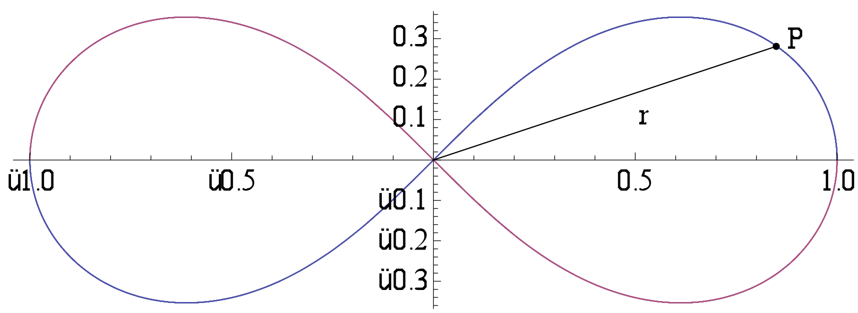
Scott Binski
Senior Capstone
Dr. Hagedorn
Fall 2008

Constructions on the Lemniscate

The Lemniscatic Function and Abel's Theorem

I. History of the Lemniscate

The lemniscate is a curve in the plane defined by the equation $(x^2 + y^2)^2 = x^2 - y^2$. Its graphical representation is the following (values r and points P will be important later):



The lemniscate is of particular interest because, even if it has little relevance today, it was the catalyst for immeasurably important mathematical development in the 18th and 19th centuries. The figure 8-shaped curve first entered the minds of mathematicians in 1680, when Giovanni Cassini presented his work on curves of the form $((x-a)^2 + y^2)((x+a)^2 + y^2) = b^4$, appropriately known as the ovals of Cassini (Cox 463). Only 14 years later, while deriving the arc length of the lemniscate, Jacob Bernoulli became the first mathematician in history to define arc length in terms of polar coordinates (Cox 464).

The first major result of work on the lemniscate came in 1753, when, after reading Giulio Carlo di Fagnano's papers on dividing the lemniscate using straightedge and compass, Leonhard Euler proved that

$$\int_0^\alpha \frac{1}{\sqrt{1-t^4}}dt + \int_0^\beta \frac{1}{\sqrt{1-t^4}}dt = \int_0^\gamma \frac{1}{\sqrt{1-t^4}}dt$$

where $\alpha, \beta \in [0,1]$, $\gamma = \frac{\alpha\sqrt{1-\beta^4}+\beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2} \in [0,1]$. This identity was essential to the theory of elliptic integrals (Cox 473).

Amazingly, Ferdinard Eisenstein's criterion for irreducibilty is also a product of work on the lemniscate. Because he asserts his criterion for both $\mathbb{Z}$ and $\mathbb{Z}[i]$, it is believed that he derived it while researching complex multiplication on the lemniscate (Cox 497).

II. Arc Length of the Lemniscate

If the origin is our starting point, movement about the lemniscate begins in the first quadrant and proceeds into the fourth quadrant. After arriving back at the origin, movement then continues into the second quadrant and finally into the third quadrant.

It will be useful to consider the equation of the lemniscate in terms of polar coordinates, i.e. $x = r\cos\theta$ and $y = r\sin\theta$. We immediately obtain the equation $r^4 = \mathrm{r}^2(\cos^2\theta - \sin^2\theta)$. This is easily simplified to obtain $r^2 = \cos 2\theta$. This polar representation of the lemniscate affords us a simple calculation of arc length, which is essential to the lemniscatic function. The arc length formula in polar coordinates is

$$arc\ length = \int_0^P \sqrt{dr^2 + r^2 d\theta^2} = \int_0^r \sqrt{1 + r^2\left(\frac{d\theta}{dr}\right)^2}\, dr.$$

Now by differentiating our equation $r^2 = \cos 2\theta$, we see that $2r = -\sin 2\theta * \frac{2d\theta}{dr}$, which gives $\frac{d\theta}{dr} = -\frac{r}{\sin 2\theta}$. Thus,

$$1 + r^2\left(\frac{d\theta}{dr}\right)^2 = 1 + r^2\left(-\frac{r}{\sin 2\theta}\right)^2 = 1 + \frac{r^4}{\sin^2 2\theta}.$$

Noting that $\sin^2 2\theta = 1 - \cos^2 2\theta = 1 - r^4$, it follows that

$$1 + r^2\left(\frac{d\theta}{dr}\right)^2 = 1 + \frac{r^4}{1 - r^4} = \frac{1}{1 - r^4}.$$

Now our expression becomes

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

We let ϖ, a variant of π, denote the arc length of one loop of the lemniscate. This designation is appropriate because the circumference of the circle is 2π and the circumference of the lemniscate is 2ϖ. Since we obtain the arc length of the first quadrant portion of the curve when $r = 1$ in the integral above, we see that

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

This integral is improper (since the denominator is 0 for $r = 1$), but it does converge and has a numerical value of approximately 2.62206.

