Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First*

David A. Cox

Abstract. This article explores the history of the Eisenstein irreducibility criterion and explains how Theodor Schönemann discovered this criterion before Eisenstein. Both were inspired by Gauss's *Disquisitiones Arithmeticae*, though they took very different routes to their discoveries. The article will discuss a variety of topics from 19th-century number theory, including Gauss's lemma, finite fields, the lemniscate, elliptic integrals, abelian groups, the Gaussian integers, and Hensel's lemma.

The Eisenstein irreducibility critierion is part of the training of every mathematician. I first learned the criterion as an undergraduate and, like many before me, was struck by its power and simplicity. This article will describe the unexpectedly rich history of the discovery of the Eisenstein criterion and in particular the role played by Theodor Schönemann.

For a statement of the criterion, we turn to Dorwart's 1935 article "Irreducibility of polynomials" in this MONTHLY [**9**]. As you might expect, he begins with Eisenstein:

> The earliest and probably best known irreducibility criterion is the Schoenemann-Eisenstein theorem:
>
> *If, in the integral polynomial*
>
> $$a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
>
> *all of the coefficients except a_0 are divisible by a prime p, but a_n is not divisible by p^2, then the polynomial is irreducible.*

Here's our first surprise—Dorwart adds Schönemann's name in front of Eisenstein's. He then gives a classic application:

> An important application of this theorem is the proof of the irreducibility of the so-called "cyclotomic polynomial"
>
> $$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1,$$
>
> where p is prime.

doi:10.4169/amer.math.monthly.118.01.003

*This paper originally appeared in the journal *Normat*, published by the Swedish National Center for Mathematics Education and the Mittag-Leffler Institute in cooperation with the Mathematical Societies of Denmark, Finland, Iceland, Norway, and Sweden. The author thanks the Editor of Normat for permission to reprint the article in this MONTHLY with minor changes from the original.

If, instead of $f(x)$, we consider $f(x+1)$, where

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + p,$$

the theorem is seen to apply directly, and the irreducibility of $f(x+1)$ implies the irreducibility of $f(x)$.

The combination "Schönemann-Eisenstein" (often "Schoenemann-Eisenstein") was common in the early 20th century. An exception is Dorrie's delightful book *Triumph der Mathematik*, published in 1933 [**8**], where he states the "Satz von Schoenemann." Another exception is van der Waerden's *Moderne Algebra* from 1930 [**29**], where we find the "Eisensteinscher Satz."[1]

Given the influence of van der Waerden's book on succeeding generations of textbook writers, we can see how Schönemann's name got dropped. But how did it get added in the first place? Equally important, how did Eisenstein's get added? And why both names? To answer these questions, we need to explore some 19th-century number theory. This is a rich subject, so by necessity my treatment will be far from complete. I will instead focus on specific highlights to trace the development of these ideas. There will be numerous quotes (translated into English when necessary[2]) to illustrate how mathematics was done at the time and what it looked like. We begin with Gauss.

GAUSS. *Disquisitiones Arithmeticae* [**13**], published in 1801, contains an amazing amount of mathematics. In particular, Gauss proves that when p is prime, the cyclotomic polynomial $x^{p-1} + \cdots + x + 1$ is irreducible. His proof uses an explicit representation of the roots and is not easy. However, he also uses the following general result that relates irreducibility over $\mathbb{Z}$ to irreducibility over $\mathbb{Q}$:

42.

If the coefficients $A, B, C \ldots N; a, b, c \ldots n$ of two functions of the form

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \ldots\ldots + N \ldots\ldots\ldots\ldots (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \ldots\ldots + n \ldots\ldots\ldots\ldots (Q)$$

are all rational and not all integers, and if the product of (P) and (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$$

then not all the coefficients $\mathfrak{A}, \mathfrak{B} \ldots \mathfrak{Z}$ can be integers.

This is what we now call *Gauss's lemma*. His proof is essentially the same one that appears in abstract algebra texts, though he states the result in the contrapositive form and never uses the term "polynomial." Gauss also doesn't use the three dots $\cdots$ that are standard today.

Another major result of *Disquisitiones* is Gauss's proof that $x^n - 1 = 0$ is solvable by radicals. The modern approach to solvability by radicals allows the introduction of arbitrary roots of unity, which implies that $x^n - 1 = 0$ is trivially solvable. Gauss instead followed the inductive strategy pioneered by Lagrange, where one constructs

[1] The 1930 edition included a reference to Schönemann that was dropped in the 1937 second edition.

[2] See `http://www.cs.amherst.edu/~dac/normat.pdf` for a version of the article that gives the quotes in their original languages.

the roots recursively using polynomials of strictly smaller degree that are solvable by radicals. In modern terms, this gives an explicit description of the intermediate fields of the extension

$$\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/p})$$

when p is prime. This has degree $p-1$ by the irreducibility of $x^{p-1}+\cdots+x+1$. From here, Gauss obtains his wonderful result about dividing the circle into n equal arcs by straightedge and compass.

The second paragraph of Section VII of *Disquisitiones* begins with a famous passage:

> The principles of the theory we are going to explain actually extend much farther than we will indicate. For they can be applied not only to circular functions but just as well to other transcendental functions, e.g. to those which depend on the integral $\int \frac{dx}{\sqrt{(1-x^4)}}$ and also to various types of congruences. Since, however, we are preparing a large work on those transcendental functions and since we will treat congruences at length in the continuation of these *Disquisitiones*, we have decided to consider only circular functions here.

In this quote, the reference to circular functions is clear. But what about transcendental functions that depend on the integral $\int \frac{dx}{\sqrt{1-x^4}}$? Here, any 19th-century mathematician would immediately think of the lemniscate $r^2 = \cos 2\theta$, whose arc length is $4\int_0^1 \frac{dx}{\sqrt{1-x^4}}$. This integral and its relation to the lemniscate were discovered by the Bernoulli brothers in the late 17th century and played a key role in the development of elliptic integrals by Fagnano, Euler, and Legendre in the 18th century. Gauss's "large work" on these functions never appeared, though fragments found after Gauss's death contain some astonishing mathematics (see [**3**]).

The quote also mentions "various types of congruences" that will be discussed "in the continuation of these *Disquisitiones*." The published version of *Disquisitiones* had seven sections, but Gauss drafted an eighth section, *Disquisitiones generales de congruentiis*, that studied polynomial congruences $f(x) \equiv 0 \bmod p$, where $f \in \mathbb{Z}[x]$ and p is prime (see pp. 212–242 of [**14**, vol. II] or pp. 602–629 of the German version of [**13**]). In modern terms, Gauss is studying the polynomial ring $\mathbb{F}_p[x]$. Here are some of his results:

- The existence and uniqueness of factorizations of polynomials modulo p.
- A formula for the number of monic irreducible degree-n polynomials modulo p. His result is

$$\frac{1}{n}\left(p^n - \sum p^{\frac{n}{a}} + \sum p^{\frac{n}{ab}} - \sum p^{\frac{n}{abc}} \text{ etc.}\right)$$

  where the sum $\sum p^{\frac{n}{a}}$ is over all distinct prime factors of n, $\sum p^{\frac{n}{ab}}$ is over all pairs of distinct prime factors of n, and similarly for the remaining terms in the formula.

