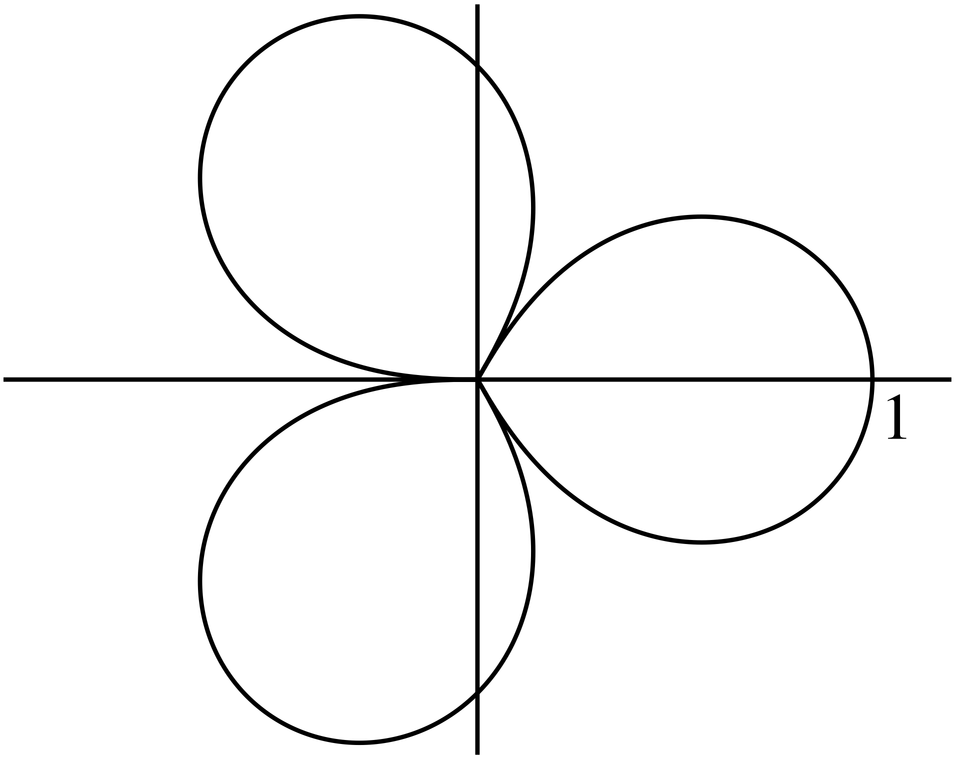
Geometry and Number Theory on Clovers

David A. Cox and Jerry Shurman



(Appeared in October 2005 **Monthly**.)

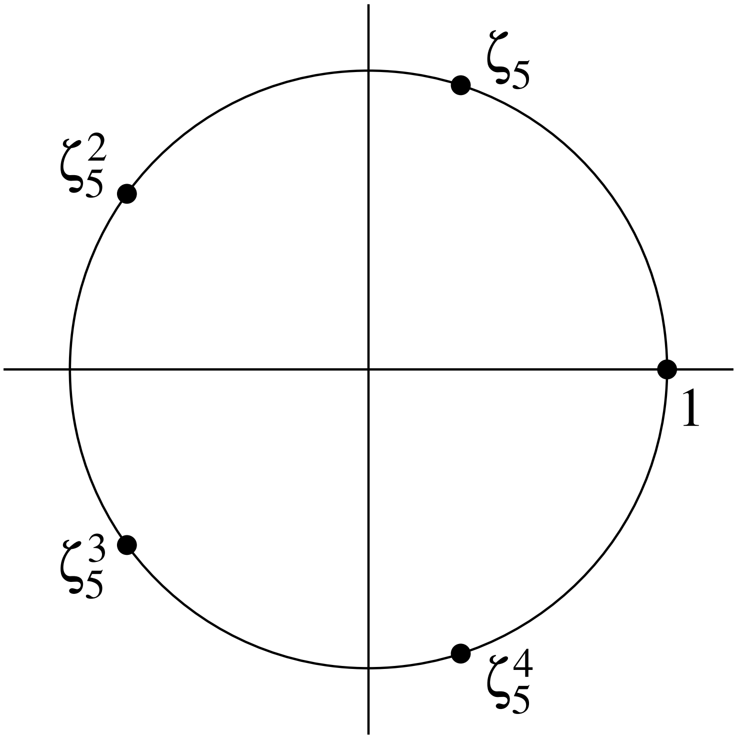
Gauss's Theorem (1797)

The circle is divisible into n arcs of equal length by a Euclidean construction if and only if

$$n = 2^a p_1 \cdots p_r$$

where $a \geq 0$ and $p_1, \ldots, p_r$ are distinct Fermat primes.

(Fermat prime: $p > 2$, $p = 2^u + 1$. Necessarily $u = 2^e$.)



- Euclidean constructions, and geometric constructions in general, go back to antiquity. They are not innately systematic.

- Gauss's theorem is novel in that it completely characterizes the capability of Euclidean constructions in one particular situation. Analogously to Descartes, Gauss translated a geometrical situation into an algebraic one, where it can be analyzed more systematically.

- Gauss's argument is the first proto-example of Galois theory.

