Some Milestones of Lemniscatomy

Norbert Schappacher

UFR de mathématique et d'informatique,
7 rue René Descartes,
67084 Strasbourg Cedex, France

e-mail: schappa@math.u-strasbg.fr

This little article is an attempt to kindle the reader's interest in some modern research in the domain of complex multiplication by sketching a few episodes from the history of the very first example of this theory, the lemniscatic elliptic integral and the corresponding elliptic functions. Even though treating such an example offers elementary proofs of some key properties, our exposition is not mathematically self-contained. All we hope is that it will motivate the reader to look up some of the further literature which we indicate. At the same time, we have tried to draw attention to the differences between the various periods of the history of lemniscatomy, and to a few historical details which may not be generally known.

1 Prelude in Antiquity.[1]

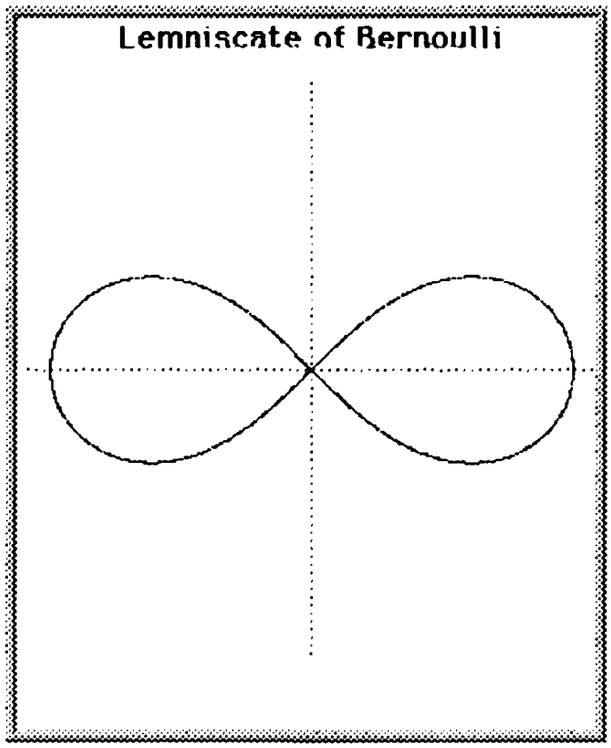
The story from which we are about to tell a few instructive episodes does not really begin, but is vaguely suggested to begin, in the dawn of times, or rather in the twilight of Greek mathematics, where the sources which are extant today do not quite permit us to know what was said and thought, and at what time.

The leading Neo-Platonist of his time, *Proclus* from Lykia (on today's maps, this is roughly the region between Fethiye and Antalya) lived from 410 to 485 AD, and went from Alexandria, where he got his education, to Athens. His numerous works, most of which are strongly philosophical or even religious in character, also include a Commentary on Book I of Euclid's Elements. These were basically notes for his own elementary mathematics courses in the Neo-Platonic Academy, but for us they constitute the richest extant source on the history of Greek geometry. At one point Proclus tells us about the work of a certain *Perseus*, about whom we do not know anything else today. Proclus quotes a distich of Perseus's,

$$\begin{array}{c} \textit{Τρεις γραμμας επι πεντε τομαις ευρων} \bullet\bullet - \bullet \\ \textit{Περσευς των δ'ενεκεν δαιμονας ιλασατο.} \end{array}$$

"Finding three ... curves upon five sections, Perseus thanked the gods therefor." The precise interpretation of these lines and of some of Proclus's explanations, as well as the missing word(s) at the end of the first verse are open to discussion. But Proclus seems to suggest that Perseus had considered what reminds us today of pictures one draws to motivate Morse theory: Imagine a torus, not the way it would float on the water, but being immersed vertically into water, and look at the curves marked on the torus by the water level. Increasing the depth of the immersion, one finds sometimes an oval, sometimes a pair of circles, but if the water touches precisely the inner hole of the torus, the resulting curve looks somewhat like a figure-eight, or, as Proclus puts it, like a horse fetter: *εοικυα τη του ιππου πεδη*, locking, say, the ankles of the horse's

[1] See [Thomas (1941), pp. 360–365], [Heath (1921), pp. 203–206, 529–535], [Brieskorn & Knörrer (1986), §1.6].



forelegs. In the case where the diameter of the hole in the torus equals that of the ring of the torus, this curve is precisely

2 The Lemniscate of the Bernoulli Brothers.[2]

The Swiss brothers Jakob and Johann Bernoulli hit upon the lemniscate almost exactly three hundred years ago from a completely different point of view, which brings us quite a bit closer to what we want to explain in this paper. They proposed the curve as the solution to an integral, more precisely to the differential equation

$$\frac{dr}{\sqrt{ar}} = \frac{2a\,dz}{\sqrt{az(a^2 - z^2)}}, \tag{1}$$

where a is a (positive) parameter. This differential equation itself was the answer, found by the Bernoullis, to the so-called problem of

[2]See [Bos 1993] and references given there. For the computations at the end of the section see [Siegel 1969, §1.1].

paracentric isochrones which had been posed by Leibniz. The curve "integrates" (1) in the sense that the integral of the right-hand side of (1) measures the arc-length of the lemniscate.

We see that, at the end of the seventeenth century, it was considered desirable and satisfactory to describe an integral as giving the arc-length of a curve—which in turn could be given by an explicit equation or be mechanically constructed. This attachment to rectilinear integration is quite different from our modern standards. Today we usually insist on expressing an integral formally, for instance, expand it into a power series if no closed formula is available. Still, the increasing use of computer packages like MATHEMATICA or MAPLE which also produce beautiful pictures may bring back a bit of the 17th century's predilection for geometric solutions to analytic problems.

To actually get the lemniscate from integrating the right-hand side of (1), Johann Bernoulli renormalized slightly, and looked for functions $x(z), y(z)$ satisfying

$$\frac{a}{\sqrt{2}} \frac{2a\,dz}{\sqrt{az(a^2 - z^2)}} = \sqrt{(dx)^2 + (dy)^2}. \tag{2}$$

It is not too hard to guess (and even easier to check) that

$$x(z) = \sqrt{az + z^2} \qquad y(z) = \sqrt{az - z^2}$$

do the job. So we see that x and y satisfy the following algebraic equation identically in z.

$$(x^2 + y^2)^2 = 2a^2(x^2 - y^2) \tag{3}$$

This is the standard equation of the lemniscate (with parameter a). The name, by the way, was chosen by Jakob Bernoulli, in an article published in 1694. The Greek word $\lambda\eta\mu\nu\iota\sigma\kappa o\varsigma$ is related to $\tau o\ \lambda\tilde{\eta}\nu o\varsigma$, wool—cf. the French *laine*—, and originally means a woolen band. This is a softer metaphor than Perseus's horse-fetter.

The points $P(x, y)$ in the (x, y)-plane satisfying equation (3) are characterized geometrically by the fact that the product of the distances from P to the point $(-a, 0)$ and from P to the point $(+a, 0)$ is constant, equal to a^2.

We will not need to look at more general curves which also go under the name of lemniscates. In fact, for our purposes we will even normalize the parameter and assume that $2a^2 = 1$. Doing this and rewriting (3) in terms of $r = \sqrt{x^2 + y^2}$ gives

$$2x^2 = r^2 + r^4 \qquad \text{and} \qquad 2y^2 = r^2 - r^4.$$

This clearly yields a parametrization of the lemniscatic arc in terms of the variable r. Considering the leaf in the first quadrant, the integral giving the arc-length on the lemniscate then comes out to be

$$s(r) = \int_0^r \frac{dr}{\sqrt{1 - r^4}} \qquad (0 \leq r \leq 1). \tag{4}$$

3 Elementary Arithmetic of Elliptic Integrals: the Count of Fagnano, Euler, and Legendre.[3]

We now enter an era of the history of our subject where new discoveries were made through the formal manipulation of integrals. This is especially visible in the works of the count G.C. di Fagnano (1682–1766). In fact, they are somewhat disconcerting for the modern reader because of the great number of formulas which do not easily betray the line of thought that led to them. But his various investigations about the lemniscate constitute the first milestone in the history of lemniscatomy, i.e., of the division of the lemnsicate.

[3]We do not know any comprehensive, detailed reference for this section. We are not convinced, for instance, by the speculations in [Ayoub 1984]. Of course, all historical accounts of the theory of elliptic functions—see for instance the encyclopedic [Brill, Noether 1892–93], and in particular the thorough study [Houzel 1978]—talk about Fagnano, Euler, Lagrange, Legendre, etc. Still, it is not superfluous to actually refer to the collected works [Fagnano 1750], second volume, esp. no.s xxxii, xxxiii, xxxiv. There is a nice discussion of Fagnano and Euler in the (somewhat rare) book [Enneper 1876, pp. 477ff]. More accessible is the account of Fagnano's doubling of the lemniscatic arc in [Siegel 1969, 1.1] and in the related short note [Siegel 1959].

