The Many Names of (7, 3, 1)

EZRA BROWN
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061-0123
brown@math.vt.edu

In the world of discrete mathematics, we encounter a bewildering variety of topics with no apparent connection between them. But appearances are deceptive.

For example, combinatorics tells us about difference sets, block designs, and triple systems. Geometry leads us to finite projective planes and Latin squares. Graph theory introduces us to round–robin tournaments and map colorings, linear algebra gives us (0, 1)–matrices, and quadratic residues are among the many pearls of number theory. We meet the torus, that topological curiosity, while visiting the local doughnut shop or tubing down a river. Finally, in these fields we encounter such names as Euler, Fano, Fischer, Hadamard, Heawood, Kirkman, Singer and Steiner.

This is a story about a single object that connects all of these.

Commonly known as (7, 3, 1), it is all at once a difference set, a block design, a Steiner triple system, a finite projective plane, a complete set of orthogonal Latin squares, a doubly regular round-robin tournament, a skew-Hadamard matrix, and a graph consisting of seven mutually adjacent hexagons drawn on the torus.

We are going to investigate these connections. Along the way, we'll learn about all of these topics and just how they are tied together in one object—namely, (7, 3, 1). We'll learn about what all of those people have to do with it. We'll get to know this object quite well!

So let's find out about the many names of (7, 3, 1).

Combinatorial designs

The first place we meet (7, 3, 1) is in the set $Q_7 = \{1, 2, 4\}$. These are the nonzero perfect squares (mod 7), and their six nonzero differences, $1 - 2$, $1 - 4$, $2 - 4$, $2 - 1$, $4 - 1$, and $4 - 2$, yield each of the six distinct nonzero residues (mod 7) exactly once. Notice that Q_7 is a collection of 3 numbers mod 7, such that every nonzero integer mod 7 can be represented in exactly one way as a difference (mod 7) of distinct elements of Q_7. More generally, a (v, k, λ) *difference set* is a set S of k nonzero integers mod v such that every nonzero integer n mod v can be represented as a difference of elements of S in exactly λ different ways. Thus, Q_7 is a (7, 3, 1) difference set; from here on, we'll usually call it (7, 3, 1).

Difference sets have been the objects of a great deal of attention over the years, even before Singer constructed many families of them in his fundamental paper [**18**]. The first one students usually meet is (7, 3, 1) (or, rather, Q_7). We notice that $Q_{11} = \{1, 3, 4, 5, 9\}$ is a (11, 5, 2) difference set, since each nonzero number mod 11 can be written as a difference of elements of Q_{11} in exactly two ways (try it), and

$$Q_{47} = \{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}$$

is a (47, 23, 11) difference set (oh, go ahead and try it).

There's a pattern here: Q_{11} and Q_{47} are the nonzero squares mod 11 and 47, respectively, and this is no accident. It is not too tough to prove that the nonzero squares mod p form a difference set, where $p = 4n + 3$ is a prime. All we need are a few

facts about numbers, but first let us set some notation. Let p be a prime number; write $[1..n]$ to mean the set $\{1, \ldots, n\}$. Write $a \equiv b \bmod p$ to mean that $a - b$ is an integral multiple of p, and call a a square mod p when there exists an x with $x^2 \equiv a \bmod p$. Let $Z_p^\times$ denote the nonzero integers mod p, let Q_p denote the nonzero squares mod p, and let $GCD(n, k)$ denote the greatest common divisor of n and k.

Here are the facts, with some (hints) about how to verify them:

- $Z_p^\times$ is a group under multiplication mod p. (The multiples of p form a subgroup of the integers, and Z_p is the resulting quotient group.)
- The squares in $Z_p^\times$ are a subgroup of $Z_p^\times$. (The squares are closed under multiplication, and $Z_p^\times$ is a finite group.)
- The product of a square and a nonsquare mod p is a nonsquare mod p, and the product of two nonsquares mod p is a square mod p. (The squares and nonsquares are the two cosets in $Z_p^\times$ mod the subgroup of squares.)
- If $p = 4n + 3$, then -1 is not a square mod p. (The key here is Lagrange's Theorem.)
- If $GCD(a, p) = 1$, then multiplication by a permutes the elements of $Z_p^\times$. (If $GCD(a, p) = 1$ and $ax \equiv ay \bmod p$, then $x \equiv y \bmod p$.)

