52}$$

Exercise 4.53. Combine (4.50) and (4.52) to obtain

$$\sum_{k=0}^{n-1} \zeta_n^{k^2} = (-2i)^{(n-1)/2} \prod_{r=1}^{(n-1)/2} \sin(4\pi r/n)\,. \tag{4.54}$$

Exercise 4.55. Verify that $\sin(4\pi r/p) > 0$ if $r < n/4$ and $\sin(4\pi r/p) < 0$ if $n/4 < r \le (n-1)/2$. Deduce that the product of sines in (4.54) is positive if $n \equiv 1, 7 \pmod 8$ and negative if $n \equiv 3, 5 \pmod 8$. Conclude that the right-hand side of (4.54) is a positive real number if $n \equiv 1 \pmod 4$ and i times a positive real number if $n \equiv 3 \pmod 4$.

Finally, we must show that in the composite case we still have $\left|\sum_{k=0}^{n-1} \zeta_n^{k^2}\right| = \sqrt{n}$. Observe that

$$\begin{aligned} \left|\sum_{k=0}^{n-1} \zeta_n^{k^2}\right| &= \left|\prod_{j=1}^{(n-1)/2} \left(1 - \zeta_n^{-2(2j-1)}\right)\right| \\ &= \left|\prod_{j=1}^{(n-1)/2} \left(1 - \zeta_n^{-(2j-1)}\right)\right| \cdot \left|\prod_{j=1}^{(n-1)/2} \left(-1 - \zeta_n^{-(2j-1)}\right)\right| \end{aligned} \tag{4.56}$$

by (4.52) and (4.36).

Exercise 4.57. Note that for each $1 \leq l \leq n-1$, the first product in the last line of (4.56) contains a term which is equal to $1-\zeta_n^j$ for exactly one of $j = l, n-l$. Similarly, for each $1 \leq l \leq n-1$, the second product in the last line of (4.56) contains a term which is equal to $-1-\zeta_n^j$ for exactly one of $j = l, n-l$. Prove the identities $|1-\zeta_n^l| = |1-\zeta_n^{n-l}|$ and $|-1-\zeta_n^l| = |-1-\zeta_n^{n-l}|$, and use them to deduce that

$$\left|\sum_{k=0}^{n-1} \zeta_n^{k^2}\right|^2 = \left|\prod_{j=1}^{n-1} \left(1-\zeta_n^j\right)\right| \left|\prod_{j=1}^{n-1} \left(-1-\zeta_n^j\right)\right| . \tag{4.58}$$

Since $\prod_{j=1}^{n-1} \left(z-\zeta_n^j\right) = z^{n-1} + z^{n-2} + \cdots + z + 1$, conclude that

$$\left|\sum_{k=0}^{n-1} \zeta_n^{k^2}\right|^2 = n \tag{4.59}$$

Finally, (4.59) and Exercise 4.55 together complete the proof of Theorem 4.48.

Gauss's fourth proof of quadratic reciprocity is now almost immediate. Following [Lem00], we show:

Lemma 4.60. *If m and n are relatively prime, we have*

$$\tau_{mn}(a) = \tau_m(an)\tau_n(am) .$$

Proof. Since m and n are relatively prime, we can write each $0 \leq k \leq mn-1$ as $k = \alpha m + \beta n$; moreover, as k runs from 0 to $mn-1$, the pairs (α, β) run over all mn distinct pairs of $\alpha \pmod n$ and $\beta \pmod m$. Therefore

$$\begin{aligned}
\tau_{mn}(a) &= \sum_{k=0}^{mn-1} \zeta_{mn}^{ak^2} \\
&= \sum_{\alpha=0}^{n-1} \sum_{\beta=0}^{m-1} \zeta_{mn}^{a(\alpha m+\beta n)^2} \\
&= \sum_{\alpha=0}^{n-1} \sum_{\beta=0}^{m-1} \zeta_{mn}^{a\alpha^2 m^2 + a\beta^2 n^2} \\
&= \left(\sum_{\alpha=0}^{n-1} \zeta_{mn}^{a\alpha^2 m^2}\right) \left(\sum_{\alpha=0}^{m-1} \zeta_{mn}^{a\alpha^2 n^2}\right) \\
&= \tau_n(am)\tau_m(an)
\end{aligned}$$

since $\zeta_{mn}^m = \zeta_n$ and $\zeta_{mn}^n = \zeta_m$. □

Now if p and q are distinct odd primes, we have

$$\tau_{pq}(1) = \tau_q(p)\tau_p(q) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\tau_q(1)\tau_p(1) \tag{4.61}$$

using Lemma 4.60 and (4.22). If $p, q \equiv 1 \pmod 4$, then Theorem 4.48 implies $\tau_{pq}(1) = \sqrt{pq}$, $\tau_p(1) = \sqrt{p}$, and $\tau_q(1) = \sqrt{q}$; therefore $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. If $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, then Theorem 4.48 implies $\tau_{pq}(1) = i\sqrt{pq}$, $\tau_p(1) = \sqrt{p}$, and $\tau_q(1) = i\sqrt{q}$; once again $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. Finally, if $p \equiv 1 \pmod 4$ and $q \equiv 3$

(mod 4), then Theorem 4.48 implies $\tau_{pq}(1) = \sqrt{pq}$, $\tau_p(1) = i\sqrt{p}$, and $\tau_q(1) = i\sqrt{q}$; so (4.61) tells us that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$. This proves quadratic reciprocity.

4.5. **Cubic periods.**

5. Gauss's First Proof of the Fundamental Theorem of Algebra

References

[BE81] Bruce C. Berndt and Ronald J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 107–129.

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998.

[Car60] L. Carlitz, *A note on Gauss' first proof of the quadratic reciprocity theorem*, Proc. Amer. Math. Soc. **11** (1960), 563–565.

[Cox77] H. S. M. Coxeter, *Gauss as a geometer*, Historia Math. **4** (1977), no. 4, 379–396.

[Dun04] G. Waldo Dunnington, *Carl Friedrich Gauss, Titan of science*, MAA Spectrum, Mathematical Association of America, Washington, DC, 2004, Reprint of the 1955 original [Exposition Press, New York], With an introduction and commentary by Jeremy Gray, With a brief biography of the author by Fritz-Egbert Dohse.

[Eul63] Leonhard Euler, *Novi comm. acad. Petrop.*, no. 8, 105–28.

[Gau08] Carl Friedrich Gauss, *Commentationes Societatis Regiae Scientiarum Gottingensis*, vol. Vol. 16, Göttingen, 1808.

[Gau11] ———, *Summatio quarumdam serierum singularium*, Comment. Soc. Reg. Sci. Gottingensis **1** (1811).

[Gau66] ———, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn., 1966.

[Lag75] Joseph-Louis Lagrange, *Nouv. mém. acad. Berlin*, 352ff.

[Leg98] Adrien Marie Legendre, *Essai sur la théorie des nombres*, Duprat, 1798.

[Lem00] Franz Lemmermeyer, *Reciprocity laws, from Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[Smi59] David Eugene Smith, *A source book in mathematics*, 2 vols, Dover Publications Inc., New York, 1959.