III. Defining the Lemniscatic Function

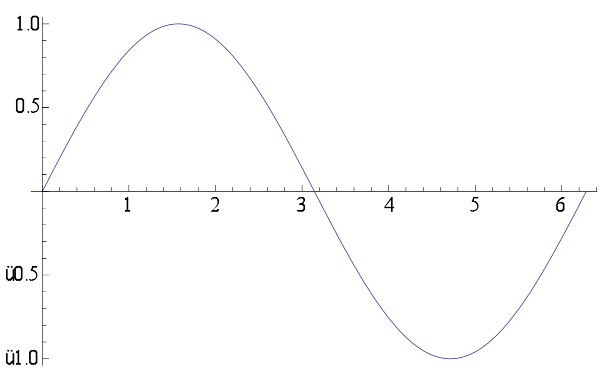
The lemniscate may appear peculiar at first glance, but many parallels exist between it and the sine function. For example, we may define the sine function as the inverse function of an integral in the following way:

$$y = \sin s \Leftrightarrow s = \sin^{-1} y = \int_0^y \frac{1}{\sqrt{1-t^2}}\,dt.$$

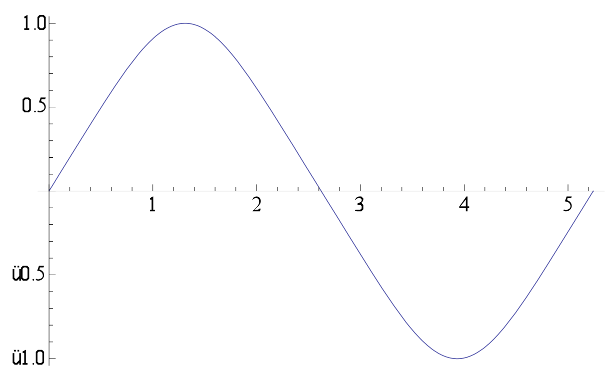
The lemniscatic function $r = \varphi(s)$ may also be defined as the inverse function of an integral (with obvious similarity):

$$r = \varphi(s) \Leftrightarrow s = \int_0^r \frac{1}{\sqrt{1-t^4}}\,dt.$$

The input values of this function, like the sine function, are arc lengths. Now recalling movement about the lemniscate, we may define our function $r = \varphi(s)$ for all real numbers. To do so, we let $r = \varphi(s)$ be the signed polar distance (from the origin) of the point corresponding to the arc length s. By signed polar distance, we simply mean that $r = \varphi(s)$ is a positive value in the first and fourth quadrants, while it is a negative value in the second and third quadrants. Defining our function in such a way yields a graph that is nearly indistinguishable from the familiar graph of the sine function. They are presented here for comparison:



$\sin s$



$\varphi(s)$

IV. Basic Properties of $\varphi(s)$

The sine function satisfies several interesting identities:

Proposition A: If $f(x) = \sin x$, then:

1) $f(x + 2\pi) = f(x)$
2) $f(-x) = -f(x)$
3) $f(\pi - x) = f(x)$
4) $f'^2(x) = 1 - f^2(x)$

The lemniscatic function $\varphi(s)$ satisfies similar identities. In fact, we may regard the lemniscatic function as a generalization of the sine function for a different curve (noting that the output values of $\varphi(s)$ are radii, while the output values of $\sin x$ are y-coordinates). Of course, the sine function is only relevant with respect to the unit circle, whereas $\varphi(s)$ pertains to the lemniscate. We see that the following is true of the lemniscatic function:

Proposition B: If $f(s) = \varphi(s)$, then:

1) $f(s + 2\varpi) = f(s)$
2) $f(-s) = -f(s)$
3) $f(\varpi - s) = f(s)$
4) $f'^2(s) = 1 - f^4(s)$

The first three of these identities are not difficult to observe. Since the total arc length of the lemniscate is 2ϖ, it is clear that $\varphi(s)$ has period equal to 2ϖ. So $\varphi(s + 2\varpi) = \varphi(s)$. It is readily deduced from the graphical representation of the lemniscate that arc length values s and $-s$ correspond to points that are symmetric about the origin. Thus we see that $\varphi(-s) = -\varphi(s)$. It is also clear that s and $\varpi - s$ correspond to points that are symmetric about the x-axis. Thus $\varphi(\varpi - s) = \varphi(s)$.

