Uniqueness of the Projective Plane of Order Eight

1. Introduction. A finite projective plane with n+1 points on each of its lines is said to be of order n. Such planes are known to exist whenever n is a prime or prime power, there being at least the Desarguesian plane coordinatized by the finite field with n elements [8]. For some time it has been known [9] that for order 9 there are some non-Desarguesian planes. It is an easy exercise to construct the planes of orders 2, 3, 4, and 5 and to verify that they are unique. The results of Bruck and Ryser [1] include as a special case the nonexistence of planes of order 6 although this special case had been shown earlier by Tarry [7]. The combined results of Pierce [5] and Hall [2] show the uniqueness of the plane of order 7. In this paper we show the uniqueness of the plane of order 8, thus showing that 9 is the smallest order of a non-Desarguesian plane.

The demonstration of the uniqueness of the plane of order 8 is based on Norton's complete list of Latin squares of order 7 [4], there being a total of 147 varieties of these, an omission in Norton's list having been found by Sade [6]. By a theoretical argument it is necessary to consider only 100 of these, and machine calculations, described in section 4 of this paper carried out on SWAC at the University of California, Los Angeles, went far enough so that it was not difficult to complete the work by hand. The completion of the search is given in section 5 of this paper.

2. Theoretical basis for calculation. Let A, B, C be the vertices of a triangle in a plane of order n. Call AB the line at infinity L_{∞} , AC the line x=0, and BC the line y=0. Label the n-1 remaining lines through A as x=1, x=2, \cdots , x=n-1 in any order and also the n-1 remaining lines through B as y=1, \cdots , y=n-1 in any order. A point B not on B0 will then lie on a unique line B1 and a unique line B2. Then assign to B3 the coordinates B3.

The n-1 lines through C=(0,0) apart from AC and BC will intersect each of $x=1,\cdots,x=n-1$ once and each of $y=1,\cdots,y=n-1$ once. Such a line L will intersect L_{∞} in some infinite point and will also contain (0,0) and n-1 points (i,j) where i and j take values 1 to n-1. With L associate the permutation $\begin{pmatrix} 0,1,\cdots,n-1\\0,a_1,\cdots,a_{n-1} \end{pmatrix}$ if $(0,0),(1,a_1),\cdots,(n-1,a_{n-1})$ are the finite points of L. The n-1 different L's yield permutations:

and the array (2.1) will form a Latin square of order n-1. Since a line through C intersects each of $y=1, \dots, y=n-1$ once, each row of (2.1) contains each of $1, \dots, n-1$ once. Since a line x=i intersects the n-1 L's in different points the i-th column will contain each of $1, 2, \dots, n-1$ once. The three constraints, row, column, digit correspond respectively to a line through C, a line x=i and

a line y = j. The interchanging of these three constraints corresponds therefore to an interchange of the roles of the vertices A, B, C in the construction of het Latin square. A permutation of the rows is merely a permutation of the order in which the lines through C are taken. A permutation of the columns corresponds to a relabeling of the lines x = c through A and a substitution on the digits corresponds to a relabeling of the lines y = c through B. Thus, these equivalent forms of Latin squares obtained by permuting rows, permuting columns, and substituting on digits, amount to no more than relabeling the lines of the three-net of pencils through the vertices of a triangle A B C excluding the sides. And an interchange of constraints corresponds to altering the roles of the vertices A, B, C in obtaining the square (2.1). It is immediate that any Latin square of order n-1 may be used as an array (2.1) corresponding to a three-net of the pencils through three points A, B, C excluding the sides. It is not immediate nor even true that any Latin square yields a three-net which can be extended to a complete plane. (However, for countably infinite planes this and more is true.) $\lceil 3 \rceil$.

Norton [4] has given a list of the Latin squares of order seven to within the equivalences of permuting rows, columns, substituting digits and interchanging the constraints. Norton lists 146 varieties. Sade [6] found an omission and verified that with this additional variety included the list is complete.

