8. A *Steiner quadruple system* is a BIBD (v, k, λ), with $k = 4$ and $\lambda = 1$. Show that $v = 12n + 1$ or $12n + 4$. Generalize. [*Hint:* See Problem 3.]

9. a) Write the code words in the code based on the (7, 3, 2) BIBD of Example 3. How many errors can this code detect? How many can it correct?

b) Repeat part (a) for the code based on the affine plane of order 3, a BIBD (9, 3, 1).

10. You can add rows to the incidence matrix given in the text in a way that doesn't give a BIBD. For example, you can add rows that have four or more 1s. By Theorem 7.3.3, if the Hamming distance between any two (new and old) code words is at least 3, you will still be able to correct a single error while having more code words.

a) Explain why, if you want to be able to correct single errors, there is no point in adding code words with one, two, or three 1s.

b) Find all seven code words with four 1s that have a Hamming distance of at least 4 from each other and from the seven code words in the original matrix. How do these new code words relate to the code words?

c) Find the two other code words that are a Hamming distance of at least 3 from each other and the 14 already found.

d) Suppose that you have a set of n code words, each a seven-dimensional vector of 0s and 1s, and that each code word is a Hamming distance of at least 3 from every other code word. Find the total number of vectors possible (including code words and noncode words). Explain why every code word has seven vectors at a Hamming distance of 1 from it. Explain why n can be no larger than 16.

7.4 Finite Analytic Geometry

We can imitate the analytic geometry and transformations presented in Chapters 4 and 6 for finite geometries whenever we have algebraic structures corresponding to the arithmetic of the real numbers. Finite fields provide the analog that we use, although a more general approach is possible. (See Blumenthal [4].) Fields are number systems having many of the familiar properties of the four usual operations of addition, subtraction, multiplication, and division. Although there are other fields, we concentrate on the fields of integers modulo a prime number. (See Gallian [6] for more information on fields.)

Example 1 Let $\mathbf{Z}_3$ be the set $\{0, 1, 2\}$ together with addition and multiplication modulo 3. That is, after doing the usual arithmetic, we subtract multiples of 3 until we get back to a number in the given set. For example, $2 + 2 = 4$ becomes 1 $(mod\ 3)$ because $4 - 3 = 1$. We write $2 + 2 \equiv 1\ (mod\ 3)$. Think of the three numbers in the set placed around a circle (Fig. 7.8). The following tables give all additions and multiplications. $\mathbf{Z}_3$ is a field.

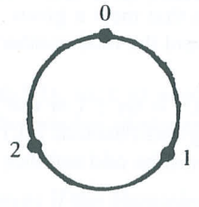

Figure 7.8

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

●

Example 2 Let $\mathbf{Z}_5$ be the set $\{0, 1, 2, 3, 4\}$ together with addition and multiplication modulo 5, given in the following tables. For example, $3 \times 4 \equiv 2\ (mod\ 5)$ because $3 \times 4 = 12 \equiv 12 - 5 - 5 = 2\ (mod\ 5)$. $\mathbf{Z}_5$ is a field.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

●

Definition 7.4.1 By $\mathbf{Z}_n$ we mean the set $\{0, 1, \ldots, n - 1\}$ together with addition and multiplication modulo n. That is, after doing the usual arithmetic, we subtract multiples of n until we get back to a number in the given set.

Example 3 Although $\mathbf{Z}_4$ satisfies many familiar algebraic properties, it misses one of the defining properties to qualify as a field. The number 2 doesn't have a multiplicative inverse. That is, none of the numbers in the set $\{0, 1, 2, 3\}$ when multiplied by 2 and reduced modulo 4 give us 1, the multiplicative identity. Thus we can't divide by 2. We leave the addition and multiplication tables for $\mathbf{Z}_4$ as an exercise. ●

Theorem 7.4.1 $\mathbf{Z}_p$ is a field iff p is a prime. There is, up to isomorphism, exactly one field with p^k elements, where p is a prime number.

