

---

# Geometry and Number Theory on Clovers

---

David A. Cox and Jerry Shurman

---

**1. INTRODUCTION.** In 1826 Abel discovered that the *lemniscate*, the curve  $(x^2 + y^2)^2 = x^2 - y^2$  pictured in Figure 1, can be divided into  $n$  arcs of equal length by straightedge and compass if and only if  $n$  is a power of 2 times a product of distinct Fermat primes [1, p. 314]. By an earlier theorem of Gauss, these are exactly the values of  $n$  for which a regular  $n$ -gon is constructible by straightedge and compass or, equivalently, the values of  $n$  for which the circle can be divided into  $n$  arcs of equal length.

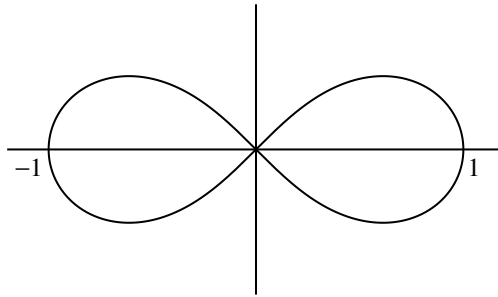


FIGURE 1. The lemniscate.

This paper places these results in a more general context by investigating geometric constructions on the plane curve defined by the polar equation

$$r^{m/2} = \cos\left(\frac{m}{2}\theta\right), \quad (1)$$

where  $m$  is a fixed positive integer. According to [29], a *sinusoidal spiral* is a curve defined by  $r^a = \cos(a\theta)$  for fixed  $a$  in  $\mathbb{Q}$ . Hence (1) is the sinusoidal spiral with  $a = m/2$  for  $m$  in  $\mathbb{Z}^+$ . We call this curve the  $m$ -*clover*. The  $m$ -clovers with  $m = 1, 2,$  and  $4$  are the cardioid, the circle, and the lemniscate, respectively. The 3-clover, called simply the *clover* in this paper, appears not to have been studied before. The first four  $m$ -clovers and their equations are shown in Figure 2.

We study two types of constructions on  $m$ -clovers: straightedge and compass, and origami (paper folding). This is the “geometry” in the title of the paper. The capabilities of both constructions are known for the circle. We remind the reader that a *Fermat prime* is a prime  $p$  greater than 2 of the form  $2^u + 1$  with  $u \geq 0$  and a *Pierpont prime* is a prime  $p$  greater than 3 of the form  $2^u 3^v + 1$  with  $u, v \geq 0$ .

**Theorem 1 (Circle Theorem).** *Let  $n$  be a positive integer. Then the following statements are true:*

- (1) *The circle can be divided into  $n$  arcs of equal length by straightedge and compass if and only if  $n = 2^a p_1 \cdots p_r$ , where  $a \geq 0$  and  $p_1, \dots, p_r$  are distinct Fermat primes.*
- (2) *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  $p_1, \dots, p_r$  are distinct Pierpont primes.*

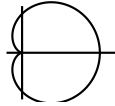
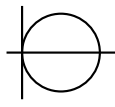
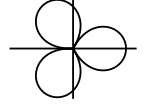
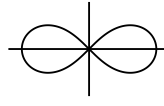
$m$	Equation	Name	Graph
1	$r^{1/2} = \cos(\frac{1}{2}\theta)$ or $r = \frac{1}{2}(1 + \cos \theta)$	Cardioid	
2	$r = \cos \theta$	Circle	
3	$r^{3/2} = \cos(\frac{3}{2}\theta)$ or $r^3 = \frac{1}{2}(1 + \cos(3\theta))$	Clover	
4	$r^2 = \cos(2\theta)$	Lemniscate	

FIGURE 2.  $m$ -clovers for  $m = 1, 2, 3, 4$ .

As already noted, the first part of the circle theorem is due to Gauss. The second part was proved by Pierpont [18] in 1895. Also as noted, the circle is the 2-clover. The circle theorem extends to the other  $m$ -clovers in Figure 2 as follows:

**Theorem 2 (Cardioid Theorem).** *Let  $n$  be a positive integer. Then the cardioid can be divided into  $n$  arcs of equal length by straightedge and compass.*

**Theorem 3 (Clover Theorem).** *Let  $n$  be a positive integer. Then 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  $p_1, \dots, p_r$  are distinct Pierpont primes such that  $p_i = 5$ ,  $p_i = 17$ , or  $p_i \equiv 1 \pmod{3}$ .*