The Field of Euclidean Numbers

Identify points of the plane with complex numbers. Then the Euclidean numbers form a subfield $\mathcal{E}$ of $\mathbf{C}$ characterized by the following properties.

1. Let $z = x + iy \in \mathbf{C}$. Then $z \in \mathcal{E}$ if and only if $x, y \in \mathcal{E}$.

2. Let $z \in \mathbf{C}$. Then $z \in \mathcal{E}$ if and only if there is a Galois extension $\mathbf{Q} \subset L \subset \mathbf{C}$ such that $z \in L$ and $[L : \mathbf{Q}] = 2^u$ for some $u \geq 0$.

(In particular, $\mathcal{E}$ is closed under linear and quadratic equations. The Euclidean numbers are the complex numbers derivable from $\mathbf{Q}$ by finitely many steps involving algebra and square roots.)

Arithmetic of $\mathbf{Z}$

Let p be prime in $\mathbf{Z}$. Then

$$|(\mathbf{Z}/p\mathbf{Z})^{\times}| = p - 1.$$

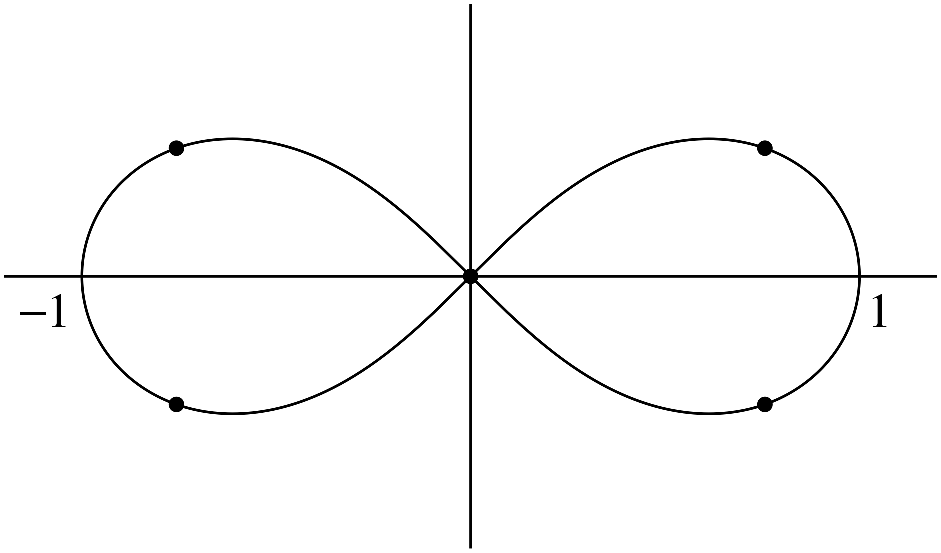
This is a power of 2 if and only if $p = 2$ or p is a Fermat prime.

More generally, the group $(\mathbf{Z}/n\mathbf{Z})^{\times}$ describes the automorphisms of the field $\mathbf{Q}(\zeta_n)$. Its order is a power of 2 if and only if n is a number in Gauss's Theorem. This is the gist of Gauss's argument.

Abel's Theorem (1826)

The lemniscate can be divided into n arcs of equal length by straightedge and compass for the same values of n as in Gauss's Theorem.

Note: we do not have the lemniscate itself.



$$(x^2 + y^2)^2 = x^2 - y^2$$

(This was also known earlier to Gauss.)

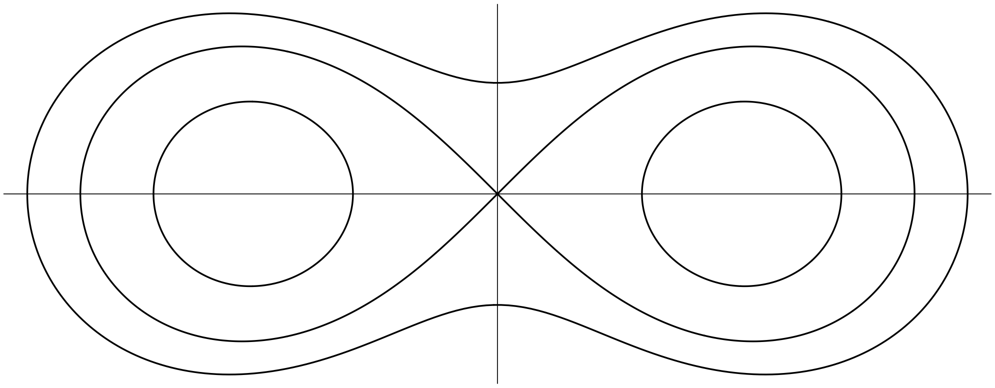
Geometric Origin of the Lemniscate

The lemniscate is a special case of the locus of points P satisfying the condition

$$|P-(-a,0)|\cdot|P-(a,0)|=b^2.$$

For the lemniscate, $a=b$.

The condition is the multiplicative analogue of the additive condition that defines an ellipse.



This goes back to the French astronomer Cassini (1680) and to the Bernoullis, independently of each other (1694).