Proof. See Gallian [6, 213 and 328]. ■

We can use any field to form an analytic model of affine or projective geometries, just as we did with the real numbers in Chapters 4 and 6. The number of elements in a field is its *order* and equals the order of the corresponding affine or projective plane. Using algebra, we can develop matrices with entries from any field to describe the affine transformations and collineations of the corresponding geometries. As in Chapter 4, we need three coordinates for points so that the transformations can move the origin. For a field $\mathbf{F}$, $\mathbf{F}^3$ is the three-dimensional vector space over $\mathbf{F}$. If you are familiar with abstract algebra, you can show that the affine planes defined (and projective planes defined later) do indeed satisfy the axioms of Section 7.2. The proofs that these systems satisfy the axioms follow the proofs for the usual analytic models using the real numbers. (See Karteszi [7].)

Definition 7.4.2 Given a field $\mathbf{F}$, define $\mathbf{AF}^2$, the *affine plane over* $\mathbf{F}$, as follows. The *points* of $\mathbf{AF}^2$ are column vectors $(x, y, 1)$ of $\mathbf{F}^3$, and the *lines* are row vectors $[a, b, c]$ from $\mathbf{F}^3$, where a and b are not both 0. Two row vectors represent the same line iff one is a scalar

multiple of the other by a nonzero element of **F**. A point $(x, y, 1)$ is *on* a line $[a, b, c]$ iff $ax + by + c1 \equiv 0 \ (mod\ 5)$.

Example 4 The 25 vectors of $\mathbf{AZ}_5^2$ form an affine plane of order 5. To find the line through points $(2, 2, 1)$ and $(1, 4, 1)$, we need to solve the system of two equations $a \cdot 2 + b \cdot 2 + c \cdot 1 \equiv 0 \ (mod\ 5)$ and $a \cdot 1 + b \cdot 4 + c \cdot 1 \equiv 0 \ (mod\ 5)$. The solution is $[3, 4, 1]$ or any of its multiples, modulo 5, such as $[2 \cdot 3, 2 \cdot 4, 2 \cdot 1] \equiv [1, 3, 2] \ (mod\ 5)$. (Note that the Euclidean line through $(2, 2)$ and $(1, 4)$ is $y = -2x + 6$, which becomes $[2, 1, -6]$ and, by multiplying by 4, is equivalent to $[3, 4, 1]$ modulo 5.) Figure 7.9 illustrates the five lines $[m, 4, 0]$ through the origin, more familiarly known as $y = mx$. (In $\mathbf{Z}_5$, 4 acts as -1 does in ordinary arithmetic.) Each line can be considered to cycle both horizontally and vertically, as the numbers in $\mathbf{Z}_5$ cycle. For example, line $[2, 4, 0]$ goes over 1 and up 2 from one point to the next: $(0, 0, 1)$, $(1, 2, 1)$, $(2, 4, 1)$, $(3, 1, 1)$, $(4, 2, 1)$, and back to $(0, 0, 1)$. The "vertical" line $[1, 0, 0]$ provides the sixth line through the origin guaranteed by Theorem 7.2.3. Every other point $(x, y, 1)$ also has six lines on it, each parallel to one of these six. ●

Exercise 1 Give algebraic conditions for two lines $[a, b, c]$ and $[a', b', c']$ to be parallel. Verify that two such lines are equal or don't intersect.

As in Chapter 4, we represent affine transformations by 3×3 invertible matrices whose bottom row is [0 0 1]. For a field of order n, there are at most n^6 such matrices because only six entries aren't fixed, but not all are invertible. We can use the determinant of a matrix $(mod\ n)$ to determine whether that matrix is invertible. We use a combinatorial argument to find the number of invertible matrices with the bottom row of [0 0 1]. Again, as in Chapter 4, the images of points $(0, 0, 1)$, $(1, 0, 1)$, and $(0, 1, 1)$ determine an affine transformation. The condition that the matrix is invertible implies that these points must be mapped to three distinct points not all on the same line. For the field of order n, the affine plane has n^2 points and $(0, 0, 1)$ can be mapped to any of them. Once we know where $(0, 0, 1)$ goes, $(1, 0, 1)$ has $n^2 - 1$ places to go. For $(0, 1, 1)$ there remain $n^2 - n$ places to go because it can't be mapped to any of the n points on the line

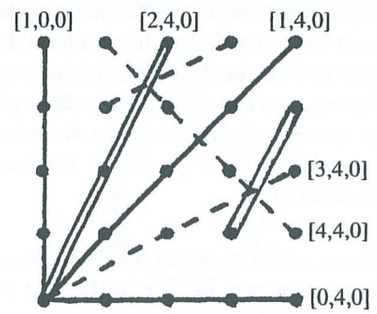

Figure 7.9 The lines through $(0, 0, 1)$ in $\mathbf{AZ}_5^2$.

through the other two points. Thus there are $n^2(n^2 - 1)(n^2 - n) = n^6 - n^5 - n^4 + n^3$ affine plane transformations over the field of order n.