This is not only so from our point of view, but Fagnano himself must have realized the importance of his discoveries. In fact, a lemniscate appears in the inscription on his tombstone in the Church of Santa Maria Magdalena in Senigallia: *Veritas Deo* ∞ *gloria*....

In 1718, Fagnano published the following seminal result (which is easily checked):

$$(5) \qquad \int_0^z \frac{dz}{\sqrt{1-z^4}} = 2\int_0^u \frac{du}{\sqrt{1-u^4}}, \qquad \text{if } z = \frac{2u\sqrt{1-u^4}}{1+u^4}.$$

Before explaining its significance, let us discuss C.L. Siegel's comments about this result—see [Siegel 1959]. He tried to divine how Fagnano obtained (5). We mention his comments not because we find this kind of mathematical psychology across the centuries very convincing. But Siegel's observations prepare us for later stages of the history of our subject.

Siegel's first conjecture is that Fagnano may have found (5) by analogy with the arclength of the circle

$$(6.0) \qquad \text{arc sin}(r) = \int_0^r \frac{dr}{\sqrt{1-r^2}} \qquad (0 \le r \le 1).$$

Here, the substitutions

$$(6.1) \qquad r = \frac{2s}{1+s^2}, \qquad s = \frac{2t}{1-t^2}$$

lead, respectively, to

$$(6.2) \qquad \frac{dr}{\sqrt{1-r^2}} = 2\frac{ds}{1+s^2}, \qquad \frac{ds}{\sqrt{1+s^2}} = 2\frac{dt}{1-t^2}.$$

The essential difference between the circle and the lemniscate is that (6.2) reduces (6.0) to an elementary integral, whereas in (5) we find the same lemniscatic arclength on both sides.

Siegel also writes [Siegel 1959, p. 250] that (5) "in fact belongs to the theory of complex multiplication", because we may break up the

relation between z and u using the Gaussian integer $\alpha = 1 + i$ and its complex conjugate $\overline{\alpha} = 1 - i$ (thus $\alpha\overline{\alpha} = 2$, $\alpha^4 = \overline{\alpha}^4 = -4$):

$$(7.1) \qquad z = \alpha \frac{t}{\sqrt{1 - t^4}}, \qquad t = \overline{\alpha} \frac{u}{\sqrt{1 - u^4}},$$

and these two algebraic relations yield, respectively, the differential equations:

$$(7.2) \qquad \frac{dz}{\sqrt{1 - z^4}} = \alpha \frac{dt}{\sqrt{1 - t^4}}, \qquad \frac{dt}{\sqrt{1 - t^4}} = \overline{\alpha} \frac{du}{\sqrt{1 - u^4}}.$$

Siegel claims [Siegel 1959, p. 251] that the possibility to decompose (5) into the simpler steps (7) was "obviously relevant to Fagnano's success". Since there is no mention of complex numbers or of formulas like (7) in Fagnano, this probably says more about Siegel's insights than about Fagnano's.

Instead of trying to slip further into Fagnano's mind let us now explain why his result was such a breakthrough. Fagnano's theorem (5) means that the differential equation

$$\frac{dz}{\sqrt{1 - z^4}} = 2 \frac{du}{\sqrt{1 - u^4}}$$

can be *integrated algebraically*. Indeed, given u, there is an algebraic formula (5) for z such that the lemniscatic integral from 0 to z is twice that from 0 to u. We may also look at (5) the other way around: suppose we are given z, or more precisely (remembering the way we obtained (4) above), suppose we are given a point (x, y), say in the first quadrant, which lies on the lemniscate, so that $2x^2 = z^2 + z^4$ and $2y^2 = z^2 - z^4$. Then, if u satisfies the algebraic equation deduced from (5),

$$(8) \qquad z^2u^8 + 4u^6 + 2z^2u^4 - 4u^2 + z^2 = 0,$$

and if (x', y') lies on the lemniscate and in the first quadrant satisfying $2x'^2 = u^2 + u^4, 2y'^2 = u^2 - u^4$, then the lemniscatic arc between the origin and (x', y') has half the length of that between the origin and (x, y).

In this sense, Fagnano found the multiplication by 2 of the lemniscatic integral.[4] The method also leads to the trisection of the total lemniscatic arc in the first quadrant. To see this, note that the relation between u and z in (5) really should be written

$$z^2 = \frac{4u^2(1-u^4)}{(1+u^4)^2}.$$

This leaves two possible signs for the root, and the minus sign yields the equation

$$\frac{dz}{\sqrt{1-z^4}} = -2\frac{du}{\sqrt{1-u^4}}.$$

In this case, the points $(x,y),(x',y')$ on the lemniscate and in the first quadrant such that $2x^2 = z^2 + z^4$ and $2y^2 = z^2 - z^4$, resp. $2x'^2 = u^2+u^4, 2y'^2 = u^2-u^4$, are situated such that the arc between the origin and (x,y) has half the length of the arc from (x',y') to the point $(1,0)$. Thus, if $z = u$ in this case, $(x,y) = (x',y')$ marks one third of the arc from $(0,0)$ to $(1,0)$. The condition $z = u$ implies that $z^4 = 2\sqrt{3} - 3$.

As mentioned before, Fagnano's algebraic divisions by 2 and by 3 of the lemniscatic arc seem to be the first explicit examples of lemniscatomy in the history of mathematics. It is, however, amusing to note that some eighty years before Fagnano, P. de Fermat, working in an entirely different context, had developed a proof by infinite descent which, when translated into our language of elliptic curves, uses the bisection of the lemniscatic arc—see [Goldstein 1995, pp. 91–103], and the end of section 5 below.

According to Jacobi [Stäckel, Ahrens 1908, p. 23], the 23rd of December 1751 was the birthday of the theory of elliptic functions, because it was on this day that Euler received the collection [Fagnano 1750] from the Berlin Academy for internal review. Euler immediately started to generalize Fagnano's results and presented his first publication on elliptic integrals on January 17, 1752—see [Euler

[4] Siegel's formulas (7) do the same for the multiplication by $1+i$ and its complex conjugate. This possibility of arithmetic operations involving irrational integers, i.e., the presence of 'complex multiplication' is a special feature of the lemniscatic integral which we will understand more clearly further on.

1761]. This note was the beginning of a whole sequence of articles by Euler on this topic which, taken together, run to almost 400 well-filled pages. Of all this production, history has essentially retained only the general *addition theorem of elliptic integrals.*[5] In the special case of the lemniscatic integral, this fundamental result reads as follows—see [Siegel 1969, p. 9]:

$$(9) \qquad \int_0^u \frac{du}{\sqrt{1-u^4}} + \int_0^v \frac{dv}{\sqrt{1-v^4}} = \int_0^r \frac{dr}{\sqrt{1-r^4}},$$

$$\text{if } r = \frac{u\sqrt{1-v^4} + v\sqrt{1-u^4}}{1+u^2v^2}.$$

It expresses r algebraically in terms of u and v, if the arc from the double point of the lemniscate all the way to the point of modulus r is as long as those to u and to v added together.

In the spirit of this article, we refrain from discussing more general *elliptic integrals*. After Euler these were classified and systematized in particular by Legendre—see [Legendre 1825–28]. The unfortunate name for this class reflects the fact that the arclength of an ellipse is also given by an "elliptic integral". However, it is not an integral "of the first kind" like (4), i.e., it is not an integral of the form $\int \frac{dx}{\sqrt{P(x)}}$ for a polynomial P of degree 3 or 4, but rather "of the second kind", i.e., of the form $\int \frac{t^2 dx}{\sqrt{P(x)}}$ for a polynomial P of degree 4. An important concrete question which does lead to an elliptic integral of the first kind is the mathematical theory of the pendulum.

The elliptic integrals constitute the first examples of integrals arising naturally which (exceptions apart) cannot be integrated in terms of elementary functions. By the way, as R. Remmert pointed out to me, it would be nice to see an explicit elementary *proof* of this fact, for instance for our lemniscatic integral (4).

[5]This selective injustice of history has infuriated some later writers who criticize that too much credit was given in particular to Legendre, to the detriment of Euler's contributions—see for example [Enneper 1876, pp. 490f], [Plana 1863]. These are emotions of the past. But in the otherwise excellent recent article [Belhoste 1996, p. 3], there is a surprising sentence creating the wrong impression that Euler treated only the lemniscatic integral.

Let us close this section with a few variations on the lemniscatic integral (4):

$$(10)\quad \int_1^\infty \frac{dx}{\sqrt{4x^3-4x}} = \int_0^1 \frac{dr}{\sqrt{1-r^4}} = \frac{1}{4}\int_0^1 \frac{dt}{t^{\frac{3}{4}}(1-t)^{\frac{1}{2}}} = \frac{\Gamma(\frac{1}{4})^2}{4\sqrt{2\pi}}.$$

These identities, which we leave as an exercise, follow from the substitutions: $x = \frac{1}{\sqrt{r}}$ and $r^4 = t$, and from standard properties of Euler's beta integral. The last expression occurs in [Legendre 1811, p. 209f]. It is the first special case of a general formula (due to Lerch, and known as the formula of Chowla and Selberg) which relates elliptic integrals with complex multiplication to special values of the gamma function—see [Schappacher 1988, p. 123–125], see also [Henniart 1987].