Arc Length on the Lemniscate

The polar equation of the lemniscate is

$$r^2 = \cos(2\theta).$$

The general differential arc length formula in polar coordinates is

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

On the lemniscate this works out easily to

$$ds = \frac{dr}{\sqrt{1 - r^4}},$$

so the arc length of the lemniscate is the elliptic integral

$$s = \int_{t=0}^{r} \frac{dt}{\sqrt{1 - t^4}}.$$

(The integral is called *elliptic* because such integrals arose in trying to find the arc length of the ellipse.)

Here we derived the arc length of the lemniscate from the general formula for arc length in polar coordinates. In fact the general polar arc length formula was determined precisely in order to find the arc length of the lemniscate.

In modern calculus classes this connection is often lost: the polar arc length formula is given and used, the polar equation of the lemniscate is given, but the intriguing integral that expresses the lemniscate arc length, and the ease of this integral's derivation from the polar arc length formula are not, because the integral is not one that can not be worked by elementary techniques.

It is much more interesting.

Just as Gauss's argument can be viewed as the proto-example of Galois theory, Abel's argument — while long and elementary — can be viewed as the proto-example of complex multiplication and class field theory.

The proof of Abel's theorem makes use of the ring $\mathbf{Z}[i]$ of Gaussian integers. From a modern perspective, the argument uses objects analogous to those in Gauss's argument: the structure of the quotient ring

$$(\mathbf{Z}[i]/n\mathbf{Z}[i])^{\times},$$

and the realization of this quotient ring as the Galois group of a field extension $\mathbf{Q}(i) \subset L$. Here L is constructed from $\mathbf{Q}(i)$ by adjoining the x-coordinate of an n-division point of an elliptic curve.

Pierpont's Theorem (1896)

The circle can be divided into n arcs of equal length by origami if and only if

$$n = 2^a 3^b p_1 \cdots p_r$$

where $a, b \geq 0$ and $p_1, \ldots, p_r$ are distinct Pierpont primes.

(Pierpont prime: $p > 3$, $p = 2^u 3^v + 1$.)

According to Sequence A005109 of Sloane's On-Line Encyclopedia of Integer Sequences, the first forty Pierpont primes are

$$\begin{aligned}\mathcal{P} = \{&5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193,\\ &257, 433, 487, 577, 769, 1153, 1297, 1459\\ &2593, 2917, 3457, 3889, 10369, 12289,\\ &17497, 18433, 39367, 52489, 65537,\\ &139969, 147457, 209953, 331777,\\ &472393, 629857, 746497, 786433,\\ &839809, 995329\}.\end{aligned}$$

Pierpont's theorem holds for all forty primes in $\mathcal{P}$, while the pending clover theorem applies to thirty-eight of them and the origami leminiscate theorem applies to thirty-five.

The Field of Origami Numbers

The origami numbers form a subfield $\mathcal{O}$ of $\mathbf{C}$ characterized by the following properties.

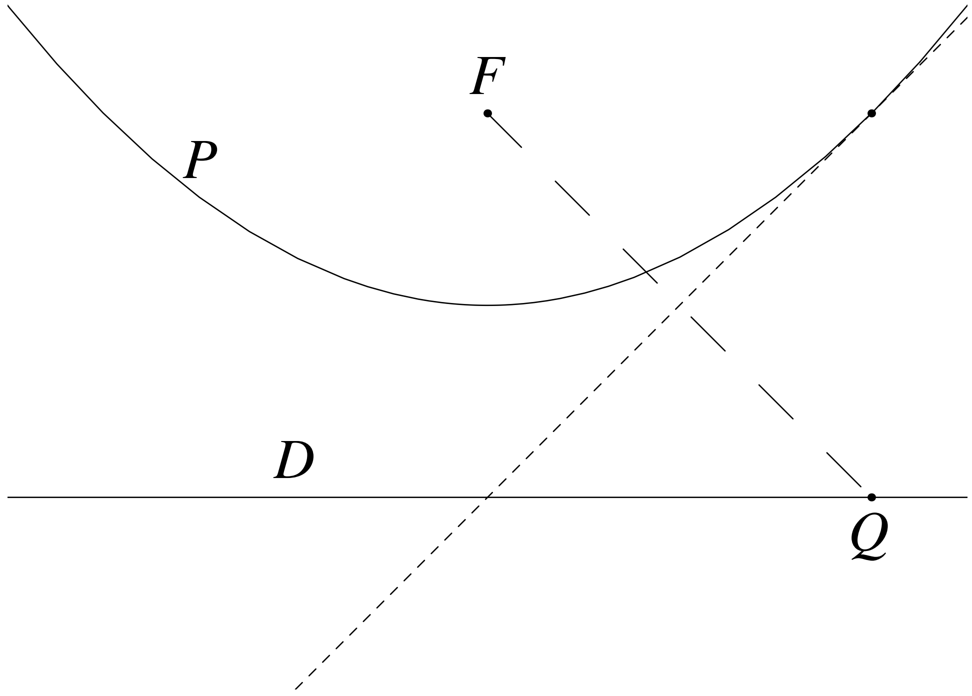
1. Let $z = x + iy \in \mathbf{C}$. Then $z \in \mathcal{O}$ if and only if $x, y \in \mathcal{O}$.

