ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 27, Number 1 Winter 1997

# EISENSTEIN AND THE JACOBIAN VARIETIES OF FERMAT CURVES

ALLAN ADLER

ABSTRACT. In this paper we present evidence that Eisenstein knew something about the Jacobian varieties of Fermat curves, including the curve of degree 7. More precisely, the evidence suggests that Eisenstein had some way of knowing that certain differentials on these Fermat curves are reducible to elliptic differentials without explicitly reducing them. Our argument depends on a close examination of Gauss' first memoir [**39**] on biquadratic residues and of three related papers [**12, 13, 14**] of Eisenstein. In particular, we include a certain amount of expository material that may be of independent interest to many readers. We do not insist that the hypothesis presented here is necessarily true. We also point to evidence against it and to interesting directions for further study of Eisenstein's work.

**0. Introduction.** The discovery that every prime of the form $4n+1$ is the sum of two squares is due to Fermat[1] [**34**], [**35**][2], [**36**][3] along with results for representing the numbers in the form $a^2+2b^2$ and $a^2+3b^2$. Proofs of these results were published by Euler [**27, 28**]. In Gauss' Disquisitiones [**38**, Section 182, pp. 159–163], the results are proved again as simple consequences of his theory of binary quadratic forms. A striking refinement of the results for primes of the form $4n+1$ appears in Gauss' paper [**39**]. It is that refinement, rarely included in courses on number theory, which concerns us here.

To state Gauss' result, let $p = 4n + 1$ be a prime number. Then Gauss' theorem says that $p$ can be written in the form $a^2 + b^2$ where $a$ and $b$ are integers and where $2a$ is congruent modulo $p$ to the binomial coefficient $\binom{2n}{n}$. Since the absolute value of $a$ is necessarily less than

AMS *Subject Classification Numbers* (1980). 01A55, 10A03, 10A10, 10A15, 10B35, 10D25, 12C20, 14H40, 14H45, 14K07, 14K22, 32A05, 33A25.
*Key words and phrases.* Abelian function, binomial coefficient, CM type, complex multiplication, diagonal hypersurface, Eisenstein sum, elliptic curve, elliptic function, Fermat curve, Gauss sum, Jacobi sum, Klein curve, Kronecker congruence relation, Lemniscatic function, permutation twist.
Received by the editors on July 29, 1992, and in revised form on September 15, 1995.

$p/2$, the integer $a$ is determined by its residue class modulo $p$. Hence Gauss' theorem provides one with a formula for $a$. The proof given by Gauss is summarized in Section 1 of this paper. In Section 2 we present Eisenstein's proof [**12**] of a similar result for expressing primes in the form $a^2 + 2b^2$ and $a^2 + 7b^2$. Both Gauss' proof and Eisenstein's proof are based on properties of Jacobi sums. However, in the introduction to [**12**], Eisenstein tells us that he has alternative proofs of his results for $a^2 + 2b^2$ and $a^2 + 7b^2$ using elliptic functions. It is our purpose, in this paper, to investigate what this proof of Eisenstein might have been.

Important clues are found in the proofs using Jacobi sums, which is one reason for including them here. But what is crucial for our investigations is Eisenstein's proof in [**14**] of Gauss' theorem on primes of the form $a^2+b^2$. In this proof, Eisenstein uses elliptic functions, and it is natural to suppose that the argument he had in mind for the cases $a^2 + 2b^2$ and $a^2 + 7b^2$ ran along similar lines. We therefore study in Section 4 the argument which Eisenstein uses in [**14**] to prove Gauss' theorem. This requires a preliminary discussion in Section 3 of elliptic functions based on Abel's paper [**1**]. In Section 5 we give a similar proof in the case $p = 8n+3$. In Section 6 we indicate how, using some assumptions which we do not justify, one might construct one for the cases $p = 7n + 1, 2, 4$.

In Section 7 we discuss the lessons of the earlier sections of the paper. It is our main historical hypothesis in this article that Eisenstein had some way of knowing that certain differentials on the Fermat curve of degree 7 are reducible to elliptic integrals without explicitly transforming them. We find it difficult to avoid the conclusion that Eisenstein possessed some knowledge of the Jacobian varieties of Fermat curves, but what it was that Eisenstein might have known and in what form is not clear. However, we do mention at the end of Section 7 an alternative to the hypothesis which we have proposed in this article. We also propose directions for the further study of Eisenstein's work.

Some remarks about the style of the various sections of this article are necessary. In those sections where results of Gauss or Eisenstein are presented, we have tried to remain faithful to the methods and concepts which they actually used in their articles. We do, however, make comments using modern ideas and it should be understood that we do not claim that either Gauss or Eisenstein actually possessed these modern

concepts. To do so would be to commit the error of anachronism[4]. Instead, such comments are addressed to the modern reader. In Section 3 we use a mixture of modern notions and formulas from Abel. I have no doubt that it could be rewritten in a manner that would have satisfied Eisenstein's contemporaries, but I have not attempted to do so. Similarly, I have not attempted to base the discussion on the foundations of elliptic functions given in Eisenstein's *Genaue Untersuchung* [**20**]. In Section 4 I have tried to follow Eisenstein [**14**] closely. In Section 5 I present a proof, which I believe Eisenstein would have understood, for the case $p = 8n + 3$ using elliptic functions. One of the lessons of Section 5 is the role of differentials on Fermat curves. I do not have a proof along these lines for the cases $7n + 1, 2, 4$, and the purpose of Section 6 is to investigate how one might at least discover the elements of such a proof. It freely uses modern concepts to deal with those elements. The same applies to the corresponding portions of Section 7. One can hope that, after the elements have been found, one can write such a proof in the style of Eisenstein. But, for the moment, the discussion is among our contemporaries, not Eisenstein's, and modern terminology and concepts are therefore used in Sections 6 and 7.

The author's introduction to the work of Eisenstein came from André Weil's book [**81**] and the subsequent search, initiated by Weil, for a geometric proof of the Chowla-Selberg formula. The author was therefore motivated in 1979 to purchase a copy of [**15**]. While browsing through the articles, he noticed the article [**12**] and began to study it. Subsequent examination of [**81**] showed that there was no mention of this work, and it appeared that this was an opportunity to pursue study of Eisenstein in directions not already considered in [**81**]. Nevertheless, many of the directions which the author was encouraged to pursue by Weil in connection with the Chowla-Selberg formula turned out to be quite useful to this study as well.

Since it has apparently not been noticed elsewhere, the author wishes to point out that the editors of [**15**] omitted diagrams which were originally part of the article [**16**] and without which the article is rendered incomprehensible. This suggests that the articles were assembled and copied by Chelsea Publishing Company but not, however, read. If so, the reason the diagrams were omitted is easy to understand. In the journal in which the article [**16**] appeared, the diagrams for the articles were all collected at the end of the volume, as was a common practice

at the time. Therefore, if the article was not read when copied for [**15**], the editors would have been unaware that they were not also copying the necessary diagrams. The reader interested in obtaining the diagrams may look for them in Crelle's Journal **28** (1844) at the end of the volume or in Cayley's translation [**10**] of the article.

In the list of references at the end of the article, we have given multiple citations of the works of certain authors under a single bibliographic entry. Our purpose in doing so has generally been to give more historical information about the date and journal where the work appeared while, at the same time, providing a reference in brackets to the author's collected works, where the article is likely to be more accessible to the reader. In such cases, page references are to the collected works unless otherwise indicated. Footnotes in the body of the article refer to notes collected near the end of the article, just before the bibliography. For the convenience of the reader who happens to run across a note in isolation at the end of the article, each note ends with a pointer to the section, page, and line number of the present article where the footnote occurs.

**1. Gauss' proof of Gauss' theorem.** In this section we present Gauss' proof that a prime of the form $4n+1$ can be written in the form $a^2+b^2$ where $2a$ is congruent modulo $p$ to the binomial coefficient $\binom{2n}{n}$. In order to save space, we have condensed the argument from Gauss' 28 page paper into just a few pages, cutting a few corners in the process. The reader who finds our presentation too terse or who would like to read something closer to the original is referred either to Gauss' paper itself [**39**], to the German translation in [**40**] or to the author's amateurish bilingual Latin-English edition [**5**] of Gauss' paper.[5] Apart from its utility for this paper, we hope that our presentation here of Gauss' results and the translation [**5**] will facilitate the study of Gauss' work by people who do not speak Latin or German, in turn facilitate the study of Weil's paper [**83**] and perhaps encourage a few individuals to add Latin to their repertoire.

**Theorem 1.1.** *Let $p$ be a prime of the form $4n+1$. Then we can write $p$ in the form $a^2+b^2$ where $a$ and $b$ are integers and where $a$*

*satisfies the congruence*

$$2a \equiv \binom{2n}{n} \pmod{p}. \tag{1.2}$$

*Proof.* Consider the sum of $(x^4+1)^{2n}$ as $x$ runs over the nonzero elements of the field $\mathbf{F}_p$ with $p$ elements. One can expand $(x^4+1)^{2n}$ using the binomial theorem. Summing over the multiplicative group $\mathbf{F}_p^\times$ of $\mathbf{F}_p$, we find that the sum is equal to

$$-2 - \binom{2n}{n}. \tag{1.3}$$

On the other hand, let $A_0$ denote the group of biquadratic residues modulo $p$, $A_2$ the quadratic residues modulo $p$ not in $A_0$, and let $A_1$ and $A_3$ denote the other two cosets of $A_0$ in $\mathbf{F}_p^\times$. We denote by $(ij)$ the number of elements $x$ of $A_i$ such that $x+1$ lies in $A_j$. With this notation, we have

$$\sum{}'(x^4+1)^{2n} \equiv 4(00) - 4(01) + 4(02) - 4(03) \pmod{p}, \tag{1.4}$$

where the summation runs over all $x$ in $\mathbf{F}_p^\times$. Let $e$ denote an element of $A_1$. Then $16(ij)$ is the number of solutions modulo $p$ of[6]

$$1 + e^i x^4 \pm e^j y^4 = 0, \tag{$1.5_{ij}$}$$

with $x$ and $y$ in $A_0$, where the sign is $(-1)^n$. One recognizes equation $(1.5_{ij})$ to be a twisted form of the Fermat equation $a^4+b^4+c^4=0$. Gauss divides his proof into the two cases $n$ even and $n$ odd. For $n$ even, $-1$ belongs to $A_0$ and $(1.5_{ij})$ can be written as

$$1 + e^i x^4 + e^j y^4 = 0. \tag{1.6}$$

If $(x,y)$ is a solution of $(1.5_{ij})$ in this case, then $(1/x, y/x)$ is a solution of $(1.5_{-i,j-i})$ and $(y,x)$ is a solution of $(1.5_{ji})$, so that

$$(i\,j) = (-i\;\; j-i) \quad \text{and} \quad (i\,j) = (j\,i). \tag{1.7}$$

If we form a symmetric matrix $S$ whose entries are the $(ij)$, then these relations imply that $S$ is given by

$$S = \begin{pmatrix} (00) & (01) & (02) & (03) \\ (01) & (03) & (12) & (12) \\ (02) & (12) & (02) & (12) \\ (03) & (12) & (12) & (01) \end{pmatrix}. \tag{1.8}$$

Hence the basic $(ij)$'s are (00), (01), (02), (03) and (12). If we denote by $u$ the column vector all of whose entries equal 1, then since $-1$ lies in $A_0$ when $n$ is even, we have

$$S \cdot u = \begin{pmatrix} n-1 \\ n \\ n \\ n \end{pmatrix} \tag{1.9}$$

which imposes three independent conditions[7] on the entries of $S$. Gauss then considers the number of solutions of

$$1 + x^4 + ey^4 + e^2 z^4 \tag{1.10}$$

with $x, y$ and $z$ nonzero elements of $\mathbf{F}_p$. This is a diagonal variety of degree 4. As $x$ runs over $\mathbf{F}_p^\times$, $x^4$ runs over $A_0$ and one can group the solutions of (1.10) according to which $A_i$ contains $1 + x^4$. The number of solutions in each group is readily computed, and one obtains for the total number of solutions

$$64[(00) \cdot (12) + (01)^2 + (02) \cdot (03) + (03) \cdot (12)]. \tag{1.11}$$

On the other hand, as $y$ runs over $\mathbf{F}_p^\times$, $ey^4$ runs over $A_1$ and one can group the solutions of (1.10) according to which $A_i$ contains $1 + ey^4$. Again, it is easy to compute the number of solutions in each group, and one obtains for the total number of solutions

$$64[(01) \cdot (02) + (03) \cdot (12) + (12) \cdot (02) + (12)^2]. \tag{1.12}$$

Equating the two expressions (1.11) and (1.12) for the total number of solutions of (1.10) with $x, y$ and $z$ nonzero and using the relations in (1.9), one finds that[8]

$$p = a^2 + b^2$$

where

$$a = 4 \cdot (02) - 4 \cdot (12) + 1 \tag{1.13}$$

and

$$b = 2 \cdot (03) - 2 \cdot (01).$$

Using these expressions for $a$ and $b$ and the relations (1.9), one finds that

$$\begin{aligned} 16 \cdot (00) &= p - 6a - 11 \\ 16 \cdot (01) &= p + 2a - 4b - 3 \\ 16 \cdot (02) &= p + 2a - 3 \\ 16 \cdot (03) &= p + 2a + 4b - 3. \end{aligned} \tag{1.14}$$

For $n$ odd, the argument up to this point is quite similar. In this case, $-1$ belongs to $A_2$, and the number of solutions of $(1.5_{ij})$ is the same as the number of solutions of

$$1 + e^i x^4 + e^{j+2} y^4 = 0. \tag{1.15}$$

In this case, the matrix $S$ has the form

$$\begin{pmatrix} (00) & (01) & (02) & (03) \\ (10) & (10) & (03) & (01) \\ (00) & (10) & (00) & (10) \\ (10) & (03) & (01) & (10) \end{pmatrix} \tag{1.16}$$

and the identity (1.9) is replaced by

$$S \cdot u = \begin{pmatrix} n \\ n \\ n-1 \\ n \end{pmatrix}. \tag{1.17}$$

Arguing as before, one obtains two expressions for the number of solutions of (1.10), namely,

$$64[(00) \cdot (10) + (01) \cdot (03) + (02) \cdot (01) + (03) \cdot (10)] \tag{1.18}$$

and

$$64[(00)\cdot(10)+(10)^2+(00)\cdot(03)+(01)\cdot(10)].$$

Equating these and using the equations (1.4), one finds that

$$p=a^2+b^2$$

where

$$a=4\cdot(00)-4\cdot(01)+1 \tag{1.19}$$

and

$$b=2\cdot(01)-2\cdot(03).$$

Using these expressions for $a$ and $b$ and the relations (1.17), one finds in this case that

$$\begin{aligned} 16\cdot(00)&=p+2a-7\\ 16\cdot(01)&=p+2a+4b+1\\ 16\cdot(02)&=p-6a+1\\ 16\cdot(03)&=p+2a-4b+1. \end{aligned} \tag{1.20}$$

In either case, substituting the values we have obtained for (00), (01), (02) and (03) into equation (1.4), we obtain

$$\sum{}'(x^4+1)^{2n}\equiv -2-2a \pmod p. \tag{1.21}$$

Comparing (1.21) with the value obtained in (1.3), we conclude with Gauss that

$$2a\equiv\binom{2n}{n} \pmod p. \tag{1.22}$$ □

**2. Eisenstein's generalization of Gauss' theorem.** Turning now to Eisenstein, we consider in this section a paper [**12**] entitled, "Zur Theorie der quadratischen Zerfallung der Primzahlen $8n+3$, $7n+2$ und

$7n+4$," which appeared in Crelle's Journal in 1848. In it, Eisenstein derives results which are similar to the theorem of Gauss which we discussed in Section 1. To be precise, Eisenstein shows that if $p$ is a prime of the form $8n+3$, then $p$ can be written in the form $a^2+2b^2$ where $2a$ is congruent to the binomial coefficient $\binom{4n+1}{n}$ modulo $p$; while if $p$ is a prime of the form $7n+2$ or $7n+4$, then $p$ can be written in the form $a^2+7b^2$, where $2a$ is congruent modulo $p$ to $\binom{3n}{n}$ if $p=7n+2$ and to $\binom{3n+1}{n}$ if $p=7n+4$.

