ABEL'S THEOREM ON THE LEMNISCATE

MICHAEL ROSEN
Department of Mathematics, Brown University, Providence, RI 02906

Introduction. As is well known, one of the great accomplishments of Gauss's youth was the proof that a regular polygon of 17 sides could be constructed with ruler and compass. In the seventh chapter of *Disquisitiones Arithmeticae* [2] he shows how this result follows from his arithmetic theory of cyclotomic numbers. In general he shows that a regular n-gon can be constructed with ruler and compass if $n = 2^a p_1 p_2 \cdots p_t$ where the p_i are distinct Fermat primes. He also asserts that he has a proof of the converse and warns the reader not to attempt to construct other polygons "and so spend his time uselessly."

In the introduction to Chapter 7 Gauss states that the principles underlying his theory apply not only to circular functions (sine, cosine, etc.) but also to a much larger class of transcendental functions "for example those that depend on the integral $\int dt/\sqrt{1-t^4}\ldots$." He says that he is preparing a comprehensive work on this subject. Unfortunately this treatise never materialized. The functions in question are nowadays called elliptic functions. Gauss's unpublished papers reveal that by 1801, when *Disquisitiones Arithmeticae* appeared, he was already in possession of large parts of elliptic function theory (see [3]). The epoch-making works of Abel and Jacobi were to appear some twenty-five years later.

Gauss kept a mathematical diary [3] from 1796 to 1814. It was not found until 1898, forty-three years after his death. There are 146 entries, all of them short notices of new results. The entry of March 21, 1797, reads as follows, "Lemniscata geometrice in quinque partes dividitur." In other words, he had discovered how to divide the lemniscate into five equal parts with ruler and compass. Among other things this result is remarkable because it shows that at this early date Gauss already knew something about complex multiplication of elliptic functions.

Abel, of course, knew nothing of Gauss's diary. He was, however, very familiar with *Disquisitiones Arithmeticae* and was especially intrigued (as was Jacobi) with the remarks, mentioned above, about "a much larger class of transcendental functions." In 1826, while working on the division equation for elliptic functions, he gained insight into Gauss's theory. He wrote to Holmboe: "On that same occasion I have lifted the mystery which had rested over Gauss' theory of the division of the circle; I now see as clear as daylight how he has been led to it."* His work on elliptic functions was coming along at a rapid pace and he wrote to Crelle and Holmboe with obvious excitement about his forthcoming treatise: "...in which there are many queer things which I flatter myself will startle someone; among others it is about the division of arcs of the lemniscate. You will see how pretty it is!" (For this and the previous quote see Chapter 13 of [6].)

The finished work, "Recherches sur les fonctions elliptiques," appeared in two parts in volumes 2 and 3 of *Crelle's Journal der Mathematik*. The two articles take up 197 pages. They lay the foundations of the theory of elliptic functions and contain a cornucopia of beautiful results. Among these is the following gem, which seems to have been virtually forgotten.

THEOREM. *The lemniscate can be divided into n equal parts with ruler and compass if $n = 2^a p_1 p_2 \cdots p_t$ where the p_i are distinct Fermat primes.*

---

*I would like to thank Professor H. Edwards of the Courant Institute for bringing this quote to my attention.

Michael Rosen received his Ph.D. from Princeton University in 1963. He has spent most of his academic career at Brown University, where he is now Professor of Mathematics. He has been on leave three times: at Brandeis University, 1965–66; at the University of Wisconsin (Madison), 1971–72; and at the University of California (Berkeley), 1979–80. His main research interests are algebraic number fields and algebraic function fields. He is coauthor with Ken Ireland of *Elementary Number Theory—Including an Introduction to Equations over Finite Fields*. —*Editors*

This result is the exact analogue of Gauss's result for the circle. Clearly, it goes far beyond what Gauss recorded in the diary entry of March 21, 1797.

The main object of this paper is to give a reasonably elementary proof of Abel's theorem and its converse. For the most part we use only the beginnings of elliptic function theory (see, for example, the first chapter of [5], [7], or [8]). Our proof differs from that of Abel in that we use Galois theory (which was unavailable to him) and relies on the properties of the Weierstrass $\mathcal{P}$ function rather than the lemniscate function $\phi(z)$ (to be defined below). Nevertheless the main point of both proofs is the same; the functions involved admit complex multiplication by the ring of Gaussian integers $Z[i]$.

In Section 1 we review the Galois-theoretic proof of Gauss's theorem and recast it in such a way that the later work on lemniscate appears as a natural generalization. In Section 2 we define the lemniscate, discuss its arc-length, define the lemniscate function $\phi(z)$, and discuss the remarkable properties of this function discovered by Abel (and independently by Gauss and Jacobi). In Section 3 we briefly review the elements of the theory of elliptic functions. In Section 4 we relate the function $\phi(z)$ to the Weierstrass $\mathcal{P}$-function. Finally, in Section 4 we give our proof of Abel's theorem and its converse. To the best of our knowledge, a proof of the converse of Abel's theorem has not previously appeared in print.

In addition to presenting some material of great historical interest we hope this paper will serve as an introduction to the arithmetic theory of elliptic curves, an area of mathematics which is alive and well and being pursued with great intensity by number-theorists of the present day.