2. Let $z \in \mathbf{C}$. Then $z \in \mathcal{O}$ if and only if there is a Galois extension $\mathbf{Q} \subset L \subset \mathbf{C}$ such that $z \in L$ and $[L : \mathbf{Q}] = 2^u 3^v$ for some $u, v \geq 0$.

(In particular, $\mathcal{O}$ is closed under equations of degree up to four. The origami numbers are the numbers derivable from $\mathbf{Q}$ by finitely many steps involving algebra, square roots, and cube roots.)

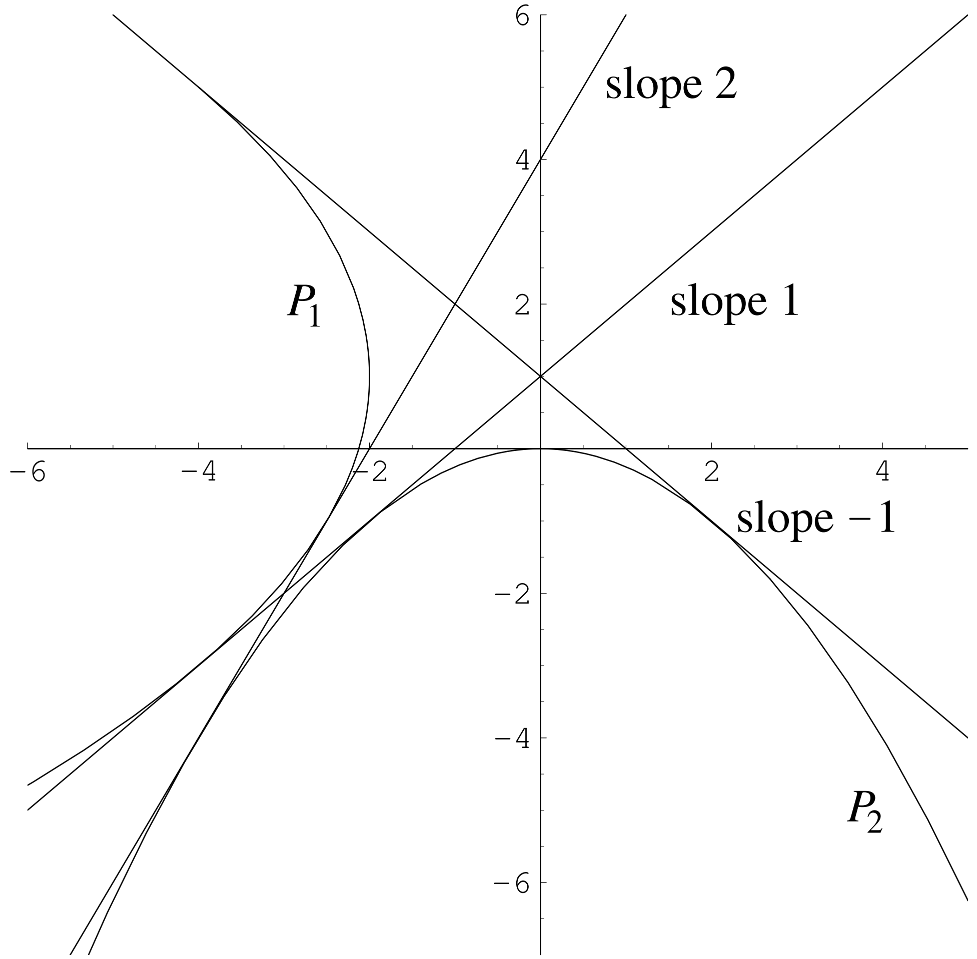
Gist of Pierpont's argument: $|(\mathbf{Z}/n\mathbf{Z})^\times| = 2^u 3^v$ if and only if n is a number as in the theorem.

Folding a Parabola Tangent



Given a point F and a line D, the folds that take F to points Q of L are the tangent lines of the parabola with focus F and directrix D.

Solving a Cubic by Origami



The cubic equation

$$x^3 + bx^2 + cx + d = 0$$

is solved by slopes of the common tangents of the two parabolas

$$(y + c)^2 = -4d(x - b), \qquad x^2 = -4y.$$

The $\mathbf{m}$-clover

For any positive integer m the m-clover is the set of points in the plane satisfying the polar equation

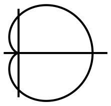
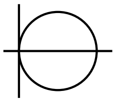
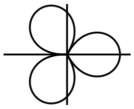
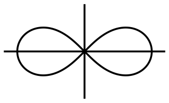
$$r^{m/2} = \cos(\tfrac{m}{2}\theta).$$

For m odd the polar equation can be taken as

$$r^m = \tfrac{1}{2}\Big(1 + \cos(m\theta)\Big).$$

The lemniscate arc length and Abel's Theorem are essentially related to the square lattice $\mathbf{Z}[i]$. The m-clovers were discovered in trying to find a corresponding geometric object and theorem for the triangular lattice $\mathbf{Z}[\zeta_3]$.