Definition 7.4.3 For a field **F**, define $\mathbf{PF}^2$, the *projective plane over* **F**, as follows. The *points* of $\mathbf{PF}^2$ are the nonzero column vectors (x, y, z) of $\mathbf{F}^3$, where two vectors represent the same point iff one is a scalar multiple of the other by a nonzero element of **F**. The *lines* of $\mathbf{PF}^2$ are nonzero row vectors $[a, b, c]$ from $\mathbf{F}^3$, where two row vectors represent the same line iff one is a scalar multiple of the other by a nonzero element of **F**. A point (x, y, z) is *on* a line $[a, b, c]$ iff $ax + by + cz = 0$.

Example 5 Consider the projective plane $\mathbf{PZ}_3^2$ (Fig. 7.10). $\mathbf{Z}_3^3$ has $3^3 = 27$ vectors. The 26 nonzero vectors pair up to give 13 points because of the two nonzero scalars, 1 and 2. The figure emphasizes that $\mathbf{PZ}_3^2$ adds four points and one line to $\mathbf{AZ}_3^2$, which is represented in Fig. 7.3. As there are four points on each line, we can define both $H(AB, CD)$ and $AB//CD$ from Chapter 6 if A, B, C, and D are distinct collinear points. These definitions satisfy Axioms (i)–(vii) and (ix) of Chapter 6. ●

Exercise 2 Verify that Axioms (viii) and (x) of Chapter 6 fail in $\mathbf{PZ}_3^2$.

Recall that the transformations of the projective plane, called collineations, can be represented by invertible 3×3 matrices. As before, two matrices represent the same collineation if one is a nonzero scalar multiple of the other. As in Chapter 6, a collineation is determined by where it sends four points, no three of which are collinear. Problem 7 shows that $(n^2 + n + 1)(n^2 + n)(n^2)(n - 1)^2 = n^8 - n^6 - n^5 + n^3$ collineations exist for the projective plane over a field of order n.

Theorem 7.4.2 The set of affine transformations for $\mathbf{AF}^2$ and the collineations for $\mathbf{PF}^2$ each form a group.

Proof. We replace the specific field **R** with the general field **F** in the proofs of Theorem 4.4.5 and Theorem 6.4.3. ■

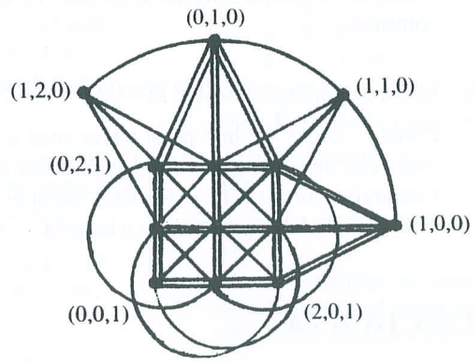

Figure 7.10 A representation of $\mathbf{PZ}_3^2$.

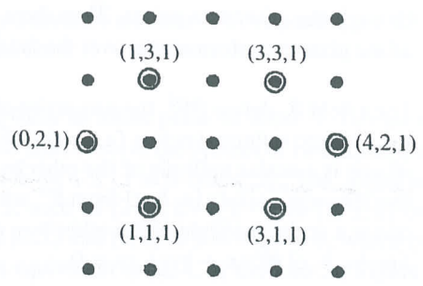

Figure 7.11 The oval $4x^2 + 2y^2 + 4x + 2y + 3 = 0$ in $\mathbf{AZ}_5^2$.