4 The Galois Theory of Lemniscatomy: from Gauss to Abel.

Carl Friedrich Gauss finished writing his momentous book *Disquisitiones Arithmeticæ* [Gauss 1801] when he was 21 years old. It transported arithmetic to a new theoretical level. It also contained the complete solution of a longstanding problem: in the final section VII [Gauss 1801, pp. 592–665], Gauss determined precisely the regular n-gons which can be constructed by ruler and a pair of compasses alone. The well-known answer is: those for which n is of the form $2^\nu p_1 \cdots p_r$ where $\nu \geq 1$ and the p_i are distinct odd prime numbers of the form $2^m + 1$.

This result is obtained from an algebraic analysis of what we call today the field extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, for any odd prime p. Indeed, Gauss carries out the "Galois theory" (Galois was -13 years old when Gauss's book was completed) of this particular cyclic extension, exhibiting distinguished primitive generators of all intermediate fields and what we would call their behaviour under automorphisms.

In the field $\mathbb{C}$ of complex numbers, the n-th roots of unity can be

given analytically as $\exp(2\pi ir/n)$ with $r = 0, 1, \ldots, n-1$. So the seventh section of the *Disquisitiones Arithmeticæ* develops the theory of the extensions generated by the division values of the function $x \mapsto e^{\pi ix}$. Now, in the introduction to this section, Gauss writes: "The principles of the theory we are about to set out extend to a much broader context... For they may be applied not only to the circular functions, but with equal success to many other transcendental functions, e.g., to those which are related to the integral $\int \frac{dx}{\sqrt{1-x^4}}$."[6] He also announces a forthcoming study of those transcendental functions (which was never published). Gauss probably had in mind (at least) the elliptic integrals of the first kind and their inverse functions—see for instance [Houzel 1978, p. 17].

Gauss's *Nachlass* (papers published only after his death) contains various sets of notes on the lemniscatic integral, its inverse function, and other related functions [Gauss (III), pp. 404ff]. But it was Niels Henrik Abel who first published a systematic theory along these lines—see [Abel 1827–28]. In this seminal article, Abel shifts attention from the elliptic integral to its inverse function. Formally, his theory deals with the function φ characterized by the equivalence

$$(11) \qquad \varphi(\alpha) = x \qquad \Longleftrightarrow \qquad \alpha = \int_0^x \frac{dx}{\sqrt{(1-c^2x^2)(1+e^2x^2)}}.$$

The special case of the lemniscatic integral corresponds to the choice of parameters $c = e = 1$. Abel calls the functions φ *elliptic functions*—much to Legendre's chagrin, who used this name for the corresponding integrals, and did not like to see his terminology chucked.

To be sure, formula (11) presents the problem of the dependence of this integral on choices of the root and of the path of integration. These questions were solved in general only after Riemann—see for instance [Siegel 1969, pp. 29–37]. Abel proceeds with care, in a rather piecemeal way. We specialize right away to the lemniscatic case $c = e = 1$ which interests us here. There Abel puts (see also

[6][Gauss 1801, p. 593]: "Ceterum principia theoriæ, quam exponere aggredimur, multo latius patent, quam hic extenduntur. Namque non solum ad functiones circulares, sed pari successu ad multas alias functiones transcendentes applicari possunt, e. g. ad eas quæ ab integrali $\int \frac{dx}{\sqrt{1-x^4}}$ pendent."

(10) above):

$$\omega = 2\int_0^1 \frac{dr}{\sqrt{1-r^4}}. \tag{12}$$

Then he defines φ first on the interval $[0, \frac{\omega}{2}]$ of positive real numbers. After this he passes to the imaginary interval $i \cdot [0, \frac{\omega}{2}]$ by the rule

$$\varphi(\alpha i) = i\varphi(\alpha) \qquad (i = \sqrt{-1}), \tag{13}$$

and finally he uses parity, and double periodicity modulo 2ω and $2\omega i$, to define φ on all of $\mathbb{C}$. We will not follow Abel's developments in detail here, but rather present things from Weierstrass's point of view in the next section. This will break the chronological order of our exposition, but should make it more accessible to the reader.

The main result about lemniscatomy that Abel finds in [Abel 1827–28] is analogous to Gauss's cyclotomic result: the division of the entire lemniscate into n equal parts is possible by ruler and a pair of compasses alone if n is of the form $2^\nu p_1 \cdots p_r$ where $\nu \geq 1$ and the p_i are distinct odd prime numbers of the form $2^m + 1$. The main reason for this is that Abel can exhibit a cyclic "Galois action" on the $\varphi(\frac{r\omega}{n})$ $(r = 1, \ldots, n-1)$ if n is a prime number of the form $4\nu + 1$—see [Abel 1827–28, no.s 36, 37].

Those who like rare plants and pointless beauty may appreciate to see explicit geometric constructions of the division of the circle or the lemniscate into, say, $17 = 2^{2^2} + 1$ equal parts. (Gauss himself did not give this but computed algebraically, up to 10 decimal digits, the 19th and the 17th roots of unity in [Gauss 1801, no.s 353, 354].) It so happens that both constructions can be looked up in the 75th volume of *Crelle's Journal* from 1873—see [Schröter 1873] and [Kiepert 1873].

5 Lemniscatic Elliptic Functions from the Point of View of Weierstrass Theory and Elliptic Curves.

In order to have a modern analytic language for what follows, let us briefly recall here the Weierstrass theory of elliptic functions as far as we need it to treat the lemniscatic integral and its inverse function. In using this theory from now on, rather than Jacobi's formalism which dominated the greater part of the 19th century, we choose to skip an important part of the historical development. Even though Jacobi's system was rooted in a period where the definition of classes of functions by abstract properties was not yet established, his formalism could capture anything that can be couched in Weierstrass's approach, and Jacobi's theta series sometimes provide greater flexibility.[7]

We assume some basic familiarity with Weierstrass theory—see for instance [Siegel 1969, pp. 56–89], [Silverman 1986, chap. VI], [Freitag, Busam 1995, chap. V], or [Remmert 1991, pp. 71–74].

The theory starts with a lattice. In order to get out the lemniscatic integral at the end, we take $\Lambda = \mathbb{Z} + \mathbb{Z}i \subset \mathbb{C}$. For every $\nu \geq 3$, the series

$$G_\nu(\Lambda) = \sum_{\lambda \in \Lambda}{}' \frac{1}{\lambda^\nu} = \sum_{m,n \in \mathbb{Z}}{}' \frac{1}{(n+mi)^\nu}$$

converges absolutely. Here the prime signifies that undefined terms are deleted from the sum, i.e., we restrict to nonzero $\lambda = n + mi$. The G_ν are called Eisenstein series, but this is another story...

Our lattice admits *complex multiplication* in the sense that multiplication by i takes the lattice Λ into itself. Therefore we find: $G_\nu(\Lambda) = 0$ *unless* ν *is divisible by 4.* Also, the lattice Λ is invariant under complex conjugation, so that all the $G_{4k}(\Lambda)$ are real numbers.

[7] Let us note in passing that the Chelsea reprint of Jacobi's Collected Works has recently been made available again by the AMS. See also the 550 page almost day-to-day scientific biography of Jacobi, [Königsberger 1904].

Proposition. *For all* $k = 1, 2, 3 \ldots$, *one has* $G_{4k}(\Lambda) > 0$.

The proof follows from the theory of modular forms, more precisely, from the Fourier development of G_ν considered as functions on all complex lattices—see for instance [Serre 1970, VII.4.2].

In Weierstrass's setup one defines

$$g_2 = 60G_4, \qquad g_3 = 140G_6.$$

Thus, for our lattice Λ, we have $g_3(\Lambda) = 0$, and we can define the positive real number $\omega > 0$ by the relation

$$g_2(\Lambda) = 4\omega^4. \tag{14a}$$

In other words, defining $L = \omega \cdot \Lambda$ to be the lattice with basis $\omega, i\omega$, we have

$$g_2(L) = 4. \tag{14b}$$

Note that $g_3(L) = g_3(\Lambda) = 0$.