THEOREM 1. *Let $p = 4n + 3$ be a prime. Then the nonzero squares mod p form a $(4n + 3, 2n + 1, n)$ difference set.*

Proof. For convenience, by a square (respectively, nonsquare) we will mean a member of Q_p (respectively, a member of $Z_p^\times - Q_p$). Let $x \in [1..p - 1]$. Since $x \not\equiv 0 \bmod p$, it follows that x has an inverse in $Z_p^\times$; denote this inverse by x^{-1}. (For example, if $p = 19$, then $7^{-1} = 11$ because $7 \cdot 11 = 77 \equiv 1 \bmod 19$.)

Now let R be the set of pairs of squares, that is, let $R := \{(a, b) \in [1..p - 1]: a \text{ and } b \text{ are squares}, a \neq b\}$. We say that the pair (a, b) *represents* x if $a - b \equiv x (\bmod p)$; write $N(x)$ to mean the number of pairs in R that represent x. Define the map σ_x on ordered pairs mod p by

$$\sigma_x(a, b) = \begin{cases} (x^{-1}a, x^{-1}b), & \text{if } x \text{ is a square;} \\ (-x^{-1}b, -x^{-1}a), & \text{if } x \text{ is a nonsquare.} \end{cases}$$

For example, both 5 and 6 are squares mod 19 and 7 is a nonsquare mod 19; if $x = 7$, then we have

$$\sigma_7(5, 6) = (-7^{-1} \cdot 6, -7^{-1} \cdot 5) = (-11 \cdot 6, -11 \cdot 5) = (10, 2),$$

all arithmetic being done mod 19.

The first thing to observe is that if (a, b) represents x, then $\sigma_x(a, b)$ represents 1. For, if $a - b \equiv x (\bmod p)$, then $x^{-1}a - x^{-1}b = x^{-1}(a - b) \equiv x^{-1}x \equiv 1 (\bmod p)$. Also, $-x^{-1}b - (-x^{-1}a) \equiv x^{-1}(a - b) \equiv 1 (\bmod p)$. Now if x is a square, then $x^{-1}a$ and $x^{-1}b$ are both squares, and so $(x^{-1}a, x^{-1}b)$ represents 1. If x is a nonsquare, then$-x^{-1}$ is a square, so $-x^{-1}b$ and $-x^{-1}a$ are squares, and $(-x^{-1}b, -x^{-1}a)$ represents 1. Thus, every representation of x leads to a representation of 1.

On the other hand, $\sigma_{x^{-1}}$ is an inverse map of σ_x, so that if (c, d) represents 1, then $\sigma_{x^{-1}}(c, d)$ represents x. Thus, for all x, every representation of 1 leads to a representation of x.

We conclude that $N(x) = N(1)$ for all $x \in [1..p - 1]$, and so every $x \in [1..p - 1]$ has the same number of representations. This lets us count R: it contains $N(1) \cdot (p - 1) = N(1) \cdot (4n + 2)$ pairs.