The last part of Proposition A is simply a restatement of the familiar identity $\cos^2 x = 1 - \sin^2 x$, where $\cos x$ is, of course, the derivative of $\sin x$. Now although the similarity between this identity and the corresponding identity for the lemniscatic function is clear, this is the least intuitive identity of $\varphi(s)$. We now prove:

Proposition: $\varphi'^2(s) = 1 - \varphi^4(s)$

Proof: Since $\varphi'(s)$ is periodic, it is clear that the identity need only be proved for $-\varpi \leq s \leq \varpi$. Furthermore, since $\varphi'(s) = \varphi'(-s)$ and $\varphi'(s + \varpi) = -\varphi'(s)$, we must only show that

$$\varphi'(s) = \sqrt{1 - \varphi^4(s)}, \quad 0 \leq s \leq \frac{\varpi}{2}.$$

To do so, we differentiate both sides of the arc length integral with respect to s, yielding

$$1 = \frac{1}{\sqrt{1-\varphi^4(s)}}\varphi'(s), \quad 0 \le s < \frac{\varpi}{2}.$$

Thus we easily obtain the desired relation for $0 \le s < \frac{\varpi}{2}$. And since both sides of the above equation are continuous functions on the interval $[0, \frac{\varpi}{2}]$, it follows that the equation also holds for $s = \frac{\varpi}{2}$. This completes the proof. ■

V. The Addition Law for $\varphi(s)$

The sine function satisfies the addition law $\sin(x+y) = \sin x \cos y + \cos x \sin y$. So if we say $f(x) = \sin\,(x)$, then $f(x+y) = f(x)f'(y) + f'(x)f(y)$. We will derive a similar result for $\varphi(s)$, beginning with the following identity:

$$\int_0^\alpha \frac{1}{\sqrt{1-t^4}}dt + \int_0^\beta \frac{1}{\sqrt{1-t^4}}dt = \int_0^\gamma \frac{1}{\sqrt{1-t^4}}dt$$

where $\alpha, \beta \in [0,1]$ and $\gamma = \frac{\alpha\sqrt{1-\beta^4}+\beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2} \in [0,1]$.

By letting $x, y,$ and z equal the three integrals above, respectively, and applying the φ function to both sides of the equation, we obtain

$$\varphi(x+y) = \varphi(z) = \gamma = \frac{\alpha\sqrt{1-\beta^4}+\beta\sqrt{1-\alpha^4}}{1+\alpha^2\beta^2}, \quad 0 \le x+y \le \frac{\varpi}{2}.$$

Now since $\varphi(x) = \alpha$ and $\varphi(y) = \beta$, we have

$$\varphi(x+y) = \frac{\varphi(x)\sqrt{1-\varphi^4(y)}+\varphi(y)\sqrt{1-\varphi^4(x)}}{1+\varphi^2(x)\varphi^2(y)}, \quad 0 \le x+y \le \frac{\varpi}{2}.$$

And the last of our basic φ properties implies that $\sqrt{1-\varphi^4(x)} = \varphi'(x)$, yielding

$$\varphi(x+y) = \frac{\varphi(x)\varphi'(y)+\varphi(y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(y)}, \quad 0 \le x+y \le \frac{\varpi}{2}.$$

Now since both sides of this equation are analytic functions of x that are defined for all values x when y is any fixed value, the equation holds true for all values x and y. Thus we have a simply stated addition law for the lemniscatic function φ that bears an obvious resemblance to the familiar sine function addition law (the latter bears no denominator). The subtraction law for $\varphi(s)$ is easily derived from the addition law. Since $\varphi(-x) = -\varphi(x)$ and $\varphi'(-x) = \varphi'(x)$ (note that the latter is a direct consequence of the former),

$$\varphi(x-y) = \frac{\varphi(x)\varphi'(y) - \varphi(y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(y)}.$$