Recall that, in modern terminology, an *elliptic function* with respect to a lattice $\Gamma \subset \mathbb{C}$ is a meromorphic function f on $\mathbb{C}$ such that for all $z \in \mathbb{C}$ and $\gamma \in \Gamma$, one has $f(z + \gamma) = f(z)$. The first example of such an elliptic function, which is holomorphic except for double poles at the lattice points, is the *Weierstrass-P-function*:

$$\wp(z, \Gamma) = \frac{1}{z^2} + \sum_{\gamma \in \Gamma}{}' \frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}.$$

It satisfies the fundamental differential equation

$$\wp'(z, \Gamma)^2 = 4\ \wp(z, \Gamma)^3 - g_2(\Gamma)\ \wp(z, \Gamma) - g_3(\Gamma).$$

For the particular lattice $L = \omega\Lambda$ defined above, it reads:

$$\wp'(z, L)^2 = 4\ \wp(z, L)^3 - 4\ \wp(z, L). \tag{15}$$

This allows us to establish the link between (10), (12), and (14a):

$$(16) \qquad \omega = 2\int_{-\frac{\omega}{2}}^{0} dz = 2\int_{1}^{\infty} \frac{dx}{\sqrt{4x^3 - 4x}} = 2\int_{0}^{1} \frac{dr}{\sqrt{1 - r^4}}$$

$$= \frac{\Gamma(\frac{1}{4})^2}{2\sqrt{2\pi}} = 2.62205755\ldots.$$

In fact, all we have to check is the second equality. It follows from the substitution $x = \wp(z, L)$ once we know that $\wp(-\frac{\omega}{2}, L) = \wp(\frac{\omega}{2}, L) = 1$. To see this, recall that $\wp$ is an even function of z, so $\wp'$ is odd. $\wp'$ has a pole of order three at each lattice point. Its zeros (mod L) are therefore $\frac{\omega}{2}, \frac{i\omega}{2}, \frac{\omega+i\omega}{2}$. By (15), the corresponding values of $\wp(z, L)$ are $0, \pm 1$. But the above proposition and the well-known Taylor expansion [Serre 1970, VII.2.3]:

$$(17) \qquad \wp(z, L) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (4k - 1) G_{4k}(L) z^{4k-2}$$

show that $\wp(\frac{\omega}{2}, L) > 0$.

The function $\wp(z, L)$ is the inverse function of the lemniscatic integral in the context of Weierstrass theory, where one considers the integral $\int dx/y$ related to the Weierstrass equation (15): $y^2 = 4x^3 - 4x$. It must no be confused with the inverse function φ for the integral (4) studied by Abel and Eisenstein, and also already by Gauss in his unpublished papers [Gauss III, pp. 404ff] where it is written sin lemn. The relation with Weierstrass's formalism is as follows—see [Hurwitz 1899, §3]:

$$(18) \qquad \text{sin lemn}(z) = \varphi(z) = \sqrt{\frac{1}{\wp(z, L)}}.$$

The following theorem holds in general, for any lattice $L \subset \mathbb{C}$.

Addition theorem. *For $u, v \in \mathbb{C}$ such that $u - v \notin L$, one has*

$$\wp(u + v, L) = -\wp(u, L) - \wp(v, L) + \frac{1}{4}\Big(\frac{\wp'(u, L) - \wp'(v, L)}{\wp(u, L) - \wp(v, L)}\Big)^2.$$

And for $z \in \mathbb{C}$, one has

$$\wp(2z, L) = -2\wp(z, L) + \frac{1}{4}\Big(\frac{\wp''(z, L)}{\wp'(z, L)}\Big)^2.$$

The way we stated it here, this seems purely analytic. In fact, it can be deduced from the observation that the difference of both sides of the first equation is a holomorphic function of u, once v is fixed; it is then constant, and indeed zero. But if we combine it with the differential equation (15), we get the following consequence which we state only for the case of our lattice $L = \omega\Lambda$.

Corollary. *The map*

$$\Phi : \mathbb{C}/L \longrightarrow E(\mathbb{C}) = \{(x:y:z) \in \mathbb{P}_2(\mathbb{C}) \mid y^2z = 4x^3 - 4xz^2\} \subset \mathbb{P}_2(\mathbb{C})$$

which sends $z + L$ for $z \notin L$ to the point $(\wp(z, L) : \wp'(z, L) : 1)$, and $0 + L$ to the point $\mathbf{0} = (0 : 1 : 0)$, is a bijection from the complex torus $\mathbb{C}/L$ onto the complex points of the elliptic curve $E : y^2 = 4x^3 - 4x$. Φ transforms the addition on $\mathbb{C}/L$ into the geometric group law on the cubic E (the chord and tangent process) with neutral element $\mathbf{0}$.

Bijectivity is an easy consequence of the basic properties of meromorphic functions on $\mathbb{C}/L$. The geometric group law on a cubic curve in the projective plane works as follows. Given two points P and Q on the curve, draw the line through both. (If $P = Q$, take the tangent to the curve at this point). Since the curve is cubic and we work in the projective plane, this line will meet the curve in 3 points (counting multiplicities): P, Q, R. Now take for the "sum" $P \oplus Q$ the third point of intersection with the curve of the line through R and $\mathbf{0}$. This last twist in the construction is necessary to make $\mathbf{0}$ the neutral element, and in fact turn the whole operation into an (abelian) group law—see [Silverman 1986, III.2], [Schappacher 1991]. But note that, in view of the position of our point $\mathbf{0}$ at infinity, lines passing through $\mathbf{0}$ are parallel to the y-axis. So this last step from R to $P \oplus Q$ leaves the x-coordinate unchanged, and only switches y to $-y$. To check, on the level of the x-coordinates, that Φ transforms the addition of complex numbers into this geometric group law, one

has to recognize in the two formulas of the addition theorem above the equations for the line through the given points $\Phi(u), \Phi(v)$ (resp. the tangent at $\Phi(z)$). The fact that the y-coordinates also work out, is left to the reader.

The curve E to which the lemniscatic elliptic integral has led us, is an elliptic curve over $\mathbb{Q}$—i.e., a nonsingular cubic with a distinguished rational point, namely $\mathbf{0}$. It may also be given by the simpler equation $y^2 = x^3 - x$. It is a famous elliptic curve—although a good part of 'its' history consists of studies that only our modern viewpoint acknowledges as being related to this curve. We are alluding here to the tradition of *diophantine analysis 'over* $\mathbb{Z}$*'*. Contrary to Diophant himself, this tradition asked for integral solutions—or for the proof that there are none, or only 'trivial' ones—of polynomial equations with integer coefficients. It starts essentially in the Arab world in the 10th century. Its first eminent representative was al-Khæzin—see [Houzel 1995, p. 6f], [Rashed 1996, p. 74f].

Fermat (1601–1665) lifted this branch of mathematics into a new era by inventing the method of infinite descent. The only proof by infinite descent of which Fermat has left us a rather detailed verbal sketch (in the margin of his Bachet-edition of Diophant's Arithmetics) concerns (among other results) the following theorem.

A theorem proved by Fermat. *There is no right triangle with rational sides whose area is a rational square.*

Since the problem alluded to is invariant under scaling the triangle, it actually is, despite its formulation, a problem 'over $\mathbb{Z}$', not 'over $\mathbb{Q}$'. Thus the theorem claims that there are no positive (or, equivalently, nonzero) integers a, b, c such that $a^2 + b^2 = c^2$ and $ab = 2A^2$, for some integer A (whose square is the area of the triangle (a, b, c)). Making the substitutions

$$x = \frac{a+c}{b} \qquad\qquad y = 2A\frac{a+c}{b^2},$$

gives a rational point (x, y), $x, y \in \mathbb{Q}$, on our elliptic curve $y^2 = x^3 - x$. Since we assumed $abc \neq 0$, we never get the trivial solutions

$(x, y) = (0, 0), (\pm 1, 0)$ in this way, nor the point at infinity **0**. Therefore Fermat's result shows that the elliptic curve E has exactly four rational points. In particular, the group of rational points $E(\mathbb{Q})$ is a finite torsion group. Translating Fermat's proof to the elliptic curve, one shows that a hypothetical non-trivial element of $E(\mathbb{Q})$ can be divided again and again by 2. This process strictly decreases the size (technically speaking, the "height") of the point involved. But the heights of rational points form a discrete set bounded below; a contradiction.[8]

Probably the first—and for a long time, the only—publication about the interrelation between elliptic integrals and diophantine analysis is due to Jacobi: [Jacobi 1835]. It was inspired by an unpublished manuscript of Euler and simply states the potential usefulness of the addition theorem for diophantine questions, without giving examples—see [Schappacher 1991, §3].