Table of First Four Clovers

m	Equation	Name	Graph
1	$r^{1/2} = \cos(\frac{1}{2}\theta)$ or $r = \frac{1}{2}(1 + \cos\theta)$	Cardioid	
2	$r = \cos\theta$	Circle	
3	$r^{3/2} = \cos(\frac{3}{2}\theta)$ or $r^3 = \frac{1}{2}(1 + \cos(3\theta))$	Clover	
4	$r^2 = \cos(2\theta)$	Lemniscate	

In general,

m even: $m/2$ leaves.

m odd: m leaves.

Principal leaf: the leaf through $(1, 0)$.

New $\mathbf{m}$-clover Division Theorems

$\mathbf{m} = 1$: For any positive integer n, the cardioid can be divided into n arcs of equal length by straightedge and compass, and therefore by origami.

$\mathbf{m} = 3$: The clover can be divided into n arcs of equal length by origami if and only if

$$n = 2^a 3^b p_1 \cdots p_r$$

where $a, b \geq 0$ and $p_1, \ldots, p_r$ are distinct Pierpont primes with each p_i being 5 or 17 or a $3k + 1$ prime.

$\mathbf{m} = 4$: The lemniscate can be divided into n arcs of equal length by origami if and only if

$$n = 2^a 3^b p_1 \cdots p_r$$

where $a, b \geq 0$ and $p_1, \ldots, p_r$ are distinct Pierpont primes with each p_i being 7 or a $4k + 1$ prime.

(No straightedge and compass theorem for $m = 3$, i.e., for the clover.)

The Set-up

Let m be fixed.

Question: For a given n, can we construct the n-division points (x, y) of the principal leaf of the m-clover?

Note that we do not already have a graph of the clover itself, despite using the computer to draw such graphs for these slides.

Intermediate quantities: The polar coordinates (r, θ) of the points.

Work backwards. Suppose that we have x and r. Then the Pythagorean equation

$$x^2 + y^2 = r^2$$

shows that finding y amounts to solving a quadratic equation. This can be done by Euclidean construction or by origami. So we need to find x and r.

Relation Between $\mathbf{x}$ and $\mathbf{r}$ on the $\mathbf{m}$-clover

Let T_n be the nth Tchebyshev polynomial, defined by

$$\cos(n\theta) = T_n(\cos(\theta)).$$

m even: $r^{m/2} = T_{m/2}(x/r)$, polynomial relation of degree $m/2$ in x.

m odd: $r^m = \frac{1}{2}\Big(1 + T_m(x/r)\Big)$, polynomial relation of degree m in x.

Relation Between x and r on the Lemniscate

$$r^4 = 2x^2 - r^2$$

So Euclidean constructions recover x from r.

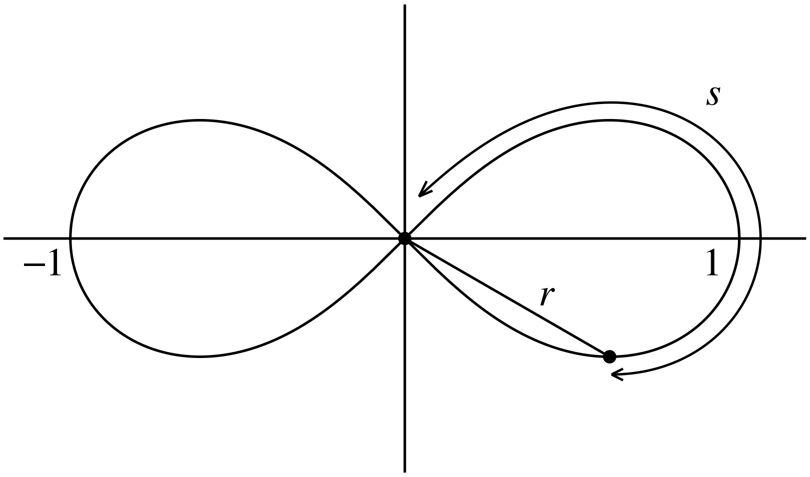
Relation Between x and r on the Clover

$$2r^6 = r^3 - 3r^2x + 4x^3$$

So origami is needed to recover x from r. Hence no straightedge and compass theorem for the clover by these methods.

Now the problem is reduced to finding r.

$\mathbf{r}$ as a Function of $\mathbf{s}$: Polar Radius on the $\mathbf{m}$-clover



The radius function is written $r = \varphi_m(s)$.

Let ϖ_m denote the arc length of the principal leaf. The n-division problem is not to compute the polar radius in general, but to start from the particular arc length values

$$s_\ell = \frac{\ell}{n}\varpi_m, \quad \ell = 1, \ldots, n-1,$$

and compute the corresponding polar radius values,

$$r_\ell = \varphi_m(s_\ell), \quad \ell = 1, \ldots, n-1.$$

$\mathbf{s}$ as a Function of $\mathbf{r}$: Arc Length on the $\mathbf{m}$-clover

No formula presents itself immediately for r as a function of s. So solve the inverse problem: find s in terms of r.