1. As is well known, a complex number α is constructible with ruler and compass if and only if $\mathbb{Q}(\alpha)$ is contained in a field K obtained from the rational numbers $\mathbb{Q}$ by a succession of quadratic extensions. It is equivalent to require that α be in a field K which is Galois over $\mathbb{Q}$ and such that $G(K/\mathbb{Q})$, the Galois group of K over $\mathbb{Q}$, has order a power of two.

Let $\zeta_n = \exp(2\pi i/n)$. One knows that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $(Z/nZ)^*$. Elementary number theory shows that the order of $(Z/nZ)^*$ is a power of two if and only if $n = 2^a p_1 p_2 \cdots p_t$ where the p_i are distinct Fermat primes. This proves Gauss's theorem.

A slightly different approach goes as follows. Map the real numbers $\mathbb{R}$ to the unit circle C by $\xi(t) = (\cos t, \sin t)$. The map ξ is onto and periodic. The periods consist of all multiples of $2\pi, \langle 2\pi \rangle$. Thus ξ gives rise to a bijection between $\mathbb{R}/\langle 2\pi \rangle$ and C. Since $\mathbb{R}/\langle 2\pi \rangle$ is a group, C can be made into a group by "transport of structure." Using the addition formulae for sine and cosine we see that the group law on C is given by $(a,b) + (c,d) = (ac - bd, ad + bc)$. The unit element of C is $(1,0)$. For n a positive integer we deduce that there are polynomials $f_n(x,y), g_n(x,y) \in Z[x,y]$ such that $n(x,y) = (x,y) + (x,y) + \cdots + (x,y) = (f_n(x,y), g_n(x,y))$. For example, $2(x,y) = (x^2 - y^2, 2xy)$ and $3(x,y) = (x^3 - 3xy^2, 3x^2y - y^3)$. Let C_n be the points of order dividing n on C. Since $C \approx \mathbb{R}/\langle 2\pi \rangle$ we see $C_n \approx Z/nZ$. Moreover,

$$C_n = \{(a,b) \in C \mid f_n(a,b) = 1 \text{ and } g_n(a,b) = 0\}.$$

Let σ be an automorphism of $\mathbb{C}$, the complex numbers, over $\mathbb{Q}$. Since $f_n(a,b)^\sigma = f_n(a^\sigma, b^\sigma)$ and $g_n(a,b)^\sigma = g_n(a^\sigma, b^\sigma)$, we see σ maps C_n into itself. Since C_n is finite, it follows that the coordinates of the points in C_n are algebraic numbers. Adjoin these coordinates to $\mathbb{Q}$ and call the resulting field K_n. From what has been said it follows that $K_n/\mathbb{Q}$ is a Galois extension. Denote the Galois group by G_n. G_n acts on C_n and, since the group law is defined by polynomials with coefficients in $\mathbb{Q}$, we see that G_n preserves the group structure of C_n. Thus we have a map from G_n to $\mathrm{Aut}(C_n)$ which is easily seen to be a homomorphism. The map is actually a monomorphism since the coordinates of the points in C_n generate K_n. Thus G_n is isomorphic to a subgroup of $\mathrm{Aut}(C_n) \approx \mathrm{Aut}(Z/nZ) \approx (Z/nZ)^*$. The proof of Gauss's theorem now follows as before.

This second proof may seem overly elaborate, but, as we shall see, many of the ideas involved will be useful later.

2. A lemniscate may be defined geometrically as the locus of all points such that the product of the distances to two fixed points is a constant. This definition gives rise to a family of curves. We normalize matters by requiring the fixed points to be $(-\sqrt{2}/2,0)$ and $(\sqrt{2}/2,0)$ and the constant to be $\frac{1}{2}$. The equation of the resulting curve is $r^2 = \cos 2\theta$ in polar coordinates and $(x^2 + y^2)^2 = x^2 - y^2$ in Cartesian coordinates. Its shape is the familiar figure eight. (See Fig. 1.) A convenient reference for this material is the first chapter of Siegel's book [**8**].

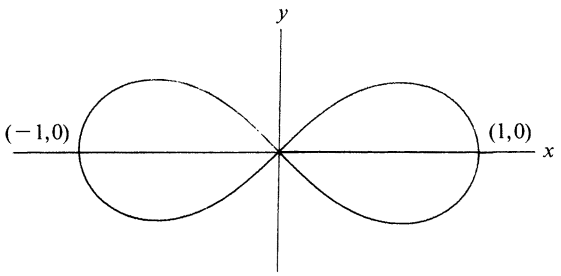

FIG. 1

If we use the formula for arc-length in polar coordinates $ds^2 = dr^2 + r^2 d\theta^2$, we find for the lemniscate $ds = dr/\sqrt{1 - r^4}$. If we measure arc-length starting from the origin and passing into the first quadrant we see r increases from 0 to 1 and s is a monotonically increasing function of r. Explicitly, $s = \int_0^r dt/\sqrt{1 - t^4}$. Let $\omega/2 = \int_0^1 dt/\sqrt{1 - t^4}$. The total arc-length of the lemniscate is then 2ω. The constant ω is to the lemniscate what π is to the circle. To five places its value is 2.62057....

As s is a monotonically increasing function of r on $[0,1]$, r can be expressed as a function of s on $[0,\omega/2]$: set $r = \phi(s)$. This is Abel's notation. Gauss wrote sinlemn(s).