Gauss also had a theory of finite fields, though his approach is not easy for the modern reader because of his reluctance to introduce roots of polynomial congruences. Here is what Gauss says about the congruence $\xi \equiv 0 \bmod p$, where ξ is a polynomial with integer coefficients:

> ... but nothing prevents us from decomposing ξ, nevertheless, into factors of two, three or more dimensions [degrees], whereupon, in some sense, *imaginary* roots could be attributed to them. Indeed, we could have shortened incomparably all our following investigations, had we wanted to introduce such imaginary quantities by taking the same liberty some more recent mathematicians have taken; ...

Over the complex numbers, Gauss was the first to prove the existence of roots of polynomials. He was critical of those who simply assumed that roots exist, so he clearly wasn't going to assume that congruences of higher degree have solutions.

We refer the reader to [**11**] for a fuller account of Gauss's work on finite fields. Unfortunately, none of this was available until after Gauss's death in 1855. In particular, Schönemann was unaware of these developments when he rediscovered many of Gauss's results in the 1840s.

ABEL. Gauss's cryptic comments about the integral $\int \frac{dx}{\sqrt{1-x^4}}$ in *Disquisitiones* had a profound influence on Abel. He developed the theory of elliptic functions (as did Jacobi), based on the equation

$$y^2 = (1 - c^2x^2)(1 + e^2x^2), \tag{1}$$

and his elliptic functions were inverse functions to the elliptic integrals

$$\int \frac{dx}{y} = \int \frac{dx}{\sqrt{(1 - c^2x^2)(1 + e^2x^2)}}. \tag{2}$$

Setting $e = c = 1$ gives $\int \frac{dx}{\sqrt{1-x^4}}$. In Abel's time, it was well known that this integral is intimately related to arc length on the lemniscate shown in Figure 1 (see [**3**] for the history of this relation).

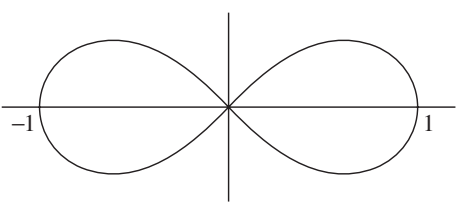

Figure 1. The lemniscate $r^2 = \cos 2\theta$.

It follows that dividing an arc of the lemniscate starting at the origin into m pieces of equal arc length can be interpreted as a relation between integrals, which Abel and Eisenstein would write as

$$\int_0 dy/\sqrt{1 - y^4} = m \int_0 dx/\sqrt{1 - x^4}. \tag{3}$$

This is the *m-division problem* for the lemniscate. When the entire lemniscate is divided into m pieces of equal length, equation (3) led Abel and Eisenstein (and Gauss before them, though unpublished) to a polynomial $P_m(x)$ of degree m^2 satisfied by the polar coordinates of the m-division points of the lemniscate. We will explain how this works when we discuss Eisenstein later in the article.

The mathematics involved here is surprisingly rich. The study of elliptic integrals such as (2) eventually become the study of *elliptic curves* such as (1). The book [**22**] gives a nice introduction to elliptic curves and their relation to elliptic integrals. These days, the m-division problem for elliptic integrals is described in terms of the m-division points on elliptic curves. See [**22**] and [**28**] for more on this important topic in modern number theory.

For Abel and his contemporaries, a central question was whether polynomial equations such as $P_m(x) = 0$ were "solvable algebraically," which these days means solvable by radicals. Abel was uniquely qualified to pose this question, since just four years earlier he had proved that the general quintic was not solvable by radicals.

In his great paper *Recherches sur les functions elliptiques* [**1**, pp. 263–388], published in volumes 2 and 3 of Crelle's journal[3] in 1827 and 1828, Abel considers the equation $P_{2n+1}(x) = 0$ coming from the $(2n + 1)$-division problem for the elliptic integral (2). Here is what he has to say about this equation:

> Thus finally the solution of the equation $P_{2n+1} = 0$ is reduced to a single equation of degree $2n + 2$; but *in general* this equation does not appear to be solvable algebraically. Nevertheless one can solve it completely in many particular cases, for example, when $e = c$, $e = c\sqrt{3}$, $e = c(2 \pm \sqrt{3})$ etc. In the course of this memoir I will concern myself with these cases, of which the first is especially remarkable, both for the simplicity of its solution, as well as by its beautiful application to geometry.
>
> Indeed among other theorems I arrived at this one:
>
> "One can divide the entire circumference of the lemniscate into m parts *by ruler and compass only*, if m is of the form 2^n or $2^n + 1$, the last number being at the same time prime, or if m is a product of several numbers of these two forms."
>
> This theorem is, as one sees, precisely the same as that of M. *Gauss*, relative to the circle.

The reduction to an equation of degree $2n + 2$ was done by classical methods of Lagrange. The mind-blowing result about ruler and compass constructions on the lemniscate ($e = c$) can be stated more formally as follows.

Abel's Theorem on the Lemniscate. *The lemniscate can be divided into m pieces of equal arc length by ruler and compass if and only if m is a power of* 2 *times a product of distinct Fermat primes.*

We will say more about Abel's theorem later in the article. Other aspects of Abel's quote are equally mind-blowing when considered from the modern perspective of elliptic curves:

- The cases $e = c$, $e = c\sqrt{3}$, $e = c(2 \pm \sqrt{3})$, etc. that Abel can solve by radicals correspond to elliptic curves with complex multiplication (see [**4**] for an introduction). Abel was the first to identify this important class of elliptic curves.
- By class field theory, division points of elliptic curves with complex multiplication generate abelian extensions and hence have abelian Galois groups. Since abelian groups are solvable, Galois theory implies that the division equations $P_{2n+1}(x) = 0$ are solvable by radicals.
- When the curve doesn't have complex multiplication, Abel was more cautious: they do "not appear to be solvable algebraically." By deep work of Serre on Galois

[3] The *Journal für die reine und angewandte Mathematik*, founded by August Leopold Crelle in 1826.

representations of elliptic curves [**27**], we now know that with at most finitely many exceptions, these equations aren't solvable by radicals.

Again we are in the presence of remarkably rich mathematics.

Abel thought deeply about why his equations $P_{2n+1}(x) = 0$ were solvable by radicals when the curve has complex multiplication. He realized that the underlying reason was the structure of the roots and how they relate to each other. His general result appears in his *Mémoire sur une classe particulière d'équations résolubles algébriquement* [**1**, pp. 478–507], which was published in Crelle's journal in 1829. The article begins:

> Although the algebraic solution of equations is not possible in general, there are nevertheless particular equations of all degrees which admit such a solution. Examples are the equations of the form $x^n - 1 = 0$. The solution of these equations is based on certain relations that exist among the roots.

The first sentence refers to Abel's result on the unsolvability of the general quintic and the solution of $x^n - 1 = 0$ described by Gauss in *Disquisitiones*. To give the reader a sense of what he means by "relations that exist among the roots," Abel takes a prime n and considers the cyclotomic equation $x^{n-1} + \cdots + x + 1 = 0$. Let $\theta(x) = x^\alpha$, where α is a primitive root modulo n. Then the roots are given by

$$x,\ \theta(x) = x^\alpha,\ \theta^2(x) = x^{\alpha^2},\ \theta^3(x) = x^{\alpha^3}, \ldots,\ \theta^{n-2}(x) = x^{\alpha^{n-2}},\ \text{where } \theta^{n-1}(x) = x.$$

Abel goes on to say that the same property appears in a certain class of equations that he found in the theory of elliptic functions. He then states the main theorem of the paper:

> In general I have proved the following theorem:
>
> „If the roots of an equation of arbitrary degree are related among themselves in such a way, that *all* of the roots can be rationally expressed in terms of one of them, which we designate by x; if in addition, designating by θx, $\theta_1 x$ two other arbitrary roots, one has
>
> $$\theta\theta_1 x = \theta_1\theta x,$$
>
> the equation in question is always solvable algebraically. . . ."