This works on the m-clover exactly as it worked on the lemniscate. Recall the polar differential arc length formula,

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

On the m-clover this works out to

$$ds = \frac{dr}{\sqrt{1 - r^m}},$$

so the arc length of the m-clover is the integral

$$s = \int_{t=0}^{r} \frac{dt}{\sqrt{1 - t^m}}.$$

$\varpi_{\mathbf{m}}$: the Length of the Principal Leaf

The principal leaf has length

$$\varpi_m = 2\int_0^1 \frac{dt}{\sqrt{1-t^m}}.$$

Let $u = t^m$. Then

$$\varphi_m = \frac{2}{m}\int_0^1 u^{1/m-1}(1-u)^{1/2-1}\,du.$$

This is a beta integral. It works out to

$$\varpi_m = 2\sqrt{\pi}\frac{\Gamma(\frac{1}{m}+1)}{\Gamma(\frac{1}{m}+\frac{1}{2})}.$$

So $\varpi_1 = 4$, $\varpi_2 = \pi$, and $\lim_m \varpi_m = 2$ since the leaves get flatter as their number increases.

The Arc Length Integral When $\mathbf{m=2}$

$$s = \int_{t=0}^{r} \frac{dt}{\sqrt{1-t^2}}$$

so the derivative of s as a function of r satisfies

$$\frac{ds}{dr} = \frac{1}{\sqrt{1-r^2}}$$

so the derivative of r as a function of s satisfies

$$\left(\frac{dr}{ds}\right)^2 = 1 - r^2.$$

Also, $r(\pi/2) = 1$ and $r'(\pi/2) = 0$. So studying the radius as the inverse function of the arc length integral shows that it satisfies a differential equation that identifies it as a periodic function,

$$r = \sin(s).$$

Arc Length and Radius on the m-clover

For $0 \le r \le 1$ and $0 \le s \le \varpi_m/2$, arc length and polar radius are inverse functions,

$$s = \int_{t=0}^{r} \frac{dt}{\sqrt{1-t^m}} \qquad \Longleftrightarrow \qquad r = \varphi_m(s).$$

As with $m = 2$, the radius therefore satisfies the differential equation

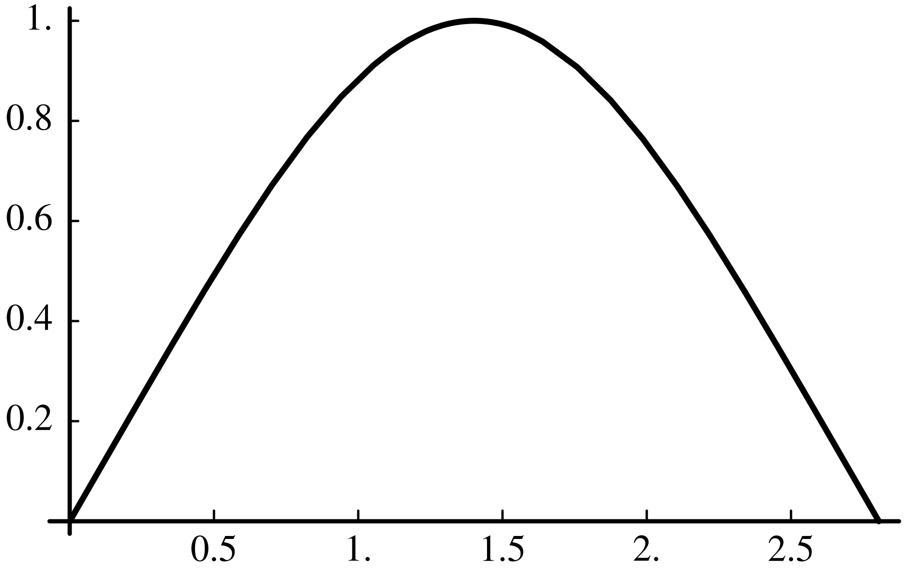
$${\varphi_m'}^2 = 1 - \varphi_m^m$$

with the initial conditions

$$\varphi_m(\varpi_m/2) = 1, \quad \varphi_m'(\varpi_m/2) = 0.$$

This function can be considered m-clover analogue of the sine function.

The 3-clover Sine



The 1-clover sine is a parabola over $[0, 4]$, the 2-clover sine is the usual sine on $[0, \pi]$, the 4-clover sine is what Gauss called the lemniscate sine, and as $m \to \infty$ the m-clover sine tends to a piecewise linear function on $[0, 2]$.

The Insight of Gauss and Abel

For $m = 4$ the elliptic integral

$$s = \int_{t=0}^{r} \frac{dt}{\sqrt{1-t^4}}$$

is the inverse function of a doubly periodic function of a complex variable. The periods are (essentially) the square lattice $\mathbf{Z}[i]$.

That is, the right idea is to study

$$r = \varphi_4(s)$$

as such a function of s.

This applies when $m = 3$ as well, and the periods are (essentially) the triangular lattice $\mathbf{Z}[\zeta_3]$.

φ In Terms of $\wp$ for the Clover

Then φ is defined in terms of the Weierstrass $\wp$-function having period lattice $\varpi\mathbf{Z}[\zeta_3]$,

$$\varphi(s) = \tfrac{4}{3}\,\wp(\tfrac{i}{\sqrt{3}}(\varpi + s)).$$

Byproduct of the argument:

$$140 \sum_{\varpi\mathbf{Z}[\zeta_3]}{}' \frac{1}{\omega^6} = \tfrac{27}{16}.$$

(Similarly $60{\sum}'_{\varpi_4\mathbf{Z}[i]}\,\omega^{-4} = 4$, a result that goes back to Landau.)