7.4.1 Ovals in finite projective planes

The preceding paragraphs indicate how well finite planes mimic many familiar geometric concepts. Mathematicians also have explored other traditional geometric concepts in a finite setting. In a finite plane a simple non-algebraic way to describe the analog to conics is to use ovals. In Euclidean geometry, no three points on a conic are collinear. For only a finite number of points, not very many sets can fulfill this property. Figure 7.11 shows a set of six points in $\mathbf{AZ}_5^2$ with no three on the same line. Some exploring will reveal that no other point can be added to this set. Indeed, in $\mathbf{AZ}_p^2$ and in $\mathbf{PZ}_p^2$, with $p > 2$, we can never find more than $p + 1$ points with no three points collinear. (When $p = 2$, all four points in $\mathbf{AZ}_2^2$ form a set with no three points collinear. We omit this special case.) Conveniently, these sets in $\mathbf{PZ}_p^2$ correspond to second-degree equations. A second-degree equation in an affine plane might give fewer than the expected number of points because an affine plane can be seen as the corresponding projective plane minus a line and its points. Therefore ovals, the analog to conics, are usually defined for projective planes. (See Beck et al. [2] and Karteszi [7, 110–119] for more information on ovals in projective planes and finite analytic geometry.)

Definition 7.4.4 In a projective plane of order n, an *oval* is a set of $n + 1$ points, no three of which are collinear. A line is *tangent* to an oval iff the line and the oval have just one point in common.

Theorem 7.4.3 Every point on an oval has exactly one tangent to the oval.

Proof. Let P be any point on an oval and $P_1, \ldots, P_n$ be the other points on the oval. The definition of an oval guarantees that the lines PP_i for $i > 0$ are all distinct, accounting for n of the $n + 1$ lines through P. The remaining line cannot intersect the oval except at P, so it must be a tangent. ■

PROBLEMS FOR SECTION 7.4

1. Use $\mathbf{AZ}_3^2$ in this problem.
   a) Find the line on (1, 2, 1) and (0, 1, 1).
   b) Find the intersection of the line in part (a) with [2, 2, 2].
   c) Draw a picture to illustrate the effect of the affine transformation $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ on the affine plane $\mathbf{AZ}_3^2$. Is the effect in $\mathbf{AZ}_3^2$ similar to the effect of that matrix on the real affine plane? Explain.
   d) Repeat part (c) for $\begin{bmatrix} 0 & 2 & 2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, and $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$.
2. Repeat Problem 1, using the affine plane $\mathbf{AZ}_5^2$. Generalize.
3. Suppose that you try to form an affine plane using $\mathbf{Z}_4$, which isn't a field.
   a) Find a line that doesn't have four points on it.
   b) Find two distinct lines with more than one point of intersection.
   c) Find two lines with different slopes but no points of intersection.
   d) Which of the axioms of an affine plane fail when you try to use Z_4?
   e) Repeat parts (a)–(d) for $\mathbf{Z}_6$, replacing *four* with *six* in part (a).
4. Use the projective plane $\mathbf{PZ}_7^2$ in this problem.
   a) Find the point on lines [2, 3, 1] and [3, 1, 4].
   b) Find a complete quadrangle, as defined in Section 6.1.
   c) For the three collinear points $P = (0, 0, 1)$, $Q = (1, 0, 1)$, and $R = (1, 0, 0)$, find a point S such that $H(PQ, RS)$, as defined in Section 6.1. Is S unique?
5. Repeat Problem 4, using the projective plane $\mathbf{PZ}_5^2$.
6. Define a projectivity in $\mathbf{PF}^2$. (See Section 6.4.) Count the number of projectivities if the field has order n. [*Hint:* See Theorem 6.4.1.]
7. Show that $(n^2 + n + 1)(n^2 + n)(n^2)(n - 1)^2 = n^8 - n^6 - n^5 + n^3$ collineations exist in a projective plane over a field of order n.
8. a) Find the points on the oval $x^2 + y^2 - z^2 = 0$ in $\mathbf{PZ}_3^2$. (For simplicity, you may assume throughout that $z = 0$ or $z = 1$.)
   b) Repeat for $x^2 + y^2 - 2z^2 = 0$ in $\mathbf{PZ}_3^2$.
   c) Describe the points not on either of the ovals in parts (a) and (b).
   d) Repeat for $x^2 + 2y^2 - kz^2 = 0$ in $\mathbf{PZ}_5^2$, where $k = 1, \ldots, 4$.
9. Find the points in the affine plane $\mathbf{AF}_5^2$ on ovals $x^2 + y^2 = 1$, $x^2 + 4y = 0$, and $x^2 + 3y^2 = 1$. Explain the difference in numbers of points.