In case $p=3n+1$, $p=8n+1$ and $p=7n+1$, such results were known to Jacobi [**46, 47**] and, judging from Eisenstein's introductory remarks, similar results were known to Cauchy as well. Eisenstein mentions that he has a general result to the effect that if $\lambda$ is a prime of the form $4n+3$ and if $p$ is a prime of the form $m\lambda+1$, then four times a certain power of $p$ can be written in the form $c^2+\lambda d^2$, where $c$ is congruent modulo $p$ to

$$(\beta_1 \cdot m)!(\beta_2 \cdot m)!(\beta_3 \cdot m)!\ldots \tag{2.1}$$

and where $\beta_1, \beta_2, \beta_3, \ldots$ run over the quadratic nonresidues modulo $\lambda$ which are between 0 and $\lambda$. He points out that a similar result already occurs on page 171 of the version of Jacobi's paper in Crelle (cf. [**46**, p. 260]). Thus, Eisenstein, although he was quite pleased with his earlier results along these lines, nevertheless acknowledges that they are not far removed from the results of his contemporaries. In this paper, however, he feels that a significant step has been taken in that the cases $8n+3$, $7n+2$ and $7n+4$ were not amenable to the methods of cyclotomy as they had been practiced by his colleagues. Eisenstein obtains his results by considering Jacobi sums for fields of order $p^2$ and $p^3$ instead of merely $p$. Today we define Gauss sums and Jacobi sums with reference to any finite field, but the first step from prime fields to general finite fields was taken by Eisenstein, which is why Stickelberger [**78**] refers to them as Eisenstein sums. The proofs given by Eisenstein are similar in spirit to that of Gauss. We will sketch them here. In order to enhance legibility, we will avoid notation such as $\mathbf{F}_{p^2}$ in favor of the older notation $GF(p^2)$ of L.E. Dickson. Thus, for every prime power $q$, we will denote the field with $q$ elements either by $\mathbf{F}_q$ or by $GF(q)$.

**The case $p=8n+3$.** Let $p$ be a prime of the form $8n+3$, let

$e = (p^2 - 1)/8$, and let $\omega$ be a primitive eighth root of unity such that $\omega^2 = i$. Let $\mathcal{P}$ be a prime of $\mathbf{Z}[\omega]$ lying over $p$. Then we can identify $\mathbf{Z}[\omega]/\mathcal{P}$ with $GF(p^2)$ and we denote by $f$ the image[9] of $\omega$ in $GF(p^2)$. For every nonzero element $x$ of $GF(p^2)$, let $[x] = \omega^j$, where $x^e = f^j$. Then $[x]$ is the eighth power residue symbol. Let tr denote the trace from $GF(p^2)$ to $GF(p)$. The following lemma is contained in the discussion at the bottom of page 511 of [**12**].

**Lemma 2.2.** *Let*

$$T = \sum [k]^\nu [k']^{-\nu} \tag{2.3}$$

*where $\nu$ is an odd number and where the sum runs over all pairs $k, k'$ of nonzero elements of $GF(p^2)$ such that* $\mathrm{tr}\,(k + k') = 2$. *Then we have $T = p$.*

*Proof.* Fix $\nu$. For each $\alpha$ in $GF(p)$, let

$$S_\alpha = \sum [k]^\nu [k']^{-\nu} \tag{2.4}$$

where the summation runs over all pairs $k, k'$ such that $k + k' = 1 + i\alpha$. Then we can write $k = k'l$ and obtain

$$S_\alpha = \sum [l]^\nu = -[-1] = 1 \tag{2.5}$$

where the summation runs over all $l \neq -1$ in $GF(p^2)^\times$. Since $T = \sum S_\alpha$ with $\alpha$ running over $GF(p)$, we have $T = p$. □

**Definition 2.6.** Let $\nu$ be an integer. We define $\Gamma_\nu$ by

$$\Gamma_\nu = \sum [k]^\nu \tag{2.7}$$

where the summation runs over all $k$ in $GF(p^2)$ with $\mathrm{tr}\,(k) = 2$.

The following lemma occurs on page 513 of [**12**] (Equation (1)).

**Lemma 2.8.** *Let $\nu$ be odd. Then $|\Gamma_\nu|^2 = p$.*

*Proof.* By Lemma 2.2, we have

$$p = T = \sum [k]^{\nu} [k']^{-\nu} \tag{2.9}$$

where the summation runs over all pairs $k, k'$ in $GF(p^2)$ such that $\mathrm{tr}\,(k + k') = 2$. For every integer $\mu$, let

$$U_{\mu} = \sum [k]^{\mu} [k']^{-\mu}$$

where $k, k'$ runs over all pairs for which $\mathrm{tr}\,(k) = 0$ and $\mathrm{tr}\,(k') = 2$. Then

$$U_{\mu} = \left( \sum [k]^{\mu} \right) \cdot \left( \sum [k']^{-\mu} \right) = 0 \tag{2.10}$$

provided that $\mu$ is odd. Therefore, we have

$$p = T - U_{\nu} - U_{-\nu} = \sum [k]^{\nu} [k']^{-\nu} \tag{2.11}$$

where the $k, k'$ run over all pairs such that $\mathrm{tr}\,(k + k') = 2$ and $\mathrm{tr}\,(k)\mathrm{tr}\,(k') \neq 0$. Then letting $2x_1 = \mathrm{tr}\,(k)$ and $2x_2 = \mathrm{tr}\,(k')$ in the summation, we have

$$p = |\Gamma_n|^2 \cdot \sum \left( \frac{x_1 x_2}{p} \right) \tag{2.12}$$

where $(\div)$ denotes the Legendre symbol, and where the summation runs over all nonzero $x_1, x_2$ in $GF(p)$ such that $x_1 + x_2 = 1$. Since that summation is equal to 1, we are done. □

**Definition 2.13.** For $0 \leq j \leq 7$, let $\sigma_j$ denote the number of elements $z$ of $GF(p)$ such that $[1 + zi] = \omega^j$. We also define the polynomial $\phi(u)$ by

$$\phi(u) = \sum_{j=0}^{7} \sigma_j u^j. \tag{2.14}$$

**Lemma 2.15** [**12**, Section 3]. *We have*

$$\begin{aligned} \Gamma_1 &= \Gamma_3 = a + b\sqrt{-2} \\ \Gamma_5 &= \Gamma_7 = a - b\sqrt{-2} \\ \Gamma_2 &= \Gamma_6 = 1 \\ \Gamma_4 &= -1 \\ \Gamma_0 &= p \end{aligned} \tag{2.16}$$

*where $a$ and $b$ are integers.*

*Proof.* One sees at once that $\Gamma_\nu = \phi(\omega^\nu)$. Furthermore, if we interpret the subscripts as integers modulo 8, then $\sigma_j = \sigma_{3j}$ because $[1+zi] = \omega^j$ if and only if $[1 - zi] = [1 + zi]^q = \omega^{3j}$. Therefore, $\Gamma_\nu = \Gamma_{3\nu}$ for all $\nu$. Let

$$\begin{aligned} a &= \sigma_0 - \sigma_4, \qquad & b &= \sigma_1 - \sigma_5 \\ c &= \sigma_2 - \sigma_6, \qquad & d &= \sigma_3 - \sigma_7. \end{aligned} \tag{2.17}$$

Obviously, $a, b, c$ and $d$ are integers. Furthermore, $c = 0$, $b = d$, and we have

$$\begin{aligned} \Gamma_1 &= \Gamma_3 = a + b\sqrt{-2} \\ \Gamma_5 &= \Gamma_7 = a - b\sqrt{-2}. \end{aligned} \tag{2.18}$$

If $\nu$ is even, then $[z]^\nu = 1$ for all $z$ in $GF(p)^\times$. For such $\nu$, we have

$$\Gamma_\nu = \sum_{z \in GF(p)} [1 + zi]^\nu = \frac{1}{p-1} \sum{}' [x + yi]^\nu \tag{2.19}$$

where the primed summation runs over all pairs $x, y$ of elements of $GF(p)$ with $x \neq 0$. If $\nu = 0$, then $\Gamma_0 = p$. Otherwise,

$$\Gamma_\nu = \frac{-1}{p-1} \sum_{y \in GF(p)^\times} [iy]^\nu = -[i]^\nu. \tag{2.20}$$

If $\nu = 2\mu$, then we get

$$\Gamma_\nu = -[-1]^\mu = (-1)^{\mu+1}. \tag{2.21}$$

**Theorem 2.22.** *Write* $\Gamma_1 = a + b\sqrt{-2}$ *as in Lemma* 2.16. *Then*

$$a = 4\tau + 1 - 2n, \tag{2.23}$$

*where* $\tau$ *is the number of* $z$ *in* $GF(p)$ *such that* $1 \le z \le (p-1)/2$ *and such that* $1 + zi$ *is an eighth power residue. In particular, we have*

$$a \equiv (-1)^n \pmod 4. \tag{2.24}$$

*Proof.* Since $(-1)^n = (1-2)^n \equiv 1 - 2n \pmod 4$, the second assertion follows from the first. As for the first, we have

$$8\sigma_0 = \sum_{\nu=0}^{7} \phi(\omega^\nu) = 4a + p + 1 \tag{2.25}$$

by Lemma 2.15. Therefore, $a = 2\sigma_0 - 2n - 1$. But since $1 + zi$ is an eighth power residue if and only if $1 - zi$ is, we have $\sigma_0 = 1 + 2\tau$ with $\tau$ as above. It follows that $a = 4\tau + 1 - 2n$. □

**Theorem 2.26.** *The number* $\Gamma_1$ *lies in the ideal* $\mathcal{P}$ *and*

$$\Gamma_7 \equiv \binom{4n+1}{n} \pmod{\mathcal{P}}. \tag{2.27}$$

*In particular, if we write* $\Gamma_7 = a + b\sqrt{-2}$ *with* $a$ *and* $b$ *integers as in Lemma* 2.15, *we have*

(1) $a^2 + 2b^2 = p$

(2) $2a \equiv -\binom{4n+1}{n} \pmod p$

(3) $a \equiv (-1)^n \pmod 4$

(4) $a = 2\sigma_0 - (p+1)/4$.

*Proof.* That $a$ and $b$ are integers follows from Lemma 2.15. Assertions (3) and (4) are contained in Theorem 2.22. The assertion (1) follows from Lemma 2.8. Therefore, we just have to prove (2) and the assertions about $\Gamma_1$ and $\Gamma_7$. In general,

$$\Gamma_\nu = \sum_{z \in GF(p)} (1 + zi)^{e\nu} \pmod{\mathcal{P}}. \tag{2.28}$$

Since $e = (p^2-1)/8$, and since we can take $0 \le \nu \le 7$, we can write $e\nu = \alpha + \beta p$ with $0 \le \alpha, \beta \le p-1$. Then we have

$$\Gamma_\nu = \sum_{z \in GF(p)} (1+zi)^\alpha (1-zi)^\beta \pmod{\mathcal{P}}. \tag{2.29}$$

For $\nu = 1$, we have $\alpha = 3n+1$ and $\beta = n$, so $\alpha + \beta < p-1$. Therefore, $\Gamma_1 \equiv 0 \pmod{\mathcal{P}}$ since the only powers of $z$ occurring in the summation have exponent less than $p-1$. This proves that $\Gamma_1$ belongs to $\mathcal{P}$. For $\nu = 7$, we have $\alpha = 7n+2$ and $\beta = 5n+1$, so that $p-1 < \alpha + \beta < 2(p-1)$. Therefore,

$$\Gamma_7 \equiv \sum i^{a-b} \frac{(7n+2)!(5n+1)!}{a!b!(7n+2-a)!(5n+1-b)!} \pmod{\mathcal{P}} \tag{2.30}$$

where the summation runs over all pairs $a, b$ such that $0 \le a \le 7n+2$ and $0 \le b \le 5n+1$ with $a+b = 8n+2$. By Wilson's theorem,

$$a!b! \equiv (-1)^{b+1} \pmod{p} \tag{2.31}$$

so that

$$\Gamma_7 \equiv \sum \frac{(7n+2)!(5n+1)!}{(7n+2-a)!(5n+1-b)!} \pmod{\mathcal{P}} \tag{2.32}$$

with the same summation convention as in equation (2.30). Every such pair $a, b$ is represented in one and only one way in the form

$$a = r + 3n + 1, \qquad b = -r + 5n + 1, \tag{2.33}$$

where $0 \le r \le 4n+1$. Therefore,

$$\Gamma_7 \equiv \sum_{r=0}^{4n+1} \frac{(7n+2)!(5n+1)!}{(4n+1-r)!r!} \pmod{\mathcal{P}}. \tag{2.34}$$

The righthand side of equation (2.34) is just

$$\frac{(7n+2)!(5n+1)!}{(4n+1)!} \cdot 2^{4n+1}. \tag{2.35}$$

Using Wilson's theorem again and the fact that 2 is a quadratic nonresidue modulo $p$, we have

$$\Gamma_7 \equiv -\binom{4n+1}{n} \pmod{\mathcal{P}} \tag{2.36}$$

as required. To prove (2), note that since $\Gamma_1$ belongs to $\mathcal{P}$, we have

$$2a \equiv \Gamma_1 + \Gamma_7 \equiv \Gamma_7 \equiv -\binom{4n+1}{n} \pmod{\mathcal{P}}. \tag{2.37}$$

We note, as Eisenstein did, that by Theorem 2.26 the study of the decomposition of $p$ into $a^2 + 2b^2$ is reduced to finding the number of elements $z$ such that $[1 + zi] = 1$, and that this is equivalent to finding all $\xi + i\eta$ in $GF(p^2)$ such that the trace of $(\xi + i\eta)^8$ is equal to 2. Eisenstein leaves us with the algebraic curve

$$\xi^8 - 28\xi^6\eta^2 + 70\xi^4\eta^4 - 28\xi^2\eta^6 + \eta^8 = 1 \tag{2.38}$$

and the task of finding its rational points over $GF(p)$. Actually, the form

$$\operatorname{tr}\left((\xi + i\eta)^8\right) = 2 \tag{2.39}$$

is more useful since we can write it as

$$(\xi + i\eta)^8 + (\xi - i\eta)^8 = 2, \tag{2.40}$$

which shows that our curve is a twisted form of the Fermat curve of degree 8. He points out that computing $\sigma_0$ is equivalent to computing the number of solutions of

$$y^2 = x^8 - 28x^6 + 70x^4 - 28x^2 + 1 \tag{2.41}$$

in $GF(p)$. □

**The cases $p = 7n+2$ and $p = 7n+4$.** Now let us turn to Eisenstein's proof for $7n + 2$ and $7n + 4$, abandoning the notation and conventions which we adopted for the case $p = 8n + 3$. Let $p$ be a prime of the form $7n + 2$ or $7n + 4$, let $\zeta = \exp(2\pi i/7)$, and let $\mathcal{P}$ be a prime of $\mathbf{Z}[\zeta]$

lying over $p$. We can identify $\mathbf{Z}[\zeta]/\mathcal{P}$ with $GF(p^3)$ and denote by $f$ the image of $\zeta$ in $GF(p^3)$. Let $e = (p^3-1)/7$, and for $x$ in $GF(p^3)$, let $[x] = \zeta^i$ if $x^e = f^i$. Then we have $[x] = 1$ for all $x$ in $GF(p)^\times$. Denote by $\eta_1, \eta_2$ and $\eta_4$ the elements of $\mathbf{Z}[\zeta]$ given by

$$\begin{aligned} \eta_1 &= 3\zeta + 3\zeta^6 + 1 \\ \eta_2 &= 3\zeta^2 + 3\zeta^5 + 1 \\ \eta_4 &= 3\zeta^4 + 3\zeta^3 + 1. \end{aligned} \tag{2.42}$$

Let tr denote the trace from $GF(p^3)$ to $GF(p)$. For $0 \le j \le 6$, let $\sigma_j$ denote the number of elements $z$ of $GF(p^3)$ such that $\mathrm{tr}\,(z) = 3$ and $[z] = \zeta^j$. We denote by $\phi(u)$ the polynomial defined by

$$\phi(u) = \sum_{j=0}^{6} \sigma_j u^j. \tag{2.43}$$

For any integer $\nu$, we will write $\Gamma_\nu$ to denote $\phi(\zeta^\nu)$. The proof of the following lemma is quite similar to the proofs of Lemmas 2.2 and 2.8 and will be omitted.

**Lemma 2.44.** *Suppose* 7 *doesn't divide* $\nu$. *Let*

$$T = \sum [k]^\nu [k']^{-\nu} \tag{2.45}$$

*where the summation runs over all pairs* $k, k'$ *in* $GF(p^3)$ *such that* $\mathrm{tr}\,(k + k') = 3$. *Then* $T = -p^2$. *Furthermore,* $|\Gamma_\nu|^2 = p$.

**Lemma 2.46.** *If we interpret the subscripts modulo 7, we have*

$$\sigma_\nu = \sigma_{p\nu}$$

*for all* $\nu$. *Consequently,*

$$\begin{aligned} \Gamma_1 &= \Gamma_2 = \Gamma_4 \\ \Gamma_3 &= \Gamma_5 = \Gamma_6 \end{aligned} \tag{2.47}$$

*and we have*

$$\begin{aligned} \Gamma_1 &= a + b\sqrt{-7} \\ \Gamma_3 &= a - b\sqrt{-7} \end{aligned} \tag{2.48}$$

*with $a$ and $b$ rational integers.*

*Proof.* For $z$ in $GF(p^3)$ the conditions $\mathrm{tr}\,(z) = 3$ and $[z] = \zeta^j$ hold if and only if the conditions $\mathrm{tr}\,(z^p) = 3$ and $[z^p] = \zeta^{pj}$ hold. This implies the first assertion. The identity $\overline{\Gamma_\nu} = \Gamma_{3\nu}$ follows at once from equation (2.47), and the definition of $\Gamma_\nu$. We have

$$\Gamma_1 = \sigma_0 + \sigma_1(\zeta + \zeta^2 + \zeta^4) + \sigma_6(\zeta^3 + \zeta^5 + \zeta^6) = a + b\sqrt{-7} \tag{2.49}$$

where

$$a = \sigma_0 - \frac{\sigma_1 + \sigma_6}{2}, \qquad b = \frac{\sigma_1 - \sigma_6}{2}. \tag{2.50}$$

Therefore $2a$ and $2b$ are integers. By equations (2.50), we have $a^2 + 7b^2 = p$ and therefore $(2a)^2 + 7(2b)^2 = 4p$. Reducing modulo 8, we see that neither $2a$ nor $2b$ can be odd, so $a$ and $b$ are both integers. □

**Corollary 2.51.** *Let $a$ be the integer defined in Lemma* 2.46. *Then* $a \equiv p^2 \pmod 7$ *and* $p^2 + 6a = 7\sigma_0$.