It is an easy consequence of the addition law that $\varphi(2x) = \frac{2\varphi(x)\varphi'(x)}{1+\varphi^4(x)}$. Although it is slightly more difficult, we can also obtain the tripling formula $\varphi(3x)$ using nothing more than the addition law and the subtraction law. To begin, it is clear that

$$\varphi(x+y) + \varphi(x-y) = \frac{2\varphi(x)\varphi'(y)}{1+\varphi^2(x)\varphi^2(y)}.$$

Then by replacing x and y with $2x$ and x, respectively, we have

$$\varphi(3x) + \varphi(x) = \varphi(2x+x) + \varphi(2x-x) = \frac{2\varphi(2x)\varphi'(x)}{1+\varphi^2(2x)\varphi^2(x)}.$$

Now using the doubling formula $\varphi(2x) = \frac{2\varphi(x)\varphi'(x)}{1+\varphi^4(x)}$, we obtain

$$\varphi(3x) + \varphi(x) = \frac{2\frac{2\varphi(x)\varphi'(x)}{1+\varphi^4(x)}\varphi'(x)}{1+\left(\frac{2\varphi(x)\varphi'(x)}{1+\varphi^4(x)}\right)^2\varphi^2(x)}.$$

And finally, since $\varphi'^2(x) = 1 - \varphi^4(x)$, we have our result:

$$\varphi(3x) = \varphi(x)\frac{3-6\varphi^4(x)-\varphi^8(x)}{1+6\varphi^4(x)-3\varphi^8(x)}.$$

VI. A Theorem for Multiplication by Integers

We have already seen formulas for $\varphi(2x)$ and $\varphi(3x)$. In fact, formulas of the form $\varphi(nx)$ may be generalized for all positive integers n by the following theorem:

Theorem A: *Given an integer $n > 0$, there exist relatively prime polynomials$P_n(u), Q_n(u) \in \mathbb{Z}[u]$ such that if n is odd, then*

$$\varphi(nx) = \varphi(x)\frac{P_n(\varphi^4(x))}{Q_n(\varphi^4(x))}$$

and if n is even, then

$$\varphi(nx) = \varphi(x)\frac{P_n\big(\varphi^4(x)\big)}{Q_n\big(\varphi^4(x)\big)}\varphi'(x).$$

Furthermore, $Q_n(0) = 1$.

Proof: For the case $n = 1$, it is clear that $P_1(u) = Q_1(u) = 1$. And for the case $n = 2$, we know from the beginning of this section that $\varphi(2x) = \varphi(x)\frac{2}{1+\varphi^4(x)}\varphi'(x)$. Thus $P_2(u) = 2$ and $Q_2(u) = 1 + u$. Now that we have established these cases, we can prove the theorem by induction on n. Let us assume that the theorem holds for $n - 1$ and n. Implementing the addition and subtraction laws, we see that

$$\varphi\big((n+1)x\big) = -\varphi\big((n-1)x\big) + \frac{2\varphi(nx)\varphi'(x)}{1 + \varphi^2(nx)\varphi^2(x)}.$$

Now if n is even and $n - 1$ is odd,

$$\varphi\big((n+1)x\big) = -\left(\varphi(x)\frac{P_{n-1}\big(\varphi^4(x)\big)}{Q_{n-1}\big(\varphi^4(x)\big)}\right) + \frac{2\left(\varphi(x)\frac{P_n\big(\varphi^4(x)\big)}{Q_n\big(\varphi^4(x)\big)}\varphi'(x)\right)\varphi'(x)}{1 + \left(\varphi(x)\frac{P_n\big(\varphi^4(x)\big)}{Q_n\big(\varphi^4(x)\big)}\varphi'(x)\right)^2\varphi^2(x)}.$$

Then since $\varphi'^2(x) = 1 - \varphi^4(x)$, we have

$$\varphi\big((n+1)x\big) = \varphi(x)\frac{P_{n+1}\big(\varphi^4(x)\big)}{Q_{n+1}\big(\varphi^4(x)\big)},$$

where $Q_{n+1}(u) = Q_{n-1}(u)\big(Q_n^2(u) + uP_n^2(u)(1-u)\big)$ and
$P_{n+1}(u) = -Q_n^2(u)P_{n-1}(u) + P_n(u)(1-u)\big(2Q_n(u)Q_{n-1}(u) - uP_n(u)P_{n-1}(u)\big).$

Thus $P_{n+1}(u), Q_{n+1}(u) \in \mathbb{Z}[u]$.