Abel's "classe particulière" consists of all polynomials that satisfy the hypothesis of his theorem. To see what this means in modern terms, let $K \subseteq L$ be a Galois extension with primitive element α. For each element σ_i of the Galois group $\mathrm{Gal}(L/K)$, there is a polynomial $\theta_i(x) \in K[x]$ such that $\sigma_i(\alpha) = \theta_i(\alpha)$. Then one easily computes that

$$\sigma_i\sigma_j(\alpha) = \theta_j(\theta_i(\alpha)).$$

The switch of indices is correct—you should check why. Since σ_i is determined by its value on α,

$$\sigma_i\sigma_j = \sigma_j\sigma_i \iff \theta_j(\theta_i(\alpha)) = \theta_i(\theta_j(\alpha)).$$

Since the $\theta_i(\alpha)$ are the roots of the minimal polynomial $f(x)$ of α over K, we see that $f(x)$ is in the "classe particulière" if and only if $\mathrm{Gal}(L/K)$ is commutative. Abel's

theorem now follows easily from Galois theory since commutative Galois groups are solvable.

Besides proving his general theorem, Abel intended to give two applications:

> After having developed this theory in general, I will apply it to circular and elliptic functions.

The version published in Crelle's journal has a section on circular functions, but ends with the following footnote by Crelle:

> *) The author of this memoir will give applications to elliptic functions on another occasion.

Alas, Abel died shortly after this article appeared.

AFTER ABEL. Abel's "classe particulière" had an important influence on Kronecker, Jordan, and Weber. Specifically:

- In 1853, Kronecker [**18**, vol. IV, p. 11] defined $f(x) = 0$ to be "abelian" provided it has roots $x, \theta(x), \ldots, \theta^{n-1}(x)$, $x = \theta^n(x)$. Here, as for Abel, θ is a rational function. This special case of Abel's "classe particulière" corresponds to polynomials with cyclic Galois groups.
- In 1870, Jordan [**17**, p. 287] defined $f(x) = 0$ to be "abelian" in terms of its Galois group:

  > We thus call *abelian equations* all of those whose group only contains substitutions that are exchangeable among each other.

  Here, "exchangeable" is Jordan's way of saying "commutative." He then proves [**17**, p. 288] that for irreducible equations, his definition is equivalent to Abel's "classe particulière."
- The first two volumes of Weber's monumental *Lehrbuch der Algebra* were published in 1894 and 1896. He gives the name "abelian" to Abel's "classe particulière" [**30**, vol. I, p. 576] and later defines a commutative group to be "abelian" [**30**, vol. II, p. 6]. As far as I know, this is the first appearence of the term "abelian group" in the modern sense.[4]

The definition of "abelian group" given in introductory algebra courses seems so simple. But in the background is a rich history involving Gauss, Abel, the leminiscate, elliptic functions, complex multiplication, and solvability by radicals.

SCHÖNEMANN. Unlike the other people mentioned so far, Theodor Schönemann is not a familiar name. He has no biography at the MacTutor History of Mathematics archive [**21**]. According to the *Allgemeine Deustsche Biographie* [**2**, vol. 32, pp. 293–294], Schönemann lived from 1812 to 1868 and was educated in Königsberg and Berlin under the guidance of Jacobi and Steiner. He got his doctorate in 1842 and became Oberlehrer and eventually Professor at a gymnasium in Brandenburg an der Havel. Lemmermeyer's book [**19**] includes several references to Schönemann's work in number theory, and some of his results are mentioned in Dickson's classic *History*

[4] In 1870, Jordan used the term "groupe abélien" to refer to a group closely related to a symplectic group over a finite field [**17**, Livre II, §VIII].

of the Theory of Numbers [**7**], especially in the chapter on higher congruences in the first volume.

For us, Schönemann's most important work is a long paper printed in two parts in Crelle's journal in 1845 and 1846. The first part [**24**], consisting of §§1–50, appeared as *Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist* (*Foundations of a general theory of higher congruences, whose modulus is a real prime number*). In the preface, Schönemann refers to Gauss:

> The famous author of *Disquisitiones Arithmeticae* had intended a general theory of higher congruences for Section Eight of his work. Since, however, this Section Eight did not appear, and also, as far as I know, the author did not publish anything on this subject, nor indicate anything precisely ...

Schönemann suspects that he may have been scooped by Gauss, but is not worried:

> ... the loss of first discovery would be compensated by my knowing of having met in my own and independent way such a spirit.

Indeed, Schönemann had been scooped by Gauss, and as we will see later in the article, also by Galois. Hence we should change "a spirit" to "spirits" in the quote, in which case the sentiment is even more apt.

Similar to what Gauss did, Schönemann gave a careful treatement of polynomials modulo p, including unique factorization. But then, in §14, he did something different. Let $f(x) \in \mathbb{Z}[x]$ be monic of degree n and irreducible modulo p, and let $\alpha \in \mathbb{C}$ be a root of $f(x)$ (proved to exist by Gauss). Given polynomials $\varphi, \psi \in \mathbb{Z}[x]$, Schönemann defined $\varphi(\alpha)$ and $\psi(\alpha)$ to be *congruent modulo* (p, α), written $\varphi(\alpha) \equiv \psi(\alpha) \pmod{p, \alpha}$, if $\varphi(\alpha) = \psi(\alpha) + pR(\alpha)$ for some $R \in \mathbb{Z}[x]$. He then proves that the "allgemeine Form eines kleines Restes" ("general form of a smallest remainder") is $a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1}$, where $a_i \in \{0, \ldots, p-1\}$. This gives a field with p^n elements.

We can recast Schönemann's construction as follows. The root α is an algebraic integer and $\mathbb{Z}[\alpha]$ is a ring under multiplication. The equivalence relation $\varphi(\alpha) \equiv \psi(\alpha) \pmod{p, \alpha}$ means that $\varphi(\alpha)$ and $\psi(\alpha)$ give the same coset in the quotient ring $\mathbb{Z}[\alpha]/\langle p\rangle$, where $\langle p\rangle = p\mathbb{Z}[\alpha]$ is the ideal generated by p. We will see later that $\mathbb{Z}[\alpha]/\langle p\rangle$ is a field since $f(x)$ is irreducible modulo p. Thus $\mathbb{Z}[\alpha]/\langle p\rangle$ is the modern version of Schönemann's finite field. In what follows, we will write $\mathbb{F}_{p^n}$ instead of $\mathbb{Z}[\alpha]/\langle p\rangle$ since this field has p^n elements.

Here are some other results proved by Schönemann:

- The elements of $\mathbb{F}_{p^n}$ are the roots of $x^{p^n} - x$. He wrote this as $x^{p^n} - x \equiv 0 \pmod{p, \alpha}$.
- $f(x) \equiv (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{n-1}}) \pmod{p, \alpha}$. Thus $\mathbb{F}_{p^n}$ is the splitting field of $f(x)$ modulo p. The Galois group (generated by Frobenius) is implicit in this factorization of f.