*Proof.* The second assertion implies the first. As for the first, we have $p^2 = \phi(1) = \sigma_0 + 3\sigma_1 + 3\sigma_3$ and $2a = \sigma_0 - \sigma_1 - \sigma_3$ by Lemma 2.44. Therefore, $p^2 + 6a = 7\sigma_0$. □

**Lemma 2.52.** *Let $k$ run over all nonzero elements of $GF(p^3)$ such that* $\mathrm{tr}\,(k) = 3$. *Let $k' = k^p$ and $k'' = k'^p$. If $r, s$ and $t$ are nonnegative integers such that $r + s + t < 2(p-1)$, then*

$$\sum k^r k'^s k''^t = 0. \tag{2.53}$$

*Proof.* Let $\alpha, \beta$ be a basis over $GF(p)$ for the solutions of $\mathrm{tr}\,(z) = 0$. Then we can write $k = 1 + x\alpha + y\beta$ where $x, y$ run over $GF(p)$. Since $x$ and $y$ belong to $GF(p)$, we have $x^p = x$ and $y^p = y$. Therefore, $k'$ and $k''$ have degree 1 in $x$ and $y$. The summation therefore represents the average over $GF(p)^2$ of a polynomial in $x, y$ and by hypothesis the

degree of the polynomial is $< 2(p-1)$. Since only terms of the form $x^{p-1}y^{p-1}$ can survive in this summation, the sum is zero. □

**Lemma 2.54.** *If we let $k$ run over all the elements of trace 3 in $GF(p^3)$ and write $k'$ to denote $k^p$, then we have*

$$\sum k^{p-1}k'^{p-1} = 1. \tag{2.55}$$

*Proof.* Let $\alpha, \beta$ be a basis over $GF(p)$ for the space of solutions of $\mathrm{tr}\,(z) = 0$. Then denoting the above summation by $S$, we have

$$\begin{aligned} S &= \sum_{j=0}^{p-1} ((-1)^j \alpha^j \beta^{p-1-j}) \cdot ((-1)^{p-1-j} \alpha^{p(p-1-j)} \beta^{pj}) \\ &= \sum_{j=0}^{p-1} (\alpha\beta^p)^j \cdot (\alpha^p\beta)^{p-1-j}. \end{aligned} \tag{2.56}$$

Summing this geometric progression, we have

$$S = \frac{\alpha^p \beta^{p^2} - \alpha^{p^2}\beta^p}{\alpha\beta^p - \alpha^p\beta} = (\alpha\beta^p - \alpha^p\beta)^{p-1}. \tag{2.57}$$

If we take $\alpha = \eta_1$ and $\beta = \eta_2$, then we have

$$\begin{aligned} \alpha\beta^p - \alpha^p\beta &= \begin{cases} \eta_1\eta_4 - \eta_2^2 & \text{if } p = 7n+2 \\ \eta_1^2 - \eta_2\eta_4 & \text{if } p = 7n+4 \end{cases} \\ &= \begin{cases} 21 & \text{if } p = 7n+2 \\ -21 & \text{if } p = 7n+4. \end{cases} \end{aligned} \tag{2.58}$$

In either case, $\alpha\beta^p - \alpha^p\beta$ lies in $GF(p)^\times$, so

$$S = (\alpha\beta^p - \alpha^p\beta)^{p-1} = 1. \tag{2.59}$$ □

**Lemma 2.60.** *Let $k$ and $k'$ be as in Lemma 2.54. Let $u$ and $v$ be nonnegative integers such that $u + v = 2(p-1)$. In order that the summation*

$$\sum k^u k'^v \tag{2.61}$$

*be nonzero, it is necessary and sufficient that* $u = v = p - 1$.

*Proof.* The sufficiency follows from Lemma 2.54. Conversely, suppose first that $u > p - 1$ and $v < p - 1$. Then $u = p - 1 + w$ with $w > 0$, and we have

$$\sum k^u k'^v = \sum k^{w-1} k'^{v+1} = 0 \tag{2.62}$$

by Lemma 2.52 since $(w-1) + (v+1) = w + v = p - 1 < 2(p-1)$. On the other hand, suppose that $u < p - 1$ and $v > p - 1$. Then we can write $v = p - 1 + x$ with $x > 0$, and we have

$$\sum k^u k'^v = \sum k^u k'^{x-1} k'' = 0, \tag{2.63}$$

where $k'' = k'^p$, by Lemma 2.52, since $u + (x-1) + 1 = u + x = p - 1 < 2(p-1)$. □

**Theorem 2.64.** *Let* $p$ *be prime of the form* $7n + 2$ *or* $7n + 4$. *Then* $\Gamma_1$ *lies in the ideal* $\mathcal{P}$ *and modulo* $\mathcal{P}$ *we have*

$$\Gamma_3 \equiv \begin{cases} -\left(\dfrac{3n}{n}\right) & \text{if } p = 7n + 2 \\ \left(\dfrac{3n+1}{n}\right) & \text{if } p = 7n + 4. \end{cases} \tag{2.65}$$

*If we write* $\Gamma_3 = a - b\sqrt{-7}$ *as in* (2.48), *then we have*

(1) $p = a^2 + 7b^2$

(2) $a \equiv p^2 \pmod 7$

(3) $7\sigma_0 = 6a + p^2$

(4) $2a \equiv \begin{cases} -\left(\dfrac{3n}{n}\right) \pmod p & \text{if } p = 7n + 2 \\ \left(\dfrac{3n+1}{n}\right) \pmod p & \text{if } p = 7n + 4. \end{cases}$

*Proof.* Assertions (1), (2) and (3) follow from Lemma 2.44, Lemma 2.46 and Corollary 2.51. If we can show that $\Gamma_1$ belongs to $\mathcal{P}$ and that

$\Gamma_3$ satisfies the congruence we claim for it, then modulo $\mathcal{P}$ we will have

$$2a \equiv \Gamma_1 + \Gamma_3 \equiv \Gamma_3 \equiv \begin{cases} (-1)^n \binom{3n}{n} & \text{if } p = 7n+2 \\ (-1)^{n+1} \binom{3n+1}{n} & \text{if } p = 7n+4, \end{cases} \tag{2.66}$$

and (4) will follow at once. If 7 does not divide $\nu$, we have

$$\Gamma_\nu \equiv \sum z^{e\nu} \pmod{\mathcal{P}} \tag{2.67}$$

where $e = (p^3-1)/7$ and the summation runs over all $z$ in $GF(p^3)$ with $\mathrm{tr}\,(z) = 3$. If we write $e\nu = \alpha + \beta p + \gamma p^2$ with $0 \le \alpha, \beta, \gamma \le p-1$, then we have

$$\Gamma_\nu \equiv \sum z^\alpha z'^\beta z''^\gamma \pmod{\mathcal{P}} \tag{2.68}$$

where $z$ has the same meaning as in equation (2.67) and where $z' = z^p$ and $z'' = z'^p$. If $p = 7n+2$, then we have

$$(\alpha, \beta, \gamma) = \begin{cases} (4n+1, 2n, n) & \text{if } \nu = 1 \\ (5n+1, 6n+1, 3n) & \text{if } \nu = 3. \end{cases} \tag{2.69}$$

On the other hand, if $p = 7n+4$, then we have

$$(\alpha, \beta, \gamma) = \begin{cases} (2n+1, 4n+2, n) & \text{if } \nu = 1 \\ (6n+3, 5n+2, 3n+1) & \text{if } \nu = 3. \end{cases} \tag{2.70}$$

In either case, when $\nu = 1$ we have $\alpha + \beta + \gamma = p-1$ so the summation defining $\Gamma_1$ vanishes modulo $\mathcal{P}$ by Lemma 2.52. This proves that $\Gamma_1$ lies in $\mathcal{P}$. Now suppose that $\nu = 3$. Then we have $\alpha + \beta + \gamma = 2(p-1)$ and

$$\begin{aligned} \Gamma_3 &\equiv \sum z^\alpha z'^\beta (3 - z - z')^\gamma \\ &\equiv (-1)^\gamma \sum z^\alpha z'^\beta (z + z')^\gamma \pmod{\mathcal{P}} \end{aligned} \tag{2.71}$$

by Lemma 2.52. Expanding $(z+z')^\gamma$, we have

$$\Gamma_3 \equiv (-1)^\gamma \sum_z \sum_{\delta+\varepsilon=\gamma} \binom{\gamma}{\delta} z^{\alpha+\delta} z'^{\beta+\delta} \pmod{\mathcal{P}}. \tag{2.72}$$

By Lemma 2.60, only the term with $\alpha + \delta = \beta + \varepsilon = p - 1$ survives the summation over $z$, so that

$$\Gamma_3 \equiv (-1)^{\gamma} \binom{\gamma}{p-1-\alpha} \pmod{\mathcal{P}}. \tag{2.73}$$

Since $p \equiv n \pmod 2$, equations (2.69), (2.70) and (2.73) now imply that

$$\Gamma_3 \equiv \begin{cases} -\binom{3n}{n} \pmod{\mathcal{P}} & \text{if } p = 7n+2 \\ \binom{3n+1}{n} \pmod{\mathcal{P}} & \text{if } p = 7n+4 \end{cases} \tag{2.74}$$

and we are done. □

Eisenstein does not pause to interpret $\sigma_0$ as he did for primes of the form $8n+3$. However, it is easy for us to supply such an interpretation, just as it would have been easy for Eisenstein. By definition, $\sigma_0$ is the number of elements $x$ of $GF(p^3)$ such that $\mathrm{tr}\,(x) = 3$ and $[x] = 1$. Therefore, $7\sigma_0$ is the number of elements $y$ of $GF(p^3)$ such that $\mathrm{tr}\,(y^7) = 3$. Since $[z] = 1$ for all nonzero elements $z$ in $GF(p)$, we can replace 3 by any nonzero element of $GF(p)$. Therefore, $7(p-1)\sigma_0$ is the number of nonzero elements $y$ of $GF(p^3)$ such that $\mathrm{tr}\,(y^7) \neq 0$. Consequently, computing $\sigma_0$ is equivalent to computing the number of elements $y$ of $GF(p^3)$ such that $\mathrm{tr}\,(y^7) = 0$. We note that the equation $\mathrm{tr}\,(y^7) = 0$ defines a twisted form of the Fermat curve of degree 7.

Eisenstein has brought to our attention the utility of Fermat curves twisted by permutation representations of the Galois group. More generally, one can consider diagonal hypersurfaces twisted by permutation representations. What can be said about them and their zeta functions? The special case $\mathrm{tr}_{L/K}(x^d) = 0$, where $L/K$ is an extension of **A**-fields seems particularly appealing. Since the permutation representations of Aut $(\tilde{\mathbf{Q}})$ separate points of Aut $(\tilde{\mathbf{Q}})$, it seems that the special study of permutation twisted diagonal hypersurfaces ought to probe deeply into Aut $(\tilde{\mathbf{Q}})$.

**3. Complex multiplication of the lemniscatic function.** Although Eisenstein's arguments are quite interesting, what is of primary

concern to us in this paper is his brief allusion,[10] in the introduction to the paper [**12**], to the relation of his results to the theory of elliptic functions. He gives no clue here as to what he has in mind. Beyond referring to his proofs [**13**, p. 453] of biquadratic and sextic reciprocity using elliptic functions and to his priority dispute with Jacobi [**13**, p. 477], he merely promises to discuss the relevant principles on a more suitable occasion.

Eisenstein's paper [**12**] appeared in Crelle's Journal in 1848. Two years later, he published his paper [**14**], entitled, "Über die Irreductibilität und andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie." In this paper we find an important clue to what he has in mind regarding the relation of elliptic functions to the results of [**12**], namely, we find a new proof of Gauss' congruence formula for the decomposition of a prime of the form $4n+1$ as the sum of two squares. In this and the next section, we will examine Eisenstein's proof of Gauss' theorem. The proof is based on some properties of the equations for complex multiplication of the elliptic curve defined by

$$y^2 = 1 - x^4 \tag{3.1}$$

by primes in the Gaussian integers.[11] For primes of degree 1, these properties were obtained earlier in the first [**13**] of Eisenstein's series of papers on elliptic functions. In Section 3 of [**14**], Eisenstein gives a proof of this property which works for primes of degree 1 and primes of degree 2 simultaneously. In this and the next section, we will present his proof in [**14**] of these properties, drawing freely on the earlier paper [**13**].

The lemniscatic function $x = \phi(t)$ is defined as the inverse function of the definite integral

$$t = \int_0^x \frac{dx}{\sqrt{1-x^4}}. \tag{3.2}$$

If we let $m$ be an element of the ring $\mathbf{Z}[i]$ of Gaussian integers, and we let $y = \phi(mt)$, then we have

$$mt = \int_0^y \frac{dy}{\sqrt{1-y^4}}. \tag{3.3}$$

The functions $x = \phi(t)$ and $y = \phi(mt)$ are related by the partial differential equation

$$\frac{dy}{\sqrt{1-y^4}} = m \cdot \frac{dx}{\sqrt{1-x^4}} \tag{3.4}$$

with the boundary condition that $y$ vanishes when $x$ does. We have the identities

$$\begin{aligned} \phi(it) &= i\phi(t) \\ \phi(t+t') &= \frac{\phi(t)\sqrt{1-\phi(t')^4} + \phi(t')\sqrt{1-\phi(t)^4}}{1+\phi(t)^2\phi(t')^2} \end{aligned} \tag{3.5}$$

from [**13**, p. 300]. The second of these identities is the addition formula for the lemniscatic function. Using these identities separately, one can in principle obtain an expression for $\phi(mt)$ where $m$ is any Gaussian integer. However, in practice, the task is often very time consuming. It is therefore not without surprise that we read at the beginning of the paper [**13**, p. 299, equation (2)] that for odd Gaussian integers $m$, we can express $y$ in terms of $x$ in the form

$$y = x \cdot \frac{A_0 + A_1x^4 + A_2x^8 + \cdots + A_nx^{4n}}{1 + B_1x^4 + B_2x^8 + \cdots + B_nx^{4n}} \tag{3.6}$$

where $4n + 1 = |m|^2$ with $n$ an integer and where the coefficients[12] are Gaussian integers. Eisenstein states this in [**13**] without proof and without a suitable reference. As he is usually attentive to even the smallest details of his arguments, the omission is somewhat puzzling. On the other hand, in [**14**, p. 540], he indicates that formulas such as (3.6) are well known from the work of Abel and Jacobi. Actually, one can find similar formulas in the work of Jacobi [**48**, pp. 265-267] for multiplication of elliptic functions by integers and Eisenstein even shares the notation $U/V$ found on page 265 of [**48**]. However, I have not found an explicit statement of a formula such as (3.6) for multiplication of the lemniscatic function by odd Gaussian integers in either the work of Jacobi or the work of Abel. Therefore, in this section, we will present a proof (cf. Proposition 3.18 below) of equation (3.6) based on the lucid paper of Abel [**1**] and, in the next section, we will return to Eisenstein's proof of Gauss' theorem using the lemniscatic function.