These 147 squares form the starting point in our search for planes of order 8. We seek to complete these by adding as many as possible additional lines not through A, B, or C. It is however sufficient to treat only 100 of the 147, effecting a saving of approximately one-third of the machine time. Norton lists his squares according to the number of intercalates which they contain, an intercalate being a sub-array of the type:

$$(2.2) \qquad \begin{array}{ccc} a & \cdots & b \\ & \cdot & & \cdot \\ & \cdot & & \cdot \\ & \cdot & & \cdot \\ & b & \cdots & a \end{array}$$

If the columns of the intercalate (2.2) are the *i*-th and *j*-th then the four points (i, a), (i, b), (j, a), and (j, b) are such that no three lie on a line and so they form a quadrilateral. The diagonal points of this quadrilateral are the points A, B, C. Conversely if A, B, C are the diagonal points of a quadrilateral these four points yield an intercalate in the array (2.1). Now in a plane of order 8 there are $73 \cdot 72 \cdot 64 \cdot 49/1 \cdot 2 \cdot 3 \cdot 4$ quadrilaterals and there are $73 \cdot 72 \cdot 64/1 \cdot 2 \cdot 3$ triangles. Now for some quadrilaterals the diagonal points may lie on a line. (Indeed in the Desarguesian plane of order 8 this is always the case.) Thus the triangles of a plane of order 8 are diagonal points of quadrilaterals at most $73 \cdot 72 \cdot 64 \cdot 49/1 \cdot 2 \cdot 3 \cdot 4$ times and as there are $73 \cdot 72 \cdot 64/1 \cdot 2 \cdot 3$ triangles there must be a triangle A, B, C which yields a square with at most 49/4 intercalates and thus at most 12 intercalates. Hence in constructing a plane of order 8 we may start from a square of order 7 with at most 12 intercalates. Such squares are numbers 1 through 99 of Norton's list and the omission found by Sade.

3. Completion of squares to the full plane. The one hundred squares of order 7 used in the search for planes of order 8 could all be normalized so that the first

two lines read, adding an initial 0 for C = (0, 0),

It is sufficient to deal with the finite points (i, j) $i, j = 0, 1, \dots, 7$ constructing an affine plane of order 8 since the completion to a projective plane by adding infinite points and L_{∞} is trivial. The pencil through (1, 1) will include the lines x = 1, y = 1 and the line $0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7$ of (3.1). The remaining lines through (1, 1) will go through the points (2, 3), (3, 4), (4, 5), (5, 6),and (6, 7) of the second line of (3.1) and there will also be a line through (1, 1) parallel to the second line of (3.1). These six lines will thus have the appearance:

Here X's stand for digits to be filled in. Similarly when the six lines of (3.2) have been added to the lines given by one of the 100 squares there will be five more lines of the pencil through (2,3) whose appearance will be:

Earlier calculations of the lines of (3.2) were made on the Engineering Research Associates 1101 Computer. For each of the 100 squares a number of possibilities for (3.2) was found, there being between 20 and 25 for each of the 100 squares on the average. In this search the 1101 was used to perform somewhat complicated sorting procedures. Of the 7! = 5040 permutations of the form $X \ 1 \ X \ X \ X \ X$ there are 1478 which are consistent with (3.1) in that they do not agree with either line of (3.1) in as many as two places. These are distributed as follows:

The set of 5040 permutations was easily built up on punched cards and the 1478 consistent cards were sorted from these. These 1478 permutations were taken as input for the ERA 1101 and were handled in two stages. In the first stage permutations were eliminated which were inconsistent with any one of the five remaining lines of a particular square and the consistent lines were punched as

output on tape. For each of the squares the number of consistent lines was approximately 115 to 120. This was a fast code, most of the time being taken up by punching outputs, and averaged about three minutes for each square. The second stage involved taking the 115 to 120 consistent lines for each square and forming the six lines (3.2) from these in every possible way. This was relatively slow taking about half an hour for each square and yielding, as remarked above, about twenty solutions for each square. In every case tried, except for the Desarguesian plane, only three or four further lines could be added. But working by hand it took at least an hour to test the construction of further lines given a square and the lines of (3.2).

