Self-Inscribed Polygons with Vertices on Nonsingular Cubic Curves

N. S. Mendelsohn and R. Padmanabhan
Department of Mathematics and Astronomy
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

To Alan J. Hoffman on his 65th birthday (may he live to one hundred and twenty!).

Submitted by Robert E. Bixby

ABSTRACT

We study the problem of representing the connected self-inscribed polygons as configurations on a nonsingular cubic curve in the complex projective plane such that the triple (a, b, c) is an edge in the polygon iff the three points on the cubic curve corresponding to a, b, and c are collinear in the projective plane. Employing classical algebraic and number theoretic techniques such as the resultant of polynomials, solving vector equations over $\mathrm{GF}(p)$, and primitive roots, and using the symbolic manipulation package MAPLE on our mainframe, we succeed in deciding the problem of faithful representation of difference set designs $\{0,1,3\}$ mod n for all $n \leqslant 100$.

1. INTRODUCTION

Let $A_1, A_2, \ldots, A_n$ be the n vertices of a polygon with sides $A_1A_2, A_2A_3, \ldots, A_{n-1}A_n, A_nA_1$. If each of the sides has one of the remaining vertices incident with it, then the polygon is said to be self-inscribed. Figure 1 shows a self-inscribed 10-gon which is actually drawn in a real projective plane. A self-inscribed n-gon is a special case of a configuration n_3 which consists of n points and n lines with each line incident with three of the points and each point incident with three of the lines. All such configurations exist in a free projective plane.

655 Avenue of the Americas, New York, NY 10010 0024-3795/89/$3.50

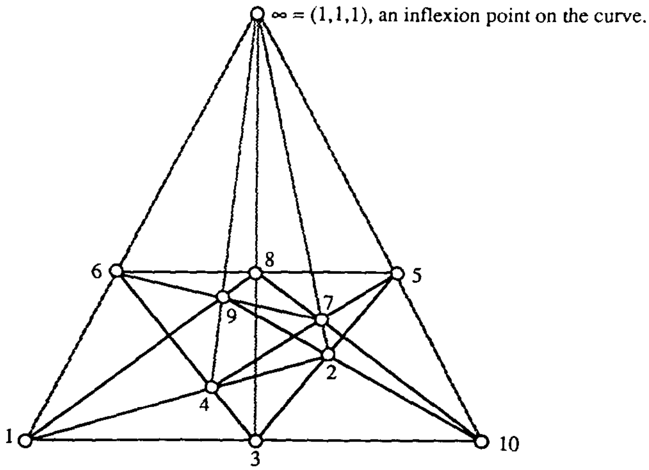

FIG. 1. $\{1,2,4\}$ mod 10. See Theorem 3.3 in [7] for the proof leading to the further incidence relations of the diagram. An irreducible cubic in the real projective plane containing the above 10_3 configuration is $x^2y+(-2-\sqrt{2})xy^2-2x^2z+(2+2\sqrt{2})xz^2+(2+2\sqrt{2})y^2z-(4+3\sqrt{2})yz^2+3xyz=0$.

The actual embedding of the above 10_3 is realized by Table 1. [Taken from Mendelsohn, Padmanabhan, and Wolk, Remarks on n-clusters on cubic curves, in Combinatorial Design Theory, *Ann. Discrete Math.* 34:371–378 (1987).]

TABLE 1

	x	y	z
1	1	0	0
2	0	1	0
3	0	0	1
4	$2+\sqrt{2}$	1	0
5	0	$2+\sqrt{2}$	2
6	$2+\sqrt{2}$	1	1
7	1	2	1
8	$\sqrt{2}$	$\sqrt{2}$	1
9	$1+\sqrt{2}$	0	1
10	$1+\sqrt{2}$	1	1
∞	1	1	1

We now confine our consideration to the classical case of a projective plane coordinated by a field (or even a division ring). For $n = 10$, the isomorphism classes of these configurations have been known for a long time (see e.g. [2, pp. 95–132]), and the latest classification appears in [4]. For $n > 11$ only scanty information was available until recently.

Since a line and a cubic have at most three common points, we address, in what follows, the natural question whether self-inscribed polygons can be drawn in the real or the complex plane with all vertices of the polygon lying on a nonsingular cubic curve. While not completely solving these problems, we do give procedures for carrying out the determination.

2. BASIC INFORMATION

Let C be a complex cubic curve without singular points, and let p be one of the points of inflection of C. Let G be the group $S_1 \times S_1$, where S_1 is the group of unimodular complex numbers under multiplication. Since G is Abelian, we will assume it is written additively and denote the identity element by 0 in the additive notation.