Denote by $E$ the elliptic curve belonging to the equation

$$w^2 = 1 - z^4. \tag{3.7}$$

We take the point $(z, w) = (1, 0)$ as the origin of $E$ and denote it by $e$. The choice of $E$ uniquely determines a group law on $E$. Let us introduce, with Abel [**1**, p. 265], two new functions to accompany $\phi(t)$, namely,

$$f(t) = \sqrt{1 - \phi(t)^2} \tag{3.8}$$

and

$$F(t) = \sqrt{1 + \phi(t)^2}. \tag{3.9}$$

Referring to page 268 of Abel's paper, we find that the addition formulas are given by

$$\begin{aligned} \phi(\alpha+\beta) &= \frac{\phi(\alpha)\cdot f(\beta)\cdot F(\beta) + \phi(\beta)\cdot f(\alpha)\cdot F(\alpha)}{1+\phi(\alpha)^2\phi(\beta)^2} \\ f(\alpha+\beta) &= \frac{f(\alpha)\cdot f(\beta) - \phi(\alpha)\cdot\phi(\beta)\cdot F(\alpha)\cdot F(\beta)}{1+\phi(\alpha)^2\phi(\beta)^2} \\ F(\alpha+\beta) &= \frac{F(\alpha)\cdot F(\beta) + \phi(\alpha)\cdot\phi(\beta)\cdot f(\alpha)\cdot f(\beta)}{1+\phi(\alpha)^2\phi(\beta)^2}. \end{aligned} \tag{3.10}$$

If we now put $z = \phi(t)$ and $w = f(t)\cdot F(t)$, we obtain a parametrization of $E$ which maps 0 to the point $e$. Using the addition formula given above, we can now write the group law on $E$ explicitly in the form

$$\begin{aligned} &(z_1, w_1) + (z_2, w_2) \\ &\quad = \left( \frac{z_1 w_2 + z_2 w_1}{1 + z_1^2 z_2^2}, \frac{w_1 w_2 (1 - z_1^2 z_2^2) - 2 z_1 z_2 (z_1^2 + z_2^2)}{(1 + z_1^2 z_2^2)^2} \right). \end{aligned} \tag{3.11}$$

Our parametrization, which we will call $\Phi$, defines a homomorphism of the additive group of complex numbers onto the group $E$. The endomorphism ring of $E$ is isomorphic to the ring $\mathbf{Z}[i]$ of Gaussian integers. We can identify $\mathbf{Z}[i]$ with the endomorphism ring by requiring that $\Phi$ be a morphism of $\mathbf{Z}[i]$ modules. Denote by $\mathcal{M}$ the endomorphism of $E$ corresponding to the Gaussian integer $m$. Then $\mathcal{M}$ is a morphism of degree $|m|^2$ from $E$ to itself.

Now let $x = \phi(t)$ and $y = \phi(mt)$. Denote by $R$ the ring of all polynomials in $x$ with coefficients in the ring of Gaussian integers. Denote by $S$ the multiplicative semigroup consisting of all polynomials in $R$ whose constant term is equal to 1. Denote by $R'$ the ring consisting of all rational functions of the form $r/s$ with $r$ in $R$ and $s$ in $S$.

**Lemma 3.12.** *Let $m$ be an odd Gaussian integer, and let $G$ be one of the functions $\phi, f, F$. Then the function*

$$\frac{G(mt)}{G(t)} \tag{3.13}$$

*lies in $R'$.*

*Proof.* Let us say that a number $n$ has property $X$ if $n$ is a Gaussian integer such that the lemma is true with $m$ replaced by $n$. Using equation (3.5), we see that $\pm n$ and $\pm in$ all have property $X$ if and only if $n$ does. Using the addition formulas (3.10) with $\alpha = \beta$, we obtain the duplication formula [**1**, p. 279]

$$\begin{aligned} \phi(2\beta) &= \frac{2\phi(\beta)\cdot f(\beta)\cdot F(\beta)}{1+\phi(\beta)^4} \\ f(2\beta) &= -1 + \frac{2f(\beta)^2}{1+\phi(\beta)^4} \\ F(2\beta) &= -1 + \frac{2F(\beta)^2}{1+\phi(\beta)^4}. \end{aligned} \tag{3.14}$$

Combining equations (3.14) with the addition formulas (3.10) and equation (3.5), we see that $n$ has property $X$ if and only if $n \pm 2$ and $n \pm 2i$ have property $X$. Starting with the trivial observation that $\pm 1$ and $\pm i$ have property $X$ and using the hypothesis that $m$ is not divisible by $1 + i$, it now follows by induction that $m$ has property $X$. □

**Lemma 3.15.** *Let $x = \phi(t)$ and $y = \phi(mt)$, where $m$ is an odd Gaussian integer. Then $y$ is a rational function of $x$ of the form $y = U/V$ where $U$ and $V$ are relatively prime, with $U$ in $R$ and $V$ in $S$. We can write $U = xW$ with $W$ in $R$. Furthermore, $V$ and $W$ both have degree $|m|^2 - 1$.*

*Proof.* It follows from Lemma 3.12 that $y$ is a rational function of $x$ of the form $U/V$ with $u$ in $R$ and $V$ in $S$ and that $U = xW$ with $W$ in $R$. Furthermore, we can assume that $U$ and $V$ have no factor in common. Denote by $z$ the rational function on $E$ which associates to a point $(a, b)$ on $E$ the coordinate $a$. Then what we have shown is that there is a morphism $\mathcal{N}$ of $\mathbf{P}^1(\mathbf{C})$ onto itself such that the diagram

$$\begin{array}{ccc} E & \xrightarrow{\mathcal{M}} & E \\ \downarrow{\scriptstyle z} & & \downarrow{\scriptstyle z} \\ \mathbf{P}^1(\mathbf{C}) & \xrightarrow{\mathcal{N}} & \mathbf{P}^1(\mathbf{C}) \end{array} \tag{3.16}$$

is commutative, or what is the same, that

$$\mathcal{N}(x) = U/V = y. \tag{3.17}$$

Since $x$ divides $U$ and does not divide $V$, it follows that $y$ vanishes whenever $x$ does. Now consider the endomorphism $\mathcal{M}$ of $E$. It has degree $p = |m|^2$, which is an odd number[13]. It follows that $\mathcal{N}$ also has degree $p$. Therefore the maximum of the degrees of $U$ and $V$ is $p$. Furthermore, the morphism $\mathcal{M}$ is unramified. Therefore, the branch points of the morphism $\mathcal{N}$ must lie among the branch points of $z$, that is to say, at the points $\pm 1$ and $\pm i$ of $\mathbf{P}^1(\mathbf{C})$. In particular, 0 and $\infty$ are not branch points of $\mathcal{N}$. Since $\infty$ is not a branch point of $\mathcal{N}$, the degree of $U$ minus the degree of $V$ cannot exceed 1. Similarly, since 0 is not a branch point of $\mathcal{N}$, the degree of $V$ minus the degree of $U$ cannot exceed 1. If we replace $t$ by $it$, we change $x$ into $ix$, but the value of $y/x$ is unchanged. Therefore, writing $U = xW$ as above, we have $y/x = W/V$, and we conclude that $W$ and $V$ are really polynomials in $x^4$. It follows that the degree of $W$ equals the degree of $V$. Therefore, $U$ has degree $p$, $V$ and $W$ have degree $p - 1$, and the lemma is proved. □

**Proposition 3.18.** *Let $m$ be a Gaussian integer which is not divisible by $1 + i$, and let $4n + 1 = |m|^2$ be its norm, where $n$ is an integer. Let $x = \phi(t)$ and $y = \phi(mt)$. Then we can write $y$ as a rational function of $x$ in the form of equation* (3.6) *where $A_0, A_1, \ldots, A_n$ and $B_1, B_2, \ldots, B_n$ are all Gaussian integers, and where $A_n$ and $B_n$ are*

*both nonzero. Furthermore, the numerator and denominator have no factor in common.*

*Proof.* This follows at once from Lemma 3.12 and Lemma 3.15. □

**Corollary 3.19** (cf. [**13**, pp. 299–301]). *Let $m$ be a Gaussian integer which is congruent to 1 modulo $2+2i$, let $x = \phi(t)$, and let $y = \phi(mt)$. Then we have*

$$y = x \cdot \frac{A_0 + A_1 x^4 + A_2 x^8 + \cdots + A_{n-1} x^{4(n-1)} + x^{4n}}{1 + A_{n-1} x^4 + A_{n-2} x^8 + \cdots + A_1 x^{4(n-1)} + A_0} \tag{3.20}$$

*where $p = 4n+1 = |m|^2$, and where $A_0, A_1, \ldots, A_{n-1}$ are Gaussian integers.*

*Proof.* There is only one analytic function $g(x)$ such that

$$g'(x) = m \cdot \sqrt{\frac{1 - g(x)^4}{1 - x^4}} \tag{3.21}$$

subject to the boundary conditions $g(0) = 0$ and $g'(0) = m$. The uniqueness can be seen by writing $g(x)$ as a power series with undetermined coefficients. The condition $g'(0) = m$ then determines the power series for the righthand side of equation (3.21) in terms of the power series for $g(x)$. One can then determine the coefficients of $g(x)$ by induction. The existence of $g$ follows from Proposition 3.18. In fact, $g(x) = U/V$ where $U$ and $V$ are as in Proposition 3.18. Since the degree of $U$ is greater than the degree of $V$, it follows that as $x$ goes to infinity so does $y$. If we put $z = 1/y$ and $w = 1/x$, then we have

$$\frac{dz}{\sqrt{1 - z^4}} = m \cdot \frac{dw}{\sqrt{1 - w^4}}, \tag{3.22}$$

where $w$ vanishes when $z$ does and $dz/dw$ has the value $m$ at $w = 0$. Therefore, by what we have just proved about the differential equation (3.21), we have

$$\frac{1}{y} = z = w \cdot \frac{A_0 + A_1 w^4 + A_2 w^8 \cdots + A_n w^{4n}}{1 + B_1 w^4 + B_2 w^4 + \cdots + B_n w^{4n}}. \tag{3.23}$$

Since $w = 1/x$, we conclude that

$$y = x \cdot \frac{B_n + B_{n-1}x^4 + \cdots + B_1 x^{4(n-1)} + x^{4n}}{A_n + A_{n-1}x^4 + \cdots + A_1 x^{4(n-1)} + A_0 x^{4n}}. \tag{3.24}$$

By the uniqueness of $g$ and by comparison of equations (3.6) and (3.24), we find that $A_n^2 = 1$ and

$$A_k = B_{n-k}A_n \tag{3.25}$$

for $0 \leq k \leq n$, where we let $B_0 = 1$. If we let

$$\varpi = \int_0^1 \frac{dx}{\sqrt{1-x^4}}, \tag{3.26}$$

then $\phi(\varpi) = 1$, and from the addition formula we have

$$\phi((1 + 2\alpha + 2\beta i) \cdot \varpi) = (-1)^{\alpha+\beta} \tag{3.27}$$

for every pair of rational integers $\alpha, \beta$. Letting $t = \varpi$, we have $x = 1$, and equation (3.25) implies that

$$y = \frac{A_0 + A_1 + \cdots + A_n}{1 + B_1 + B_2 + \cdots + B_n} = A_n. \tag{3.28}$$

If we write $m$ as $1 + 2\alpha + 2\beta i$, then it follows from equations (3.27) and (3.28) that

$$A_n = y = \phi((1 + 2\alpha + 2\beta i) \cdot \varpi) = (-1)^{\alpha+\beta}. \tag{3.29}$$

Therefore, if $m$ is congruent to 1 modulo $2 + 2i$, we have $A_n = 1$. □

**Corollary 3.30.** *Let $m$ be an odd Gaussian integer, let $x = \phi(t)$, and let $y = \phi(mt)$. Then we can expand $y$ in a power series in $x$ of the form*

$$y = \sum_{n=0}^{\infty} c_{4n+1} x^{4n+1} \tag{3.31}$$

*where the $c_{4n+1}$ are Gaussian integers.*

*Proof.* This follows immediately from Proposition 3.18. □

**4. Eisenstein's proof of Gauss' theorem using the lemniscatic function.** In this section we present Eisenstein's proof of Gauss' theorem using the lemniscatic function. We begin with the following proposition, which can be found with its proof in [**14**, Section 3.2–3, pp. 547–548].

**Proposition 4.1.** *Let $M$ be an indeterminate, and consider the expansion of $\phi(Mt)$ in powers of $x = \phi(t)$. Then we can write the expansion in the form*

$$\phi(Mt) = \sum_{n=0}^{\infty} \frac{1}{\rho_{4n+1}} \cdot H_{4n+1}(M) \cdot x^{4n+1} \tag{4.2}$$

*where $H_{4n+1}(M)$ is a polynomial in $M$ with integer coefficients and content 1 and $\rho_{4n+1}$ is an integer. The polynomial $H_{4n+1}(M)$ is divisible by $M$ but not by $M^2$. Furthermore, if $q$ is a Gaussian prime number which divides $\rho_{4n+1}$, then the norm $|q|^2$ of $q$ is $\leq 4n+1$.*

*Proof.* We can expand $\sqrt{1-x^4}$ as a power series in $x$ and integrate term by term to obtain

$$t = x + \beta_5 x^5 + \beta_9 x^9 + \cdots . \tag{4.3}$$

We can therefore write $x$ as a power series in $t$ with rational coefficients

$$x = \phi(t) = t + \gamma_5 t^5 + \gamma_9 t^9 + \cdots . \tag{4.4}$$

Replacing $t$ by $Mt$ in the expansion of $\phi$, we have

$$\phi(Mt) = Mt + \gamma_5 M^5 t^5 + \gamma_9 M^9 t^9 + \cdots . \tag{4.5}$$

If we take $t$ as in equation (4.3), then any power of $t$ is also a power series in $x$ with rational coefficients. In particular, we can write

$$t^{4n+1} = x^{4n+1} + \beta_{4n+5}^{(4n+1)} x^{4n+5} + \beta_{4n+9}^{(4n+1)} x^{4n+9} \cdots \tag{4.6}$$

for all $n \geq 1$. Substituting the power series expansion (4.3) of $t$ into the power series expansion (4.5) of $\phi(Mt)$, we obtain

$$\phi(Mt) = M + \sum_{n=1}^{\infty} G_{4n+1}(M) x^{4n+1} \tag{4.7}$$

where

$$\begin{aligned} G_{4n+1}(M) = \beta_{4n+1} M + \gamma_5 \beta_{4n+1}^{(5)} M^5 \\ + \gamma_9 \beta_{4n+1}^{(9)} M^9 + \cdots + \gamma_{4n+1} M^{4n+1} \end{aligned} \tag{4.8}$$

is a polynomial of degree at most $4n+1$ with rational coefficients. Let $\rho_{4n+1}$ be the lowest common denominator of the coefficients of $G_{4n+1}(M)$, and let $H_{4n+1}(M) = \rho_{4n+1} G_{4n+1}(M)$. Then $H_{4n+1}(M)$ has integer coefficients and content 1. Furthermore, since $\beta_{4n+1}$ is nonzero, it follows that $H_{4n+1}(M)$ is divisible by $M$ but not by $M^2$. Now let $q$ be a Gaussian prime number, and suppose that $q$ divides $\rho_{4n+1}$. If $q = \pm 1 \pm i$, then the norm of $q$ is 2, which is $< 4n+1$. On the other hand, suppose that $q$ is odd. If we write $y = \phi(mt)$ as a power series in $x = \phi(t)$, we see from Corollary 3.30 that, for any Gaussian integer $m$, the coefficient $c_{4n+1}$ of $x^{4n+1}$ in the expansion of $y$ in powers of $x$ is a Gaussian integer. But we have

$$c_{4n+1} = \frac{1}{\rho_{4n+1}} H_{4n+1}(m), \tag{4.9}$$

so that, for every Gaussian integer $m$, we have

$$H_{4n+1}(m) \equiv 0 \pmod{q}. \tag{4.10}$$

Since $q$ is an odd Gaussian prime, as $m$ runs over all odd Gaussian integers the congruence class of $m$ modulo $q$ will run over all residue classes modulo $q$. It follows that $H_{4n+1}(M)$ has $|q|^2$ distinct roots modulo $q$. Therefore, the degree of $H_{4n+1}$ must be $\geq |q|^2$. But $H_{4n+1}$ has degree $\leq 4n+1$, so we have $4n+1 \geq |q|^2$. □

The following corollary of Proposition 4.11 occurs in effect in [**14**, Section 3, p. 548].

**Corollary 4.11.** *Let $m$ be an odd Gaussian prime number, let $x = \phi(t)$, and let $y = \phi(mt)$. Then, in the expansion* (3.31) *of $y$ as a power series in $x$, if $4n+1 < |m|^2$ we have*

$$c_{4n+1} \equiv 0 \pmod{m}. \tag{4.12}$$

*Proof.* Let $H_{4n+1}(M)$ and $\rho_{4n+1}$ be as in Proposition 4.1. Then, by Corollary 3.30 and Proposition 4.1, we have

$$H_{4n+1}(m) = \rho_{4n+1} c_{4n+1} \tag{4.13}$$

for all $n$. By Proposition 4.1, $M$ divides $H_{4n+1}(M)$ and therefore $H_{4n+1}(m)$ is divisible by $m$. Furthermore, Proposition 4.1 also implies that $m$ does not divide $\rho_{4n+1}$ when $4n+1 < |m|^2$. Therefore, for such $n$, the congruence (4.12) must hold. □

The next corollary of Proposition 4.11 occurs in [**14**, Sections 3 and 4].

**Corollary 4.14.** *Let $m$ be an odd Gaussian prime number, $x = \phi(t)$ and $y = \phi(mt)$. Then in Corollary* 3.19*, the Gaussian integers $A_0, A_1, \ldots, A_{n-1}$ are all divisible by $m$.*

*Proof.* According to Corollary 4.11, the coefficient $c_{4n+1}$ of $x^{4n+1}$ in the power series expansion of $y$ is divisible by $m$ whenever $4n+1 < |m|^2$. Therefore, we can write $y$ in the form

$$y = mS + x^p T \tag{4.15}$$

where $p = |m|^2$ and where $S$ and $T$ are power series in $x$ with coefficients in $\mathbf{Z}[i]$. Since $y = U/V$, with $U$ and $V$ as in Lemma 3.15, we have

$$U = m \cdot S \cdot V + x^p \cdot T \cdot V. \tag{4.16}$$

Therefore, all of the terms of $U$ of degree $< p$ have coefficients which are divisible by $m$, which proves the Corollary. □

Our last corollary of Proposition 4.11 occurs in [**14**, p. 550].