6 The Higher Arithmetic of the Lemniscatic Function: Gotthold Eisenstein (and Gauss again).

Only about 20 years separate Abel's article from Eisenstein's work on the arithmetic of the lemniscatic function. The world of number theory was still under the spell of Gauss's *Disquisitiones Arithmeticæ*. But this book contains a lot more than just cyclotomy. In fact, its chapter VII on cyclotomy is the least arithmetic, the most algebraic of all. One mildly arithmetic aspect of chapter VII concerns the irreducibility of the cyclotomic polynomial $X^{p-1} + \ldots + 1$. The analogue of this for lemniscatomy, i.e., the irreducibility of the equation for

[8] See [Goldstein 1995] for a thorough investigation of this whole circle of ideas. See also, for instance, [Weil 1984, chap. I, §XI]. Fermat's result concerns a special case of the problem of congruent numbers which, in the modern analysis, leads to an infinite family of elliptic curves all of which are isomorphic to E over $\mathbb{C}$ (in fact, over the algebraic numbers $\overline{Q}$). There is a whole introductory book on this subject: [Koblitz 1984]. See also [Schappacher 1989].

the division of the lemniscate into m equal parts for an odd prime number m in the ring $\mathbb{Z}[i]$, was *not* proved in Abel's article. This is one of the critical remarks with which Eisenstein opens his sequence of articles [Eisenstein 1850], the milestone treated in this section. Of course, one voices such criticism only if one can do better; Eisenstein shows the irreducibility of the lemniscatomic equation by applying what is well-known today as "Eisenstein's irreducibility criterion". It was developed for this purpose. [9]

Eisenstein's Irreducibility Criterion (for $\mathbb{Z}[i]$). *Let $m \in \mathbb{Z}[i]$ be a prime element, and let $f = \sum_{\nu=0}^{n} a_{n-\nu} X^n \in \mathbb{Z}[i][X]$. Assume that $a_0 = 1$, a_ν is divisible by m for all $\nu = 1, \ldots, n$, and $a_n = i^a m$ for some $a = 1, \ldots, 4$. Then f is irreducible.*

There are three types of prime numbers m in the euclidean ring $\mathbb{Z}[i]$. First there is $1 + i$ which divides the rational prime 2. Indeed, one has $(1 + i)(1 - i) = 2$. Now, $1 - i = -i(1 + i)$, so, up to units, there is only one prime number dividing 2 in $\mathbb{Z}[i]$. Second, given a rational prime number p of the form $4k + 1$, Gauss had shown it is a sum of two squares in a unique way: $p = a^2 + b^2 = (a + bi)(a - bi)$. Here, the two factors are not the same up to units, and we have two different primes of $\mathbb{Z}[i]$ dividing p. Eisenstein calls these primes $a + bi$ *zweigliedrig* (because they have a real and an imaginary term). Third, the rational prime numbers p of the form $4k + 3$ are also prime elements in $\mathbb{Z}[i]$. Eisenstein calls them *eingliedrig*. Now, let $m \in \mathbb{Z}[i]$ be any prime element not dividing 2, either *zweigliedrig* or *eingliedrig*. Gauss had already proposed a way to privilege one of the four elements $i^a \cdot m$, $a = 1, \ldots, 4$, representing the same prime. He had called m a *primary prime* ("*primäre Primzahl*") if $m \equiv 1 \pmod{(2 + 2i)}$. Given m, there is always a unique unit i^a satisfying $i^a m \equiv 1 \pmod{(2 + 2i)}$ because the unit group of residues

[9] The criterion is formulated, proved, and slightly generalized in [Eisenstein 1850, pp. 541–544]. Eisenstein also transfers "Gauss's lemma" from $\mathbb{Z}[X]$ to $\mathbb{Z}[i][X]$: the product of two monic polynomials with rational coefficients that are not all integers cannot have integer coefficients [Gauss 1801, no. 42]. Eisenstein had already stated and used his criterion in [Eisenstein 1846]. But at that time he managed to apply it only to the lemniscatomic equation for primes $m \in \mathbb{Z}[i]$ dividing a rational prime of the form $p = 4k + 1$. He settled the general case before August 1847—see [Eisenstein 1847].

$(\mathbb{Z}[i]/(2+2i))^* = (\mathbb{Z}[i]/(1+i)^3)^*$ consists precisely of the classes of the four units i^a.

In proving that the m-th lemniscatomic equation satisfies the irreducibility criterion Eisenstein discovered and emphasized [Eisenstein 1850, p. 549 and *passim*] the following result about the lemniscatic function (18):

Eisenstein's Theorem. *If m is a primary prime number in $\mathbb{Z}[i]$ and $\mathbb{N}m = m\overline{m} \in \mathbb{Z}$, then there exist polynomials $P, Q \in \mathbb{Z}[i][X]$ such that one has the following identity of complex functions:*

$$\varphi(mt) = \frac{\varphi(t)^{\mathbb{N}m} + m\ P(\varphi(t))}{1 + m\ Q(\varphi(t))}. \tag{19}$$

Eisenstein stresses how important it is that there are no undetermined units in this formula. Part of the reason for this remark seems to be related to his latent—and sometimes not so latent—rivalry with Jacobi. The latter had published a two page note in Crelle's journal [Jacobi 1846] dismissing the earlier partial version of Eisenstein's theorem in [Eisenstein 1846, p. 301] as an easy consequence of his general theory. But this human aspect should not distract us from Eisenstein's remarkable insight. In fact, his theorem says that we have the following (coefficientwise) congruence between rational functions of $\varphi(t)$:

$$\varphi(mt) \equiv \varphi(t)^{\mathbb{N}m} \pmod{m}. \tag{20}$$

Note that the right-hand side of (20) depends only on the prime ideal[10] $\mathfrak{p} = (m) = m \cdot \mathbb{Z}[i]$, not on the particular generator m, whereas the left-hand side does depend on the condition that m be primary; otherwise the congruence does not hold in general.

In other words, Eisenstein shows (and obviously appreciates) that Gauss's normalization of the prime numbers in $\mathbb{Z}[i]$ defines a map-

[10]Ideals were introduced only by Dedekind. On the other hand, Eisenstein alludes explicitly [Eisenstein 1850, p. 595] to Kummer's works [Kummer 1847] which introduced ideal numbers—see also below.

ping from ideals prime to $(1+i)$, to complex multipliers of the lemniscatic function,

$$(21)\quad \psi : \mathfrak{p} \mapsto m, \qquad \text{where } \mathfrak{p} = m\mathbb{Z}[i],\ m \equiv 1\ (2+2i),$$

which describes the reduction modulo $\mathfrak{p}$ of the action of the normalized generator m in terms of the q-th power automorphism $x \mapsto x^q$ mod $\mathfrak{p}$ for $q = \mathbb{N}\mathfrak{p}$. Following our trained reflexes, we call this map the *Frobenius automorphism* relative to the finite field $\mathbb{F} = \mathbb{Z}[i]/\mathfrak{p}$. It generates the Galois group of any finite extension of $\mathbb{F}$. (When Eisenstein's paper went to press, Georg Frobenius was less than one year old. On the other hand, the "Frobenius" automorphism is explicitly visible on roots of unity, and this was the model that Eisenstein tried to generalize.) To project even further into the future, the map ψ is a very explicit and simple example of an (algebraic) Hecke character—see [Hecke 1918], [Hecke 1920], [Neukirch 1992, Kap. VII]—, i.e., a *Größencharakter* of type A_0 in the sense of [Weil 1955c].

Before continuing these observations, let us try to stay closer to the text. It is not obvious what exactly intrigued Eisenstein in his formula (19). Compared to other papers of his, the sequence of articles [Eisenstein 1850] proceeds at a rather slow pace. At times, the 27 year old man—who had just about two more years to live at the time of this publication—simply alludes to striking applications of his result without actually carrying them out—see for instance [Eisenstein 1850, p. 559].

Let us put this work into the perspective of his earlier paper [Eisenstein 1846]. Recall that the supreme challenge in higher arithmetic after the *Disquisitiones Arithmeticæ* was to construct the theory of *higher reciprocity laws*. Now, Eisenstein, in [Eisenstein 1846], managed to deduce the biquadratic reciprocity law from the special case of the above theorem where m is *zweigliedrig*.

For two distinct primary prime numbers m, n such that n is *zweigliedrig*, the 4-th power residue symbol $\left[\frac{m}{n}\right]$ is defined to be the power of i such that $\left[\frac{m}{n}\right] \equiv n^{\frac{\mathbb{N}_{m-1}}{4}} \pmod{m}$. In [Eisenstein 1846, p.

306], this symbol is written in the form

$$\left[\frac{m}{n}\right] = \frac{\prod_r \varphi(\frac{2nr\omega}{m})}{\prod_r \varphi(\frac{r\omega}{m})},$$

with r ranging over a certain set of residues mod m. Then the reciprocity law

$$\left[\frac{n}{m}\right] = (-1)^{\frac{\mathbb{N}m-1}{4}\cdot\frac{\mathbb{N}n-1}{4}} \left[\frac{m}{n}\right]$$

follows easily from Eisenstein's theorem. (The case of two *eingliedrig* primes m, n, for which the theorem was not available in 1846, is elementary.)

In the same vein, the later series of articles culminates in a final section [Eisenstein 1850, pp. 613–619] proving the reciprocity law for 8-th power residues. Preceding parts [Eisenstein 1850, pp. 575–613] set the stage for this, preparing in particular for the arithmetic of the field of 8-th roots of unities.

Let us now come back to the general lemniscatic arithmetic in Eisenstein's work of 1850. In [Eisenstein 1850, p. 558], Eisenstein arrives at the following easy consequence of his theorem (19).

