MATHEMATICAL PERSPECTIVES

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 53, Number 1, January 2016, Pages 117–120
http://dx.doi.org/10.1090/bull/1521
Article electronically published on September 4, 2015

ABOUT THE COVER: GAUSS AND THE *DISQUISITIONES ARITHMETICÆ*

GERALD L. ALEXANDERSON AND LEONARD F. KLOSINSKI

In 1801 Carl Friedrich Gauss published his *Disquisitiones Arithmeticæ* [3], perhaps the most important single work ever written in the theory of numbers. In this we find more than one proof of the Law of Quadratic Reciprocity, a statement about the integers that had been observed before, first by Euler (who else?). But Euler was not able to give an acceptable proof, and at this point we realize that Legendre had a proof but it was not very clear [2]. Clarity was left to Gauss. Then something odd happened. Once Gauss proved it, he proved it again. Mind you, this proof was not entirely independent of the first. But then in 1808 Gauss in another publication proved it again with a third proof and a fourth. Then he returned to it yet again, for a fifth proof and a sixth proof. What was going on? Did he deep down not understand why it worked and just kept trying to find out what the proof really should have been like in order to convince readers? After all, a person can prove something without understanding it very well. This happens to mere mortals all the time, offering a proof by contradiction, for example, that succeeds in proving a statement but gives little insight into why something is true. Was it bad notation? Was the problem approached from the wrong direction? Were there cases to which the proof did not apply? It's hard to know for sure, but what we do know is that Gauss kept trying and trying.

So what does it say? The best formulation and the one that explains the use of the word "reciprocity" is: if p and q are distinct odd primes, then

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

Now, what does $(\frac{n}{q})$ mean? It is called a Legendre symbol, and when it equals 1 it means that $x^2 \equiv n (\mathrm{mod}\, q)$, for at least one integer x; that is, n is congruent