4. Description of the SWAC code. Making one hundred separate runs SWAC took each 7×7 square with no more than twelve intercalates and constructed the six lines of (3.2) and the five lines of (3.3), punching them as output whenever all eleven were found. The method employed was to try, for each of the X's in (3.2) and (3.3), all possibilities $0, 1, \dots, 7$ compatible with previously assigned X's. To specify the criteria of compatibility let $P_i(j)$ be the j-th element of the i-th row of the 7×7 square augmented by an initial column of zeros, and $P_i'(j)$ the similar element of (3.2).

For any (i, j) referring to an X in (3.2) all $P_{k'}(l)$ with k < i or with k = i and l < j will be assumed already assigned. The restrictions on $P_{i'}(j)$ are then

- (a) $P_{i}'(j) \neq 1$,
- (b) $P_i'(j) \neq i + 2 \text{ if } i < 6$,
- (c) $P_i'(j) \neq P_i'(l)$ for any l < j,
- (d) $P_i'(j) \neq P_k'(j)$ for any k < i,
- (e) If for any l < j or l = 2 or l = i + 2 we have $P_i'(l) = P_k(l)$, then $P_i'(j) \neq P_k(j)$.

The first three conditions insure that each row of (3.2) is a permutation. The last two prevent any such row from agreeing in two positions with any previous row of (3.2) or any row of the 7×7 square.

For an element $P_{i}''(j)$ of (3.3) we have conditions like these plus an additional condition similar to (e) but with P replaced by P'. In the following discussion we shall consider only the assignment of the $P_{i}'(j)$; the case of the $P_{i}''(j)$ is more complicated due to the extra condition but is basically the same.

To apply these criteria we construct the set of allowable values of $P_i(j)$. If

$$S^* = \{1\} \ \bigcup \ \left\{ \begin{array}{ll} \{i+2\} & \text{if} & i < 6 \\ \phi & \text{if} & i = 6 \end{array} \right\} \ \bigcup \ \{P_i'(l) \ | \ l < j\},$$

then any $P_i'(j)\epsilon \bar{S}^*$ (the complement of S^*) will satisfy (a), (b), and (c). Similarly (d) and (e) will be satisfied if $P_i'(j)\epsilon \bar{S}_j$, where

$$S_{j} = \{ P_{k}'(j) | k < i \} \bigcup \{ P_{k}(j) | P_{k}(2) = 1 \text{ or } P_{k}(i+2) = i+2$$
or $P_{k}(l) = P_{i}'(l) \text{ for some } l < j \}.$

(Because of (3.1) the conditions $P_k(2) = 1$ and $P_k(i+2) = i+2$ imply k=1 and k=2 respectively. This convenient simplification is not essential.) Hence $S = \bar{S}^* \cap \bar{S}_j$ is the set of values of $P_i'(j)$ compatible with those already assigned. To select a $P_i'(j)$ one computes S^* , S_j , and S. Suppose first that S is not

empty. Then $P_{i'}(j)$ is taken to be the smallest element of S, and one moves on to the next unfilled position in (3.2). If this position is in the same row S^* is replaced by $S^* \cup \{P_{i'}(j)\}$, j replaced by j+1 (or j+2 if j=i+1), and the new S_j calculated. On moving to a new row i is increased by 1, j put equal to 1, and S^* set equal to $\{1, i+2\}$ if i < 6 or $\{1\}$ if i = 6. When (3.2) is completely filled one starts a similar process in (3.3); when this is filled one records all the $P_{i'}(j)$ and $P_{i''}(j)$.

Suppose now that for some (i, j) the corresponding S is empty. This means that the previously assigned $P_{i'}(j)$'s must be changed. One therefore "backtracks," returning to the previously considered $P_{i}(j)$ by reducing j or, if necessary to move up to the preceding row, by reducing i and putting j = 8. In the former case one gets back the old S^* by removing the element $P_{i'}(j)$; in the latter one puts $S^* = \{0, 1, \dots, 7\}$. The old S_i could be re-computed, or it could have been saved from the time of its previous use. Since the calculation of S_i is somewhat complicated, and since there is much back-tracking and advancing within a row but not much between rows, it was decided to save the S_i within each row but to re-compute them on back-tracking to another row.