In general

$$\wp(z+\tilde{z}) = -\wp(z) - \wp(\tilde{z}) + \tfrac{1}{4}\left(\frac{\wp'(z) - \wp'(\tilde{z})}{\wp(z) - \wp(\tilde{z})}\right)^2.$$

Combining these results gives the addition law for the clover (next slide).

Addition Law for the Clover

Let $s, t, s+t$ lie in $[0, \varpi]$. Let

$$a = \varphi(s),\ a' = \varphi'(s),\ b = \varphi(t),\ b' = \varphi'(t).$$

Then

$$\varphi(s+t) = 2\frac{C_{00} + C_{10}a' + C_{01}b' + C_{11}a'b'}{(4a + 4b + a^2b^2)^2}$$

where

$$\begin{aligned} C_{00} &= -8 + 4a^3 + 4b^3 + 4a^2b + 4ab^2 \\ &\qquad - a^4b^2 - a^2b^4 - 6a^2b^2, \\ C_{10} &= 8 + 4a^2b + 12ab^2 + 4b^3 - a^2b^4, \\ C_{01} &= 8 + 4ab^2 + 12a^2b + 4a^3 - a^4b^2, \\ C_{11} &= -8 + 4a^2b + 4ab^2. \end{aligned}$$

Consequence: If $\varphi(s)$ and $\varphi(t)$ are origami numbers then so is $\varphi(s+t)$.

Connection to Class Fields

The polar radius of the point $\ell\varpi/n$ of the way around the principal leaf is

$$r = \tfrac{4}{3}\,\wp(\varpi i\sqrt{3}\,\tfrac{n+\ell}{3n}).$$

Since $\varpi i\sqrt{3} \in \varpi\mathbf{Z}[\zeta_3]$, this r-value is the first coordinate of a division point of the elliptic curve

$$y^2 = 4x^3 - 27/16.$$

(Note: x and y here are not the x and y of the clover's environment.)

Class field theory and complex multiplication say that such first coordinates generate abelian extensions of imaginary quadratic fields. This is the idea of the proof of the clover theorem, to be sketched at the end of the talk.

Duplication Formula for the Clover

Let $r = \varphi(s)$, $r' = \varphi'(s)$. Let $\tilde{r} = \varphi(2s)$. Then

$$\tilde{r} = 2\frac{-16 + 32r^3 - 16r^6 + (16 + 40r^3 - 2r^6)r'}{(8r + r^4)^2}.$$

This shows that that if the polar radius $\tilde{r}$ of a division point is known, then the corresponding r and r' for dividing the clover into twice as many pieces satisfy a polynomial relation involving the datum $\tilde{r}$.

Also, since ${r'}^2 = 1 - r^3$, we can eliminate r' by taking a square.

The Simplest Example

In particular set

$$s = \varpi/4.$$

Then $2s = \varpi/2$ is half the arc length of the principal leaf, and the corresponding 2-division radius $\tilde{r} = \varphi(2s)$ on the left side of the duplication formula is

$$\tilde{r} = 1.$$

Square the relation

$$1 = 2\frac{-16 + 32r^3 - 16r^6 + (16 + 40r^3 - 2r^6)r'}{(8r + r^4)^2}$$

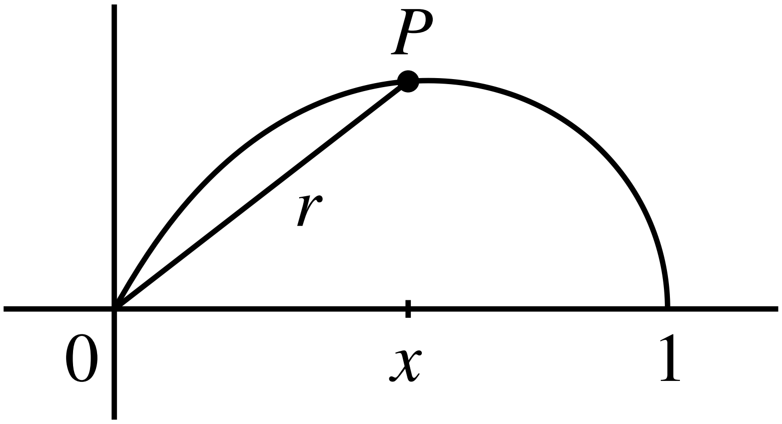
and substitute ${r'}^2 = 1 - r^3$ to get

$$r^2(2+r)^2(4-2r+r^2)^2(-8+8r+8r^3+r^4)^2 = 0.$$

So the positive real root r must satisfy the relation

$$-8 + 8r + 8r^3 + r^4 = 0.$$

(Continued on next slide.)



Solving the quartic polynomial gives

$$r = -2 - \sqrt{3} + \sqrt{3(3+2\sqrt{3})} \approx 0.671619,$$

and then the cubic equation that gives x in terms of r gives the 4-division x-coordinate

$$x \approx 0.531137.$$

The radius r is constructible by straightedge and compass, but the minimal polynomial of x over $\mathbf{Q}$ has degree 12, so constructing the point P requires origami.