PROJECTS FOR CHAPTER 7

1. a) In a BIBD explain why, if $\lambda > 0$, then $k \geq 2$. Explain why BIBDs with $k = 2$ are easy to construct but not particularly interesting.
   b) Use Theorem 7.3.1 to find all triples (v, k, λ) with $v \leq 25$ for which there could be a BIBD (v, k, λ) with $v > k > 2$ and $\lambda = 1$. [*Hint:* Explain why $k \leq 5$.]
   c) For each triple (v, k, λ) in part (b), try to construct a BIBD. Explore if a different (nonisomorphic) BIBD can have the same values for v, k, and λ.
   d) Try to construct BIBDs with $(v, k, 2)$ for $v \leq 19$ that aren't built from BIBDs with $(v, k, 1)$ by simple repetition.
2. Explore the affine and projective planes $\mathbf{AF}_4^2$ and $\mathbf{PF}_4^2$, where $\mathbf{F}_4$ is the field of order four with the following addition and multiplication.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

3. a) Define points and planes for the affine space $\mathbf{AF}^3$, where $\mathbf{F}$ is a field of order n.
   b) Count the number of points, lines, and planes in $\mathbf{AF}^3$.
   c) Count the number of affine transformations in $\mathbf{AF}^3$.
   d) Count the number of points and lines in $\mathbf{AF}^k$, the k-dimensional affine space over the field $\mathbf{F}$. [*Hint:* How many lines are there on each point?]
   e) Explain why the number of affine transformations in $\mathbf{AF}^k$ is $n^k \prod_{j=0}^{k-1}(n^k - n^j)$ if $\mathbf{F}$ is of order n.

4. **a)** Repeat Project 3, parts (a), (b), and (d) for projective spaces $\mathbf{PF}^3$ and $\mathbf{PF}^k$.
   b) Explain why $\mathbf{PF}^3$ has $(n^3+n^2+n+1)(n^3+n^2+n)(n^3+n^2)(n^3)(n-1)^3$ collineations.
5. Program a computer to search for projective planes of orders 4 and 5, using the symmetries of a regular polygon as in Section 7.3.
6. Define a point to be *exterior* to an oval if two tangents to the oval are on that point. Define a point to be *interior* to an oval if no tangents to the oval are on that point. Choose different ovals and find their interior and exterior points. Look for formulas counting the number of exterior and interior points for an oval in PZ_p^2. Prove your formulas.
7. Explore Desargues's theorem (see Section 6.1) in $\mathbf{PZ}_p^2$ for various $p > 2$. (Explain why Desargues's theorem isn't interesting in $\mathbf{PZ}_2^2$.) (Smart [9] has an axiomatization of Desargues's configuration, which is shown in Fig. 6.4.)
8. The axiomatic system for a *weak hyperbolic plane* has the undefined terms *point*, *line*, and *on* and the following axioms.
   i) Every two distinct points have exactly one line on them both.
   ii) There are at least four points with no three on the same line.
   iii) Given a line and a point not on that line, there are at least two lines on that point with no point in common with the given line.
   a) Show that any set of $n \geq 5$ points is a weak hyperbolic plane if you take the lines to be all subsets of two elements.
   b) Find a model of a weak hyperbolic plane with some lines having only one point on them.
   c) Find a model of a weak hyperbolic plane with six points, every line with at least two points on it, and two lines with different numbers of points on them.