Corollary. *Let m and n be distinct primary prime numbers and put $q = \mathbb{N}n$. Let $k \in \mathbb{Z}[i]$, and let $F(k)$ be a polynomial expression with coefficients in $\mathbb{Z}[i]$, in the division values $\varphi(\frac{rk(1+i)\omega}{m})$, where r ranges modulo m. Then there exists a polynomial expression T in the same values such that*

$$F(k)^q = F(nk) + nT.$$

He recognized this corollary—see [Eisenstein 1850, p. 559]—as the essential tool to understand the arithmetic of the extensions generated by division values of φ in the same way as Kummer had developed the arithmetic of cyclotomic fields in [Kummer 1847]. This encourages us to sketch a few consequences of the corollary using some of the further development of algebraic number theory. Let us switch at the same time from $\varphi(z)$ to $\wp(z, L)$—recall the comparison (18)—, and also treat $\wp'(z, L)$ along with $\wp(z, L)$.

Call $K = \mathbb{Q}(i)$ our base field and recall the notation of the corollary of section 4 above. Given a primary prime m, we want to study the arithmetic of the field $K_m = K(E_m)$ generated over K by the coordinates of all m-division points $E_m = \Phi(\frac{1}{m}L/L)$. Let n be any primary prime of K which is unramified in K_m. Then n acts on the points of E_m via:

$$\Phi\Big(\frac{(a+bi)\omega}{m}\Big) \qquad \mapsto \qquad \Phi\Big(n\,\frac{(a+bi)\omega}{m}\Big).$$

Here, $a + bi$ ranges over $\mathbb{Z}[i]/(m)$. Eisenstein's corollary means that we can describe this action by reducing modulo the ideal $n \cdot \mathfrak{o}_{K_m}$ in the ring of integers $\mathfrak{o}_{K_m}$ of K_m, i.e. (as n is unramified), modulo any prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{K_m}$ dividing $\mathfrak{p} = n\mathbb{Z}[i]$. In fact, the points of E_m reduce injectively modulo $\mathfrak{P}$ because m and n are relatively prime. We may do better if we use the fact that K_m/K is an abelian extension. For the field generated just by the x-coordinates of points in E_m, this follows already from Abel's work. To see it for our field K_m, one may adapt the proof in [Silverman, Tate 1992, VI.5] to our elliptic curve.

Since K_m/K is abelian, the Frobenius automorphism of the extension of finite fields $(\mathfrak{o}_{K_m}/\mathfrak{P})$ / $(\mathbb{Z}[i]/\mathfrak{p})$ lifts to a unique automorphism $\sigma_\mathfrak{p} \in \mathrm{Gal}(K_m/K)$, and, in the notation of (21), we find for all m-division points that

$$\Phi\Big(\frac{(a+bi)\omega}{m}\Big)^{\sigma_\mathfrak{p}} = \Phi\Big(\psi(\mathfrak{p}) \cdot \frac{(a+bi)\omega}{m}\Big), \tag{22}$$

where ψ was defined in (21). In modern parlance—much used recently in the context of Wiles's proof of Fermat's Last Theorem—, this just means that ψ gives the (abelian) mod m Galois representation of the elliptic curve E.

Let us note in passing that the extensions generated by division values of the elliptic curve $y^2 = x^3 - x$ generate in fact *all* abelian extensions of $\mathbb{Q}(i)$. This special case of what is known as "Kronecker's Jugentraum" was proved (with slight incorrectnesses) by Takagi in his thesis [Takagi 1903]; see also [Schappacher 1997].

Eisenstein remarks that the corollary extends to powers n^μ instead of n, with q replaced by q^μ, and in particular: "one has $F(k)^{q^\mu} =$

$F(k) + nT$ if $n^\mu \equiv 1 \pmod{m}$" [Eisenstein 1850, p. 558]. (Note the analogy with what happens for roots of unity.) Even without taking powers, we get the same conclusion if we take m dividing $n-1$. In other words, we see that all the $n-1$-division points on the elliptic curve $y^2 = x^3 - x$ are invariant under Frobenius, i.e., their reduction is defined already over the finite field $\mathbb{Z}[i]/\mathfrak{p}$. Since there are $\mathbb{N}(n-1)$ torsion points, and they remain distinct after reduction, the curve has at least that many rational points over this finite field—in fact, these are all.

This result about the number of points of E over $\mathbb{Z}[i]/\mathfrak{p}$ (counting also points at infinity!) was conjectured after numerical experiments by Gauss: see the last entry, dated 9 July 1814, of his mathematical diary [Gauss 1976], where he calls this conjecture a "most important observation, found by induction, which links the theory of biquadratic residues with the lemniscatic functions in the most elegant manner" (*Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscatis elegantissime nectens*). In fact, Gauss worked with the model $x^2 + y^2 + x^2y^2 = 1$ of the curve E which corresponds to the equation satisfied by his two basic lemniscatic functions sin lemn and cos lemn, whereas we took $y^2 = x^3 - x$, or equivalently $y^2 = 4x^3 - 4x$, because it corresponds to the Weierstrass equation (15) relating the basic functions $\wp, \wp'$.

Eisenstein met Gauss once. It is not clear whether he learned about Gauss's conjecture. It was published only after Gauss's death (and Gauss died three years after Eisenstein). When Gauss's entry became known later in the 19th century, people did apparently not link it with Eisenstein's work. Dedekind for instance checked the conjecture numerically for all primes of norm less than 100. Fricke recognized the equation of the curve as the one linking Gauss's lemniscatic functions, but it was not until 1921 that the conjecture was proved, by Gustav Herglotz (the teacher of Emil Artin). His concise article [Herglotz 1921] uses the Weierstrass theory, albeit with notation that has not quite survived to the present day. He does allude to Eisenstein's irreducibility criterion in the original lemniscatic context, but otherwise does not seem to derive inspiration from

Eisenstein's paper—however, see also [Herglotz 1922, p. 455f]. A modern account, in the spirit of the Weil conjectures can be found in [Ireland, Rosen 1982, 11-5].

Today one defines the L-function of the elliptic curve E over $K = \mathbb{Q}(i)$ by the infinite product over prime ideals of $\mathbb{Z}[i]$ different from $(1+i)$

$$(23) \qquad L(E/K,s) = \prod_{\mathfrak{p}} \frac{1}{1 - a_{\mathfrak{p}} \mathbb{N}\mathfrak{p}^{-s} + \mathbb{N}\mathfrak{p}^{1-2s}} \; (s \in \mathbb{C},\ \Re(s) > \frac{3}{2}),$$

where $a_{\mathfrak{p}} = \mathbb{N}\mathfrak{p} + 1 - N_{\mathfrak{p}}$ for $N_{\mathfrak{p}}$ the number of points of E over the finite field $\mathbb{Z}[i]/\mathfrak{p}$. Using Gauss's conjecture proved by Herglotz, we find for a *zweigliedrig* prime $\mathfrak{p} = n\mathbb{Z}[i]$, $n = a + bi$ primary: $a_{\mathfrak{p}} = a^2 + b^2 + 1 - (a-1)^2 - b^2 = 2a = \psi(\mathfrak{p}) + \overline{\psi(\mathfrak{p})}$. And for an *eingliedrig* prime $\mathfrak{p} = p\mathbb{Z}[i]$: $a_{\mathfrak{p}} = p^2 + 1 - (p-1)^2 = 2p = 2\psi(\mathfrak{p}) = \psi(\mathfrak{p}) + \overline{\psi(\mathfrak{p})}$. Since for any $\mathfrak{p}$, one clearly has $\psi(\mathfrak{p})\overline{\psi(\mathfrak{p})} = \mathbb{N}\mathfrak{p}$, this proves that

$$(24) \qquad L(E/K,s) = L(\psi,s) \cdot L(\overline{\psi},s),$$

where we define the Hecke L-series of a Hecke character by the rule

$$(25) \qquad L(\psi,s) = \prod_{\mathfrak{p}} \frac{1}{1 - \psi(\mathfrak{p})^s \mathbb{N}\mathfrak{p}^{-s}}.$$

For a general elliptic curve with complex multiplication, the analogous result was obtained by Deuring approximately 100 years after Eisenstein's work—see [Deuring 1953+]. In the 1950's the time was ripe because the progress of abstract algebraic geometry and, more specifically, Weil's work on points of (abelian) varieties over finite fields, had provided the necessary theoretical basis for discussing arithmetic applications and in particular the reduction of algebraic curves modulo primes which we naïvely took for granted in the above discussion of our special case.

The beginning 1950s also saw the generalization of the theory of complex multiplication to higher dimensional abelian varieties by Taniyama and Shimura. Eisenstein's theorem was thus generalized in this higher dimensional theory to the crucial congruence relation of

[Shimura, Taniyama 1961, chap. III, §13]—see also [Giraud 1968] for the grothendieckian digest of this relation. But Eisenstein's work had not been entirely forgotten between 1850 and 1950. In fact, Leopold Kronecker had not only generalized Eisenstein's congruence to arbitrary transformations between elliptic curves [Kronecker 1886, p. 439], but also greatly emphasized the importance of this "fundamental congruence". Thus, Shimura and Taniyama [*loc. cit.*, p. 110] call their theorem a "generalization of Kronecker's congruence formula".