Abel shows that ϕ can be extended to a meromorphic function for a complex variable z. He shows that $\phi(z)$ is doubly periodic with

$$L = \langle 2\omega, 2\omega i \rangle = \{2m\omega + 2ni\omega \mid m,n \in Z\}$$

as a period lattice. The exact period lattice is $\langle (1 + i)\omega, (1 - i)\omega \rangle$. This fact will be useful later. He finds all the zeros and poles of $\phi(z)$. The zeros are the points of the lattice $\langle \omega, \omega i \rangle$ and the poles are obtained from the zeros by adding $(\omega + \omega i)/2$. Fig. 2 shows the location of the zeros and poles in a fundamental parallelogram $\{z \mid 0 \leq \mathrm{Re}z, \mathrm{Im}z < 2\omega\}$. He gives the following

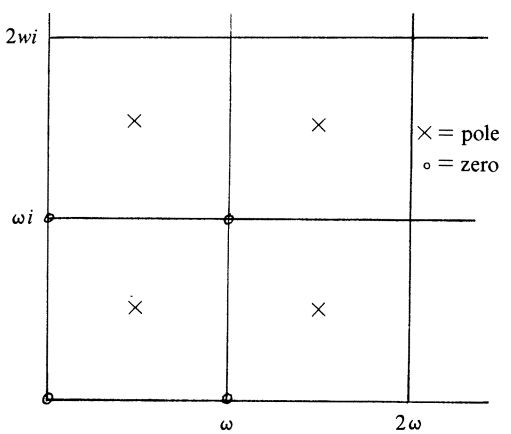

FIG. 2

product formula for $\phi(z)$:

$$\phi(z) = z\prod_{\alpha}\left(1 - \frac{z^4}{\alpha^4}\right)\prod_{\beta}\left(1 - \frac{z^4}{\beta^4}\right)^{-}$$

where α runs through the zeros and β through the poles in the region $0 \leqslant \arg z < \pi/2$. He also proves the addition formula (discovered much earlier by Euler; see [**8**])

$$\phi(s+t) = \frac{\phi(s)\sqrt{1-\phi(t)^4} + \phi(t)\sqrt{1-\phi(s)^4}}{1+\phi(s)^2\phi(t)^2}.$$

All this and much else was discovered years earlier by Gauss, but had remained unpublished.

We will not prove these results. With the use of the modern theory of complex variables they may be considered exercises, albeit hard ones. It is quite amazing that Gauss, Abel, and Jacobi were able to prove all this when the theory of functions of a complex variable was still in its infancy.

To investigate the question of dividing the lemniscate into n equal parts with ruler and compass, we are reduced to asking the following question.

Question: For which integers n are the numbers $\phi(k2\omega/n)$, $k = 0,1,\ldots,n-1$ constructible?

Note that the corresponding problem for the circle concerns the numbers $\sin(k2\pi/n)$.

3. Both for technical reasons and because the modern reader is much more likely to be familiar with the Weierstrass $\mathcal{P}$ function than with Abel's function $\phi(z)$, we will reformulate the question of the previous section. Before doing so we briefly review the properties of the $\mathcal{P}$ function which we will need. For proofs the reader can consult [**5**], [**7**], or [**8**].

Let $\omega_1, \omega_2 \in \mathbb{C}$ be complex numbers such that ω_2/ω_1 is not real, and $\Lambda = \langle \omega_1, \omega_2 \rangle = \{m\omega_1 + n\omega_2 | m, n \in Z\}$, the corresponding lattice. A meromorphic function $f(z)$ on $\mathbb{C}$ is called elliptic with respect to Λ if $f(z+\lambda) = f(z)$ for all $z \in \mathbb{C}$ and $\lambda \in \Lambda$. The elements of Λ are called periods of $f(z)$. The set of functions which are elliptic with respect to Λ form a field which we denote by $\mathfrak{M}(\Lambda)$. From another point of view, $\mathfrak{M}(\Lambda)$ is the field of meromorphic functions on the Riemann surface $\mathbb{C}/\Lambda$.

Let $D(\Lambda) = \{r\omega_1 + s\omega_2 | 0 \leqslant r, s < 1\}$. $D(\Lambda)$ is called a fundamental parallelogram for Λ since the translates of $D(\Lambda)$ by elements of Λ simply cover the plane. If $f(z) \in \mathfrak{M}(\Lambda)$ and $f(z)$ has no pole on $D(\Lambda)$, then $f(z)$ is a constant. This fundamental fact is proved as follows. If $f(z)$ has no pole on $D(\Lambda)$, it has no pole on $\mathbb{C}$ by periodicity. Thus $f(z)$ is continuous on the closure of $D(\Lambda)$, which is compact. It follows that $f(z)$ is bounded on $D(\Lambda)$ and by periodicity on all of $\mathbb{C}$. By Liouville's theorem a bounded entire function is a constant.

Does $\mathfrak{M}(\Lambda)$ have any nonconstant functions? The answer is yes. Define

$$\mathcal{P}(z;\Lambda) = z^{-2} + \Sigma'\left((z-\lambda)^{-2} - \lambda^{-2}\right)$$

where the sum is over all $\lambda \in \Lambda, \lambda \neq 0$. Since the lattice Λ is fixed in this discussion, we suppress it in the notation and write simply $\mathcal{P}(z)$. Note that $\mathcal{P}(-z) = \mathcal{P}(z)$ and $\mathcal{P}'(-z) = -\mathcal{P}'(z)$; i.e., $\mathcal{P}(z)$ is an even and $\mathcal{P}'(z)$ is an odd function.