**Corollary 4.17.** *Let $m$ be a Gaussian prime number which is congruent to $i^\nu$ modulo $2+2i$. Let $x = \phi(t)$, $y = \phi(mt)$, and write $y = U/V$ as in Lemma 3.15. Then we have*

$$U \equiv i^\nu x^p \pmod{m} \tag{4.18}$$

*and*

$$V \equiv 1 \pmod{m}$$

*where $p = |m|^2$. In particular, $y \equiv i^\nu x^p \pmod{m}$.*

*Proof.* First suppose that $m$ is congruent to 1 modulo $2+2i$. In that case, we are done by Corollary 4.14 and Corollary 3.30. If $m$ is congruent to $i^\nu$ modulo $2+2i$, we can write $m = i^\nu m_0$, where $m_0$ is congruent to 1 modulo $2+2i$. Then we have

$$\frac{y}{x} = \frac{\phi(mt)}{\phi(t)} = i^\nu \cdot \frac{\phi(m_0 t)}{\phi(t)} = \frac{U_0}{V_0} \tag{4.19}$$

where $U_0$ and $V_0$ are polynomials with Gaussian integer coefficients such that $U_0 \equiv x^p \pmod{m}$ and $V_0 \equiv 1 \pmod{m}$. The corollary follows at once. □

We note that Corollary 4.17 amounts to the recognition of the Frobenius endomorphism as a complex multiplication in the endomorphism ring of the elliptic curve $E$. Although we do not need the irreducibility of the polynomial $W$, let us also note, as Eisenstein did, that it follows from Corollary 4.17 and the fact that $W(0) = m$, using the Eisenstein irreducibility criterion. Eisenstein is also aware of the analogy of $W$ to the cyclotomic polynomial, as he remarks on page 540 of [**14**].

**Eisenstein's proof of Gauss' theorem.** Let $p$ be a prime of the form $4n+1$. That $p$ is the sum of two squares was already proved by Euler. Therefore we can write $p$ in the form $m\overline{m}$ where $m$ is a Gaussian prime number which is congruent to 1 modulo $2+2i$. Let $x = \phi(t)$ and $y = \phi(mt)$. Then, by Corollary 4.17 we can write $y$ in the form $U/V$, and we have

$$y \equiv x^p \pmod{m}. \tag{4.20}$$

Therefore, by Corollary 3.30, the coefficient $c_p$ of $x^p$ in the power series expansion of $y$ satisfies

$$c_p \equiv 1 \pmod{m}. \tag{4.21}$$

It follows that the coefficient of $x^{p-1}$ in

$$\frac{1}{m}\frac{dy}{dx} \tag{4.22}$$

is congruent to $\overline{m}$ modulo $m$. On the other hand, we have

$$\frac{1}{m}\frac{dy}{dx} = \sqrt{\frac{1-y^4}{1-x^4}}. \tag{4.23}$$

But modulo $m$, we have

$$\sqrt{\frac{1-y^4}{1-x^4}} \equiv \sqrt{\frac{(1-x^4)^p}{1-x^4}} = (1-x^4)^{2n}. \tag{4.24}$$

The coefficient of $x^{p-1}$ in the expression on the right is $(-1)^n\binom{2n}{n}$. It follows that

$$\overline{m} \equiv (-1)^n \binom{2n}{n} \pmod{m}. \tag{4.25}$$

If we write $m = a + bi$, then we have

$$2a \equiv (-1)^n \binom{2n}{n} \pmod{p}. \tag{4.26}$$

This value of $a$ differs by at most a harmless sign from the value obtained by Gauss. □

**5. Generalized Eisenstein elliptic function proof for $p = 8n + 3$.** to the best of my knowledge, the proof considered at the end of the last section is the only clue we have from Eisenstein's published work as to what he has in mind for applying elliptic functions to the primes of the form $8n + 3$, $7n + 2$ and $7n + 4$. It is natural to suppose that Eisenstein planned to imitate his proof of Gauss' theorem by using elliptic functions belonging to elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-7})$ and by decomposing the

Frobenius endomorphism in the endomorphism rings of these elliptic curves. Eisenstein himself refers briefly to papers of Abel and Jacobi in volume III of Crelle's Journal in connection with the study of singular moduli. I am not aware of any of Eisenstein's work which deals explicitly with elliptic functions for the case of complex multiplication by $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-7})$. However, I don't think Eisenstein would have made his claim without being certain that he could back it up. It is perhaps also worth mentioning that the elliptic curves with complex multiplication by the rings of integers of $\mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-7})$ are precisely those elliptic curves with an endomorphism of degree 2. In this section and the next, we will generalize Eisenstein's proof of Gauss' theorem considered at the end of Section 4. More precisely, we will prove Theorem 2.26(2) using elliptic functions.

The first step in Eisenstein's proof of Gauss' theorem was a proof of what we now call the Kronecker congruence formula in the lemniscatic case. Kronecker's own proof of the Kronecker congruence formula (equation (64), p. 439 of [**69**]) did not appear until 1886, almost 40 years after Eisenstein's publication in the lemniscatic case. I am not aware of any publication of such congruence relations before [**69**] other than the publication in the lemniscatic case in [**14**]. Kronecker himself, when discussing the antecedents of his congruence refers to Euler's congruences [**22**] for multiplication of sine and tangent.[14] I don't know why he did not also mention the work of Eisenstein.[15] Under the hypothesis that Eisenstein did indeed have a proof along the lines described in the last section using elliptic functions of the results of [**12**], then it is natural to suppose that Eisenstein also proved the congruence formula for elliptic curves with complex multiplication by the rings of integers of $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-7})$. Therefore, we will assume that he did so.

Denote by $E$ the elliptic curve defined by

$$y^2 = 1 + 4x^2 + 2x^4. \tag{5.1}$$

If we let

$$T = \frac{x}{y}\sqrt{-2}, \tag{5.2}$$

then we have

$$\frac{dT}{\sqrt{1 + 4T^2 + 2T^4}} = \sqrt{-2} \cdot \frac{dx}{\sqrt{1 + 4x^2 + 2x^4}}. \tag{5.3}$$

This shows that $E$ has complex multiplication by the ring $J$ of integers of the quadratic field $\mathbf{Q}(\sqrt{-2})$. Let $m = a + b\sqrt{-2}$ be an element of $J$ such that $a^2 + 2b^2$ is an odd prime number $p$. Then, by the congruence relation which we suppose that Eisenstein proved, we can find polynomials $V(x)$ and $W(x)$ of degree $p-1$ with coefficients in $J$ such that

$$\frac{dX}{\sqrt{1+4X^2+2X^4}} = m \cdot \frac{dx}{\sqrt{1+4x^2+2x^4}}, \tag{5.4}$$

where $X = xW/V$ and such that

(i) $V(0) = 1$

(ii) $V \equiv 1 \pmod{mJ[x]}$

(iii) $W \equiv \pm x^{p-1} \pmod{mJ[x]}$.

Replacing $m$ by $-m$ if necessary, we may assume that the sign in (iii) is $+$. We can rewrite equation (5.4) in the form

$$\frac{1}{m} \cdot \frac{dX}{dx} = \sqrt{\frac{1+4X^2+2X^4}{1+4x^2+2x^4}}, \tag{5.5}$$

and equate the coefficients of $x^{p-1}$ in the two sides of equation (5.5). Modulo $m$, we have by (ii), (iii) and equation (5.4) that $X$ is congruent to $x^p$ modulo $m$. Therefore, the coefficient of $x^{p-1}$ on the left side of (5.5) is congruent modulo $m$ to the complex conjugate $\overline{m}$ of $m$. It also follows that the right side of (5.5) is congruent modulo $m$ to $(1+4x^2+2x^4)^N$ where $N = (p-1)/2$. Therefore, $\overline{m}$ is congruent modulo $m$ to the coefficient of $x^{p-1}$ in

$$(1+4x^2+2x^4)^N, \tag{5.6}$$

in perfect analogy with Eisenstein's proof in the lemniscatic case. But, unlike the lemniscatic case, *it is not apparent how to compute this coefficient.* The difference between the two situations is that, in the lemniscatic case, one needed a coefficient of a power of $1-x^4$, which has only two terms, and one can compute the coefficient using the binomial theorem. In the present case, we have a power of $1+4x^2+2x^4$, which has three terms, and there is no simple expression for the coefficient. In order really to imitate Eisenstein's proof in the lemniscatic case, we

need somehow to replace (5.6) by a suitable expression with only two terms, say, of the form $(1 - x^r)^s$. Here is how we do that.

If we now put

$$x = k \cdot \left( z + \frac{\omega}{z} \right), \qquad y = \frac{w}{(1-i) \cdot z^2} \tag{5.7}$$

where $\omega$ is a primitive eighth root of unity and $k$ is a root of

$$2\omega k^2 + 1 = 0, \tag{5.8}$$

then equation (5.1) becomes

$$w^2 = 1 - z^8. \tag{5.9}$$

Therefore, we can regard the equations (5.7) as defining a mapping $\psi$ of the curve $\mathcal{C}$ defined by equation (5.9) onto the elliptic curve $E$. If, in the expression for $y$, we write $u^4$ instead of $w$, then instead of equation (5.9) we get the equation

$$u^8 = 1 - z^8 \tag{5.10}$$

of a Fermat curve of degree 8. While we prefer to work with the hyperelliptic curve $\mathcal{C}$, let us note that we could just as easily base our discussion on the Fermat curve. If we pull the differential $dx/y$ back to $\mathcal{C}$ via $\psi$, we obtain the differential $\eta$ on $\mathcal{C}$ defined by

$$\eta = \frac{k \cdot (z^2 - \omega)}{w} \cdot dz. \tag{5.11}$$

Examples of hyperelliptic integrals reducible to elliptic integrals had already been considered by Euler [**31**, pp. 78–79]. Furthermore, in Richelot's paper [**76**] of 1846, which Eisenstein must surely have known about, an explicit reduction of the integral $\int \frac{f(x)dx}{\sqrt{1+x^8}}$ to elliptic integrals is given. Finally, Richelot refers to Legendre [**73**, p. 254], equation (VI) for the reducibility in general of the integral $\int \frac{P(x)dx}{\sqrt{\beta+\gamma x^2+\delta x^4+\gamma x^6+\beta x^8}}$ to elliptic integrals.[16] Therefore, we may suppose that Eisenstein knew about the reducibility of the differential $\eta$ to a differential on an elliptic curve. We can now complete the proof of Theorem 2.26(2) as follows.

Now suppose that $p$ is of the form $8n+3$. Let $K$ be the extension of $\mathbf{Q}$ generated by $k$, and let $\mathcal{P}$ be a prime of $K$ lying over $mJ$. Let $f(x)$ be an algebraic function of the variable $x$ such that

$$X = k' \cdot \left( f + \frac{\omega^3}{f} \right) \tag{5.12}$$

where $k = \pm\omega \cdot k'$ and the sign is chosen such that we have

$$k^p \equiv k' \pmod{\mathcal{P}}. \tag{5.13}$$

Reducing equation (5.12) modulo $\mathcal{P}$ and using the Kronecker congruence relation and the equations (5.7), we have

$$\begin{aligned} k' \cdot \left( f + \frac{\omega^3}{f} \right) \equiv X \equiv x^p &\equiv \left( k \cdot \left( z + \frac{\omega}{z} \right) \right)^p \\ &\equiv k' \cdot \left( z^p + \frac{\omega^3}{z^p} \right) \pmod{\mathcal{P}}. \end{aligned} \tag{5.14}$$

Let $f$ be the solution of equation (5.12) which is congruent to $z^p$. Equation (5.4) then becomes

$$\frac{k'(f^2 - \omega^3)}{\sqrt{1 - f^8}} \cdot df = m \cdot \frac{k(z^2 - \omega)}{\sqrt{1 - z^8}} \cdot dz. \tag{5.15}$$

We can rewrite equation (5.15) as

$$\frac{1}{m} \cdot \frac{df}{dz} = \frac{k}{k'} \cdot \frac{z^2 - \omega}{f^2 - \omega^3} \cdot \sqrt{\frac{1 - f^8}{1 - z^8}} \tag{5.16}$$

and compute the coefficient of $z^{p-1}$ modulo $\mathcal{P}$ on each side of equation (5.16). Since $f$ is congruent to $z^p$ modulo $\mathcal{P}$, the coefficient is congruent to $\overline{m}$ modulo $\mathcal{P}$. Since $m \equiv 0 \pmod{\mathcal{P}}$, the coefficient is congruent to $m + \overline{m} = 2a$ modulo $\mathcal{P}$. Since $f$ is congruent to $z^p$ and we have

$$\frac{k}{k'} \cdot \frac{z^2 - \omega}{f^2 - \omega^3} \cdot \sqrt{\frac{1 - f^8}{1 - z^8}} \equiv \pm \frac{1}{\omega} \cdot \frac{z^2 - \omega}{-\omega^3} \cdot (1 - x^8)^N \tag{5.17}$$

modulo $z^p$ and $\mathcal{P}$, where $N = (p-1)/2 = 4n+1$. Therefore, the coefficient of $z^{p-1}$ in the righthand side of equation (5.16) is congruent modulo $\mathcal{P}$ to

$$\pm\frac{1}{\omega}\cdot\frac{1}{-\omega^3}\cdot(-1)^n\binom{4n+1}{n} = \pm\binom{4n+1}{n}, \tag{5.18}$$

which proves Eisenstein's results in the case $p = 8n+3$.

**6. Fermat curves and Eisenstein's theorem.** As we noted in the last section, what made it possible to complete the proof of the case $8n+3$ was the fact that the elliptic curve with complex multiplication by $\mathbf{Z}[\sqrt{-2}]$ occurs in the Jacobian variety of the curve

$$w^2 = 1 - z^8 \tag{6.1}$$

and therefore of the Fermat curve

$$u^8 = 1 - z^8. \tag{6.2}$$

This amounted to saying that the differential defined by equation (5.11) is reducible to an elliptic differential. Using contemporary knowledge of the Fermat curves, it is therefore natural to expect that a proof in the cases $7n+2, 4$ would involve the Fermat curve $\Phi_7$ defined by

$$X^7 + Y^7 + Z^7 = 0 \tag{6.3}$$

and its differentials. The differentials on the Fermat curve $\Phi_7$ are spanned by residues of the form

$$\omega_{abc} = \operatorname{Res}\left(\frac{7\cdot X^aY^bZ^c}{X^7+Y^7+Z^7}\cdot\left(\frac{dX}{X}\wedge\frac{dY}{Y} - \frac{dX}{X}\wedge\frac{dZ}{Z} + \frac{dY}{Y}\wedge\frac{dZ}{Z}\right)\right) \tag{6.4}$$

where $a, b, c$ are integers such that $0 < a, b, c < 7$ and $a+b+c = 7$. Calculating these residues as Griffiths [**41**] does, we get in local coordinates with $Z = 1$ that

$$\begin{aligned}\omega_{abc} &= \operatorname{Res}\left(\frac{7\cdot X^aY^b}{X^7+Y^7+1}\cdot\frac{dX}{X}\wedge\frac{dY}{Y}\right)\\ &= \operatorname{Res}\left(\frac{X^aY^b}{Y^7}\cdot\frac{dX}{X}\wedge\frac{d(X^7+Y^7+1)}{X^7+Y^7+1}\right)\\ &= \frac{X^{a-1}dX}{Y^{7-b}}.\end{aligned} \tag{6.5}$$

The Fermat curve $\Phi_7$ is invariant under automorphisms of $\mathbf{P}^2(\mathbf{C})$ of the form

$$\phi_{ijk}([X,Y,Z]) = [\zeta^i X, \zeta^j Y, \zeta^k Z], \tag{6.6}$$

where $\zeta$ is a primitive seventh root of unity, as well as under permutations of the coordinates. Let

$$H = \{\phi_{ijk} \mid i + 2j + 4k \equiv 0 \pmod 7\}. \tag{6.7}$$

Then $H$ is a group. The quotient $H\backslash\Phi_7$ may be realized as a plane curve via the mapping (cf. [**44**])

$$[X,Y,Z] \longmapsto [XY^2Z^4, YZ^2X^4, ZX^2Y^4] = [A,B,C]. \tag{6.8}$$

The image consists of all points $[A,B,C]$ of the projective plane such that

$$A^3B + B^3C + C^3A = 0. \tag{6.9}$$

This image is the famous curve of genus 3 with 168 automorphisms, also known as the Klein curve[**54**].[17] It is isomorphic to the modular curve $X(7)$ of level 7 and its automorphism group is isomorphic to the group $PSL_2(\mathbf{F}_7)$. Denote this curve by $\mathcal{C}$. The Jacobian variety of $\mathcal{C}$ is isomorphic (cf. [**6**]) to the product of three copies of an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}$ of the imaginary quadratic field $\mathbf{Q}(\sqrt{-7})$. The differentials on $\mathcal{C}$ are simply the differentials on $\Phi_7$ which are invariant under $H$. A basis for the invariant differentials is given by

$$\omega_{124} = \frac{dX}{Y^5}, \qquad \omega_{412} = \frac{X^3dX}{Y^6}, \qquad \omega_{241} = \frac{XdX}{Y^3}. \tag{6.10}$$

The curves $\mathcal{C}$ and $\Phi_7$ are defined over the field $\mathbf{Q}$ of rational numbers. Since the mapping $\Phi_7 \to \mathcal{C}$ given in equation (6.8) is defined over the field of rational numbers, the reduction of that mapping modulo a prime $p$ will commute with the $p$th power mapping $f_p$.