©2015 American Mathematical Society

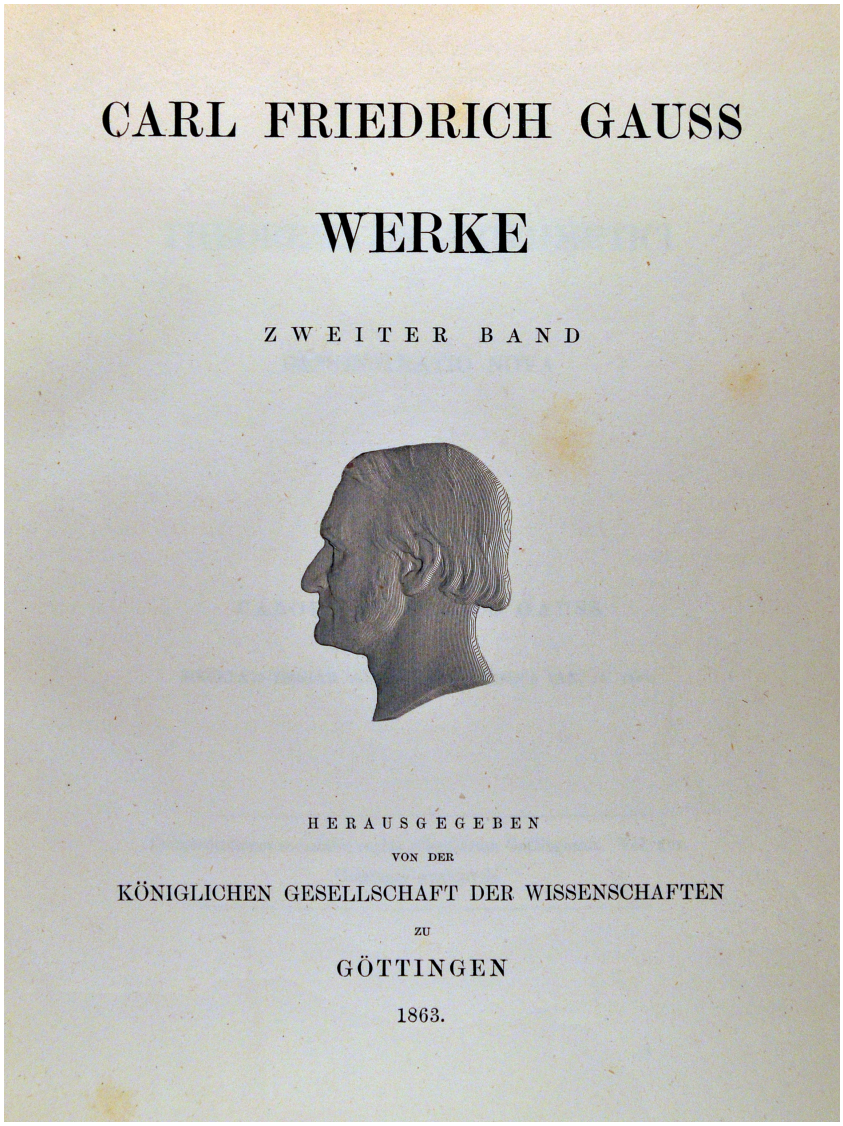

FIGURE 1. CLEAR COPY OF THE COVER. The title page of volume 2 of Gauss's complete works (1863), the volume containing his proof of the Law of Quadratic Reciprocity.

to a square of an integer, modulo q, but if it equals -1, then n is not congruent to a square. It allows one to find the squares in modular arithmetic, for given primes. For large primes this is, without this theorem, no easy task. Of course, it is possible to state the theorem without the Legendre symbol and in some ways it is more clear: If p and q are distinct odd primes, then the congruences

$$x^2 \equiv p(\mathrm{mod}\, q),$$
$$x^2 \equiv q(\mathrm{mod}\, p)$$

are both solvable or both unsolvable unless both p and q are of the form $4k + 3$, k an integer, in which case one of the congruences is solvable and the other is not. Without the Legendre symbol, the "reciprocity" is not so obvious. It should be kept in mind when exploring the history of the theorem that Euler and Legendre did not know the notation above since the congruence notation was first used by Gauss. On the other hand, Gauss could not have written it in the earlier form since he did not have available to him the Legendre symbol!

As mentioned earlier, Gauss first gave proofs of the law in his *Disquisitiones Arithmeticæ*, but then in 1808 he provided two new proofs in the offprint *Summatio quarumdam serierum singularium*, in a series made available by the Göttingen Academy of Sciences but not published in a regular mathematical journal [4]. It was published much later, however, in volume 2 of Gauss's *Werke* [5] (see Figure 1). He then published a fifth and a sixth proof. After his death two additional unpublished proofs were found in his papers.

What was it that drove Gauss to find additional proofs, one after another? He thought of them highly enough that he proceeded to publish them. The existing proofs at that time were not terribly difficult or complex but at the same time not transparent or obviously valid. Gauss, with all of his power as a mathematician—often referred to as one of the three greatest mathematicians of all time (along with Archimedes and Newton)—wrote at one point, "For a whole year this theorem tormented me and absorbed my greatest efforts until, at last, I obtained a proof . . . ." At that point the floodgates opened and many mathematicians joined in the effort to produce more proofs of the quadratic reciprocity law. The copy of the *Summatio* that the authors have was the one presented by Gauss to the French mathematician, Joseph Liouville (1809–1882), and is signed by Liouville on the cover sheet. Liouville proceeded some years later to publish his own proof of the theorem. And this has continued down to the present day. By 2000 there were 196 published proofs of the theorem [6].

An aside: The run of Gauss's *Werke* that we have is the set owned by Gaston Darboux (signed by Darboux on the first endpaper) who bought the volumes as they were issued. But there are only six volumes in the set, dated from 1863 to 1903. More were to follow—they continued to be issued until 1933—but those last volumes are not in our set. The missing volumes were explained by the dealer from whom they were purchased thus: Darboux bought the volumes as they were issued up until 1903, but then he died, at which point he stopped collecting.