Both $\mathcal{P}(z)$ and $\mathcal{P}'(z)$ are in $\mathfrak{M}(\Lambda)$, and in fact $\mathfrak{M}(\Lambda) = \mathbb{C}(\mathcal{P}(z), \mathcal{P}'(z))$; i.e., every elliptic function with respect to Λ is a rational function of $\mathcal{P}(z)$ and $\mathcal{P}'(z)$. Moreover, $\mathcal{P}(z)$ and $\mathcal{P}'(z)$ are connected by the equation

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2(\Lambda)\mathcal{P}(z) - g_3(\Lambda)$$

where $g_2(\Lambda) = 60\Sigma'\lambda^{-4}$ and $g_3(\Lambda) = 140\Sigma'\lambda^{-6}$.

For $z \in \mathbb{C}$ let (z) be the unique element of $D(\Lambda)$ such that $z - (z) \in \Lambda$. The poles of $\mathcal{P}(z)$ and $\mathcal{P}'(z)$ are precisely at the points of Λ, i.e., those z such that $(z) = 0$. Those of $\mathcal{P}(z)$ have

multiplicity 2 and those of $\mathcal{P}'(z)$ have multiplicity 3. It is not known where the zeros of $\mathcal{P}(z)$ lie but, if $a \notin \Lambda$, then the zeros of $\mathcal{P}(z) - \mathcal{P}(a)$ are precisely $\{z \in \mathbb{C} | (z) = (a) \text{ or } (z) = (-a)\}$. These are simple zeros unless $(a) = (-a)$, in which case they are double zeros. The zeros of $\mathcal{P}'(z)$ are $\{z \in \mathbb{C} | (z) = \omega_1/2, \omega_2/2, \text{ or } (\omega_1 + \omega_2)/2\}$. These are all simple zeros. These facts are often sufficient to enable us to write a function in $\mathcal{R}(\Lambda)$ explicitly as a rational function of $\mathcal{P}$ and $\mathcal{P}'$.

A very important property of $\mathcal{P}$ and $\mathcal{P}'$ is the existence of an addition formula; i.e., for $z_1, z_2 \in \mathbb{C}$ with $z_1, z_2, z_1 + z_2 \notin \Lambda$, both $\mathcal{P}(z_1 + z_2)$ and $\mathcal{P}'(z_1 + z_2)$ can be expressed rationally in terms of $\mathcal{P}(z_1)$, $\mathcal{P}(z_2)$, $\mathcal{P}'(z_1)$, and $\mathcal{P}'(z_2)$. This can be seen from the following considerations. Let E be the complex points on the curve $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ together with a symbol ∞. This symbol represents the point at infinity on this curve. We call E the elliptic curve corresponding to Λ. Let ξ map $\mathbb{C}$ to E by $\xi(z) = (\mathcal{P}(z), \mathcal{P}'(z))$ for $z \notin \Lambda$ and $\xi(z) = \infty$ for $z \in \Lambda$. It can be shown that $\xi(z_1)$, $\xi(z_2)$, and $\xi(-z_1 - z_2)$ lie on a straight line. From this one deduces for $z_1, z_2 \notin \Lambda$ and $\mathcal{P}(z_1) \neq \mathcal{P}(z_2)$, i.e., $(z_1) \neq (\pm z_2)$, that

$$\mathcal{P}(z_1 + z_2) = -\mathcal{P}(z_1) - \mathcal{P}(z_2) + \frac{1}{4}\left(\frac{\mathcal{P}'(z_1) - \mathcal{P}'(z_2)}{\mathcal{P}(z_1) - \mathcal{P}(z_2)}\right)^2$$

and, if $(z_1) = (z_2) = z$, then

$$\mathcal{P}(2z) = -2\mathcal{P}(z) + \frac{1}{4}\left(\frac{\mathcal{P}''(z)}{\mathcal{P}'(z)}\right)^2.$$

If $z_1 + z_2 \in \Lambda$, i.e., $(z_1) = (-z_2)$, then the first formula continues to hold in the sense that both sides are infinite. The rational addition formula for $\mathcal{P}'(z)$ follows easily. We note that the coefficients of the rational functions giving the addition formula lie in the field generated over $\mathbb{Q}$ by $g_2(\Lambda)$ and $g_3(\Lambda)$.

It will be useful to give an algebraic interpretation of these results. By periodicity the map ξ gives rise to a map from $\mathbb{C}/\Lambda$ to E which we continue to call ξ. This map can be shown to be a bijection between $\mathbb{C}/\Lambda$ and E, and so by "transport of structure" E becomes a group. The group law on E is algebraic in the sense that there are rational functions f and g such that

$$(a,b) + (c,d) = (f(a,b,c,d), g(a,b,c,d)).$$

To see this let $\xi(z_1) = (a,b)$ and $\xi(z_2) = (c,d)$. By definition, $\xi(z_1) + \xi(z_2) = \xi(z_1 + z_2)$, or

$$(\mathcal{P}(z_1), \mathcal{P}'(z_1)) + (\mathcal{P}(z_2), \mathcal{P}'(z_2)) = (\mathcal{P}(z_1 + z_2), \mathcal{P}'(z_1 + z_2)).$$

It is now clear how the addition formulae give rise to the functions f and g.