**Theorem 4 (Lemniscate Theorem).** *Let  $n$  be a positive integer. Then the following statements are true:*

- (1) *The lemniscate can be divided into  $n$  arcs of equal length by straightedge and compass if and only if  $n = 2^a p_1 \cdots p_r$ , where  $a \geq 0$  and  $p_1, \dots, p_r$  are distinct Fermat primes.*
- (2) *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  $p_1, \dots, p_r$  are distinct Pierpont primes such that  $p_i = 7$  or  $p_i \equiv 1 \pmod{4}$ .*

The first part of the lemniscate theorem is due to Abel; the second part, and the cardioid and clover theorems, are proved in this paper. Since origami subsumes straightedge and compass, the cardioid theorem implies that the cardioid can be divided into any number of arcs of equal length by origami. On the other hand, the clover theorem mentions only origami, since our methods do not lead to straightedge and compass constructions on the clover. This is explained in Example 3 of section 3 and in the discussion following the proof of the clover theorem in section 6.

Gleason suggests [9, p. 191] that there may be infinitely many Pierpont primes, although only finitely many have been found so far. According to Sequence A005109 of Sloane's On-Line Encyclopedia of Integer Sequences [25], the known Pierpont

primes form the set

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

The second part of the circle theorem holds for all forty primes in  $\mathcal{P}$ , while the clover theorem applies to the thirty-eight primes in

$$\mathcal{P} \setminus \{257, 65537\}$$

and the second part of the lemniscate theorem applies to the thirty-five primes in

$$\mathcal{P} \setminus \{19, 163, 487, 1459, 39367\}.$$

For the circle theorem, a key ingredient is the Galois group of  $\mathbb{Q}(\zeta_p)$  over  $\mathbb{Q}$ , where  $p$  is prime and  $\zeta_p = e^{2\pi i/p}$ . This group is isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^*$ , the group of invertible elements in the quotient ring  $\mathbb{Z}/p\mathbb{Z}$ . Since straightedge and compass constructions require a Galois extension of degree  $2^u$ , Fermat primes appear in the circle theorem because

$$|(\mathbb{Z}/p\mathbb{Z})^*| = 2^u \text{ for } u \geq 0 \text{ and } p > 2 \iff p \text{ is a Fermat prime.}$$

Similarly, since origami constructions require a Galois extension of degree  $2^u 3^v$ , Pierpont primes appear in the circle theorem because

$$|(\mathbb{Z}/p\mathbb{Z})^*| = 2^u 3^v \text{ for } u, v \geq 0 \text{ and } p > 3 \iff p \text{ is a Pierpont prime.}$$

The situation is much the same for the clover and lemniscate theorems, except that in the case of the clover  $\mathbb{Z}$  is replaced with the ring

$$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 \mid a, b \in \mathbb{Z}\}, \quad \zeta_3 = \frac{1}{2}(-1 + i\sqrt{3}),$$

while the relevant ring for the lemniscate is

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \quad i = \sqrt{-1}.$$

In studying origami constructions on the clover, we use the observation (to be proved in section 6) that if  $p$  is prime and greater than 3, then

$$|(\mathbb{Z}[\zeta_3]/p\mathbb{Z}[\zeta_3])^*| = 2^u 3^v \text{ for } u, v \geq 0 \iff \begin{cases} p \text{ is a Pierpont prime such that} \\ p = 5, p = 17, \text{ or } p \equiv 1 \pmod{3}. \end{cases}$$

Thus the primes in the clover theorem have a strong connection to the arithmetic of  $\mathbb{Z}[\zeta_3]$ . Similarly, given a prime  $p$  greater than 3, we will see in section 7 that

$$|(\mathbb{Z}[i]/p\mathbb{Z}[i])^*| = 2^u 3^v \text{ for } u, v \geq 0 \iff \begin{cases} p \text{ is a Pierpont prime such} \\ \text{that } p = 7 \text{ or } p \equiv 1 \pmod{4}. \end{cases}$$

This describes the primes in the second part of the lemniscate theorem.

The most difficult task will be to interpret  $(\mathbb{Z}[\zeta_3]/p\mathbb{Z}[\zeta_3])^*$  and  $(\mathbb{Z}[i]/p\mathbb{Z}[i])^*$  as the appropriate Galois groups. The tools required for this are elliptic functions, class field theory, and complex multiplication. This is the “number theory” in the title of the paper. For the lemniscate, the elegant proof of the first part of the lemniscate theorem given by Rosen in [21] provides most of what we need. Creating a similar theory for the clover will occupy a large part of this paper.