In the vast motivic generalization of the theory of Shimura and Taniyama, one may use Eisenstein's theorem as the one special check which implies the general identity of the "cocycles" describing on the one hand Langlands's Taniyama group and on the other, the motivic Galois group of a category of motives constructed from abelian varieties with complex multiplication—see [Schappacher 1994, §**0**, and §4.4.4].

7 Special L-values and p-adic L-functions: Adolf Hurwitz.

Let us come back to the analytic theory of section 5 above. Differentiating (17) twice in z, we get

$$\wp''(z,L) = \frac{6}{z^4} + \sum_{k=1}^{\infty}(4k-1)(4k-2)(4k-3)G_{4k}(L)z^{4k-4}. \tag{26}$$

On the other hand, differentiating (15) once and dividing by $\wp'$ yields

$$\wp''(z,L) = 6\wp^2(z,L) - 2. \tag{27}$$

Developing both sides of this equation using (17), resp. (26), we obtain recursive formulas for the coefficients $G_{4k}(L)$. For simplicity, let us drop the fixed argument L from the notation. First, comparing the constant terms in (27), we deduce $30G_4 = 2$ which is equivalent to (14b). In z^4, we find $G_8 = \frac{6}{7}G_4^2$. Comparison at z^8 yields $G_{12} = \frac{7}{22}G_4G_8$. Continuing in this way, we get the recursion valid for all

$k \geq 2$:

$$\Big((4k-1)(4k-2)(4k-3)-12(4k-1)\Big)\,G_{4k} = 6\sum_{l+m=k}(4l-1)(4m-1)G_{4l}G_{4m},$$

where the sum is over positive integers l, m that add up to k. Therefore the $G_{4k}(L)$ are all rational numbers. Equivalently, passing from L to Λ, we obtain the following result of Hurwitz—see [Hurwitz 1897, p. 339], [Hurwitz 1899, p. 342]:

Proposition. *For every $k \geq 1$ there exists a rational number e_k such that one has*

$$\sum_{a,b\in\mathbb{Z}}{}' \frac{1}{(a+bi)^{4k}} = e_k \cdot \omega^{4k}. \tag{28}$$

Hurwitz observes the striking analogy of this statement with the well-known rationality of $\zeta(2k)/\pi^{2k}$ for the Riemann zeta function $\zeta(s)$: note that $\pi = 2\int_0^1 dx/\sqrt{1-x^2}$ and rewrite the special ζ-value as

$$\sum_{n\in\mathbb{Z}}{}' \frac{1}{n^{2k}} = \frac{(2\pi)^{2k}}{(2k)!}B_{2k}$$

with the $2k$-th Bernoulli number B_{2k}—see for instance [Neukirch 1992, VII.1.10].

In today's perspective, there is no single natural generalization of the Riemann zeta function whose special values would give the expressions studied by Hurwitz. Rather, the modern approach adduces a different Hecke L-series for every value of k, namely that attached to the $4k$-th power of the Hecke character ψ:

$$L(\psi^{4k}, 4k) = \prod_{\mathfrak{p}} \frac{1}{1-\psi(\mathfrak{p})^{4k}\mathbb{N}\mathfrak{p}^{-4k}} = \frac{1}{4}\sum_{a,b\in\mathbb{Z}}{}' \frac{1}{(a+bi)^{4k}}.$$

See for instance [Harder, Schappacher 1984, §1].

In his perspective, Hurwitz tried to carry over as many properties as possible from the Bernoulli numbers to the e_k (after suitably normalizing the latter). He manages in particular for the congruences

proved in [v. Staudt 1845]. These congruences are seen today—following [Kubota, Leopoldt 1964]—as giving the possibility to p-adically interpolate the rational parts of special values of $\zeta(s)$ (and of similar Dirichlet series), thus constructing *p-adic zeta functions.* Likewise, Hurwitz's result is at the origin of the construction of p-adic L-functions for elliptic curves with complex multiplication—see [de Shalit 1987]. These p-adic considerations were crucial for the first major breakthrough by Coates and Wiles towards the Conjecture of Birch and Swinnerton-Dyer—see [Coates, Wiles 1977]. The Coates-Wiles theorem was in a sense completed (following, as it were, a new idea of Thaine in the theory of cyclotomic fields) by Karl Rubin in 1987. There, our elliptic curve $E : y^2 = x^3 - x$ derived from the lemniscatic integral is among the very first for which the conjecture of Birch and Swinnerton-Dyer could be verified completely: [Rubin 1987, p. 528]. In this conjecture, the finiteness of the group of rational points $E(\mathbb{Q})$ corresponds to the fact that $L(\psi, 1) \neq 0$ ($L(\psi, s)$ can be analytically continued to the whole complex plane; this was proved by Hecke), and the quotient $L(\psi, 1)/\omega$ is interpreted arithmetically in terms of homogeneous spaces of E.

Acknowledgements. With this paper, I want to thank all my Turkish colleagues and friends for their excellent hospitality and company over the years, from 1987 through 1995. Special thanks are due to Sinan Sertöz for the Ankara meeting in 1995 and these proceedings. On the other hand, I am grateful to Jean-Pierre Friedelmeyer who organized an *Atelier de lecture, histoire des mathématiques* at Strasbourg in 1996/97 where some of the texts treated here were read. While writing this article, I profited from comments by Harold Edwards, Jean-Pierre Friedelmeyer, John McCleary, Jean-Yves Merindol.

References

N.H. Abel (1827–28), Recherches sur les fonctions elliptiques, *Journal f.d. reine & angew. Math.* **2**, 101–181, **3**, 160–190 [= Œuvres complètes (Sylow, Lie, ed.s), vol. I, pp. 263–388]

R. Ayoub (1984), The lemniscate and Fagnano's contributions to elliptic integrals, *Archive Hist. Exact. Sciences* **29**, no. 2, 131–149

B. Belhoste (1996), Autour d'un mémoire inédit:la contribution d'Hermite au développement de la théorie des fonctions elliptiques; Revue d'histoires des mathématiques **2**, 1–66

H. Bos (1993), Lectures in the History of Mathematics, Hist. of Math. series, vol. 7, American Mathematical Society, *in particular:* The lemniscate of Bernoulli, pp. 101–111, *and:* The concept of construction and the representation of curves in seventeenth-century mathematics, pp. 23–36

E. Brieskorn & H. Knörrer (1986), Plane Algebraic Curves, Basel etc. (Birkhäuser)

A. Brill & M. Noether (1892–93), Die Entwicklung der Theorie der algebraischen Functionen in älterer und neuerer Zeit, Bericht erstattet der Deutschen Mathematiker-Vereinigung, *Jahresbericht DMV* **3**, 107–566

J. Coates & A. Wiles (1977), On the conjecture of Birch and Swinnerton-Dyer, *Inventiones math.* **39**, 223–251

M. Deuring (1953+), Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, *Nachr. Akademie Wiss. Gött., Math.-Phys. Klasse* 1953, 95–104; Zweite Mitteilung: 1955, 13–42; Dritte Mitteilung: 1956, 37–76; Vierte Mitteilung: 1957, 55–80

G. Eisenstein (1846), Beiträge zur Theorie der elliptischen Funktionen: I. Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsformeln, *Journal f.d. reine & angew. Math.* **30** 1846, 185–210 [= Mathematische Werke, vol. I, pp. 299–324]

G. Eisenstein (1847), Letter to C.F. Gauss dated 18 August 1847, *in:* Mathematische Werke, vol. II, pp. 845–855

G. Eisenstein (1850), Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, *Journal f.d. reine & angew. Math.* **39**, 160–179; *and the sequel:* Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhangt, nebst Anwendungen derselben auf die Zahlentheorie, *Journal f.d. reine & angew. Math.* **39**, 224–287 [= Mathematische Werke, vol. II, pp. 536–619]

A. Enneper (1876), Elliptische Functionen, Theorie und Geschichte, Halle (Nebert)

L. Euler (1761), Observationes de comparatione arcuum curvarum irrectificabilium. Novi comm. acad. sci. Petrop. **6**, 58–84 [= Mathematische Werke (Leipzig, Berlin 1912) **20**, 80–107]

G.C. di Fagnano (1750), Produzioni matematiche, vol. II, Pesaro [= Opere matematiche 1–2, Milano-Roma-Napoli 1911]

E. Freitag & R. Busam (1995), Funktionentheorie (2nd edition), *Springer Lehrbuch*, Berlin, Heidelberg

C.F. Gauss (1801), Disquisitiones Arithmeticæ, Leipzig (G. Fleischer)

C.F. Gauss (III), Werke, Göttingen (1870–1927), volume III

C.F. Gauss (1976), Mathematisches Tagebuch 1796–1814, Hrsg./Übers.: Biermann, Schuhmann, Wußing. Leipzig (Geest & Portig)