The first part of Schönemann's paper culminates in §50 with a lovely proof of the irreducibility of $\Phi_p(x) = x^{p-1} + \cdots + x + 1$. We will give the proof in modern notation. Pick a prime $\ell \neq p$ and consider the prime factorization

$$\Phi_p(x) \equiv f_1(x) \cdots f_r(x) \bmod \ell.$$

where the f_i are irreducible modulo ℓ. Standard properties of finite fields imply that for $i = 1, \ldots, r$,

$$\begin{aligned}\deg(f_i) &= \text{the minimum } n \text{ such that } \mathbb{F}_{\ell^n}^* \text{ has an element of order } p \\ &= \text{the minimum } n \text{ such that } \ell^n \equiv 1 \bmod p \\ &= \text{the order of the congruence class of } \ell \text{ in } (\mathbb{Z}/p\mathbb{Z})^*.\end{aligned} \tag{4}$$

We leave this as a fun exercise for the reader. By Dirichlet's theorem on primes in arithmetic progressions (proved just a few years before Schönemann's paper), every congruence class modulo p contains a prime. In particular, the congruence class of a primitive root contains a prime ℓ. A primitive root modulo p gives a congruence class of order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^*$, so that $n = p-1$ in (4) for this choice of ℓ. This implies that $\Phi_p(x)$ is irreducible modulo ℓ and hence irreducible over $\mathbb{Z}$. Then $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ by Gauss's lemma.

This proof is simpler than Gauss's, though it does require knowledge of finite fields and uses Dirichlet's classic result. The use of the auxiliary prime ℓ is especially elegant. When I studied Grothendieck-style algebraic geometry as a graduate student in the 1970s, I was always happy when a proof picked a prime different from the residue characteristic. This seemed so modern and cutting-edge. Little did I realize that Schönemann had used the same idea 120 years earlier.

The second part of Schönemann's paper [**25**], titled *Von denjenigen Moduln, welche Potenzen von Primzahlen sind* (*On those moduli, which are powers of prime numbers*), consists of §§51–66. In this paper, Schönemann considered the factorization of polynomials modulo p^m, and in particular, how the factorization changes as m varies. One of his major results, in §59, is what we now call *Hensel's lemma*:

> Lemma. If any monic polynomial[5] of x can be factored modulo p into two monic factors, which for this modulus have no common divisor: then this polynomial can be factored modulo p^m, ***in a unique manner***, into two factors, which are congruent to those first two factors modulo p.[6]

As a consequence, when an irreducible polynomial modulo p^m is reduced modulo p, the result must be a power of an irreducible polynomial modulo p. In §61, Schönemann asks about the converse:

> Problem. To investigate, whether the power of an irreducible polynomial modulo p is or is not irreducible modulo p^m.

An especially simple example is $(x-a)^n$, and for a polynomial congruent to $(x-a)^n$ modulo p, the first place to check for irreducibility is modulo p^2. Here is Schönemann's answer:

> ... hence one may state the theorem: ***that $(x-a)^n + pFx$ is irreducible modulo p^2, when the factor $x-a$ is not contained in Fx modulo p***....

[5] Schönemann used "Ausdruck" ("expression") for polynomial and "einfach" ("simple") for monic.

[6] The uniqueness assertion enables us to take the limit as $m \to \infty$, giving a factorization over the p-adic integers $\mathbb{Z}_p$ that reduces to the given factorization modulo p. This version of Hensel's lemma is stated in [**16**, Thm. 3.4.6], and the discussion on [**16**, p. 72] relates this to the more common version of Hensel's lemma, which asserts that for $f(x) \in \mathbb{Z}_p[x]$, a solution of $f(x) \equiv 0 \bmod p$ of multiplicity one lifts to a solution of $f(x) = 0$ in $\mathbb{Z}_p$.

As stated, this is not quite correct—one needs to assume that $\deg(F) \le n$.[7] Since $x - a$ divides $F(x)$ modulo p if and only if $F(a) \equiv 0 \bmod p$, we can state Schönemann's result as follows.

Schönemann's Irreducibility Criterion. *Let $f(x) \in \mathbb{Z}[x]$ have degree $n > 0$ and assume that there is a prime p and an integer a such that*

$$f(x) = (x - a)^n + pF(x), \quad F(x) \in \mathbb{Z}[x].$$

If $F(a) \not\equiv 0 \bmod p$, then $f(x)$ is irreducible modulo p^2.

We sketch a proof for the convenience of the reader.

Proof. Suppose $(x - a)^n + pF(x)$ has a nontrivial factorization modulo p^2, say

$$(x - a)^n + pF(x) \equiv G(x)H(x) \bmod p^2. \tag{5}$$

One can easily reduce to the case where $G(x)$ and $H(x)$ are monic. Then $(x - a)^n \equiv G(x)H(x) \bmod p$ and unique factorization imply $G(x) \equiv (x - a)^i \bmod p$ and $H(x) \equiv (x - a)^j \bmod p$, where $i, j > 0$ and $i + j = n$. Setting $x = a$ in these congruences, we see that p divides both $G(a)$ and $H(a)$ since $i, j > 0$. Then setting $x = a$ in (5) implies $pF(a) \equiv 0 \bmod p^2$, a contradiction. ∎

The pleasant surprise is that this result implies the Eisenstein criterion. To see why, suppose that $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ satisfies the hypothesis of the Eisentstein criterion. Multiplying by a suitable integer, we may assume $a_0 \equiv 1 \bmod p$. This allows us to write $f(x) = x^n + pF(x)$. Note also that $F(0) \not\equiv 0 \bmod p$ since p^2 does not divide a_n. Then $f(x)$ is irreducible modulo p^2 by Schönemann's criterion. This implies irreducibility over $\mathbb{Z}$ and hence over $\mathbb{Q}$ by Gauss's lemma.

As you might expect, Schönemann immediately applies his irreducibility criterion to a familiar polynomial:

> Let us apply the result just obtained to the expression $\dfrac{x^n - 1}{x - 1}$, where n denotes a prime number. In this case $x^n - 1 \equiv (x - 1)^n$ (mod. n), and one thus obtains
>
> $$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = (x - 1)^{n-1} + nFx.$$
>
> For $x = 1$ one obtains $n = nF(1)$ and thus $F(1) = 1$, and not $\equiv 0$ (mod. n). ***From this, it follows that $\dfrac{x^n - 1}{x - 1}$ is always irreducible modulo n^2, if n is a prime number; hence, this expression is certainly irreducible in the algebraic sense.***
>
> The ease of proof of this theorem is striking, because the proof in „Disquisitiones" requires much greater cleverness, and is much more elaborate. (See §. 50. Rem. 2.)

This proves the irreducibility of $x^{n-1} + \cdots + x + 1$ without the change of variable $x \leftrightarrow x + 1$ needed when one uses the Eisenstein criterion. Schönemann is clearly

[7] For example, let $F(x) = x^3 - p^2x + 1$. Then $x^2 + pF(x) = (px + 1)(x^2 - p^2x + p)$ even though $F(0) \not\equiv 0 \bmod p$.

pleased that his proof is so much simpler than Gauss's. (The parenthetical comment at the end of the quote refers to Schönemann's earlier proof of irreducibility from §50 of his article.)