Now if n is odd and $n-1$ is even,

$$\varphi\big((n+1)x\big) = -\left(\varphi(x)\frac{P_{n-1}\big(\varphi^4(x)\big)}{Q_{n-1}\big(\varphi^4(x)\big)}\varphi'(x)\right) + \frac{2\left(\varphi(x)\frac{P_n\big(\varphi^4(x)\big)}{Q_n\big(\varphi^4(x)\big)}\right)\varphi'(x)}{1+\left(\varphi(x)\frac{P_n\big(\varphi^4(x)\big)}{Q_n\big(\varphi^4(x)\big)}\right)^2\varphi^2(x)}.$$

Then we have

$$\varphi\big((n+1)x\big) = \varphi(x)\frac{P_{n+1}\big(\varphi^4(x)\big)}{Q_{n+1}\big(\varphi^4(x)\big)}\varphi'(x),$$

where $Q_{n+1}(u) = Q_{n-1}(u)\big(Q_n^2(u) + uP_n^2(u)\big)$ and
$P_{n+1}(u) = -Q_n^2(u)P_{n-1}(u) + P_n(u)\big(2Q_n(u)Q_{n-1}(u) - uP_n(u)P_{n-1}(u)\big)$.

Thus $P_{n+1}(u), Q_{n+1}(u) \in \mathbb{Z}[u]$. ■

Now we will illustrate these recursive formulas by deriving the case $n = 3$. We obtain the following polynomials:

$$Q_3(u) = Q_1(u)\big(Q_2^2(u) + uP_2^2(u)(1-u)\big) = 1 + 6u - 3u^2$$
$$P_3(u) = -Q_2^2(u)P_1(u) + P_2(u)(1-u)\big(2Q_2(u)Q_1(u) - uP_2(u)P_1(u)\big) = 3 - 6u - u^2.$$

So again we see that

$$\varphi(3x) = \varphi(x)\frac{3 - 6\varphi^4(x) - \varphi^8(x)}{1 + 6\varphi^4(x) - 3\varphi^8(x)}.$$

VII. Constructions on the Lemniscate

Now that we have an understanding of the lemniscatic function and its properties, we may explore constructions on the lemniscate, beginning with the following basic theorem:

Theorem B: *The point on the lemniscate corresponding to arc length s can be constructed by straightedge and compass if and only if $r = \varphi(s)$ is a constructible number.*

Proof: Noting that the lemniscate is defined by the equation $(x^2 + y^2)^2 = x^2 - y^2$ and that $r^2 = x^2 + y^2$, we see that $r^4 = x^2 - y^2$. Then by solving in terms of r, we see that:

$$x = \pm\sqrt{\frac{1}{2}(r^2 + r^4)}; \quad y = \pm\sqrt{\frac{1}{2}(r^2 - r^4)}.$$

Now since the constructible numbers are closed under square roots, x and y are constructible if $r = \varphi(s)$ is constructible. For the same reason, $r = \sqrt{x^2 + y^2}$ is constructible if x and y are constructible. ■

Example: Consider the arc length $s = \frac{\varpi}{3}$, which is one sixth of the entire arc length of the lemniscate. We see that $\varphi(3s) = \varphi(\varpi) = 0$, since the arc length ϖ corresponds to the origin. Recalling the tripling formula, this implies that

$$\varphi^8(s) + 6\varphi^4(s) - 3 = 0.$$

And using the quadratic formula (with $x = \varphi^4(s)$), this has the constructible solution

$$\varphi(s) = \sqrt[4]{2\sqrt{3} - 3}$$

VIII. Abel's Theorem

Niels Abel's theorem for constructions on the lemniscate is identical to the following theorem of Gauss for constructions on the circle:

Theorem (Gauss): *Let $n > 2$ be an integer. Then a regular n-gon can be constructed by straightedge and compass if and only if*

$$n = 2^s p_1 \cdots p_r,$$

where $s \geq 0$ is an integer and $p_1, \dots, p_r$ are $r \geq 0$ distinct Fermat primes.