J. Giraud (1968), Remarque sur une formule de Shimura-Taniyama, *Inventiones Math.* **5**, 231–236

C. Goldstein (1995), Un théorème de Fermat et ses lecteurs, Saint Denis (Presses Universitaires de Vincennes)

G. Harder & N. Schappacher, Special Values of Hecke L-functions and Abelian Integrals; *in:* Arbeitstagung Bonn 1984, *Lecture Notes in Mathematics* **1111** (Springer) 1985, 17–49

T. Heath (1921), A History of Greek Mathematics, Oxford, vol. II

G. Henniart (1987), Cyclotomie et valeurs de la fonction Γ (d'après G. Anderson), Sém. Bourbaki no. 688; Astérisque **161–162**, 1988, pp. 53–72

G. Herglotz (1921), Zur letzten Eintragung im Gaußschen Tagebuch; *in: Berichte über die Verhandlungen der Sächsischen Akademie der Wissenschaften Math.-phys. Klasse* **73**, 271–276 [= Gesammelte Schriften (Schwerdtfeger, ed.), Göttingen 1979, 415–420]

G. Herglotz (1922), Über die Entwicklungskoeffizienten der Weierstrass'schen $\wp$-Funktion; *in: Berichte über die Verhandlungen der Sächsischen Akademie der Wissenschaften Math.-phys. Klasse* **74**, 269–289 [= Gesammelte Schriften (Schwerdtfeger, ed.), Göttingen 1979, 436–456]

C. Houzel (1978), Fonctions elliptiques et intégrales abéliennes, *in:* J. Dieudonné (ed.), Abrégé d'histoire des mathématiques 1700–1900, vol. II, Paris (Hermann), pp. 1–113

C. Houzel (1995), Théorème de Fermat, à travers l'histoire de l'analyse diophantienne, brochure (17 pages), Société Mathématique de France, Paris

A. Hurwitz (1897), Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, *Nachr. Ges. Wiss. Göttingen*, 273–276 [= Mathematische Werke, vol. II, 338–341]

A. Hurwitz (1899), Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, *Mathematische Annalen* **51**, 196–226 [= Mathematische Werke, vol. II, 342–373]

K. Ireland & M. Rosen (1982), A classical introduction to modern number theory, Graduate Texts in Mathematics **84**, New York, Berlin, etc. (Springer)

C.G.J. Jacobi (1835), De usu theoriæ integralium ellipticorum et integralium abelianorum in analysi diophantea, *Journal f.d. reine & angew. Math.* **13**, 353–355 [= Gesammelte Werke (Weierstrass, Hrsg.), vol. II, 53–55]

C.G.J. Jacobi (1846), Über einige die elliptischen Functionen betreffenden Formeln, *Journal f.d. reine & angew. Math.* **30**, 269–270 [= (with one correction) Gesammelte Werke (Weierstrass, Hrsg.), vol. I, 371–372]

L. Kiepert (1873), Siebzehntheilung des Lemniscatenumfangs durch alleinige Anwendung von Lineal und Cirkel, *Journal f.d. reine & angew. Math.* **75**, 255–263; *and:* Zusatz zu der Abhandlung über Siebzehntheilung der Lemniscate S. 255 dieses Bandes, *Journal f.d. reine & angew. Math.* **75**, 348

N. Koblitz (1984), Introduction to Elliptic Curves and Modular Forms, Graduate Texts in Mathematics **97**, New York, Berlin, etc. (Springer)

L. Königsberger (1904), Carl Gustav Jacob Jacobi, Festschrift zur hundertsten Wiederkehr seines Geburtstages, Leipzig (Teubner)

L. Kronecker (1886), Zur Theorie der elliptischen Functionen, XI, Sitzungsber. Akademie Berlin (27.5. & 29.7.1886), 701–780 = Werke IV, p. 389–471.

T. Kubota & H.W. Leopoldt (1964), Eine p-adische Theorie der Zetawerte, I. Einführung der p-adischen Dirichletschen L-Funktionen, *Journal f.d. reine & angew. Math.* **214/215**, 328–339

E.E. Kummer (1847), Zur Theorie der complexen Zahlen, *Journal f.d. reine & angew. Math.* **35**, 319–326; *and:* Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren, *Journal f.d. reine & angew. Math.* **35**, 327–367 [= Collected Papers (A. Weil, ed.), vol. I (1975), Berlin, Heidelberg, New York (Springer), pp. 203–251]

A.M. Legendre (1811), Exercices de calcul intégral, Paris

A.M. Legendre (1825–28), Traité des fonctions elliptiques, 3 vol., Paris

T. Masahito (1995), Three aspects of Complex Multiplication; *in:* The intersection of history and mathematics (S. Chikara, S. Mitsuo, J.W. Dauben, ed.s), Science Networks, Historical Studies, vol. 15, Birkhäuser Verlag Basel, Boston, Wien, pp. 91–108.

J. Neukirch (1992), Algebraische Zahlentheorie, Berlin, Heidelberg, etc. (Springer)

Plana (1863), Mémoire sur la théorie des transcendantes elliptiques, *Memorie della reale Academia di Torino*, Serie seconda, **XX**, p. 292

R. Rashed (1996), Modernité classique et science arabe, *in:* L'Europe mathématique / Mathematical Europe (Goldstein, Gray, Ritter, ed.s), Paris (MSH), 67–81

R. Remmert (1991), Funktionentheorie 2, Berlin, Heidelberg etc. (Springer)

K. Rubin (1987), Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, *Inventiones math.* **89**, 527–560

J.-P. Serre (1970), Cours d'arithmétique, Paris (PUF) [in English: Graduate Texts in Mathematics **7**, New York, Berlin, etc. (Springer)]

N. Schappacher (1988), Periods of Hecke Characters, Springer Lecture Notes Math. **1301**

N. Schappacher (1989), Neuere Forschungsergebnisse in der Arithmetik elliptischer Kurven, *Didaktik der Mathematik* **17**, 149–158

N. Schappacher (1991), Développement de la loi de groupe sur une cubique; Séminaire de Théorie des Nombres Paris 1988/89, *Progress in Mathematics* **91** (Birkhäuser), 159–184

N. Schappacher (1994), CM motives and the Taniyama group; *in:* Motives (Jannsen, Kleiman, Serre, eds.), Proceedings of Symposia in Pure Mathematics **55**, part I, AMS 1994, 485–508

N. Schappacher (1997), On the History of Hilbert's Twelfth Problem, I: Paris 1900 – Zürich 1932, a Comedy of Errors, *to appear*

H. Schröter (1873), Zur *v. Staudt*schen Construction des regulären Siebzehnecks, *Journal f.d. reine & angew. Math.* **75**, 13–24

E. de Shalit (1987), Iwasawa Theory of Elliptic Curves with Complex Multiplication, *Persepctives in Mathematics* **3**, Boston, Orlando, etc. (Academic Press)

G. Shimura & Y. Taniyama (1961), Complex multiplication of abelian varieties and its application to number theory, Publ. Math. Soc. Japan **6**

C.L. Siegel (1959), Zur Vorgeschichte des Eulerschen Additionstheorems; *in:* Sammelband Leonard Euler, Akademie-Verlag Berlin [= Gesammelte Abhandlungen, vol. III, 249–251]

C.L. Siegel (1969), Topics in Complex Function Theory, New York, London, etc. (Wiley)

J.H. Silverman (1986), The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **106**, New York, Berlin, etc. (Springer)

J.H. Silverman & J. Tate (1992), Rational Points, Undergraduate Texts in Mathematics, New York, Berlin, etc. (Springer)

P. Stäckel & W. Ahrens (ed.s) (1908), Der Briefwechsel zwischen C.G.J. Jacobi und P.H. Fuss über die Herausgabe der Werke Leonhard Eulers, Leipzig

C.G.C. v. Staudt (1845), De numeris Bernoullianis, and: De numeris Bernoullianis commentatio altera, Erlangen (Junge)

T. Takagi (1903), Ueber die im Bereiche der rationalen complexen Zahlen Abel'schen Körper, Journal of the College of Science, Tokyo Imperial University **19**, article 5, 42 pages [= Collected Papers (ed.s S. Iyanaga, K. Iwasawa, K. Kodaira, K. Yosida), Tokyo - Berlin - Heidelberg - New York - London - Paris - Hong Kong - Barcelona (Springer) 1990, no. 6, pp. 13–39]

I. Thomas (1941), Selections Illustrating the History of Greek Mathematics, vol. II, Loeb Classical Library, Cambridge (Mass.) and London

A. Weil (****), Œuvres scientifiques — Collected Papers, volume II (1951–1964), New York, Heidelberg, etc. (Springer) 1979; the individual articles are quoted according to the abbreviations of this edition.

A. Weil (1984), Number Theory, An Approach through History, from Hammurapi to Legendre, Boston etc. (Birkhäuser)