Assume that, for such $p$, the differential equation

$$\frac{dU}{(1-U)^{5/7}} = m \cdot \frac{dX}{(1-X^7)^{5/7}} \tag{6.11}$$

with $m = a+b\sqrt{-7}$, has a solution where $U$ is a power series in $X$ which is congruent modulo $\mathcal{P}$ to $X^p$. For any power series $f(x)$, we denote by $\gamma(f)$ the coefficient of $X^{p-1}$ in $f$. Then comparing coefficients of $X^{p-1}$ in the identity

$$\frac{1}{m}\frac{dU}{dX} = \left(\frac{1-U^7}{1-X^7}\right)^{5/7} \tag{6.12}$$

and then reducing modulo $\mathcal{P}$, we have modulo $\mathcal{P}$ that

$$\begin{aligned} \overline{m} &\equiv \gamma\left(\left(\frac{1-U^7}{1-X^7}\right)^{5/7}\right) \\ &\equiv \gamma\left(\left(\frac{(1-X^7)^p}{1-X^7}\right)^{5/7}\right) \\ &\equiv \gamma((1-X^7)^{5n}) \end{aligned} \tag{6.13}$$

where $p = 7n+1$. But the coefficient in question is $(-1)^n\binom{5n}{n}$. By Wilson's theorem, this is congruent to $(-1)^n\binom{3n}{n}$. Since $\overline{m} \equiv 2a \pmod{\mathcal{P}}$, we conclude that

$$2a \equiv (-1)^n \binom{3n}{n} \pmod{p}.$$

We could have used any of the differentials $\eta_1, \eta_2, \eta_4$ with the same result.

To deal with the cases $p = 7n+2$ and $p = 7n+4$, I again introduce some assumptions which formally yield Eisenstein's results in the style of the preceding argument. The hint comes from Eisenstein, who considered twisted forms of the Fermat curves. In his proof of the cases $p = 7n+2, 4$ he essentially considers the twisted form of the Fermat curve given by

$$\text{tr}\,(X^7) = 0, \tag{6.14}$$

where tr denotes the trace from $GF(p^3)$ to $GF(p)$. Equation (6.16) can also be written as

$$X^7 + (X^\sigma)^7 + (X^{\sigma^2})^7 = 0. \tag{6.15}$$

This is isomorphic to the Fermat curve $\Phi_7$ over the field $GF(p^3)$, and the associated 1-cocycle of the Galois group is actually a homomorphism of the Galois group onto the group of cyclic permutations of the three coordinates. There are two such homomorphisms, however. The action of Frobenius on the twisted form may be identified with the action of Frobenius $f_p$ on the untwisted form followed by a cyclic permutation $\tau$. Then we proceed as follows. We now have two cases.

*Case* 1. *$\tau$ is left shift.* Assume that there is a formal power series solution $U = U(X)$ of the equation

$$\frac{dU}{(1-U^7)^{5/7}} = m \cdot \frac{X\,dX}{(1-X^7)^{3/7}} \tag{6.16}$$

such that $U$ is congruent to $X^p$ modulo $\mathcal{P}$. Examining the coefficient of $X^{p-1}$ in $(1/m)(dU/dX)$, we have modulo $\mathcal{P}$ that

$$\begin{aligned} \overline{m} &\equiv \gamma\left(\frac{X\cdot(1-U^7)^{5/7}}{(1-X^7)^{3/7}}\right) \\ &= \gamma(X\cdot(1-X^7)^N) \end{aligned} \tag{6.17}$$

where $N = (5p-3)/7$. In order for the exponent $N$ to be an integer, $p$ must be of the form $7n+2$. The coefficient of $x^{p-1}$ is then $(-1)^n\binom{5n+1}{n}$. By Wilson's theorem, this is congruent to $\binom{3n}{n}$ modulo $p$, hence $\overline{m} = \binom{3n}{n} \pmod p$. Therefore, we have

$$2a \equiv \binom{3n}{n} \pmod p \tag{6.18}$$

for $p = 7n+2$.

*Case* 2. *$\tau$ is right shift.* Assume that there is a formal power series solution $U = U(X)$ of the equation

$$\frac{dU}{(1-U^7)^{5/7}} = m \cdot \frac{X^3\cdot dX}{(1-X^7)^{6/7}} \tag{6.19}$$

such that $U$ is congruent to $X^p$ modulo $\mathcal{P}$. Examining the coefficient of $X^{p-1}$ in $(1/m)(dU/dX)$ we have modulo $\mathcal{P}$ that

$$\begin{aligned} \overline{m} &\equiv \gamma\left(X^3\cdot\frac{(1-U^7)^{5/7}}{(1-X^7)^{6/7}}\right) \\ &= \gamma(X^3\cdot(1-X^7)^N) \end{aligned} \tag{6.20}$$

where $N = (5p-6)/7$. In order for the exponent $(5p-6)/7$ to be an integer, we must have $p = 7n+4$, so that the coefficient is $(-1)^n\binom{5n+2}{n}$, which by Wilson's theorem is congruent to $\binom{3n+1}{n}$ modulo $p$. Therefore, we have

$$2a \equiv \overline{m} \equiv \binom{3n+1}{n} \pmod{\mathcal{P}} \tag{6.21}$$

for $p = 7n+4$.

*Remark* 6.22. The reader will note the dependence of the above arguments for $p = 7n+1, 2, 4$ on the existence of certain formal power series. I do not know how to prove these assumptions.

**7. Did Eisenstein do it?** In Section 1, we presented Gauss' proof of Gauss' theorem. We observed, as Gauss did, that the argument depended on a knowledge of the number of points of a twisted form of a Fermat curve over a finite prime field. In Section 2 we presented Eisenstein's generalization of Gauss' theorem, which he proved along similar lines, using Eisenstein sums. In this case, Eisenstein pointed out that one is computing the number of points of a twisted Fermat curve over a finite field. In the case of Gauss' paper, the Fermat curve is twisted by changing the coefficients from 1 to other values. In the case of Eisenstein's paper, the Fermat curve is twisted by a homomorphism into the group of permutations of the three variables. However, Eisenstein states that he has other ways of looking at his results and indicates that he has proofs using elliptic functions.

In Section 3 we presented Eisenstein's proof of Gauss' theorem using the lemniscatic function. In Section 4 we showed that a similar proof could be given for Eisenstein's theorem about primes of the form $8n+3$, but that it was necessary to know that a certain differential on the curve $w^2 = 1 - z^8$ is reducible to an elliptic differential. This, of course, was already known from work of Richelot and earlier work of Legendre. And, as we noted in Section 4, there is no difficulty in viewing this differential as being on the Fermat curve of degree 8 instead. In Section 5 we showed how one could arrive at Eisenstein's results for $p = 7n+1, 2, 4$ by using differentials on the Fermat curve of degree 7 and by introducing certain hypotheses which we could not justify. That proof, whatever its drawbacks, nevertheless has the same flavor

and the same characteristic final trick as the proof Eisenstein gave in the lemniscatic case and shows that proofs in the cases $7n + 1, 2, 4$, along the lines of Eisenstein's proof in the lemniscatic case are at least conceivable. This makes it tempting to suppose that Eisenstein might have actually used the Fermat curve of degree 7 in his proof by elliptic functions in the cases $7n + 1, 2, 4$.

Such a proof, if he possessed it, would have required him to prove some form of the Kronecker congruence relation for elliptic curves with complex multiplication by the ring of integers of $\mathbf{Q}(\sqrt{-7})$. He could have done this without leaving the traditional realm of elliptic functions. But there is no way that he could have completed the proof along these lines, using the same final trick, without knowing that his elliptic differential actually lived on a Fermat curve. It is unlikely that he arrived at this knowledge by explictly working with a differential on the Fermat curve and reducing it to an elliptic integral. The reason is that the necessary transformations are apparently quite complicated, and it is doubtful that Eisenstein would have found them by accident. Nor is it likely that he would have attempted it without knowing in advance that such transformations existed.

It is natural to object that the concept of the Jacobian variety lay in the future, in the work of Riemann, but that is not entirely true. For example, in the letter Galois wrote the night before his fatal duel [**37**, pp. 25–32], he discusses the problems of extending to the integrals of algebraic functions the results of the theory of elliptic integrals, and his remarks indicate that he has anticipated some of the work of Riemann.[18] Furthermore, Galois's letter was published in September, 1832, by Auguste Chevalier in *Revue Encyclopédique*, page 568, in accordance with Galois's request at the end of the letter, and was therefore a matter of public knowledge 15 years before Eisenstein published [**12**]. We may also suppose that the work of Euler was available to Eisenstein.[19] Therefore, he might have discovered Euler's papers [**29, 31**] either through his own browsings or by finding reference to such work of Euler in papers of Jacobi, such as [**49**] or otherwise. In [**29**, p. 340] he would have found the following differential equations

$$\frac{dy}{\sqrt[3]{f + gy^3}} = \frac{dx}{\sqrt[3]{f + gx^3}} \tag{7.1}$$

and

$$\frac{dy}{\sqrt[4]{f+gy^4}} = \frac{dx}{\sqrt[4]{f+gx^4}}, \tag{7.2}$$

which are the analogues of equation (6.13) for the Fermat curves of degrees 3 and 4, as well as the differential equation

$$\frac{dy}{\sqrt{b+cy^2+dy^4+ey^6+fy^8}} = \frac{dx}{\sqrt{b+cx^2+dx^4+ex^6+fx^8}}, \tag{7.3}$$

which is quite similar to the equation which arises instead of equation (5.15) in the case $p = 8n+1$. Euler asserts that none of these equations admit algebraic solutions in general and Eisenstein might have thereby been motivated to investigate whethere Euler was correct.

Alternatively, since the periods of the Fermat curve are computable using Eulerian integrals of the first kind, Eisenstein could have known something about the period lattice of the Fermat curve, and then deduced the existence of a relation to the elliptic curve. For example, Jacobi [**50**, p. 377] mentions[20] that Legendre [**73**] had investigated the hyperelliptic integral $\int_0^x (dx/\sqrt{1-x^5})$ and arrived at expressions involving the gamma functions when $x = 1$ and $x = -\infty$. Eisenstein could have imitated this. On the other hand, one knows almost without computation that the Jacobian variety of the Klein curve is the product of three copies of an elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{-7})$ (cf. [**6**, p. 138]) from knowing that a certain group acts on the curve and therefore on its period lattice. Perhaps such qualitative reasoning could have been the germ of Eisenstein's idea.[21] The examples of Richelot, Legendre, Euler and Galois are cited to show that Eisenstein could plausibly have known enough about the Jacobian variety of the Fermat curve of degree 7 to know without explicit transformation that certain of its differentials are reducible to elliptic differentials. It would be desirable to construct, using the results and concepts available in Eisenstein's time, an argument for the reducibility without giving an explicit transformation to an elliptic differential.

In this connection, we should also mention another resource available to Eisenstein, namely Abel's great memoir [**2**], which appeared in 1841 and which presented Abel's theorem for general abelian integrals, not just the hyperelliptic integrals that had been discussed in the memoirs

of Abel that had appeared before. In [**2**], Abel devotes considerable energy to discussing examples, and among these examples one finds integrals of $n$th roots of rational functions, not just square roots. However, the only thing we can say with certainty is that, as long as the gaps remain in our approach to the cases $p = 7n + 1, 2, 4$, we cannot accurately judge the technique and how far Eisenstein might have gotten with it.

We should also mention that the method given in Section 5 in the case $p = 8n + 3$ is not the only way to obtain the coefficient of $x^{p-1}$ in $(1 + 4x^2 + 2x^4)^N$ modulo $p$, where $N = (p - 1)/2$. If we denote that coefficient by $c$, then a priori we have

$$c \equiv -\sum (1 + 4x^2 + 2x^4)^N \pmod{p}, \tag{7.4}$$

where the summation runs over all elements $x$ of $GF(p)$. This sum was considered by Whiteman [**86**, p. 546]. An examination of his argument shows that at one point he introduces a change of variables similar to (5.7) to reduce to the case of the hyperelliptic curve (5.9). Thus, the computation of the coefficient $c$ modulo $p$ still seems to involve a knowledge, whether conscious or not, of the fact that the hyperelliptic curve (5.9) can be mapped onto the elliptic curve (5.1). Furthermore, Whiteman [**86**] needs to draw on other parts of Eisenstein's paper [**12**] for his argument. The computation of this coefficient is therefore not immediate and perhaps involves as much work as Eisenstein has already done in [**12**]. Nevertheless, it does suggest an alternative to the hypothesis which we have proposed in this article. It may be that what Eisenstein meant by the connection with elliptic functions is no more than the observation that the values of $a$ such that $a^2 + 2b^2 = p$ (in the case $p = 8n + 3$) or $a^2 + 7b^2 = p$ (in the cases $p = 7n + 1, 2, 4$) could be described as the coefficients of $x^{p-1}$ in certain expressions such as (5.6), the proofs being based on elliptic functions, and did not go so far as to prescribe a uniform method of computing the coefficient. In the case of the lemniscatic function, the coefficient is apparent by inspection. In the case of $p = 8n + 3$, it involves character sums which are computed by other methods.

In our opinion, this hypothesis, while perhaps true, is less satisfying precisely because it does not address the method of computing the coefficient. In the case of [**86**], some knowledge of the existence of a mapping of the hyperelliptic curve (5.9) onto the elliptic curve (5.1) is

involved. So the evidence of [**86**] tends to support the main hypothesis of this paper. Another way to obtain the coefficient $c$ modulo $p$ has in effect been given by Rajwade [**75**], who uses the Riemann hypothesis for an elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{-2})$. While we must admit that Eisenstein himself points out that he is computing the number of solutions modulo $p$ of certain equations which we can see define twisted Fermat curves, there is no evidence that Eisenstein had made any such observations in the case of elliptic curves. And we have no evidence of any knowledge of the Riemann hypothesis for curves on the part of Eisenstein.

I would also like to draw attention to the letter [**17**] from Eisenstein to his friend Stern dated July, 1849. Recall that it was Stern who had empirically discovered that the binomial congruence formulas for quadratic decompositions also held for decomposition of primes of the form $8n + 3$ as $a^2 + 2b^2$. Towards the end of the letter (page 818), Eisenstein refers to objections Stern had expressed in an earlier letter[22] to the effect that it appeared that every case treated by Eisenstein required a separate argument and that therfore it seemed not to be the way to approach the subject. Eisenstein replies that his method is perfectly general and that he has merely specialized it to the examples he discussed in order to illustrate the spirit of the method and to show that it also applies when the "determinant" is not a divisor of $p - 1$. Here he is apparently referring to the discriminant of the quadratic form in terms of which one hopes to express the prime number. Furthermore, he uses the same terminology in the introduction to [**12**] when describing how his results are qualitatively different from any that have gone before. So it is likely that he is referring to the paper [**12**] and its methods. He then writes[23]: "*Ausserdem weiß ich nur eine umfassende freilich hiervon ganz verschiedene Methode durch die elliptischen Funktionen.*" This does not sound as though Eisenstein believes that his approach via elliptic functions applies only to the lemniscatic case!

There is one last bit of evidence to consider. We find some severe criticisms of Eisenstein in a footnote at the end of Jacobi's article [**51**]. Jacobi complains about two articles of Eisenstein, namely [**18**] and [**19**], specifically about certain errors. Jacobi concluded from [**18**] that Eisenstein did not understand the period lattices of abelian functions, precisely the point which is at issue in the present article. He also

ridicules some of Eisenstein's other speculations on abelian functions in [**18**]. He also claimed that Eisenstein did not realize that the values of some infinite product expansions arising in the theory of elliptic functions depend on the order in which the factors are multiplied. This fault he finds in both the articles [**18**] and [**19**]. On the other hand, in his review [**85**] of the Chelsea edition [**15**] of Eisenstein's collected works, Weil cites the very same articles [**18**] and [**19**] of Eisenstein as containing the basic principles expounded in Eisenstein's great memoir [**20**], the *Genaue Untersuchung*. So it appears that Jacobi's opinion is in conflict with that of Weil, who devoted half of his book [**81**] to a close examination of the memoir [**20**].

Weil also quotes the opinion of Eisenstein's contemporary Dirichlet, to whom he attributes the remark in 1849 that Eisenstein "has learnt the art of self-criticism, in which he had been lacking before." Can this be a clue to other contemporary criticisms of Eisenstein's work? Weil did not give a reference for this remark of Dirichlet and in fact one cannot find it in Dirichlet's collected works. However, the letter was published by Biermann in [**7**, p. 39]. Actually, Dirichlet made the above statement in a letter in which he was trying to get a promotion [**8**] for Eisenstein. He apparently felt the need to explain why it was that the number of articles published annually by Eisenstein had decreased, so he explained it by saying, in effect, that Eisenstein had become more selective about what he published. It was not intended to be a criticism of the correctness of Eisenstein's work.