Schönemann's criterion is lovely but is unknown to most mathematicians. So how did I learn about it? My book on Galois theory [**5**] gives Eisenstein's proof of Abel's theorem on the lemniscate. In trying to understand Eisenstein, I looked at Lemmermeyer's wonderful book *Reciprocity Laws* [**19**], where I found a reference to Schönemann. When I tried to read Schönemann's paper, I couldn't find the Eisenstein criterion, in part because the paper is long and my German isn't very good, and in part because I was looking for Eisenstein's version, not Schönemann's. I looked back at Lemmermeyer's book and noticed that Lemmermeyer thanked Michael Filaseta for the Schönemann reference. I wrote to Filaseta, who replied that Schönemann proved a criterion for a polynomial to be irreducible modulo p^2. This quickly led me to §61 of the article, which is where Schönemann states his result.

BACK TO GAUSS. Besides discovering the Eisenstein criterion before Eisenstein, Schönemann also discovered Hensel's lemma before Hensel. Unfortunately, Schönemann and Hensel were both scooped by Gauss. In his draft of the unpublished eighth section of *Disquisitiones* (p. 627 of the German version of [**13**] or p. 238 of [**14**, vol. II]), Gauss takes a polynomial X with integer coefficients and studies its behavior modulo p and p^2:

> PROBLEM. *If the function X decomposes modulo p into mutually prime factors ξ, ξ', ξ'' etc., then similarly X decomposes modulo p^2 into factors Ξ, Ξ', Ξ'' etc. such that*
>
> $$\xi \equiv \Xi,\ \xi' \equiv \Xi',\ \xi'' \equiv \Xi'',\ \text{etc. (mod. } p)$$

Gauss proves this and then explains how the same principle applies modulo p^k for any k. His "PROBLEM" is weaker than Schönemann's "Lemma" because it doesn't say that the lifted factorization is unique. So what Gauss really proved was a "proto-Hensel's lemma." Nevertheless, Gauss was sufficiently pleased with this result that he recorded it in his famous mathematicial diary [**15**]. Here is entry 79, dated September 9, 1797:

> Beginning to uncover principles, by which the resolution of congruences according to multiple moduli is reduced to congruences according to linear moduli.

Here, "resolution of congruences according to multiple moduli" means factoring polynomials modulo p^k, and similarly "congruences according to linear moduli" means working modulo p. This reading of Gauss's diary entry is carefully justified in [**11**].

Besides this elementary version of Hensel's lemma, Gauss also considered the case when the factors modulo p are not distinct. For example, the congruence $X \equiv X'(x-a)^m$ (mod. p) appears near the end of Gauss's draft of the eighth section. Had he pursued this, it is quite possible that he would have followed the same path as Schönemann and discovered the Eisenstein criterion. But instead, the draft ends abruptly in the middle of a congruence: the last thing Gauss wrote was

$$0 \equiv$$

As with many other projects, Gauss never returned to finish *Disquisitiones generales de congruentiis*. It came to light only after being published in 1863 in the second volume of his collected works, and today is still overshadowed by its more famous sibling, *Disquisitiones Arithmeticae*.

MORE ON FINITE FIELDS. Besides Gauss and Schönemann, Galois also developed the theory of finite fields. In his paper *Sur la théorie des nombres*, appearing in 1830 in the *Bulletin des sciences mathématiques de Ferussac* [**12**, pp. 113–127], Galois begins with a congruence $F(x) \equiv 0 \bmod p$, or as he writes it, $Fx = 0$, where $F(x)$ is irreducible modulo p. Then he considers the roots:

> One must regard the roots of this congruence as a kind of imaginary symbol . . .

He then goes on to prove the results about finite fields discovered later by Schönemann. It appears that Schönemann was unaware of Galois's work.

Gauss would have been critical of the roots so blithely assumed to exist by Galois. Schönemann's construction via $\mathbb{Z}[\alpha]/\langle p\rangle$, on the other hand, is rigorous since it uses a root $\alpha \in \mathbb{C}$ of $f(x)$. However, the fundamental theorem of algebra is really a theorem in analysis since it ultimately depends on the completeness of the real numbers. For an algebraic version of Schönemann's construction, note that since $f(x) \in \mathbb{Z}[x]$ is monic and irreducible, $x \mapsto \alpha$ induces a ring isomorphism

$$\mathbb{Z}[x]/\langle f(x)\rangle \simeq \mathbb{Z}[\alpha].$$

Reducing $f(x)$ modulo p gives a polynomial $\bar{f} \in \mathbb{F}_p[x]$, which Schönemann assumed to be irreducible. It follows that the quotient ring $\mathbb{F}_p[x]/\langle \bar{f}(x)\rangle$ is a field. Then the isomorphisms

$$\mathbb{F}_p[x]/\langle \bar{f}(x)\rangle \simeq \mathbb{Z}[x]/\langle p,\, f(x)\rangle \simeq \mathbb{Z}[\alpha]/\langle p\rangle$$

show that Schönemann's ring $\mathbb{Z}[\alpha]/\langle p\rangle$ is in fact a finite field with p^n elements.

This algebraic version of finite fields was made explicit by Dedekind in his 1857 paper *Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus* (*Outline of a theory of higher congruences for a real prime modulus*) [**6**]. Dedekind begins the paper by noting that the subject was initiated by Gauss and had been studied by Galois and Schönemann. Dedekind was unaware of the full power of what Gauss had done, though later he became the editior in charge of publishing *Disquisitiones generales de congruentiis* in volume II of Gauss's collected works in 1863.

Dedekind's construction is essentially what we did above with the quotient ring $\mathbb{Z}[x]/\langle p,\, f(x)\rangle$, $f(x)$ irreducible modulo p, though Dedekind was writing before the concept of quotient ring was fully established. Nevertheless, he shows that this is a finite field with p^n elements, $n = \deg(f)$. For much of the 19th century, "finite field" meant this object. It has the advantage of being easy to compute with (even today, computers represent finite fields this way), but mathematically, it depends on the choice of $f(x)$ and hence is intrinsically noncanonical.

One of the first fully abstract definitions of finite field was given by E. H. Moore, whose paper [**20**] appeared in the proceedings of the 1893 international congress of mathematicians. Here is his definition:

> Suppose that we have a system of s distinct symbols or *marks**, $\mu_1, \ldots, \mu_s$ (s being some finite positive integer), and suppose that these marks may be combined by the four fundamental operations of algebra—addition, subtraction, multiplication, and division—these operations being subject to the ordinary abstract *operational identities* of algebra
>
> $$\mu_i + \mu_j = \mu_j + \mu_i;\ \mu_i\mu_j = \mu_j\mu_i;\ (\mu_i + \mu_j)\mu_k = \mu_i\mu_k + \mu_j\mu_k;\ \text{etc.}$$

and that when the marks are so combined the results of these operations are in every case uniquely determined and belong to the system of marks. Such a system we shall call a *field of order s*, using the notation $F[s]$.

We are led at once to seek *To determine all such fields of order s*, $F[s]$.

The words "system" and "marks" indicate that Moore was writing before the language of set theory was standardized. Moore went on to show that his definition was equivalent to the Dedekind-style representation of a finite field. So in 1893 we finally have a modern theory of finite fields.

The word "marks" in Moore's quote has an the asterisk that leads to the following footnote:

* It is necessary that all *quantitative* ideas should be excluded from the concept *marks*. Note that the signs $>$, $<$ do not occur in the theory.

Moore was writing for a mathematically sophisticated audience, but he didn't assume that they had the apparatus of set theory in their heads—his footnote was intended to help them understand the abstract nature of what he was saying. This is something we should keep in mind when we teach abstract algebra to undergraduates.