Note that the identity element of the group E is $\xi(0) = \infty$. Let E_n be the points of order dividing n on E. Since $E \approx \mathbb{C}/\Lambda$, $E_n \approx \frac{1}{n}\Lambda/\Lambda \approx \Lambda/n\Lambda$. Thus E_n has n^2 elements. Explicitly,

$$E_n = \left\{\left(\mathcal{P}\left(\frac{a\omega_1 + b\omega_2}{n}\right), \mathcal{P}'\left(\frac{a\omega_1 + b\omega_2}{n}\right)\right) \middle| 0 \leq a,b < n\right\}.$$

For example, the points in E_2 are $\{\infty, (e_1,0), (e_2,0), (e_3,0)\}$ where

$$e_1 = \mathcal{P}\left(\frac{\omega_1}{2}\right), \quad e_2 = \mathcal{P}\left(\frac{\omega_2}{2}\right), \quad \text{and} \quad e_3 = \mathcal{P}\left(\frac{\omega_1 + \omega_2}{2}\right).$$

Note that e_1, e_2, and e_3 are the roots of $4x^3 - g_2(\Lambda)x - g_3(\Lambda) = 0$. A consequence which is not obvious a priori is that this polynomial must have distinct roots.

4. We now return to a consideration of the lattice $L = \langle 2\omega, 2\omega i \rangle$. Let $\mathcal{P}(z)$ be the corresponding $\mathcal{P}$ function.

In the appendix we show that $g_2(L) = \frac{1}{4}$ and $g_3(L) = 0$. Thus, the elliptic curve corresponding to L is $y^2 = 4x^3 - \frac{1}{4}x$.

Notice that $iL = L$. From the definition of $\mathcal{P}(z)$ we see that $\mathcal{P}(iz) = -\mathcal{P}(z)$ and by differentiation that $\mathcal{P}'(iz) = i\mathcal{P}(z)$. Using the addition formula we find after some calculation

$$\mathcal{P}((1+i)z) = -\frac{i}{8}\frac{4\mathcal{P}(z)^2 - \frac{1}{4}}{\mathcal{P}(z)} \tag{1}$$

$$\mathcal{P}((1-i)z) = \frac{i}{8}\frac{4\mathcal{P}(z)^2 - \frac{1}{4}}{\mathcal{P}(z)} \tag{2}$$

LEMMA 1. *If $\mathcal{P}(\alpha)$ is constructible, so is $\mathcal{P}(\alpha/2)$.*

Proof. In equation (1) substitute $z = \alpha/(1+i)$. We then see that $\mathcal{P}(\alpha/(1+i))$ satisfies a quadratic equation with constructible coefficients. Thus $\mathcal{P}(\alpha/(1+i))$ is constructible. In equation (2) substitute $z = \alpha/2$. Then, since $\mathcal{P}((1-i)(\alpha/2)) = \mathcal{P}(\alpha/(1+i))$ is constructible, $\mathcal{P}(\alpha/2)$ satisfies a quadratic equation with constructible coefficients, and so $\mathcal{P}(\alpha/2)$ is constructible.

COROLLARY. *Suppose $a,b,n \in Z$ with $n \geq 1$ and $ab \neq 0$. Then the numbers*

$$\mathcal{P}((2a\omega + 2bi\omega)/2^n)$$

are constructible.

Proof. The numbers $\{\mathcal{P}(\omega), \mathcal{P}(i\omega), \mathcal{P}((1+i)\omega)\}$ are the roots of $4x^3 - \frac{1}{4}x = 0$, i.e., $\{\frac{1}{4}, -\frac{1}{4}, 0\}$. This proves the result for $n = 1$. For general n the result follows by induction using Lemma 1.

We are now in a position to relate $\mathcal{P}(z)$ and $\phi(z)$. Before doing so we make the simple remark that if $\mathcal{P}(\alpha)$ is constructible so is $\mathcal{P}'(\alpha)$ since $\mathcal{P}'(\alpha)^2 = 4\mathcal{P}(\alpha)^3 - \frac{1}{4}\mathcal{P}(\alpha)$.

PROPOSITION 1. *$\phi(\alpha)$ is constructible if and only if $\mathcal{P}(\alpha)$ is constructible.*

Proof. For the proof of Abel's theorem we only need the "if" part of the Proposition. We do this implication first.

The zeros and poles of $\phi(z)$ on $D(L)$ are $\{0, \omega, i\omega, (1+i)\omega\}$ and

$$\{(1+i)\omega/2, (3\omega + i\omega)/2, (\omega + 3i\omega)/2, (3\omega + 3i\omega)/2\},$$

respectively. The function

$$g(z) = \frac{\mathcal{P}'(z)}{(\mathcal{P}(z) - \mathcal{P}(z_0))(\mathcal{P}(z) - \mathcal{P}(z_1))}$$

has the same zeros and poles if we set $z_0 = (1+i)\omega/2$ and $z_1 = (3\omega + i\omega)/2$. Thus $\phi(z) = Ag(z)$ for some constant A. Since $\phi(\omega/2) = 1$ and $g(\omega/2)$ is constructible by the corollary to Lemma 1, we see that A is constructible. If $\mathcal{P}(\alpha)$ is constructible so is $g(\alpha)$ and thus so is $\phi(\alpha)$.