A well-known result [5, Theorem IV.16] is that there is a bijection φ mapping the points of C onto the elements of G in such a way that $\varphi(p) = 0$ and r, s, t are collinear points of the curve C iff $\varphi(r) + \varphi(s) + \varphi(t) = 0$.

The finite subgroups of G are the set of all finite cyclic groups and all direct products of two finite cyclic groups. We use C_n to denote the cyclic groups of order n.

In the case of real cubic curves without singular points the results are the same with the group G replaced by the group $H = S_1 \times C_2$. The finite subgroups of H are the cyclic groups C_n and the groups $C_n \times C_2$ with n even. In the case of finite fields, the group of the cubic curve has never been studied systematically (see, however, [3] and also Chapter II in [1]). We do know that when the field is $\mathrm{GF}(2^n)$ the group contains $C_2 \times C_2 \times C_2$ as a subgroup.

An important class of n_3 configurations is constructed as follows. The points of the n_3 are taken as the elements of C_n, which we represent by the integers mod n. Let (i, j, k) be a triple of elements of C_n such that all six differences $\pm(i - j), \pm(i - k), \pm(j - k)$ are distinct. We then take the n translates of (i, j, k), namely $(i + r, j + r, k + r)$ where $r \equiv 0, 1, 2, \ldots, n - 1$ mod n, to be the lines of the n_3 configuration. This configuration has an automorphism $(i \to i + 1)$ mod n which is cyclic on the points and lines of the configuration. One of the lines of the configuration is a triple with first component 0, say $(0, a, b)$. If a and b are relatively prime, the configuration is connected. More generally, if the greatest common divisor of a and b is prime to n, the configuration is connected and is a self-inscribed n-gon. In what follows we will use the notation $\{0, a, b\}$ mod n to name the configuration.

The problem of constructing the configuration $\{0, a, b\}$ mod n so that its vertices lie on a complex cubic curve is now reduced to the following. Find a subgroup M of G and an injection of the configuration into M given by $i \to \varphi(i)$, where $i = 0, 1, 2, \ldots, n-1$, such that for $k = 0, 1, \ldots, n-1$, $\varphi(k) + \varphi(a+k) + \varphi(b+k) = 0$, where $a+k$, $b+k$ are taken mod n. We will say, when such an injection occurs, that the configuration is embedded in the group M. Of course if M is a subgroup of a group N, the configuration is embedded in N. The only important cases are the minimal embeddings—i.e. when an embedding in a group M is not an embedding in any subgroup of M. It is possible for a group M to be a subgroup of a group N and for two embeddings to exist, one of which is minimal in M and the second in N. Except for a couple of cases, all our embeddings will be into cyclic groups.

3. EMBEDDINGS OF $\{0, a, b\}$ mod n INTO CYCLIC GROUPS

We will confine our discussion to the case $\{0, 1, 3\}$ mod n. All the algorithms used for this case translate immediately to the general case $\{0, a, b\}$ mod n.

We represent the elements of C_m as the integers mod m and consider the C_m as embedded in the ring Z_m of integers mod m. To map $\{0, 1, 3\}$ mod n into C_m, let x be an integer prime to m such that x is of order n. Furthermore, suppose x can be chosen in such a way that $1 + x + x^3 \equiv 0 \bmod m$. The mapping $i \to \varphi(i) = x^i$ is the required injection. For if $(s, s+1, s+3)$ is a triple of $\{0, 1, 3\}$ mod n, then $\varphi(s) + \varphi(s+1) + \varphi(s+3) = x^s + x^{s+1} + x^{s+3} = x^s(1 + x + x^3) \equiv 0$ mod m for $j = 0, 1, 2, \ldots, n-1$. The problem then is to find a common root of the equations $x^n - 1 = 0$ and $1 + x + x^3 = 0$ in Z_m. A necessary condition for a solution is that $n \mid \lambda(m)$, where $\lambda(m)$ is the Carmichael function[1] as defined in [6, p. 53]. It is easy to

[1]Recall that in the ring of integers (mod n), if G is the multiplicative subgroup of elements prime to n, then the Charmichael function $\lambda(n)$ is defined to be maximal order of an element of G.