After back-tracking and re-computing S one must of course avoid selecting from S the same $P_{i'}(j)$ that had been used before. This is accomplished by removing from S all elements less than or equal to the $P_{i'}(j)$ that was last used. In this way the successive selections of $P_{i'}(j)$ for a given (i, j) are strictly increasing until all possibilities are exhausted and one backtracks still farther.

After a solution is recorded the process is continued by the standard backtracking procedure, just as if one had proceded to a next step and found $S = \phi$. The whole process stops when all possibilities for $P_1'(1)$ have been exhausted.

In applying a routine of this sort it is obviously advantageous to eliminate many possibilities early in the process. In particular, in each row of (3.2) it is helpful if S_i is as large as possible for small j. In the set-up as described

$$S_1 = \{ P_k'(1) | k < i \} \cup \{ 0 \}.$$

However if we make a cyclic permutation of columns so that the first element of each row becomes the last we get

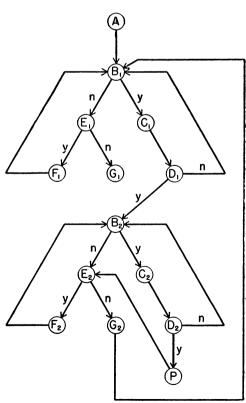
$$S_1 = \{P_k'(1) | k < i\} \cup \{1, 2\}.$$

This slightly better situation was used in the coding.

In coding this process for SWAC the significant factor was the small (256 word) high-speed memory (HSM). The program had to be stored on the magnetic drum and appropriate parts transferred to the HSM when needed. Fortunately it was just possible to squeeze into the HSM the whole procedure for handling the $P_i'(j)$ and also for the $P_i''(j)$. The delays due to drum transfers entered only in the transfer from one of these routines to the other, and in the negligible number of input and output processes. Elements of a set were represented by positions within a word; i.e., the subset $\{a_1, a_2, \dots\}$ of $\{0, 1, \dots, 7\}$ was represented by the number $\sum 2^{-a_i-1}$. This representation makes it easy to code the set operations of union, intersection, and picking the smallest element.

The general flow of the code may be described by considering fourteen subroutines as follows:

D4:	Possible	Oi Dfi	Criterion for	Successor		
Routine	Predecessors	Operation Performed	Successor	Yes	No	
Α	(G_1) (New run)	Input given square, cata- logue it by element and position	_	B_1	B_1	
B_1	A, D_1, F_1, G_2	Compute possible values available for new position	Are any values avail- able?	C_1	E_1	
C_1	B_1	Store first available value in proper position	_	D_1	D_1	
D_1	C_1	Advance position	Is first set of lines complete?	B_2	B_1	
E_1	B_1	Test whether backtrack is possible	Is a position open in which to back- track?	F_1	G_1	
F_1	E_1	Backtrack. Go back to nearest available posi- tion and recompute		B_1	B_1	
G_1	E_1	Halt or input new square		(A)	(A)	
B_2	D_1 , D_2 , F_2	As in B_1	As in B_1	C_2	E_2	
C_2	B_2	As in C_1		D_2	D_2	
D_2	C_2	As in D_1	Is second set of lines complete?	P	B_2	
E_2	B_2	Test whether backtrack would carry back into first six lines formed	Is backtrack in last five lines possible?	F_2	G_2	
$\boldsymbol{F_2}$	E_2	Backtrack as in F_1		B_2	B_2	
G_2	E_2	Backtrack to next to last position of first six lines		B_1	B_1	
P	D_2	Punch 11 lines		E_2	E_2	



5. Results of calculations. For only one of the hundred 7×7 squares was it possible to construct the six lines of (3.2) and the five of (3.3). This was Square Number 1:

and four sets of eleven lines were found for this. The computing time for a square varied from eight to fifteen minutes, averaging about twelve minutes.