EISENSTEIN. We finally get to Eisenstein, whose work on Abel's theorem on the lemniscate culminated in a long two-part paper in Crelle's journal in 1850 [**10**, pp. 536–619]. To set the stage, we use the polar equation $r^2 = \cos 2\theta$ of the lemniscate and regard r as a function of arc length s. Thus

$$r = \varphi(s)$$

means that if we start at the origin and follow the branch of the lemniscate in the first quadrant for distance s, then we end at a point with polar coordinates (r, θ). Figure 2 shows what happens when we follow the curve into the fourth quadrant.

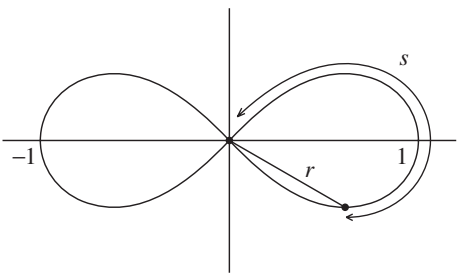

Figure 2. $r = \varphi(s)$ on the lemniscate.

An arc length calculation (see [**5**, §15.2]) shows that s is related to r via the equation

$$s = \int_0^r \frac{dr}{\sqrt{1 - r^4}}.$$

(We follow the 19th-century practice of using the same letter for the variable and limit of integration.) Combining this with $r = \varphi(s)$, we obtain

$$r = \varphi(s) \iff s = \int_0^r \frac{dr}{\sqrt{1 - r^4}}. \tag{6}$$

In other words, the lemniscatic function $r = \varphi(s)$ is the inverse function of the elliptic integral $\int_0^r \frac{dr}{\sqrt{1-r^4}}$ we first met in Section VII of *Disquisitiones*.

In the equation (6), $0 \le r \le 1$ corresponds to $0 \le s \le \varpi = \int_0^1 \frac{dr}{\sqrt{1-r^4}}$, so that ϖ is one-fourth of the total arc length of the lemniscate. In particular, $\varphi(\varpi) = 1$ and $\varphi(2\varpi) = 0$, and for any positive integer m, the radii $r = \varphi(k \cdot 2\varpi/m)$, $k = 1, \ldots, m$, give the points that divide the right half of the lemniscate into m equal pieces.

The change of variables $r = iu$ in (6) led Abel to define $\varphi(is) = i\varphi(s)$, and then Euler's addition law makes $\varphi(z) = \varphi(s + it)$ into a function of a complex variable $z \in \mathbb{C}$.[8] Further application of the addition law shows that for any Gaussian integer $m \in \mathbb{Z}[i]$, $\varphi(mz)$ is a rational function of $\varphi(z)$ and its derivative $\varphi'(z)$. This is what *complex multiplication* means for the lemniscatic function φ.

If $m = a + ib$ is an *odd* Gaussian integer, meaning that $a + b$ is odd, then $\varphi(mz)$ is a rational function of $\varphi(z)$ of a very special form. More precisely, given such an m, there are polynomials $U(x)$ and $V(x)$ with coefficients in $\mathbb{Z}[i]$ such that $y = \varphi(mz)$ is related to $x = \varphi(z)$ via

$$y = \frac{U(x)}{V(x)} = \frac{A_0 x + A_1 x^5 + \cdots + A_{(N(m)-1)/4} x^{N(m)}}{1 + B_1 x^4 + \cdots + B_{(N(m)-1)/4} x^{N(m)-1}}, \tag{7}$$

where $N(m) = a^2 + b^2$ is the norm (in the sense of algebraic number theory) of $m = a + ib$. A modern proof can be found in [**5**, Thm. 15.4.4]. Using (6), we obtain

$$\int_0^y \frac{dy}{\sqrt{1-y^4}} = m \int_0^x \frac{dx}{\sqrt{1-x^4}} \iff y = \frac{U(x)}{V(x)}.$$

In 19th-century parlance, the relation $y = U(x)/V(x)$ is an *algebraic integral* of this equality of integrals. This explains equation (3) from earlier in the article.

When m is an ordinary odd integer, we know that $r = \varphi(k \cdot 2\varpi/m)$ gives m-division points on the lemniscate. Substituting

$$y = \varphi(m \cdot (k \cdot 2\varpi/m)) = \varphi(k \cdot 2\varpi) = 0 \text{ and } x = \varphi(k \cdot 2\varpi/m) = r$$

into (7), we see that

$$0 = \frac{U(r)}{V(r)}, \text{ hence } U(r) = 0.$$

This proves that the division radii r are roots of the polynomial equation $U(x) = 0$. When $m = 2n + 1$, this is *precisely* the equation $P_{2n+1}(x) = 0$ considered by Abel.

Eisenstein used the same setup as Abel. To prove Abel's theorem on the lemniscate, he reduced to the case when $m = a + ib$ is an odd Gaussian prime. Since $U(x)$ has x as a factor, Eisenstein wrote $U(x) = xW(x)$, and the strategy of his proof was to show that $W(x)$ is irreducible. Once this is proved, Abel's theorem follows—see [**5**, §15.5].[9]

But how did Eisenstein prove that the polynomial $W(x)$ is irreducible? This is not easy. A key step for Eisenstein was when he noticed something about the coefficients of $W(x)$. He shared his thoughts with Gauss in a letter dated 18 August 1847 [**10**, p. 845]:

[8] Gauss followed the same path in 1797, though he never published his findings. See [**3**] for more details.

[9] For a complete proof of Abel's theorem on the lemniscate, the reader should consult [**5**], [**22**], or [**23**]. The last reference gives a modern proof via class field theory.

When $m = a + bi$ is an odd complex integer of norm p and $y = \dfrac{U}{V} = \dfrac{A_0x + A_1x^5 + \cdots + A_{(p-1)/4}x^p}{1 + B_1x^4 + \cdots + B_{(p-1)/4}x^{p-1}}$ is the algebraic integral of the equation

$$\int_0 dy/\sqrt{1-y^4} = m \int_0 dx/\sqrt{1-x^4},$$

I had earlier shown that for a *two-term* complex prime number m the coefficients of the numerator up to the last, which is a complex unit, and the coefficients of the denominator except the first, which $= 1$, are all divisible by m. I conjectured that this proposition is also correct when m is a *one-term* prime number ($\equiv 3 \pmod 4$ apart from sign or a complex unit as factor);

In the first part of the quote, Eisenstein sets up the situation, and after the displayed equation, describes the structure of the coefficients of the numerator and denominator. Recall that odd Gaussian primes come in two flavors:

- *Two-term* primes of the form $m = a + ib$, where $p = a^2 + b^2$ is prime and $p \equiv 1 \bmod 4$.
- *One-term* primes of the form $m = \varepsilon q$, where ε is a unit in $\mathbb{Z}[i]$ and $q \equiv 3 \bmod 4$.

Now consider the polynomial

$$W(x) = \frac{1}{x}U(x) = A_0 + A_1x^4 + \cdots + A_{(p-1)/4}x^{p-1}.$$

For a two-term prime m, Eisenstein says that he earlier had shown that the last coefficient $A_{(p-1)/4}$ is a complex unit and the other coefficients $A_0, \ldots, A_{(p-1)/4-1}$ are divisible by m. He conjectures that the same is true for one-term primes.