Note that x is a little bigger than 1/2, as it must be since the clover bulges to the right.

Proof of the Clover Theorem

The argument uses

- the arithmetic of the Eisenstein integer ring $\mathcal{O} = \mathbf{Z}[\zeta_3]$,

- class field theory and complex multiplication.

Arithmetic of $\mathbf{Z}[\zeta_3]$

Let p be prime in $\mathbf{Z}$. Let $\mathcal{O} = \mathbf{Z}[\zeta_3]$.

- If $p \neq 3$ then

$$|(\mathcal{O}/p\mathcal{O})^\times| = \begin{cases} (p-1)^2 & \text{if } p \equiv 1 \pmod 3, \\ p^2 - 1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

- If $p > 3$ then $|(\mathcal{O}/p\mathcal{O})^\times| = 2^u 3^v$ for some $u, v \geq 0$ if and only if p is a Pierpont prime $p \equiv 1 \pmod 3$ or $p = 5, 17$. (The two $p \equiv 2 \pmod 3$ solutions arise from Levi Ben Gershon's special case of the Catalan conjecture.)

Results from Class Field Theory and Complex Multiplication

Let $\mathbf{K} = \mathbf{Q}(\zeta_3)$ and let $\beta \in \mathcal{O}$ be nonzero.

There exists a *ray class field* $\mathbf{K}_\beta$ of $\mathbf{K}$ such that

$$\text{Gal}(\mathbf{K}_\beta/\mathbf{K}) \sim (\mathcal{O}/\beta\mathcal{O})^\times/\mathcal{O}^\times.$$

(Here we write $\mathcal{O}^\times$ for its image in $(\mathcal{O}/\beta\mathcal{O})^\times$.)

For any $\alpha \in \mathcal{O}$ relatively prime to β,

$$\mathbf{K}_\beta = \mathbf{K}\Big(\wp^3(\tfrac{\alpha}{\beta}\varpi)\Big).$$

A Special Case

Let n be a positive integer and let ℓ be coprime to n, $1 \leq \ell \leq n-1$. Define

$$\alpha = \begin{cases} \ell + n & \text{if } \ell + n \not\equiv 0 \pmod 3, \\ \frac{\ell+n}{1-\zeta_3} & \text{if } \ell + n \equiv 0 \pmod 3, \end{cases}$$

and

$$\beta = \begin{cases} (1-\zeta_3)n & \text{if } \ell + n \not\equiv 0 \pmod 3, \\ n & \text{if } \ell + n \equiv 0 \pmod 3. \end{cases}$$

Then the cube of the polar radius for $s = \ell\varpi/n$ is

$$\varphi^3(\ell\tfrac{\varpi}{n}) = (\tfrac{4}{3})^3 \wp^3(\tfrac{\alpha}{\beta}\varpi).$$

Also, α and β are relatively prime in $\mathcal{O}$ since gcd$(\ell, n) = 1$. So by the theorem,

$$\mathbf{K}_\beta = \mathbf{K}(\varphi^3(\ell\tfrac{\varpi}{n})).$$

The Galois group Gal$(\mathbf{K}_\beta/\mathbf{K})$ has order

$$|(\mathcal{O}/\beta\mathcal{O})^\times/\mathcal{O}^\times| = \frac{1}{6}\prod_{p^e\|n} p^{2(e-1)}|(\mathcal{O}/p\mathcal{O})^\times|.$$

This takes the form 2^u3^v for n as described in the Clover Theorem.

The proof of the Clover Theorem is completed by observing that a square root constructs $\mathbf{K}$ from $\mathbf{Q}$ while a cube root constructs the ℓ/n division radius from $\mathbf{K}_\beta$.

Kronecker's Theorem

Let $\mathbf{L}$ be any Abelian extension of $\mathbf{Q}$. Then $\mathbf{L}$ is contained in a cyclotomic extension of $\mathbf{Q}$, i.e., an extension generated by division points of a circle:

$$\mathbf{Q} \subset \mathbf{L} \subset \mathbf{Q}(\zeta_n) \quad \text{for some } n.$$

Kronecker's Jugendtraum

Let $\mathbf{K}$ be an imaginary quadratic field, $\mathbf{K} = \mathbf{Q}(\sqrt{d})$ where $d < 0$, and let E be an elliptic curve such that $j(E) = j(\mathcal{O}_{\mathbf{K}})$. Let $\mathbf{L}$ be any Abelian extension of $\mathbf{K}$. Then $\mathbf{L}$ is contained in an extension of $\mathbf{K}$ generated by the x-coordinates of division points of an elliptic curve E associated to $\mathbf{K}$:

$$\mathbf{K} \subset \mathbf{L} \subset \mathbf{K}(x(E[N])) \quad \text{for some } N.$$

In the special case $\mathbf{K} = \mathbf{Q}(i)$ we only need the squares of the x-coordinates. Similarly for $\mathbf{K} = \mathbf{Q}(\zeta_3)$ and the cubes of the x-coordinates.