But there was, of course, far more in the *Disquisitiones.* The middle sections were devoted to quadratic forms. But the last (and seventh) section raised the question of which regular polygons in the plane can be constructed by straightedge and compass, a problem deriving from a series studied by the Greeks about geometric constructions that can be carried out by using only a collapsible compass and an unmarked "ruler". Beyond the "doubling of the cube", the trisection of the angle, and the squaring of the circle—the three great problems that stymied the Greeks—there is this additional question about the constructability of regular polygons; that is, can we know the values of n for which the corresponding regular n-gon is constructible by straightedge and compass? Here is Gauss's startling conclusion: an n-gon is constructible if n is of the form $2^\alpha p_1 p_2 p_3 \cdots p_r$, where α is a nonnegative integer and the p_i are Fermat primes, that is, Fermat numbers of the form $2^{2^{k-1}} + 1$ that are actually primes. So in the formula for n there are lots of possibilities.

From the first factor, the power of 2, there are lots and lots of constructible regular polygons—a square, a regular octagon, and so on—no Fermat numbers involved. But the factors that follow, the Fermat numbers that happen to be prime, are not so common. The first Fermat prime, at least with the above notation, is the case where n is equal to 1 so the prime is $2^1 + 1$ is 3. So the equilateral triangle is constructible. Then for $n = 2$, the prime is 5, so the regular pentagon is constructible. And incidentally, since we can multiply these numbers by nonnegative powers of 2, we thus know, if Gauss's theorem is correct, that a regular hexagon is constructible and a regular 12-gon, and so on . . . , and the same sort of thing can be done with the regular pentagon to show that the regular 10-gon and regular 20-gon are constructible. Now let us go back to the third Fermat prime, 17, so the regular 17-gon is constructible since 17 is 2 to the fourth power plus 1. And it is prime. So we know about the 34-gon and the 68-gon. So far so good, but the next Fermat prime is 257 and now the simplest regular polygon is in this case getting to be rather large for the construction actually to be carried out. And the next Fermat prime is 65,537. One always constructs this regular polygon in a class by drawing a circle and calling it a regular 65,537-gon. No student in class can challenge it from the way it looks [1].

But here's the surprise. The families from those five Fermat primes, with their products and their powers of 2 out front, may be all there are. No other Fermat primes have ever been found, but even now it has not been possible to show that there are no more. So whether there are infinitely many Fermat primes (or even more than five) remains an open question. The next Fermat number after 65,537 is 4,294,967,297. It is tempting to assume that this must be prime, but Euler found a factor of it, 641, in 1732. At this point finding factors of Fermat numbers has grown into a cottage industry. Whether there are any further primes in the sequence remains an open question. Some conjecture, however, that the answer lies beyond current computing capabilities.

References

[1] Richard Courant and Herbert Robbins, *What Is Mathematics?*, Oxford University Press, New York, 1941, pp. 134–152. MR0005358 (3,144b)

[2] G. Waldo Dunnington, *Carl Friedrich Gauss: Titan of science. A study of his life and work*, Exposition Press, 1955; reprinted (with additional material by Jeremy Gray and Fritz-Egbert Dohse) by the Mathematical Association of America, Washington, DC, 2004, pp. 37–39, 76. MR0072814 (17,338f)

[3] Carl Friedrich Gauss, *Disquisitiones Arithmeticæ*, Fleischer, Leipzig, 1801.

[4] Carl Friedrich Gauss, *Summatio quarumdam serierum singularium, Exhibita Societati* D. XXIV, August (1808) (Commentationes Societatis Regiae Scientiarum Gottingensis Recentiores, Göttingen, 1811).

[5] Carl Friedrich Gauss, *Werke Zweiter Band*, Königlichen Wissenschaften zu Göttingen, 1863, pp. 9–25.

[6] Franz Lemmermeyer, *Reciprocity laws. From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000. MR1761696 (2001i:11009)

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, California

E-mail address: galexand@math.scu.edu

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, California

E-mail address: lklosinski@scu.edu