The proof of the converse is a bit more difficult. As we mentioned earlier $\phi(z)$ is periodic with respect to the lattice $M = \langle (1+i)\omega, (1-i)\omega \rangle$. Let $\mathcal{P}_1(z)$ be the $\mathcal{P}$ function corresponding to M. Since $(1+i)M = L$, we see (from definitions) that $2i\mathcal{P}((1+i)z) = \mathcal{P}_1(z)$.

The zeros and poles of $\phi(z)$ on $D(M)$ are $\{0, \omega\}$ and $\{(1+i)\omega/2, (1-i)\omega/2\}$, respectively. Comparing zeros and poles we see there is a constant B such that

$$\phi(z) = B\frac{\mathcal{P}_1(z) - \mathcal{P}_1(\omega)}{\mathcal{P}_1'(z)}.$$

Evaluating at $z = \omega/2$ and using the corollary to Lemma 1 once again we see that B is constructible.

Let $u_0 = (1+i)\omega/2$ and $u_1 = (1-i)\omega/2$. Since the zeros of $\mathcal{P}_1'(z)$ are u_0, u_1, and ω we find

$$\phi(z)^2 = \frac{B^2}{4}\frac{\mathcal{P}_1(z) - \mathcal{P}_1(\omega)}{(\mathcal{P}_1(z) - \mathcal{P}_1(u_0))(\mathcal{P}_1(z) - \mathcal{P}_1(u_1))}.$$

It follows that if $\phi(\alpha)$ is constructible so is $\mathcal{P}_1(\alpha)$.
From previous results we have

$$\mathcal{P}_1(z) = 2i\mathcal{P}((1+i)z) = \frac{1}{4}\frac{4\mathcal{P}(z)^2 - \frac{1}{4}}{\mathcal{P}(z)}.$$

Thus, if $\mathcal{P}_1(\alpha)$ is constructible so is $\mathcal{P}(\alpha)$. This completes the proof.

In Section 2 we showed that the lemniscate can be divided into n equal parts with ruler and compass if and only if the numbers $\{\phi(k2\omega/n) | k = 1,2,\ldots,n-1\}$ are constructible. In the light of Proposition 1 we are reduced to the question of finding those integers n such that the numbers $\{\mathcal{P}(k2\omega/n) | k = 1,2,\ldots,n-1\}$ are constructible.

5. Recall that E represents the complex points on the elliptic curve $y^2 = 4x^3 - \frac{1}{4}x$ together with the point at infinity. By means of $\xi(z) = (\mathcal{P}(z), \mathcal{P}'(z))$ we have an isomorphism between $\mathbb{C}/L$ and E. We now argue with E the way we did with C in our "elaborate" proof of Gauss's theorem. Since E_n is finite, we see by the same reasoning that we applied to C_n in Section 1 that the coordinates of the points in E_n are algebraic over $\mathbb{Q}$. Adjoin these coordinates to $\mathbb{Q}$ and call the resulting field K_n. Then $K_n/\mathbb{Q}$ is Galois. Let G_n denote its Galois group. G_n acts on E_n and gives rise to a monomorphism from G_n into

$$\mathrm{Aut}(E_n) \approx \mathrm{Aut}(L/nL) \approx \mathrm{Aut}(Z/nZ \oplus Z/nZ) \approx \mathrm{Gl}_2(Z/nZ).$$

At this point we do not know much about the image of G_n. Moreover, the order of $\mathrm{Gl}_2(Z/nZ)$ is never a power of two. We seem to have reached a dead end.

The situation is saved by the realization that there is some additional structure which has not been used, namely, $L = \langle 2\omega, 2\omega i\rangle = Z[i](2\omega)$; i.e., L is a $Z[i]$ module of rank one, not just an abelian group. In general, a lattice Λ is said to admit complex multiplication if the ring $\{\alpha \in \mathbb{C} | \alpha L \subseteq L\}$ is properly bigger than Z.

Since L is a $Z[i]$ module, so is $\mathbb{C}/L$ and via ξ we can make E into a $Z[i]$ module. Since, as we have seen, $\mathcal{P}(iz) = -\mathcal{P}(z)$ and $\mathcal{P}'(iz) = i\mathcal{P}'(z)$, the action of i on E is given by $i(x,y) = (-x,iy)$.

LEMMA 2. *$E_n \approx Z[i]/nZ[i]$ as $Z[i]$ modules.*

Proof. $E_n \approx \frac{1}{n}L/L \approx L/nL \approx Z[i]/nZ[i]$.

Let $F = \mathbb{Q}(i)$ and adjoin the coordinates of E_n to F. Call the resulting field F_n and let $\mathcal{G}_n$ be its Galois Group over F. Since $\mathcal{G}_n$ leaves i fixed, the action of $\mathcal{G}_n$ on E_n preserves the $Z[i]$ module structure. Thus we get a monomorphism from $\mathcal{G}_n$ into the $Z[i]$ automorphisms of E_n. Now, by Lemma 2

$$\mathrm{Aut}_{Z[i]}(E_n) \approx \mathrm{Aut}_{Z[i]}(Z[i]/nZ[i]) \approx (Z[i]/nZ[i])^*.$$

We have shown

PROPOSITION 2. *The group $\mathcal{G}_n$ is abelian. If $(Z[i]/nZ[i])^*$ is a two-group, then the numbers $\mathcal{P}((2a\omega + 2bi\omega)/n)$ and $\mathcal{P}'(2a\omega + 2bi\omega)/n)$ are constructible.*

Abel's Theorem now follows from the following easily proved Lemma.