find integers m such that $n \mid \lambda(m)$, but then there is no easy way to achieve the second condition, namely, that $x^n - 1 = 0$ and $1 + x + x^3 = 0$ have a common solution x such that $x^r \neq 1$ for $r < n$. Since the ring of polynomials with coefficients in Z_m does not have unique factorization, we cannot find a Euclidean algorithm to apply to a pair of polynomials. Still we can make a start. The polynomials $x^n - 1$ and $1 + x + x^3$ are monic, so we can carry out one division and obtain

$$x^n - 1 = q(x)(1 + x + x^3) + ax^2 + bx + c = 0.$$

Hence the x we are looking for satisfies $1 + x + x^3 = 0$ and $ax^2 + bx + c = 0$ in Z_m. If a is an invertible element of Z_m, then we carry out a second division, namely

$$1 + x + x^3 = q_1(x)(ax^2 + bx + c) + Lx + M.$$

We then look for all solutions of $Lx + M \equiv 0 \bmod m$ and check if any of them satisfy the equation $1 + x + x^3 \equiv 0 \bmod m$. We stress that there is no systematic way of finding suitable values of m. Nevertheless, we have found a number of such values using the symbolic manipulation package MAPLE on our mainframe computer.

If we specialize our search to the case where m is a prime p, we immediately are in a much better position for success. In this case the integers mod p are the elements of the Galois field GF(p), and the polynomials in one variable x form a vector space for which the integral powers of x form a basis. The x we are looking for is a common root of the cyclotomic polynomial $\varphi_n(x) = 0$ and $1 + x + x^3 = 0$ in GF(p). In general $\varphi_n(x) = 0$ and $1 + x + x^3 = 0$ do not have a common root. We first consider $\varphi_n(x)$ and $1 + x + x^3$ as polynomials with rational coefficients and take either the Bezout or the Sylvester resultant. To speed up the computation we divide $\varphi_n(x)$ by $1 + x + x^3$, getting $\varphi_n(x) = q(x)(1 + x + x^3) + f_2(x)$, where $f_2(x)$ is a polynomial of the second degree with integral coefficients. We then take the Bezout or Sylvester resultant of the two polynomials $f_2(x)$ and $1 + x + x^3$. This is always a nonzero integer r, and in general r is of order greater than n^6. Next we factor r into its prime power decomposition. If this decomposition contains a prime p such that $p > n$, then in GF(p) the equations $f_2(x) = 0$ and $1 + x + x^3 = 0$ have a common root. If x_1 and x_2 are the roots of $f_2(x) = 0$, then we check to see which satisfies $1 + x + x^3 \equiv 0 \bmod p$. In

TABLE 2

TABLE FOR EMBEDDING DESIGNS $\{0,1,3\}$ mod n INTO CYCLIC GROUPS C_m [a]

n	x	m	n	x	m	n	x	m
9	7	27	46	35	47	77	3005	3851
10	2	11	46	82	141	77	3700	4621
10	13	33	47	216	283	78	4561	22777
11	4	23	47	50412	74731	79	436687	517609
12	7	13	48	79	153	79	521602	8383481
13	36	53	48	505	577	80	79	187
15	14	31	49	133	197	80	157	401
15	76	93	50	666	1301	80	584	641
16	11	17	51	90067	136069	81	234747658	303610033
16	28	51	52	1862	20593	82	35	83
17	216	239	53	20125211	209520979	82	118	249
18	25	37	54	224	811	83	2085399523672	20019533360297
19	16	457	55	16525916	19567351	84	142	261
20	37	61	56	20	617	84	124	559
21	38	43	57	167	229	84	1989	3109
22	58	67	57	843	3079	85	50541620165	179916121591
23	25	47	57	16	4113	86	47	431
23	34	47	58	58953	65657	87	114	523
25	3978	4651	59	681	709	87	141	1567
26	51	131	59	235	827	87	12	1741
27	61	81	59	3100	3541	88	14	89
27	193	379	60	46	143	88	103	267
28	26	29	60	98	793	89	149	179

28	55	87	61	2051096448	4459734401	89	43670	159311
29	10907	21577	62	865	1117	89	3167668	6956597
30	3	31	63	263384	3093931	90	277	297
30	34	93	64	183585	204353	90	34	837
30	79	99	65	75	131	90	589	2341
31	13318	46811	65	136	393	91	738933342073	1004948196253
32	321	449	66	13	67	92	37	277
33	142	207	66	63	67	92	37494	156217
33	1321	1453	66	130	201	92	8785646	43272109
34	226	613	67	9395	13267	93	5190225171	6517097017
35	11358	26881	67	1126141	3330973	94	32105	67399
36	23	73	68	256885	442069	95	521	571
36	7	351	69	25	423	95	575911512	7533294421
37	67	149	69	34	423	96	51222	207073
37	73	149	69	2469658	14323159	97	223	971
38	724	1483	70	3929	7351	97	10308	43457
39	142	477	71	112633599223	203878759789	97	59953829	100062679
39	11	729	72	397	1297	98	394	491
40	47	241	73	256	293	98	28608	34693
41	1650854	2135117	73	633740683	1494570611	99	8264954137	30152894311
42	124	379	74	675378	1385429	100	1582139	3273601
43	136	173	75	121	151			
44	252	4357	76	1105489	2033989			
45	34376	35281	77	170	617			