This smells like the Eisenstein criterion, especially since Eisenstein notes in the letter that the constant term A_0 is m, which is not divisible by m^2. The difference is that m and the coefficients of W are Gaussian integers. A bit later in the letter, Eisenstein considers what happens if W is not irreducible over $\mathbb{Q}(i)$ [**10**, pp. 848–849]:

> ... if it is possible that W is the product of two polynomials[10] of x with Gaussian integer coefficients, and their degrees are $< p - 1$. Let $W = PQ$; since the constant term of W is $= m$, so if m is a complex prime, the constant term in one of the two polynomials P, Q is $= 1$ and the other $= m$; then the coefficients of P and Q if rational, must necessarily be integral, as one can show by the same considerations which your Eminence[11] used in the real number theory (Disq. Section I).

Here, "real number theory" means over $\mathbb{Z}$ rather than $\mathbb{Z}[i]$, and the reference to *Disquisitiones* is the first Gauss quote of this article. Thus Eisenstein is telling Gauss that

[10] Eisenstein used the term "rationalen ganzen Funktionen" ("rational entire functions").

[11] The German original says "Ew. Hochwohlgeboren," which translates literally as "your High Well Born." The word "Hochwohlgeboren" originally applied to lesser German nobility and gentry. This flowery language is reflected in the letter's salutation, "Sr. Hochwohlgeboren, dem Geheimrath pp. Prof. Dr. Gauss," which translates "To his Eminence, the Distinguished, and so on, Professor Doctor Gauss." The word "Geheimrath," now spelled "Geheimrat," originated as the German equivalent of a "Privy councillor" in the middle ages and was an honorific for distinguished professors in German universities in the 19th century.

Gauss's lemma applies to the Gaussian integers. Mind-blowing. Then Eisenstein proceeds to prove that W is irreducible using one of the standard proofs of the Eisenstein criterion.[12] In other words, Eisenstein's first proof of his criterion

- was over the Gaussian integers;
- applied to a polynomial associated with the division problem on the lemniscate; and
- appeared in a letter to Gauss.

When Eisenstein wrote up his results for publication, he realized that his criterion was much more general. The first part of his 1850 paper had the title *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt* (*On the irreducibility and some other properties of equations that depend on the division of the lemniscate*) [**10**, pp. 536–555]. This paper contains Eisenstein's version of the Eisenstein criterion:

> „If in a polynomial $F(x)$ of x of arbitrary degree the coefficient of the highest „term is $= 1$, and all following coefficients are integers (real or complex), in „which a certain (real resp. complex) prime number m appears, if further the last „coefficient is $= \varepsilon m$, where ε represents a number not divisible by m: then it is „impossible to bring $F(x)$ into the form
>
> $$(x^{\mu} + a_1 x^{\mu-1} + \ldots . + a_{\mu})(x^{\nu} + b_1 x^{\nu-1} + \ldots . + b_{\nu})$$
>
> „where μ and $\nu \geq 1$, $\mu + \nu =$ the degree of $F(x)$, and all a and b are (real resp. „complex) ***integers***; and the equation $F(x) = 0$ is accordingly irreducible."[13]

(This quote uses the same format that Eisenstein used in his paper.)

After giving the proof, Eisenstein applies his criterion to the equation $W = 0$ that arises from division of the lemniscate and also to our friend $x^{p-1} + \cdots + 1$. Eisenstein's proof that the latter is irreducible is essentially identical to the one sketched on the first page of this article.

Eisenstein's paper is the first appearance of this classic proof of the irreducibility of $x^{p-1} + \cdots + 1$. Eisenstein is clearly pleased to have found such a splendid argument:

> ... This thus gives, if you will, a new and most highly simple proof of the irreducibility of the equation $x^{p-1} + x^{p-2} + \ldots . + x + 1 = 0$; and in contrast with earlier ones **), this proof does not presuppose knowledge of the roots and the relations among them.
>
> **) Besides the proof of ***Gauss***, only that of ***Kronecker*** in volume 29 of this journal, page 280, is known to me.

We know about Gauss's proof, and Kronecker's proof [**18**, vol. I, pp. 1–4] from 1845 is simpler than Gauss's but still uses the explicit relations among the roots. But notice what the footnote does *not* mention: Schönemann's two proofs of the irreducibility of $x^{p-1} + \cdots + 1$ given in his papers of 1845 and 1846. Yet Eisenstein's paper appears in the same journal in 1850!

[12] There are two standard proofs of the Eisenstein criterion. One proof (due to Eisenstein) works by studying which coefficients of the factors are divisible by the prime. The other proof (due to Schönemann) was given earlier in this article and uses reduction modulo p together with unique factorization in $\mathbb{F}_p[x]$.

[13] The Eisenstein criterion is true over any unique factorization domain—see van der Waerden [**29**]—and hence applies over $\mathbb{Z}$ and $\mathbb{Z}[i]$.

SCHÖNEMANN COMPLAINS. Eisenstein's paper, with the offending footnote, appeared in volume 39 of Crelle's journal. In volume 40, Schönemann published a *Notiz* [**26**], which began by describing two theorems from Eisenstein's paper:

- The Eisenstein criterion for real primes (in $\mathbb{Z}$) and complex primes (in $\mathbb{Z}[i]$).
- The irreducibility of the cyclotomic polynomial $x^{p-1} + \cdots + 1$, proved using the Eisenstein criterion.

Then Schönemann goes on to say:

> ... Since ***Eisenstein*** expressly noted, that for the last theorem he only knew the proofs of ***Gauss*** and ***Kronecker***, I am led to recall that in §. 6 of my paper „Foundations of a general theory of higher congruences etc." in volume 31 of this journal, I proved the first theorem [the Eisentein criterion] for real primes and deduced the last [the irreducibility of $x^{p-1} + \cdots + 1$] from the first, and also the method used by ***Eisenstein*** is not significantly different from mine. For the last theorem, I in addition even gave an entirely different proof in §. 50 of the first part of the paper.

It seems clear that Eisenstein messed up by not citing Schönemann. However, there are some complications and confusions. First, Schönemann refers to §6 of his *Grundzüge* paper in volume 31 of Crelle's journal, yet his irreducibility criterion and its application to $x^{p-1} + \cdots + 1$ are in §61 of the second part of his paper, which appeared in volume 32. The "§. 6" in his *Notiz* should have been "§. 61." This explains part of the reason I had trouble finding Schönemann's criterion—I was looking in the wrong section!

But there was also confusion on Eisenstein's side as well. As already noted, Eisenstein's study of the division equations of the lemniscate was published in a two-part paper in Crelle's journal. The footnote quoted above appeared in the first part, in issue II of volume 39. The second part of the paper, *Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie* (*On some general properties of equations that depend on the division of the lemniscate, together with applications to number theory*) [**10**, pp. 555–619], appeared in issue III of the same volume. This paper included an *explicit reference* to Schönemann's first proof of the irreducibility of $x^{p-1} + \cdots + 1$ (the one from §50 of Schönemann's paper in volume 31). Yet somehow this proof was unknown to Eisenstein when he wrote the first part of his paper. One can speculate on why this happened, but we will never know for sure.

CONCLUSION. We are now at the end of the amazing story of how Schönemann and Eisenstein independently discovered their criteria. Since Schönemann discovered it first, the name "Schönemann-Eisenstein criterion" used by Dorwart is the most historically accurate. However, most people use Eisenstein's version, so the name "Eisenstein-Schönemann criterion" is also reasonable.