As for the articles [**18,19**] themselves, although I have read them and the article [**51**], I have not been able to do so carefully enough to form a definite impression of Eisenstein's intentions in his speculations about abelian functions in [**18**], since he is not sufficiently explicit about how he proposes to represent abelian functions. However, it does appear that the criticisms that Jacobi levels at him are not accurate. Jacobi suggests that Eisenstein is unaware of the principles regarding quadruply periodic functions that Jacobi set forth in [**52**], whereas Eisenstein refers explicitly to [**52**] in Section 2 of [**18**]. Eisenstein is critical of [**52**], but it is clear from Eisenstein's remarks that he is criticizing the foundations of Jacobi's work, not his conclusions. In Section 3 of [**18**], Eisenstein proposes different foundations and for that purpose considers functions with $n$-tuply infinite product representations. Contrary to what Jacobi seems to be suggesting,

Eisenstein is fully aware that there are no discrete subgroups of rank $n > 2$ in the additive group of complex numbers, and part of his speculations center around methods of getting around that problem, specifically by restricting his infinite products to run over values of the indices satisfying certain inequalities. Furthermore, nowhere in [**18**] does Eisenstein explicitly claim that the functions represented by his $n$-tuply infinite products will be related to Abelian functions. Although I can see how the structure of Eisenstein's paper and his remarks could have led Jacobi to conclude otherwise, it is equally possible to conclude that Eisenstein merely criticized Jacobi's foundations in Section 2 and then proceeded to describe what he considered to be a promising generalization of the infinite products he had introduced in Section 1 to study circular and elliptic functions.

One could dismiss Eisenstein's proposal as pure speculation were it not for the fact that at the end of the article, he writes:[24]

> Ganz im Allgemein läßt sich hier über die Wahl dieser Bedingungsgleichungen nichts Näheres sagen. Aber es existirt eine ganze Classe solcher Functionen, welche in sehr enger Beziehung zu gewissen Resultaten in *Zahlentheorie* stehen; und gerade für diese besondere Gattung zeigen die Ungleichheitsbedingungen, von welchen wir reden, eine sehr eigenthümliche Beschaffenheit. Man findet nämlich für diese Fälle immer eine Verbindung aus einer bestimmten Anzahl von der Werthen des Ausdrucks **N**, zu welche kommen darauf hinaus, daß sie eine ganze *Gruppe* unendlich vieler Werthe con **N**, für welche dieser Verbindung der nämliche Werth zukommt, und die als die Glieder geometrischer Reihen erscheinen, auf ein einziges **N** reducieren. Die Functionen, we welchen man auf diesem Wege geführt wird, scheinen sehr merkwürdige Eigenschaften zu besitzen; sie erröffnet ein Feld, auf dem sich Stoff zu den reichhaltigsten Untersuchungen darbietet, und welches der eigentliche Grund und Boden zu sein scheint, auf welchem die schwierigsten Theile der Analysis und Zahlentheorie in einander greifen.

It is clear from this passage that Eisenstein has something quite specific in mind and also that he believes he possesses at least some examples. What they might be is not clear from his brief comments. I feel that Eisenstein's article [**18**] deserves much closer study both by itself and in the context of Eisenstein's work as a whole. There are other clues as well as to what he might have had in mind and I plan to discuss them

in a future article.

This hint that Eisenstein was interested in functions expressible as multiply infinite products (or sums, as in his subsequent comments) might provide a missing clue as to Eisenstein's ideas for an approach to the results of [**12**] via elliptic functions. For example, and not the only one, if $p = 4n+3$ is a prime, then any abelian variety of $A$ of dimension $2n+1$ with complex multiplication by the regular representation of the ring of integers of the cyclotomic field $\mathbf{Q}(\zeta_p)$ is isomorphic to a product of $2n+1$ copies of an elliptic curve with complex multiplication by the ring of integers of $\mathbf{Q}(\sqrt{-p})$, as shown in [**6**]. The abelian functions on this abelian variety will then be closely related to theta series, which are multiply infinite sums. For $p = 7$, the abelian variety is a factor of the Jacobian variety of the Fermat curve of degree 7, but for $p > 7$, it is not.[25] Thus, the connection with the Jacobian varieties of Fermat curves might be hidden in the study of Eisenstein's multiply infinite products or sums and only valid for $p \leq 7$. In any case, it is not yet clear how the characteristic final trick of Eisenstein's lemniscatic proof can be obtained in this setting.

**Acknowledgments.** I am indebted to S. Ramanan for inviting me to Tata Institute, to Mikhail Gromov for inviting me to IHES, and to Roger Howe and Walter Feit for making it possible for me to use the closely guarded facilities of Yale University, including its excellent library and the computer used to typeset the first revision of this article since [**3**]. I am also grateful to André Weil for reading the manuscript in 1985, encouraging me to publish it and answering a number of questions regarding historical aspects of the paper; to Benedict Gross, who read and criticized portions of [**3**], and who used [**4**] to prepare some material for his number theory course at Harvard in the spring of 1990, and for his help with footnote 25; and to Harold Edwards for reading an early version of the manuscript and offering many constructive criticisms. Finally, I am indebted to Tal Kubo for his help with some bibliographic references during the final stages of preparing this manuscript when I did not have access to a good library, to Klaus Ernst and Bettina Richmond for their help with German translation in footnotes 10 and 24, and to Jim Porter for allowing me to use a computer at Western Kentucky University, where this article was revised for the last time.

## ENDNOTES

1. On p. 213 of [**34**] we find: "Toute nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux carrés, et une seule fois l'hypotenuse d'un triangle rectangle." [Section 0, p. 1, line 2]

2. The note [**35**] is not on what Diophantos wrote but in reference to some of the commentary of Bachet on Diophantos. [Section 0, p. 1, line 2]

3. Fermat actually sent the letter [**36**] to Carcavi, who then passed it on to Huygens. On p. 432, Fermat states the result and then indicates that he proved it by descent. The letter [**36**] also occurs as Letter 651 of Huygens' correspondence. [Section 0, p. 1, line 2]

4. "Anachronism consists in attributing to an author such knowledge as he never possessed..." (cf. [**84**], p. 438). [Section 0, p. 3, line 1]

5. Actually, both the Commentatio Prima and the Commentatio Secunda will be translated in the final version of [**5**]. [Section 0, p. 4, line 27]

6. If $n$ is even, then $-1$ is a fourth power $\mod p$ and the equations $1 + e^i x^4 + e^j y^4 = 0$ and $1 + e^e x^4 - e^j y^4 = 0$ have the same number of solutions. [Section 1, p. 5, line 15]

7. We can take them to be $2(12) = n - 2(02)$, $(00) = n - 1 - 3(02)$ and $(03) = 2(02) - (01)$. This expresses all $(i\ \ j)$ in terms of (01) and (02). [Section 1, p. 6, line 8]

8. After applying the relations (1.9) to the expression $p - a^2 - b^2$, one finds that it is proportional as a polynomial in (01) and (02) to the difference between (1.11) and (1.12). [Section 1, p. 6, line -2]

9. We will sometimes write $i$ for the image $f^2$ of $\omega^2 = i$ in $GF(p^2)$ when no confusion can occur. [Section 2, p. 10, line 3]

10. Eisenstein writes: "*Auf diejenigen Principien, welche der Theorie der Elliptischen Functionen zur Behandlung dieser Fragen an die Hand giebt, werde ich bei einer künftigen Gelegenheit aufmerksam machen.*" This may be translated as: "On a future occasion I will discuss those principles which the theory of elliptic functions provides for treating these questions." We note that he does not mention abelian functions,

which is somewhat problematic for the approach we have suggested here. However, see also the comments at the end of Section 7. [Section 3, p. 22, line 1]

11. The proof is found in the paper [**14**], which appeared two years after the paper [**12**]. Perhaps [**14**] is the *künftigen Gelegenheit* mentioned in footnote 10. However, I consider it unlikely that this is all Eisenstein had to say about the matter since he mentions the connection to elliptic functions in the context of a discussion of primes of the form $8n+3$ and $7n+2, 4$, not primes of the form $4n+1$. [Section 3, p. 22, line 20]

12. In [**14**] the numbering of the coefficients is the reverse of the numbering of [**13**]. We follow the numbering of [**13**]. [Section 3, p. 23, line 15]

13. We follow Eisenstein in using $p$ to denote $|m|^2$, which is an odd number and may be composite. [Section 3, p. 26, line 12]

14. Kronecker (p. 439 of [**69**], on the same page as the Kronecker congruence relation (64)), writes: "*Eben diese Congruenz* (64) *bildet den Hauptzielpunkt der vorstehen Entwickelungen; sie ist für die Theorie der Transformation der elliptischen Functionen, sowie für alle arithmetischen Anwendungen dieser Theorie von ebenso fundamentaler Bedeutung, wie es die analogen, schon aus Euler'schen Entwickelungen hervorgehenden Congruenzen*:

$$(-1)^{\frac{1}{2}(n-1)} sin\ nu \equiv (sin\ u)^n,\ (-1)^{\frac{1}{2}(n-1)} tg\ nu \equiv (tg\ u)^n \text{ (mod. } n)"$$

The word "Congruenzen" is marked by an asterisk pointing to a footnote of Kronecker citing Ch. XIV of this work of Euler. Kronecker's Werke were edited by Kurt Hensel who added a footnote to Kronecker's footnote giving the more precise reference "*Euler*, Opera, Series I, Volumen VIII, p. 258" (i.e., [**30**], p. 258). However, this more precise reference appears to be incorrect. In Ch. XIV, which Kronecker does refer to, one does find on p. 273 of [**30**] the identity

$$tang.nz = \frac{(1+t\sqrt{-1})^n - (1-t\sqrt{-1})^n}{(1+t\sqrt{-1})^n\sqrt{-1} + (1-t\sqrt{-1})^n\sqrt{-1}},$$

where $t = tang.z$ and this immediately implies the congruence relation for tangent stated by Kronecker when $n$ is an odd prime. The analogous

formula for sine is stated on p. 272 of [**30**], which quotes from p. 141 of [**30**]. The work [**30**] of Euler is also available in a recent English translation [**32**]. The relevant identities appear on p. 217. It is noteworthy that although Kronecker refers to the work of Euler, he makes no mention of that of Eisenstein. [Section 5, p. 34, line 22]

15. In [**81**], pp. 3–4, 53, Weil writes: "The first signs of an awakening interest in elliptic functions, on the part of Kronecker, appears in 1853 (*Werke* IV, p. 11); there he mentions the lemniscatic case as providing the generalization to the Gaussian field $\mathbf{Q}(i)$ of his theorem on the abelian extensions of $\mathbf{Q}$. Undoubtedly he must then have studied, besides Abel, the work of Eisenstein on the division of the lemniscate; but these (even Eisenstein's great paper of 1850) were based on Abel's formulas and notations and bore no close relation to the *Genaue Untersuchung* of 1847 which has been described in Chapters I to IV."

Weil is, of course, primarily concerned with the *Genaue Untersuchung* [**20**]. The works he says Kronecker probably read were undoubtedly [**14**] and [**23**], the only other paper of Eisenstein in 1850 being [**19**], which is on a different topic. These do contain the Kronecker relation for the case of the lemniscatic function, but there is no mention of Eisenstein in this connection in the 1853 paper [**72**]. In order to clarify the situation for myself, I turned the pages of all five volumes of Kronecker's Werke to find all of the places where he explicitly refers to Eisenstein and obtained the following list, not guaranteed to be complete: (a) (cf. [**62**], p. 9) mentions Eisenstein's paper [**25**]. (b) ibid., (cf. [**62**], pp. 10, 35) refers to Eisenstein's paper [**21**]. (c) [**63**], p. 19, refers to Eisenstein's expression of the Legendre symbol as a product of sines. Kronecker refers to this several times in other papers, e.g., [**64**], pp. 27, 33; [**66**], p. 511, where it is called an Eisenstein product; [**67**], p. 135, where an explicit reference is given to pp. 178, 179 of Eisenstein's paper in Crelle (cf. [**26**], pp. 292, 293); (d) [**65**], p. 98 mentions Eisenstein in connection with power residue laws. (e) [**68**], p. 247 cites Eisenstein's 1850 paper [**14**] on the division of lemniscate. (f) [**69**], p. 389, fn., mentions Eisenstein's work on elliptic functions. (g) [**70**], p. 129 refers explicitly to the *Genaue Untersuchungen* [**20**]. (h) [**71**], pp. 149–183, refers constantly to Eisenstein's [**13**]. In addition, in [**71**], p. 152, he refers to something as Eisenstein's invariant; on [**71**], p. 159, he cites the use of Eisenstein's work in Hurwitz' thesis [**45**], pp. 20, 24, where Hurwitz refers to the *Genaue Untersuchungen* [**20**]; on

[**71**], p. 183, he discusses what he calls Eisenstein's elliptic integral of the second kind. (i) In his letter [**61**] to Dirichlet, Kronecker mentions Eisenstein's paper [**21**] (cf. p. 415 of Vol. 5, of Kronecker's Werke, in [**77**]). (j) In his *Jugendtraum* letter to Dedekind of March 15, 1880 (cf. [**60**], vol. 5, pp. 453–457, lines 6–7), Kronecker mentions that Eisenstein in effect proved a congruence relation for the Lemniscatic case. This was six years before the congruence relation was published in [**69**], p. 439, with no mention of Eisenstein. He does however refer to Jacobi (*Werke*, Bd.I, p. 55) as having provided an antecedent for elliptic functions in the case of multiplication by rational primes. Perhaps the footnote on p. 389 of [**69**], which mentions both Eisenstein and Jacobi, is pertinent here. But I will have to read more of the works of Kronecker, Jacobi and Eisenstein to form a definite opinion.

Thus, it is clear that Kronecker was certainly aware of some aspects of the work of Eisenstein, although Weil is correct insofar as the neglect of the *Genaue Untersuchung* [**20**] is concerned. The fact that in [**69**] Kronecker never refers to Eisenstein's version of the Kronecker congruence relation for the lemniscatic integral, when contrasted with his careful reference to other work of Eisenstein, suggests strongly that this aspect of Eisenstein's work was also neglected by Kronecker. [Section 5, p. 34, line 23]

16. I have not checked whether the reduction given by Richelot and by Legendre is equivalent to the transformation we have given here. [Section 5, p. 36, line −3]

17. In [**11**], W.L. Edge has drawn attention to the differences between the version of [**54**] which appeared in Math. Ann. and that which appeared in Klein's edition of his collected works. [Section 6, p. 39, line 14]

18. It should perhaps be pointed out that, on p. 32 of [**25**], after correctly giving the degree of the equation which gives the division by $p$ of the periods as $p^{2n}-1$ for genus $n$, in effect anticipating the special case published by Jacobi (cf. [**52**], p. 50), Galois writes down what he claims is the order of the Galois group of this equation. The value he gives is easily seen to be the order of the finite general linear group $GL_{2n}(\mathbf{F}_p)$, which is not the right group but which is not a bad guess if one isn't aware of the role of the symplectic group. On the other hand, the fact that Galois, on the preceding page, claims to have generalized

Legendre's period relation to the case of abelian integrals suggests that he might have been aware of the role of the symplectic group. It happens that Jacobi ([**53**], p. 62) also claimed, without giving details, to have generalized the Legendre relation. However, Weierstrass ([**79**], p. 111), at the beginning of his paper in which he derives the general symplectic relations for what he says is the first time, mentions this claim of Jacobi (but not that of Galois) and suggests that what Jacobi had in mind was a different and much simpler relation, one which had been later published by Hädenkamp [**43**] and which I haven't seen. So it is not clear, based on this evidence, whether Galois had knowledge of the symplectic relations and made an error computing the group or whether he had the relation of Hädenkamp in mind, which gave him no clues as to the correct Galois group. [Section 7, p. 43, line 26].