Of course, the vertices of a regular n-gon correspond to the n-division points $\left(m\frac{2\pi}{n}, m = 0,1, \dots, n-1\right)$ of the circle. In the context of this theorem, Abel's theorem for the lemniscate should appear natural:

Theorem (Abel): *Let n be a positive integer. Then the following are equivalent:*

a) *The n-division points of the lemniscate can be constructed using straightedge and compass.*
b) *$\varphi\left(\frac{2\varpi}{n}\right)$ is constructible.*

c) *n is an integer of the form*

$$n = 2^s p_1 \cdots p_r,$$

where $s \geq 0$ is an integer and $p_1, \dots, p_r$ are $r \geq 0$ distinct Fermat primes.

That statement a) implies statement b) is an immediate result of Theorem B, since $\frac{2\varpi}{n}$ is, of course, an n-division point of the lemniscate. The proof that statement c) implies statement a) implements several elements of number theory, as well as the following remarkable result of Galois theory:

Theorem C: *If $L = \mathbb{Q}\left(i, \varphi\left(\frac{\varpi}{n}\right)\right)$ and n is an odd positive integer, then $\mathbb{Q}(i) \subset L$ is a Galois extension and there is an injective group homomorphism*

$$Gal\left(\frac{L}{\mathbb{Q}(i)}\right) \to \left(\frac{\mathbb{Z}[i]}{n\mathbb{Z}[i]}\right)^*$$

and $Gal\left(\frac{L}{\mathbb{Q}(i)}\right)$ is Abelian.

It is interesting to note that this is an analog of the following theorem for cyclotomic extensions:

Theorem D: *If $\zeta_n = e^{2\pi i/n}$, then*

$$Gal\left(\frac{\mathbb{Q}(\zeta_n)}{\mathbb{Q}}\right) \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

and $Gal\left(\frac{\mathbb{Q}(\zeta_n)}{\mathbb{Q}}\right)$ is Abelian.

We now verify a crucial component of the proof that statement c) implies statement a):

Proposition: *If $p = 2^{2^m} + 1$ is a Fermat prime, then*

$$\left|\left(\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]}\right)^*\right| = a\ power\ of\ 2.$$

Proof: If $m \geq 1$, then

$$p = 2^{2^m} + 1 = \left(2^{2^{m-1}} + i\right)\left(2^{2^{m-1}} - i\right) = \pi\bar{\pi},$$

where π and $\bar{\pi}$ are prime conjugates in $\mathbb{Z}[i]$. Now by the Chinese Remainder Theorem,

$$\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]} = \frac{\mathbb{Z}[i]}{\pi\bar{\pi}\mathbb{Z}[i]} \simeq \frac{\mathbb{Z}[i]}{\pi\mathbb{Z}[i]} \times \frac{\mathbb{Z}[i]}{\bar{\pi}\mathbb{Z}[i]}.$$

Now since $N(p) = N(\pi\bar{\pi}) = N(\pi)N(\bar{\pi}) = p^2$ and $N(\pi) = N(\bar{\pi})$, we have

$$\frac{\mathbb{Z}[i]}{\pi\mathbb{Z}[i]} \times \frac{\mathbb{Z}[i]}{\bar{\pi}\mathbb{Z}[i]} \simeq \mathbb{F}_p \times \mathbb{F}_p.$$

Thus we see that

$$\left|\left(\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]}\right)^*\right| = \left|\mathbb{F}_p^* \times \mathbb{F}_p^*\right| = (p-1)^2 = 2^{2^{m+1}}.$$

Now it only remains to be seen that the proposition holds for $m = 0$, or, equivalently, $p = 3$. Since $N(3) = 9$, we see that the distinct elements that compose $\left(\frac{\mathbb{Z}[i]}{3\mathbb{Z}[i]}\right)^*$ are those of the form $a + bi$, where $a, b > 0$ and $N(a + bi) < 9$. So $\left(\frac{\mathbb{Z}[i]}{3\mathbb{Z}[i]}\right)^* = \{1, 2, i, 2i, 1+i, 2+i, 1+2i, 2+2i\}$ and $\left|\left(\frac{\mathbb{Z}[i]}{3\mathbb{Z}[i]}\right)^*\right| = 8$. ■

Although we will not prove it, this proposition implies that $\varphi\left(\frac{2\varpi}{p}\right)$ is constructible.

References

Cox, David A. Galois Theory. Hoboken, NJ: John Wiley & Sons, 2004. pp. 457-508.