The outline is as follows. Section 2 studies the  $m$ -clover and its arclength. It also introduces the  $m$ -clover function  $\varphi_m$ , which plays a crucial role in the proofs of our results. Section 3 begins exploring geometric constructions on  $m$ -clovers for  $m = 1, 2, 3, 4$  and proves the cardioid theorem. Sections 4 and 5 require more

mathematical background. They describe the 3-clover function  $\varphi_3$  in terms of the Weierstrass  $\wp$ -function and use the addition law for  $\wp$  to obtain an addition law and a duplication formula for  $\varphi_3$ . Section 6 establishes the clover theorem, and section 7 proves the second part of the lemniscate theorem. The proofs use properties of certain fields constructed by class field theory and complex multiplication. The technical details for the clover theorem appear in the appendix, while the corresponding details for the lemniscate theorem are in Rosen's paper [21].

## REFERENCES

- [1] N. H. Abel, Recherches sur les fonctions elliptiques, in *Œuvres complètes de Niels Henrik Abel*, vol. 1, L. Sylow and S. Lie, eds., Grøndahl & Søn, Christiania, Norway, 1881, pp. 263–388.
- [2] R. C. Alperin, A mathematical theory of origami constructions and numbers, *New York J. Math.* **6** (2000) 119–133.
- [3] D. Auckly and J. Cleveland, Totally real origami and impossible paper folding, *Amer. Math. Monthly* **102** (1995) 215–226.
- [4] A. Baragar, Constructions using a compass and twice-notched straightedge, *Amer. Math. Monthly* **109** (2002) 151–164.
- [5] D. A. Cox, *Galois Theory*, John Wiley & Sons, New York, 2004.
- [6] ———, *Primes of the Form  $x^2 + ny^2$* , John Wiley & Sons, New York, 1989.
- [7] B. C. Edwards and J. Shurman, Folding quartic roots, *Math. Mag.* **74** (2001) 19–25.
- [8] J. W. Emert, K. I. Meeks, and R. B. Nelson, Reflections on a mira, *Amer. Math. Monthly* **101** (1994) 544–549.
- [9] A. M. Gleason, Angle trisection, the heptagon, and the triskaidecagon, *Amer. Math. Monthly* **95** (1988) 185–194.
- [10] T. Hull, A note on “impossible” paper folding, *Amer. Math. Monthly* **103** (1996) 240–241.
- [11] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.
- [12] G. A. Jones and D. Singerman, *Complex Functions: An Algebraic and Geometric Viewpoint*, Cambridge University Press, Cambridge, 1987.
- [13] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.
- [14] S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, MA, 1973.
- [15] F. Lemmermeyer, *Reciprocity Laws*, Springer-Verlag, New York, 2000.
- [16] G. E. Martin, *Geometric Constructions*, Springer-Verlag, New York, 1998.
- [17] J. Neukirch, *Class Field Theory*, Springer-Verlag, Berlin, 1986.
- [18] J. Pierpont, On an undemonstrated theorem of the Disquisitiones Arithmeticae, *Bull. Amer. Math. Soc.* **2** (1895–96) 77–83.
- [19] V. Prasolov and Y. Solovyev, *Elliptic Functions and Elliptic Integrals*, American Mathematical Society, Providence, 1997.
- [20] P. Ribenboim, *Catalan's Conjecture*, Academic Press, Boston, 1994.
- [21] M. Rosen, Abel's theorem on the lemniscate, *Amer. Math. Monthly* **88** (1981) 387–395.
- [22] T. S. Row, *Geometric Exercises in Paper Folding*, Addison & Co., Madras, 1893; also published by Open Court, Chicago, 1901; reprinted by Dover Publications, New York, 1966.
- [23] C. L. Siegel, *Topics in Complex Function Theory*, vol. 1, John Wiley & Sons, New York, 1969.
- [24] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
- [25] N. J. A. Sloane, ed. (2004), The On-Line Encyclopedia of Integer Sequences, <http://www.research.att.com/~njas/sequences/>.

- [26] C. R. Videla, On points constructible from conics, *Math. Intelligencer* **19** (1997) 53–57.
- [27] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman and Hall/CRC, Boca Raton, FL, 2003.
- [28] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, 4th ed., Cambridge University Press, Cambridge, 1963.
- [29] R. C. Yates, *Curves and Their Properties*, National Council of Teachers of Mathematics, Washington, D.C., 1974.