LEMMA 3. *$(Z[i]/nZ[i])^*$ is a two-group if and only if n is a power of 2 times a product of distinct Fermat primes.*

We now turn to the proof of the converse to Abel's theorem.

LEMMA 4. *Let M be the field generated over $F = \mathbb{Q}(i)$ by adjoining $\mathcal{P}(2\omega/n)^2$. Then M/F is Galois and the Galois group is isomorphic to $(Z[i]/nZ[i])^*$ modulo the image of the group $\{\pm 1, \pm i\}$.*

Proof. Let $L_0 = Z[i]$ be considered as a lattice in $\mathbb{C}$, and $\mathcal{P}_0(z)$ the corresponding $\mathcal{P}$ function. Let $h(z) = g_2(L_0)^{-1}\mathcal{P}_0(z)^2$. It follows from the arithmetic copy of complex multiplication that $F(h(1/n))$ is the ray class field of F corresponding to the modulus n (see page 135 of [5]). The ray class group of modulus n is precisely the group described in the statement of the lemma. We will show $h(1/n) = 4\mathcal{P}(2\omega/n)^2$ and that will complete the proof.

From the definition of $\mathcal{P}$ and $\mathcal{P}_0$ we see easily that $\mathcal{P}(2\omega z) = (2\omega)^{-2}\mathcal{P}_0(z)$. In the appendix we will show $\Sigma'\gamma^{-4} = \omega^4/15$ where the sum is over all nonzero elements of $Z[i]$. Thus $g_2(L_0) = 60\Sigma'\gamma^{-4} = 4\omega^4$. It follows that $h(z) = (4\omega^4)^{-1}(2\omega)^4\mathcal{P}(2\omega z)^2 = 4\mathcal{P}(2\omega z)^2$.

THEOREM 2. *If the lemniscate can be divided into n equal parts with ruler and compass, then n is a power of two times a product of distinct Fermat primes.*

Proof. If the hypothesis holds then $\phi(2\omega/n)$ is a constructible number. By Proposition 1, $\mathcal{P}(2\omega/n)$ is constructible. It then follows from Lemma 4 that $(Z[i]/nZ[i])^*$ is a two-group. The result is now a consequence of the "only if" part of Lemma 3.

Appendix. In Section 3 we asserted that the pair of functions $\mathcal{P}$ and $\mathcal{P}'$ corresponding to the lattice $L = \langle 2\omega, 2\omega i\rangle$ parametrize the elliptic curve $y^2 = 4x^3 - \frac{1}{4}x$. To prove this we proceed as follows.

As we have seen, $\mathcal{P}$ and $\mathcal{P}'$ parametrize $y^2 = 4x^3 - g_2(L)x - g_3(L)$ where

$$g_2(L) = 60\sum{}'\gamma^{-4} \quad \text{and} \quad g_3(L) = 140\sum{}'\gamma^{-6}.$$

Since $iL = L$ and $i^6 = -1$ we see $g_3(L) = 0$. To show $g_2(L) = \frac{1}{4}$ it is equivalent to show

PROPOSITION 3. $\Sigma(r + si)^{-4} = \omega^2/15$ *where the sum is over all nonzero Gaussian integers.*

This result was obtained by Hurwitz in [4]. In fact, he shows that, more generally, $\Sigma(r + si)^{-4n} = ((2\omega)^{4n}/(4n)!)E_n$ where the E_n are positive rational numbers. Hurwitz shows that these rational numbers have many properties analogous to the Bernoulli numbers, including an analogue of the von Staudt–Clausen theorem. Nowadays these numbers E_n are called Hurwitz numbers in his honor. It is worth noting that Gauss, in the 61st entry in his mathematical diary (see pages 515 and 516 of [3]), states a result which is equivalent to the assertion that the E_n are rational.

Hurwitz's proof of the rationality of the E_n is quite easy. However, we prefer to give another proof which has the flavor of Euler's proof that $\Sigma n^{-2} = \pi^2/6$ and which depends only on the product formula for $\phi(z)$.

For a lattice L in $\mathbb{C}$ let $|L| = \Sigma'\gamma^{-4}$, the sum being over $L - \{0\}$. Consider the three lattices $L_0 = \langle\omega, \omega i\rangle$, $L_1 = \{(m + ni/2)\omega \mid m \text{ and } n \text{ odd}\}$ and $L_2 = \{(m + ni/2)\omega \mid m \text{ and } n \text{ of opposite parity}\}$. Then $\frac{1}{2}L_0 = L_1 \cup L_2 \cup L_0$ where the union is disjoint. Clearly $|\frac{1}{2}L_0| = 16|L_0|$. It is easily checked that $(1 + i/2)L_1 = L_2$ and it follows that $|L_2| = (2/(1 + i))^4|L_1| = -4|L_1|$. Putting all this together we have $|L_1| = -5|L_0|$.