19. Weil ([**84**], p. 435) writes: "Eisenstein fell in love with mathematics at an early age by reading Euler and Lagrange...". [Section 7, p. 43, line 31]

20. Although Legendre proves general results about the reducibility of hyperelliptic integrals to elliptic integrals in the third supplement to [**73**], his work with the integral $\int_0^x \frac{dx}{\sqrt{1-x^5}}$ is confined to experiments involving numerical computations. Most regrettably, no reprint of the whole of Legendre's three volume treatise [**69**] seems to have been issued since it was first published in 1825–8. [Section 7, p. 44, line 14]

21. There is also an article [**58**] by Königsberger in which he gives criteria for such reductions, particularly in cases where there is complex multiplication. The article does rely on Riemann's theory for its exposition, but it does not seem to use it in an essential way. It is quite possible that the kind of qualitative arguments, as opposed to explicit reduction, that went into it were already known to Eisenstein. Königsberger also wrote about reduction of abelian integrals in [**56**], [**57**] and in his book [**59**]. [Section 7, p. 44, line −12]

22. Which I haven't seen and which may not be extant. [Section 7, p. 46, line 16]

23. "Apart from that, I know only one truly different comprehensive method, using elliptic functions." [Section 7, p. 46, line −11]

24. This may be translated as "We cannot say anything precise here about the choice of these [in?]equalities in general. However, there exists an entire class of such functions which stand in a very close

relation to certain results in number theory. And for just this kind, the inequality conditions of which we speak prove to be very natural conditions. In fact, for these cases one always finds a combination of a definite number of values of the expression **N** such that they [the inequalities] reduce a whole group of infinitely many **N**, appearing as the terms of a geometric progression for which this combination of the aforementioned values [of **N**] has the same integer value, to a single **N**. The functions to which one is led in this way appear to have rather remarkable properties. They open up a field in which the most prolific studies offer themselves and which appears to be the proper foundation upon which the most difficult parts of analysis and number theory come into contact." From the context, it appears that the word "Bedingungsgleichungen" in the first line of Eisenstein's remark ought to have been "Bedingungsungleichungen," and I have so indicated this with the insertion of [in?] in my translation. [Section 7, p. 48, line 15]

25. The decompositin of the Jacobian variety of the Fermat curve of degree $N$ was studied in [**42**] and [**55**]. When $N$ is prime to 6, complete results have been obtained but apparently not when $N$ is divisible by 2 or 3. In the case where $N$ is a prime number $p \geq 7$, the simple factors of the Jacobian all have dimension $(p-1)/2$ or $(p-1)/6$, hence $> 1$ for $p > 7$. [Section 7, p. 49, line 14]

## REFERENCES

**1.** Niels Henryk Abel, *Recherches sur les fonctions elliptiques*, Crelle **2** (1827), 101–181; **3** (1828), 160–187, 187–190 [Oeuvres I, article XVI, 263–388].

**2.** ———, *Mémoire sur une propriété générale d'une class très étendue de fonctions transcendantes*, Mémoires présentés par divers savants, VII, Paris, 1841, [Oeuvres I, 145–211].

**3.** Allan Adler, *On a theorem of Gauss and a proof of it by Eisenstein*, preprint, TIFR, Bombay, 1981.

**4.** ———, *Rough Translation of Gauss' paper 'Theoria Residuorum Biquadraticorum, Commentatio Prima,'* preprint, TIFR, Bombay, 1981.

**5.** ———, Bilingual edition (Latin–English) of Gauss'paper [**39**], in preparation.

**6.** ———, *Some integral representations of $PSL_2(\mathbf{F}_p)$ and their applications*, J. Algebra **72** (1981), 115–145.

**7.** Kurt-R. Biermann, *Johann Peter Gustav Lejeune Dirichlet, Dokumente für sein Leben und Wirken*, Abh. Deutschen Akad. d. Wiss., Berlin, 1959, nr. 2

**8.** ———, *Zur Geschichte der Ehrenpromotion Gotthold Eisensteins*, Forschungen und Fortschritte **32** (1958), 332–335.

**9.** B.J. Birch and W. Kuyk, eds., *Modular functions of one variable IV.* Proceedings of the International Summer School, University of Antwerp, RUCA, July 17–August 3, 1972 Lecture Notes in Math., 476, Springer-Verlag, 1975.

**10.** Arthur Cayley, *Eisenstein's geometrical proof of the fundamental theorem for quadratic residues, (translated from the original memoir, Crelle t. XXVIII (1844), with an Addition by A. Cayley)*, Quart. J. Pure and Appl. Math. **1** (1957), 186–191, [Collected mathematical papers, vol. III (Cambridge 1890), 39–43].

**11.** William Leonard Edge, *The Klein group in three dimensions*, Acta Math. **79** (1947), 153–223.

**12.** Gotthold Eisenstein, *Zur Theorie der Quadratische Zerfallung der Primzahlen* $8n+3$, $7n+2$ *und* $7n+4$, Crelle **37** (1848), 97–126 [Math. Werke II, pp. 506–535, art. 33].

**13.** ———, *Beiträge zur Theorie der elliptischen Funktionen*, Crelle **30** (1846), 185–274 [Mathematische Werke I, 299–478, art. 28, 28a-f].

**14.** ———, *Über die Irreductibilität und andere Eigenschaften der Gleichung von welcher die Theilung der ganzen Lemniscate Abhängt*, Crelle **39** (1850), 160–179; 224–287 [Mathematische Werke II, 536–619, art. 34].

**15.** ———, *Mathematische Werke*, 2 vols., Chelsea Publishing Company, New York, 1975.

**16.** ———, *Geometrischer Beweis der Fundamentaltheorems für die quadratischen Reste*, Crelle **28** (1844), 246–248 [Mathematische Werke I, 164–166, art. 23].

**17.** ———, Letter to Stern, July, 1847, Mathematische Werke II, 815–818, art. 46.

**18.** ———, *Bermerkungen zu den elliptischen und Abelschen Transcendanten*, Crelle **27** (1844), 445–450; [Mathematische Werke I, 28–34, art. 6].

**19.** ———, *Elementare Ableitung einer merkwürdigen Relation zwischen zwei unendlichen Producten*, Crelle **27** (1844), 285–288 [Mathematische Werke I, 55–58, art. 9].

**20.** ———, *Genaue Untersuchung der unendlichen Doppelproducte, aus welchen die elliptische Functionen als Quotienten zusammengesetzt sind*, Crelle **35** (1847), 153–274, [Mathematische Werke I, 357–478, art. 28f].

**21.** ———, *Allgemeine untersuchung über die Formen dritten Grades mit drei Variabeln, Welche der Kreistheilung ihre Enstehung verdanken*, Crelle **28** (1844), 289–374 and **29** (1845), 19–53 [Math. Werke I, 167–287, art. 24].

**22.** ———, *Über die Anzahl der quadratischen Formen in den verschiedenen complexen Theorieen*, Crelle **27** (1844), 311–316 [Math Werke I, 89—94, art. 12].

**23.** ———, *Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications und Transformationsformeln*, Crelle **30** (1846), 185–210 [Math. Werke I, 299–324, art. 28a].

**24.** ———, *Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze*, Crelle **39** (1850), 351–364 [Math. Werke II, 623–636, art. 36].

**25.** ———, *Beiträge der Kreistheilung*, Crelle **27** (1844), 269–278 [Math. Werke I. 45–54, art. 8].

**26.** ———, *Applications de l'Algèbre à l'Arithmétique transcendante*, Crelle **29** (1845), 177–184 [Math. Werke I, 291–298, art. 27].

**27.** Leonhard Euler, (a) *Demonstratio Theorematis Fermatiani Omnem Numerorum Primus Formae* $4n+1$ *Esse Summam Duorum Quadratorum*, Nov. comm. sci. Petr. **5** (1754/5), 1760, 3–13 [Opera Omnia, Series $I^a$, **2**, 328–337, Commentatio 241].

**28.** ———, *De numeris qui sunt aggregata duorum quadratorum*, Nov. comm. sci. Petr. **4** (1752/3), 1758, 3–40 [Opera Omnia, Series $I^a$, **2**, 295–327, Commentatio 228].

**29.** ———, *Evolutio Generalior Formularum Comparationi Curvarum Inservientium*, Nov. comm. sci. Petr. **12** (1766/7), 1768, 42–86 [Opera Omnia, Series $I^a$, **20**, 318–356, Commentatio 347].

**30.** ———, *Introductio in analysis infinitorum, tomi primi. "De multiplicatione ac divisione angulorum"*, Lausanne: Bousquet, 1748 [Opera Omnia, Series $I^a$, **8**].

**31.** ———, *De Integratione Aequationes Differentiales* $\frac{mdx}{\sqrt{1-x^4}} = \frac{ndy}{\sqrt{1-y^4}}$, Nov. comm. sci. Petr. **6** (1756/7), 1761, 37–57 [Opera Omnia, Series $I^a$, **20**, 58–79, Commentatio 251].

**32.** ———, *Introduction to analysis of the infinite, book I*, translated by John D. Blanton, published by Springer-Verlag.

**33.** Pierre de Fermat, *Oeuvres de Fermat*, edited by Paul Tannery and Jules Henry, Paris, 4 vol., 1891–1912.

**34.** ———, Letter to Mersenne, Tuesday, Dec. 25, 1640, Letter XLV, Oeuvres **2**, 212–217.

**35.** ———, Marginal note in Fermat's copy of Bachet's edition of Diophantos, Oeuvres **1**, p. 293, Obs. VII.

**36.** ———, Letter to Huygens, August 1659, Letter CI, Oeuvres **2**, 431–436.

**37.** Évariste Galois, *Oeuvres Mathématiques d' Évariste Galois*, Paris, Gauthier-Villars et fils, 1897.

**38.** Karl Friedrich Gauss, *Disquisitiones Arithmeticae*, Leipzig: G. Fleischer, 1801 [Werke, vol. I, Göttingen: Kön. Ges. d. Wiss., 1863].

**39.** ———, *Theoria Residuorum Biquadraticorum, Commentatio Prima*, [Werke, vol. II, 65–92].

**40.** ———, Untersuchungen über höhere Arithmetik Deutsch Herausgegeben von H. Maser Berlin: Springer, 1889 (reprinted by Chelsea, New York).

**41.** Phillip Griffiths, *On the periods of certain rational integrals I, II*, Annals of Mathematics **90** (1969), 460–541.

**42.** Benedict Gross and David E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Inv. Math. **44** (1978), 201–224.

**43.** Hermann Hädenkamp, *Über Transformation Vielfacher Integrale*, Crelle **22** (1841), 184–192.

**44.** Adolph Hurwitz, *Über die diophantische Gleichung* $x^3y + y^3z + z^3x = 0$, Mathematische Werke II, 427–429.

**45.** ———, *Grundlagen einer independenten Theorie der elliptischen Modulfunktionen und Theorie der Multiplikator-Gleichungen erster Stufe*, Inauguraldissertation, Leipzig, 1881; Math. Ann. **20** (1881), 528–592 [Math. Werke, **1**, 1–66].

**46.** Carl Gustav Jacob Jacobi, *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, Math. Werke VI, 254–274.

**47.** ———, Letter to C.F. Gauss, Königsberg, February 8, 1827, Mathematische Werke VII, 393–400.

**48.** ———, *Notices sur les fonctions elliptiques*, Math. Werke I, 249–275.

**49.** ———, *Considerationes Generales de Transcentibus Abelianis*, Math. Werke II, 5–16.

**50.** ———, *Anzeige von Legendre Théorie des Fonctions Elliptiques, Troisième Supplement, 169–359*, Math. Werke I, 373–382.

**51.** ———, *Note sur les fonction abéliennes*, Math. Werke II, 83–86.

**52.** ———, *De functionibus duarum variabilium quadrupliciter periodicis, quibus theoria transcendentium abelianarum inititur*, Math. Werke II, 25–50.

**53.** ———, *Note von der geodätischen Linie auf einem Ellipsoid und den verschiedenen Anwendungen einer merkwürdigen analytischen Substitution*, Crelle **19** (1839), 309–313 [Math. Werke II, 59–63].

**54.** Felix Klein, *Über die Transformation siebenter Ordnung der elliptischen Funktionen*, Math. Ann. **14** (1878/79) [Ges. Math. Abh., Bd. III, 90–136].

**55.** Neal Koblitz and David Rohrlich, *Simple factors of the Jacobian of a Fermat curve*, Can. J. Math. **30** (1978), 1183–1205.

**56.** Leo Königsberger, *Ueber die Reduction hyperelliptischer Integrale auf elliptische*, Crelle **85** (1878), 273–294.

**57.** ———, *Ueber die Reduction Abel'scher Integrale auf elliptische und hyperelliptische*, Math. Ann. **15** (1879), 174–205.

**58.** ———, *Ueber eine Beziehung der complexen Multiplication der elliptischen Integrale zur Reduction gewisser Klassen Abelscher Integrale auf elliptische*, Crelle **86** (1879), 317–352.

**59.** ———, *Vorlesungen ueber die Theorie der hyperelliptischen Integrale*, Leipzig: B.G. Teubner, 1878.

**60.** Leopold Kronecker, *Werke*, 5 vols., New York: Chelsea, 1968.

**61.** ———, Letter to Dirichlet, June 26, 1856.

**62.** ———, *De unitatibus complexis*, Inaugural Dissertation, Berlin, 1845 [Math. Werke 1, 5–73, art. 2].

**63.** ———, *Ueber das Reciprocitätsgesetzes*, Monatsb. Kön. Preuss. Akad. Wiss. Berl. (1875), 267–274 [Werke, **2**, 11–23, art. 2].

**64.** ———, *Sur la loi de réciprocité*, Bulletin des sciences mathématiques, ser. 2, pt. 1, **4** (1880), 182–192 [Werke **2**, 5–36, art. 3].

**65.** ———, *Ueber die Potenzreste gewisser complexer Zahlen*, Monatsb. Kön. Preuss. Akad. Wiss. Berl. (1880), 404–407 [Werke **2**, 95–101, art. 7].

**66.** ———, *Beweis des Reciprocitätsgesetzes für die quadratischen Reste*, Monatsb. Kön. Preuss. Akad. Wiss. Berl. (1884), 519–537 [Werke **2**, 497–522, art. 18].

**67.** ———, *Die absolut kleinsten Reste reeller Grössen*, Monatsb. Kön. Preuss. Akad. Wiss. Berl. (1885), 383–396, 1045–1049 [Werke **3**, 111–136, art. 5].

**68.** ———, *Ein Satz über Discriminanten-Formen*, Crelle **100** (1887), 79–82 [Werke **3**, 241–247, art. 9].

**69.** ———, *Zur Theorie der elliptischen Funktionen*, Sitz. Kön. Preuss. Akad. Wiss. Berl. (1883), 497–506, 525–530; (1885), 761–784; (1886), 701–780; (1889), 53–63, 123–135 [Werke, **4**, 345–495, art. 31].

**70.** ———, *Zur Theorie der elliptischen Functionen*, Sitz. Kön. Preuss. Akad. Wiss. Berl. (1889), 199–220, 255–275, 309–317; (1890), 99–120, 123–130, 219–241, 307–318, 1025–1029 [Werke **5**, 1–132, art. 1].

**71.** ———, *Die Legendre'sche Relation*, Sitz. Kön. Preuss. Akad. Wiss. Berl. (1891), 323–332, 343–358, 447–465, 905–908 [Werke **5**, 131–184, art. 2].

**72.** ———, *Über die algebraisch auflösbaren Gleichungen (I. Abhandlung)*, Mon. Kön. Preuss. Akad. Wiss. Berl. (1853), 365–374 [Werke **4**, 1–11, art. 1].

**73.** Legendre, Traité des fonctions elliptiques et des intégrales Eulériennes, avec des tables pour en faciliter le calcul numérique, 3 vols., Paris, Huzard-Courcier, 1825–1828.

**74.** Gustav Lejeune-Dirichlet, *Werke*, 2 vols., bound as one, Chelsea, New York, 1969.

**75.** A.R. Rajwade, *Certain classical congruences via elliptic curves*, J. London Math. Soc. (2) **8** (1974), 60–62.

**76.** R. Richelot, *Ueber die Reduction des Integrales* $\int \frac{fx\,dx}{\sqrt{\pm(1-x^8)}}$ *auf elliptische Integrale*, Crelle **32** (1846), 213–218.

**77.** Ernst Schering, ed., *Briefwechsel zwischen Gustav Lejeune-Dirichlet und Herrn Leopold Kronecker*, Nach. Ges. Wiss. Gött. (1885), 361–382 [Kronecker's Werke **5**, 407–431; Lejeune Dirichlet's Werke **2**, 388–411].,

**78.** Leon Stickelberger, *Ueber eine Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321–367.

**79.** Karl Weierstrass, *Beitrag zur Theorie der Abel'schen Integrale*, Beilage zum Jahresbericht über das Gymnasium zu Braunschweig in dem Schuljahre 1848–49 [Math. Werke **1**, 111–131].

**80.** André Weil, Scientific papers, vols. I, II, III, Springer Verlag, New York, 1979.

**81.** ———, *Elliptic functions according to Eisenstein and Kronecker*, Springer Verlag, New York, 1976.

**82.** ———, *Euler and the Jacobians of Elliptic curves*, Arithmetic and Geometry (vol. I, Arithmetic), 353–359, Papers dedicated to I.R. Shafarevitch on the occasion of his sixtieth birthday (Michael Artin and John Tate, ed.), Birkhäuser, Boston, 1983.

**83.** ———, *Numbers of solutions of equations in finite fields*, Scientific Papers **1**, 399–410, art. [1949b]

**84.** ———, *History of mathematics*: *Why and how*, Scientific Papers, **3**, 434–442, art. [1978b].

**85.** ———, *Review of 'Mathematische Werke, by Gotthold Eisenstein'*, Scientific Papers, **3**, 398–403, art. [1976c].

**86.** Albert Leon Whiteman, *A theorem of Brewer on character sums*, Duke Math. J. **30** (1963), 545–552.

Cherokee Station, P.O. Box 20276, New York, NY 10021
*E-mail:* adler@pulsar.cs.wku.edu
*E-mail:* ara@altdorf.a1.mit.edu