[a] $\phi(i) \equiv x^i \pmod{m}$.

virtually all cases a prime divisor p of r with $p > n$ exists. If such a prime does not exist, we look for a prime divisor p_1 of r such that $p_1^2 > n$ and seek an embedding of $\{1,2,4\}$ mod n in the group $C_p \times C_p$. This is usually easy to obtain, but does involve some ad hockery. Finally, if we do not have such a p, we look for integers m such that $n \mid \lambda(m)$, solve $f_2(x) = 0$ in Z_m, and if solutions exist check if any of the roots satisfy $1 + x + x^3 \equiv 0$ mod m. In general, this does not work, but with a computer package such as MAPLE we can go through a large list of values of m, and we have usually been successful in finding an m that works.

4. SUMMARY OF RESULTS FOR $\{0,1,3\}$ mod n

First $n \geqslant 7$, since otherwise $(0,1,3)$ does not have distinct differences. For $n = 7$, it has been shown in [7] that there is no injection of the design in any cyclic group or any direct product of two finite cyclic groups. There is an injection into $C_2 \times C_2 \times C_2$ as follows: $\varphi(0) = (1,0,0)$, $\varphi(1) = (0,1,0)$, $\varphi(2) = (0,0,1)$, $\varphi(3) = (1,1,0)$, $\varphi(4) = (0,1,1)$, $\varphi(5) = (1,1,1)$, $\varphi(6) = (1,0,1)$. For $n = 8$, there is no embedding in any cyclic group, but there is an embedding into $C_3 \times C_3$ given by $\varphi(0) = (1,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,2)$, $\varphi(3) = (2,2)$, $\varphi(4) = (2,0)$. It is known that when the configuration $\{0,1,3\}$ mod 8 is drawn on a complex cubic curve, the vertices are eight of the nine points of inflection of the curve (cf. [2, pp. 101–102]). The ninth point on the cubic corresponds to the point $(0,0)$ of $C_3 \times C_3$. The eight points of the configuration together with this ninth point are the points of an affine plane of order 3. For the remaining values of $n \leqslant 100$ there are embeddings in groups of prime order except for $n = 14, 24, 60$. For $n = 60$ there are embeddings into each of the groups C_{143} and C_{793}. For $n = 14$ there is no embedding in any cyclic group or direct product of two cyclic groups (see [6]). For $n = 24$ there is an embedding in $C_9 \times C_9$ defined by $\varphi(0) = (1,0)$, $\varphi(1) = (0,1)$, and $\varphi(2) = (1,2)$ with remaining images determined by the collinearity conditions. Table 2 gives embeddings in cyclic groups for all $n \leqslant 100$ when such mappings exist. The table is not exhaustive, but does include all embeddings in groups of prime order. Incidentally, the number of embeddings of the configuration $\{0,1,3\}$ mod n for a fixed n in a prime order group is finite. In fact, it is very small, and the order of the group may be large with respect to n. As an example, for $n = 71$ there is exactly one mapping and the order of the group is 203,878,759,789. An embedding into a group of prime order will fail to exist only when the prime power decomposition of the Bezout resultant contains no prime factor greater than n.

REFERENCES

1. C. H. Clemens, *A Scrapbook of Complex Curve Theory*, Plenum, New York, 1980.
2 D. Hilbert and S. Cohn-Vossen, *Geometry and the Imagination*, Chelsea, New York.
3 J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford U.P., 1979.
4 N. S. Mendelsohn, R. Padmanabhan, and Wolk, Representations of Desargues and Pappus-like designs on cubic curves, to appear.
5 R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.
6 S. Carmichael, *The Theory of Numbers*, Dover.
7 N. S. Mendelsohn, R. Padmanabhan, and Wolk, Designs embeddable in a plane cubic curve, *Note Mat.* VII:113–148 (1987).

Received 5 February 1988; final manuscript accepted 19 September 1988