   Define a *hyperbolic plane* to be a weak hyperbolic plane satisfying this stronger version of Axiom (iii):
   iii′) Given a line with n points on it and a point not on that line, there are exactly n lines through that point which do not have any point in common with the given line.
   d) Prove: If one line of a hyperbolic plane has n points on it, then all do. Find the number of points and lines in terms of n and prove your answers.
   e) Are your results in part (c) consistent with Theorem 7.3.1? Explain.
   f) Use a computer to find a model of a hyperbolic plane similar to that in Example 5 of Section 7.3, but with $k = 5$.
9. You can define a notion of distance in finite affine planes and so investigate isometries.
   a) For a prime p with $p = 4n+3$, define the distance in $\mathbf{AZ}_p^2$ between $(s, t, 1)$ and $(u, v, 1)$ to be $(s-u)^2+(t-v)^2$ $(mod\ p)$. For $p = 3$ and $p = 7$, verify that two distinct points have a nonzero distance between them. How many points are at each possible distance from a given point? Do the points at a given distance from a point form an oval ("circle")? If so, what is the equation of that oval?
   b) Determine which affine transformations of $\mathbf{AZ}_p^2$ are isometries; that is, they preserve the distances of part (a). Relate these isometries to the isometries of Section 4.3. [*Hint:* In Section 4.5, an affine matrix was defined to be an isometry iff its upper left submatrix was orthogonal.] Count the number of isometries in $\mathbf{AZ}_p^2$. Prove that the isometries form a group.
   c) For a prime p not of the form $4n+3$, the definition of distance in part (a) has the following curious property. There are distinct points with a distance of 0 between them. Verify this property for the primes 2, 5, 13, and 17. You can modify the distance formula for $p = 4n+1$ by multiplying the term $(t-v)^2$ by some nonzero scalar of $\mathbf{Z}_p$. Experiment with different scalars. Do the points at a specific distance from a given point form an oval? If so, what is the equation of that oval? How does the equation relate to the scalar? Investigate isometries for these planes with these distances. Count the number of isometries.
   d) Use different definitions of distance to explore parts (a) and (b). Do they change the number of isometries? Is there a common formula for the number of isometries for $\mathbf{AZ}_p^2$?
   e) Define perpendicular in $\mathbf{AZ}_p^2$ for odd primes p. Do you need different definitions for different primes?
   f) Explore similarities in $\mathbf{AZ}_p^2$, for $p = 4n+3$ and $p = 4n+1$. Count the number of similarities for $\mathbf{AZ}_p^2$ and show that they form a group.
10. Let potential code words be vectors of 0s and 1s of length n.
    a) Find the total number of these vectors.
    b) How many vectors are at a Hamming distance of 1 from a given vector?
    c) For a code to be able to correct one error, each pair of code words must be a Hamming distance of at least 3 apart. Use parts (a) and (b) to determine the maximum number of code words possible if each pair must be a distance of at least 3 apart. For various values of n, look for codes (sets of code words) that can correct one error and have as many code words as possible.
    d) Redo part (c) with codes that can correct two (or more) errors. [*Hint:* The binomial theorem may be helpful.]
    e) Redo part (c) with codes that can detect two or more errors.
11. Explore design theory. (See Anderson [1], Berman and Fryer [3] and Karteszi [7].)
12. Explore coding theory. (See Anderson [1] and Gallian [6].)
13. Explore finite geometries. (See Blumenthal [4] and Dembowski [5].)
14. Write an essay discussing the analogies between finite geometries and the familiar Euclidean (and projective) geometry. What insights can finite geometries provide?

Suggested Readings

[1] Anderson, I. *A First Course in Combinatorial Mathematics*. New York: Oxford University Press, 1989.
[2] Beck, A., M. Bleicher, and D. Crowe. *Excursions into Mathematics*. New York: Worth, 1969.
[3] Berman, G., and K. Fryer. *Introduction to Combinatorics*. New York: Academic Press, 1972.
[4] Blumenthal, L. *A Modern View of Geometry*. Mineola, N.Y.: Dover, 1961.
[5] Dembowski, P. *Finite Geometries*. New York: Springer-Verlag, 1968.
[6] Gallian, J. *Contemporary Abstract Algebra*. Lexington, Mass.: D. C. Heath, 1994.
[7] Karteszi, F. *Introduction to Finite Geometries*. Amsterdam: North Holland, 1976.
[8] Mullen, G. A candidate for the "next Fermat problem." *The Mathematical Intelligencer*, 1995, 17(3):18–22.
[9] Smart, J. *Modern Geometries*. Monterey, Calif.: Brooks/Cole, 1988.