The four ways of adding the eleven lines to Square Number 1 are:

1	2
2 1 3 5 7 0 4 6	2 1 3 5 7 0 4 6
5 1 6 4 3 7 2 0	3 1 7 4 6 2 5 0
6 1 7 0 5 4 3 2	7 1 0 6 5 4 3 2
4 1 0 7 2 6 5 3	5 1 4 7 2 6 0 3
3 1 4 6 0 2 7 5	6 1 5 2 0 3 7 4
7 1 5 2 6 3 0 4	4 1 6 0 3 7 2 5
5 6 3 7 4 1 0 2	1 7 3 6 4 2 0 5
6 7 3 1 0 5 2 4	7 0 3 1 6 5 2 4
4 0 3 2 1 7 6 5	5 4 3 2 1 7 6 0
1 4 3 0 6 2 5 7	6 5 3 0 2 4 1 7
7 5 3 6 2 4 1 0	4 6 3 7 0 1 5 2
3	4
3 2 1 3 6 0 7 5 4	4 2 1 3 7 6 4 0 5
	-
2 1 3 6 0 7 5 4	2 1 3 7 6 4 0 5
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3 7 1 4 0 5 3 2 6	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6 6 1 0 2 5 7 4 3
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3 7 1 4 0 5 3 2 6 4 1 0 2 7 6 3 5	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6 6 1 0 2 5 7 4 3 3 1 7 5 0 6 2 4
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3 7 1 4 0 5 3 2 6 4 1 0 2 7 6 3 5 3 1 6 5 2 4 7 0	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6 6 1 0 2 5 7 4 3 3 1 7 5 0 6 2 4 5 1 4 6 3 2 7 0
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3 7 1 4 0 5 3 2 6 4 1 0 2 7 6 3 5 3 1 6 5 2 4 7 0 6 1 5 7 3 0 4 2	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6 6 1 0 2 5 7 4 3 3 1 7 5 0 6 2 4 5 1 4 6 3 2 7 0 4 1 6 0 7 3 5 2 1 5 3 0 4 7 2 6 7 0 3 6 1 5 4 2
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3 7 1 4 0 5 3 2 6 4 1 0 2 7 6 3 5 3 1 6 5 2 4 7 0 6 1 5 7 3 0 4 2 6 7 3 0 4 2 1 5	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6 6 1 0 2 5 7 4 3 3 1 7 5 0 6 2 4 5 1 4 6 3 2 7 0 4 1 6 0 7 3 5 2 1 5 3 0 4 7 2 6
2 1 3 6 0 7 5 4 5 1 7 4 6 2 0 3 7 1 4 0 5 3 2 6 4 1 0 2 7 6 3 5 3 1 6 5 2 4 7 0 6 1 5 7 3 0 4 2 6 7 3 0 4 2 1 5 1 4 3 7 2 5 0 6	2 1 3 7 6 4 0 5 7 1 5 4 2 0 3 6 6 1 0 2 5 7 4 3 3 1 7 5 0 6 2 4 5 1 4 6 3 2 7 0 4 1 6 0 7 3 5 2 1 5 3 0 4 7 2 6 7 0 3 6 1 5 4 2

Of these the first two cannot be completed to planes while the third and fourth can both be completed uniquely to planes, the completion being the unique Desarguesian plane in both cases. Indeed the second is equivalent to the first so far as completion is concerned since if we interchange coordinates, replacing (x, y) by

$$(y, x)$$
 and then renumber according to the substitution $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 6 & 4 & 2 & 7 & 5 & 3 \end{pmatrix}$ the

In the fourth case if we interchange coordinates, replacing (x, y) by (y, x) and then renumber all coordinates according to the substitution $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 7 & 3 & 6 & 2 & 5 \end{pmatrix}$, Square Number 1 is unaltered and the first six lines of the fourth case become the first six lines of the third case, whence these two cases must lead to the same completions. The completion is unique and is the Desarguesian plane. In the third case this may be written:

```
0 1 2 3 4 5 6 7
1 0 6 4 3 7 2 5
2 6 0 7 5 4 1 3
3 4 7 0 1 6 5 2
4 3 5 1 0 2 7 6
5 7 4 6 2 0 3 1
6 2 1 5 7 3 0 4
7 5 3 2 6 1 4 0,
```

along with six other 8×8 squares whose top rows are the remaining lines of Square Number 1 and whose columns are the same as those of the 8×8 square above. This finally shows the uniqueness of the plane of order 8.