In the quote from Section VII of *Disquisitiones*, Gauss acknowledged two items of unfinished business: the extension from circular to transcendental functions such as Abel's lemniscatic function φ, and the study of higher congruences. Both led to major areas of modern mathematics (elliptic curves and complex multiplication in the first case, p-adic numbers and local methods in number theory in the second), and both led to the Schönemann-Eisenstein criterion. Schönemann followed higher congruences to Hensel's lemma to a question about irreducibility modulo p^2: his criterion appears in a completely natural way. Eisenstein followed Abel's work on the

lemniscate and considered the coefficients of the resulting division polynomials: his criterion appears in a completely natural way, completely different from the context considered by Schönemann. Yet both have their origin in the same paragraph in *Disquisitiones*. As I said, it is an amazing story.

ACKNOWLEDGMENTS. The English translations of the first two Gauss quotes are from the English version of [**13**]. For the third Gauss quote and the first two Schönemann quotes, I used [**11**]. I would also like to thank Annemarie and Günter Frei for help in understanding the salutation in Eisenstein's letter to Gauss. Thanks also to Michael Filaseta for his help in pointing me to the right place in Schönemann's papers and to David Leep for bringing Dorrie's book [**8**] to my attention. I am also grateful to the referees (for both *Normat* and the MONTHLY) for several useful suggestions.

I should also mention that the papers from Crelle's journal quoted in this article are available electronically through the Göttinger Digitalisierungzentrum at the web site `http://gdz.sub.uni-goettingen.de/dms/load/toc/?IDDOC=238618`.

REFERENCES

1. N. H. Abel, *Oeuvres complètes de Niels Henrik Abel*, vol. I, L. Sylow and S. Lie, eds., Grøndahl & Søn, Christiana, 1881.
2. *Allgemeine Deutsche Biographie*, Duncker & Humblot, Leipzig, 1875–1912; also available at `http://www.deutsche-biographie.de/~ndb/adb_index.html` and `http://de.wikisource.org/wiki/Allgemeine_Deutsche_Biographie`.
3. D. A. Cox, The arithmetic-geometric mean of Gauss, *Enseign. Math.* **30** (1984) 275–330; reprinted in *Pi: A Source Book*, L. Berggren, J. Borwein, and P. Borwein, eds., 3rd ed., Springer, New York, 2003, 481–536.
4. ———, *Primes of the Form* $x^2 + ny^2$, Wiley, Hoboken, NJ, 1989.
5. ———, *Galois Theory*, Wiley, Hoboken, NJ, 2004.
6. R. Dedekind, Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus, *J. Reine Angew. Math.* **54** (1857) 269–325; reprinted in *Gesammelte mathematische Werke*, vol. I, E. Noether and O. Ore, eds., Vieweg, Braunschweig, 1930, 40–67.
7. L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institute, Washington, DC, 1919–1923; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1969.
8. H. Dorrie, *Triumph der Mathematik: Hundert berühmte Probleme aus zwei Jahrtausenden mathematischer Kultur*, Fredrich Hirt, Breslau, 1933; English trans. of 5th ed. by D. Antin, *100 Great Problems of Elementary Mathematics: Their History and Solution*, Dover, Mineola, NY, 1965.
9. H. L. Dorwart, Irreducibility of polynomials, *Amer. Math. Monthly* **42** (1935) 369–381. `doi:10.2307/2301357`
10. F. G. Eisenstein, *Mathematische Werke*, vol. II; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1989.
11. G. Frei, The unpublished section eight: On the way to function fields over a finite field, in *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones arithmeticae*, C. Goldstein, N. Schappacher, and J. Schwermer, eds., Springer, Berlin, 2007, 159–198.
12. E. Galois, *Écrits et Mémoires Mathématiques D'Évariste Galois*, R. Bourgne and J.-P. Azra, eds., Gauthier-Villars, Paris, 1962.
13. C. F. Gauss, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801; reprinted in 1863 as vol. I of [**14**]; German trans. by H. Maser, *Untersuchungen über Höhere Arithmetik*, Springer, Berlin, 1889; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1965; English trans. by A. A. Clarke, Yale University Press, New Haven, 1966; reprinted by Springer, New York, 1986.
14. ———, *Werke*, König. Gesell. Wissen., Göttingen, 1863–1927; vols. I–IX available at `http://www.wilbourall.org` (search for "Carl").
15. ———, Mathematical Diary, Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliotek Göttingen, Cod. Ms. Gauß Math. 48 Cim. Ed. (Latin with German annotations); reproduced as Abrdruck des Tagebuchs (Notizenjournals), [**14**, vol. X.1, pp. 483–575]; French trans. by P. Eymard and J.-P. Lafon, Le journal mathématique de Gauss, *Rev. Hist. Sci. Appl.* **9** (1956) 21–51; English trans. by J. Gray, A commentary on Gauss's mathematical diary, 1796–1814, *Expo. Math.* **2** (1984) 97–130; German trans. by E. Schumann, with historical introduction by K.-R. Biermann, and annotations by H. Wußing and O. Neumann, *Mathematisches Tagebuch 1796–1814*, 4th ed., Ostwalds Klassiker der exakten Wissenschaften **256**, Akademische Verlagsgesellschaft Geest & Portig, Leipzig, 1985.

16. F. Gouvêa, *p-adic Numbers: An Introduction*, Springer, New York, 1993.
17. C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870; 2nd ed., 1957.
18. L. Kronecker, *Werke*, B. G. Teubner, Leipzig, 1895–1931; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1968.
19. F. Lemmermeyer, *Reciprocity Laws*, Springer, New York, 2000.
20. E. H. Moore, A doubly-infinite system of simple groups, in *Mathematical Papers Read at the International Mathematical Congress, 1893*, Cambridge University Press, Cambridge, 1896.
21. J. J. O'Connor and E. F. Robertson, Mactutor History of Mathematics archive, available at `http://www-history.mcs.st-andrews.ac.uk/history/index.html`.
22. V. Prasolov and Y. Solovyev, *Elliptic Functions and Elliptic Integrals*, American Mathematical Society, Providence, RI, 1997.
23. M. Rosen, Abel's theorem on the lemniscate, *Amer. Math. Monthly* **88** (1981) 387–395. `doi:10.2307/2321821`
24. T. Schönemann, Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, *J. Reine Angew. Math.* **31** (1845) 269–325.
25. ———, Von denjenigen Moduln, welche Potenzen von Primzahlen sind, *J. Reine Angew. Math.* **32** (1846) 93–105.
26. ———, Notiz, *J. Reine Angew. Math.* **40** (1850) 188.
27. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259–331. `doi:10.1007/BF01405086`
28. J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.
29. B. L. van der Waerden, *Moderne algebra*, Springer, Berlin, 1930.
30. H. Weber, *Lehrbuch der Algebra*, 2nd ed., Vieweg, Braunschwieg, 1898–1908; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1961.

DAVID A. COX went to Rice University and received his Ph.D. from Princeton University in 1975. After teaching at Haverford and Rutgers, he has been at Amherst College since 1979, except for a sabbatical at Oklahoma State University. His current areas of research include toric varieties and the commutative algebra of curve parametrizations, though he also has interests in number theory and the history of mathematics. He is the author of texts on number theory, computational algebraic geometry, mirror symmetry, Galois theory, and most recently toric varieties.
Department of Mathematics, Amherst College, Amherst, MA 01002-5000
dac@math.amherst.edu

Mathematics Is . . .

"Mathematics is, of all the arts and sciences, the most austere and the most remote."

G. H. Hardy, *A Mathematician's Apology*,
Cambridge University Press, Cambridge, 1967, p. 143.

—Submitted by Carl C. Gaither, Killeen, TX