As shown by Gauss and Abel

$$\phi(z) = z\prod_{\alpha}\left(1 - \frac{z^4}{\alpha^4}\right)\prod_{\beta}\left(1 - \frac{z^4}{\beta^4}\right)^{-1}$$

where $\alpha \in L_0$, $\beta \in L_1$, and $0 \leqslant \arg\alpha, \arg\beta < \pi/2$. Taking the logarithmic derivative of both

sides yields

$$z\frac{\phi'(z)}{\phi(z)} = 1 + (|L_1| - |L_0|)z^4 + \cdots.$$

We have to evaluate the left-hand side in a different way. From $z = \int_0^{\phi(z)} dt/\sqrt{1-t^4}$ we find $\phi'(z)^2 = 1 - \phi(z)^4$. Let $\phi(z) = z + cz^5 + \cdots$ be the power series expansion of $\phi(z)$ about $z = 0$. Substituting in $\phi'(z)^2 = 1 - \phi(z)^4$ and comparing coefficients of z^4 we find $c = -\frac{1}{10}$. From this we derive $z(\phi'(z)/\phi(z) = 1 - \frac{2}{5}z^4 + \cdots$.

Thus $|L_1| - |L_0| = -\frac{2}{5}$. Since also $|L_1| = -5|L_0|$, it follows that $|L_0| = \frac{1}{15}$; i.e.,

$$\sum (r + si)^{-4} = \frac{\omega^4}{15}.$$

From Proposition 3 we see that the first Hurwitz number E_1 is equal to $\frac{1}{10}$. It is now relatively simple to show that E_n is rational for all $n \geqslant 1$. For this purpose we sketch the proof of a more general proposition.

For a lattice Λ define $s_m(\Lambda) = \Sigma' \lambda^{-m}$, where $m > 2$ is an integer and the sum is over all $\lambda \in \Lambda, \lambda \neq 0$. These sums are convergent. Since $\Lambda = -\Lambda$, it follows that $s_m(\Lambda) = 0$ for m odd.

Let $\mathcal{P}(z)$ be the $\mathcal{P}$ function corresponding to the lattice Λ and $\mathcal{P}(z) = 1/z^2 + \Sigma_{n=1}^{\infty} b_n z^{2n}$ the Laurent series of $\mathcal{P}(z)$ about $z = 0$. From the definition one can calculate that $b_n = (2n+1)s_{2n+2}(\Lambda)$. See page 10 of [5] for details.

PROPOSITION 4. *Let* $\mathcal{O} = \{\gamma \in \mathbb{C} | \gamma\Lambda \subseteq \Lambda\}$ *and suppose* $\Lambda = \mathcal{O}\omega$ *for some* $\omega \in \mathbb{C}$. *Suppose further that* $s_4(\Lambda)$ *and* $s_6(\Lambda)$ *are in* $\mathbb{Q}$. *Then* $s_m(\Lambda) \in \mathbb{Q}$ *for all* $m \geqslant 4$ *and*

$$\sum_{\gamma \in \mathcal{O}}{}' \gamma^{-2n} = s_{2n}(\Lambda)\omega^{2n}.$$

Proof. Differentiating the fundamental relation $\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2(\Lambda)\mathcal{P}(z) - g_3(\Lambda)$ we find $\mathcal{P}''(z) = 6\mathcal{P}(z)^2 - \frac{1}{2}g_2(\Lambda)$. Equating coefficients leads to the following recursion formula for b_n,

$$(2n+3)(n-2)b_n = 3\sum_{k=1}^{n-2} b_k b_{n-k-1}.$$

This in turn shows that

$$s_{2n+2}(\Lambda) = \sum_{k=1}^{n-2} \gamma_{n,k} s_{2k+2}(\Lambda) s_{2n-2k}(\Lambda)$$

where $\gamma_{n,k} \in \mathbb{Q}$. Thus, if $s_4(\Lambda)$ and $s_6(\Lambda)$ are in $\mathbb{Q}$ it follows by induction that $s_m(\Lambda) \in \mathbb{Q}$ for all $m \geqslant 4$. Since every element of Λ is uniquely of the form $\gamma\omega$ with $\gamma \in \mathcal{O}$, the proposition follows immediately.

For our lattice $L = \langle 2\omega, 2\omega i \rangle$ we have $\mathcal{O} = Z[i]$, $s_4(L) = \frac{1}{15}$ (by Proposition 3), and $s_6(L) = 0$. The rationality of E_n for all $n \geqslant 1$ follows from Proposition 4.

References

1. N. H. Abel, Oeuvres Complètes, Nouvelle Edition, Oslo, 1881.
2. C. F. Gauss, Disquisitiones Arithmeticae, transl. by Arthur A. Clarke, Yale University Press, New Haven, 1966.
3. _____, Carl Friedrich Gauss Werke, vol. 10, Royal Scientific Society of Göttingen, 1917.
4. A. Hurwitz, Über die Entwicklungskoeffizienten der lemniscatischen Funktionen, Mathematische Werke, vol. 2, pp. 342–373, Birkhäuser Verlag, Basel und Stuttgart, 1962.
5. S. Lang, Elliptic Functions, Addison-Wesley, Reading, Mass., 1973.
6. O. Ore, Niels Henrik Abel, Mathematician Extraordinary, University of Minnesota Press, Minneapolis, 1957.
7. A. Robert, Elliptic Curves, Springer Lecture Notes 326, Springer-Verlag, New York, 1973.
8. C. L. Siegel, Topics in Complex Function Theory, vol. 1, Wiley-Interscience, New York, 1969.