Although it has already been remarked that the first two cases above cannot be completed to full planes, it is a curious fact that a great many consistent lines may be added. These are listed here:

0 1 2 3 4 5 6	7	0	2	3	4	5	6	7	1
1 0 4 7 5 3 2	6	3	6	0	5	1	4	2	7
2704613	5	6	4	2	7	3	0	1	5
7 5 3 6 2 4 1							3		
0 3 4 5 6 7 1	2	0	4	5	6	7	1	2	3
1 2 6 3 7 4 0	5	3	2	1	7	6	5	4	0
4 1 0 7 2 6 5	3	4	0	3	2	1	7	6	5
6 7 3 1 0 5 2	4	6	1	7	0	5	4	3	2
0 5 6 7 1 2 3	4	0	6	7	1	2	3	4	5
2 1 3 5 7 0 4	6	1	4	3	0	6	2	5	7
5021647	3	2	3	5	7	0	4	6	1
7 3 1 0 4 6 2	5	5	1	6	4	3	7	2	0
0 7 1 2 3 4 5	6								
3 1 4 6 0 2 7	5								
4 5 7 3 6 0 2	1								
	1								

Thus we have half of seven 8 X 8 squares. In projective terms we have a total of 45 lines with 9 points on a line which are consistent with themselves but which cannot be completed to the 73 lines of a projective plane.

MARSHALL HALL, JR.

Ohio State University Columbus, Ohio

J. DEAN SWIFT

University of California Los Angeles, California

ROBERT J. WALKER

Cornell University Ithaca, New York

This research was supported by the National Science Foundation and the Office of Naval Research.

Research.

1. R. H. Bruck & H. J. Ryser, "The nonexistence of certain finite projective planes," Canadian Jn. Math., v. 1, 1949, p. 88–93.

2. Marshall Hall, Jr., "Uniqueness of the projective plane with 57 points," Am. Math. Soc., Proc., v. 4, 1953, p. 912–916; Correction to "Uniqueness of the projective plane with 57 points," Am. Math. Soc., Proc., v. 5, 1954, p. 994–997.

3. D. R. Hughes, "Additive and multiplicative loops of the planar ternary rings," Am. Math. Soc., Proc., v. 6, 1955, p. 973–980.

4. H. W. Norton, "The 7 × 7 squares," Ann. Eugenics, v. 9, 1939, p. 269–307.

5. W. A. Pierce, "The impossibility of Fano's configuration in a projective plane with eight points per line," Am. Math. Soc., Proc., v. 4, 1953, p. 908–912.

6. A. Sade, "An omission in Norton's list of 7 × 7 squares," Annals Math. Statistics, v. 22, 1951, p. 306–307.

6. A. SADE, "An omission in Norton's list of 7 x 7 squares," Annals Math. Statistics, v. 22, 1951, p. 306-307.
7. G. Tarry, "Le problème des 36 officiers," Compte Rendu de l'Association Française pour l'Avancement de Science Naturel," v. 1, 1900, p. 122-123; v. 2, 1901, p. 170-203.
8. O. Veblen & W. H. Bussey, "Finite projective geometries," Am. Math. Soc., Trans., v. 7, 1906, p. 241-259.
9. O. Veblen & J. H. Maclagan-Wedderburn, "Non-Desarguesian and non-Pascalian geometries," Am. Math. Soc., Trans., v. 8, 1907, p. 379-388.

On the Location of Gauss Sums

We shall understand by a generalized Gauss sum of order k the sum

$$S_k = \sum_{m=0}^{p-1} \exp(2\pi i m^k/p), \quad (p = kf + 1, \text{ a prime}).$$

This sum can be thought of as the principal root z_0 of the reduced period equation of degree k for the so-called f-nomial periods, $z_i = k\eta_i + 1$, where, as usual,

$$\eta_i = \sum_{k=0}^{f-1} \exp(2\pi i g^{k\nu+i}/p) \quad (i=0,1,\dots,k-1).$$

Since the remaining k-1 roots of the period equation depend on the primitive root g, the singling out of one root z_0 as the principal root is justifiable.

For k = 2, it is well known that [1]

(1)
$$S_2 = \begin{cases} \sqrt{p} & \text{if } p = 4n + 1 \\ i\sqrt{p} & \text{if } p = 4n - 1. \end{cases}$$