Finally, since multiplication by -1 permutes $Z_p^\times$ and exchanges the squares and nonsquares, there are $2n + 1 = (p - 1)/2$ squares mod p; hence, R contains $(2n + 1)2n = \frac{p-1}{2}(\frac{p-1}{2} - 1)$ pairs (there are no pairs (a, a)). Equating these two values for the size of R, we see that $N(1) = (2n + 1)2n/(4n + 2) = n$. Hence, every nonzero integer mod $p = 4n + 3$ is represented n times by a difference of nonzero squares mod p—that is, the nonzero squares form a $(4n + 3, 2n + 1, n)$ difference set. ■

There are many other classes of difference sets. For example, $B_{13} = \{0, 1, 3, 9\}$ is a difference set with $v = 13$, and $B_{37} = \{1, 7, 9, 10, 12, 16, 26, 33, 34\}$ is a difference set with $v = 37$. (As an exercise, verify these statements and in so doing, determine k and λ for each. Question: Except for 0, B_{13} looks like the powers of 3 mod 13; is there a similar pattern for B_{37}?)

As we have seen, $\{1, 2, 4\}$ is a $(7, 3, 1)$ difference set. But so is any additive shift $\{1 + n, 2 + n, 4 + n\}$ (mod 7) of $\{1, 2, 4\}$. Consider all seven of these sets together; writing abc for the set $\{a, b, c\}$, we have

$$124, 235, 346, 450, 561, 602, \text{ and } 013. \tag{1}$$

This is well illustrated by rotating the triangle in FIGURE 1 counterclockwise within its circumscribing circle:

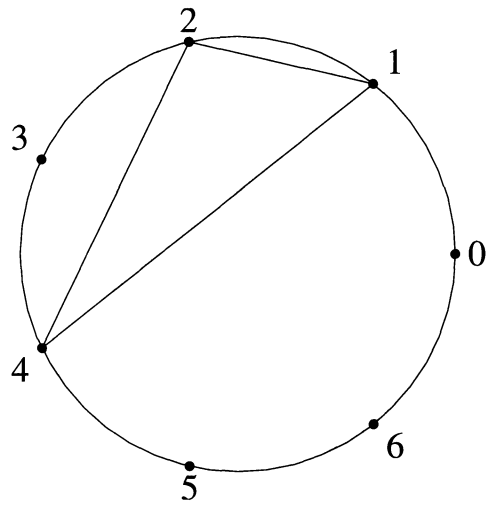

Figure 1 The (7, 3, 1) difference set

Notice that for these 7 sets (or *blocks*), whose elements are taken from a 7-element set, namely [0..6], each element appears in 3 blocks, each block has 3 elements, and each pair of elements appears together in exactly one block. The difference sets in this section give rise to some special classes of what are called *block designs*, and some more names for (7, 3, 1). So let's talk about block designs.

A *balanced incomplete block design*, or BIBD with parameters b, v, r, k, and λ is an arrangement of b blocks, taken from a set of v objects (known for historical reasons as *varieties*), such that every variety appears in exactly r blocks, every block contains exactly k varieties, and every pair of varieties appears together in exactly λ blocks. Such an arrangement is also called a (b, v, r, k, λ) design. Thus, (7, 3, 1) is a (7, 7, 3, 3, 1) design. Block designs appeared in connection with the eminent British statistician R. A. Fisher's work on the statistical design of agricultural experiments ([7], [8]),

and the first comprehensive mathematical study of the field was due to R. C. Bose [2]. Now, the five parameters are by no means independent, for it turns out that $bk = vr$ and $r(k-1) = \lambda(v-1)$ (exercise: prove it). Hence, a (b, v, r, k, λ) design is really a $(\lambda v(v-1)/(k(k-1)), v, \lambda(v-1)/(k-1), k, \lambda)$ design. If $b = v$ (and hence $r = k$), the design is said to be *symmetric*; thus, $(7, 3, 1)$ is a $(7, 3, 1)$ symmetric design.

The familiar 3×3 magic square (see FIGURE 2, on the right), in which the rows, columns, and main diagonals all add up to 15, is the source of another block design.

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array} \qquad \begin{array}{ccc} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{array}$$

Figure 2 Generating a design from a 3×3 magic square

Here's how it works: first, arrange the integers from 1 to 9 in that order in a 3×3 grid—see FIGURE 2, on the left. Allowing diagonals to wrap when they reach the edge of the grid (as if there were another copy of the grid next door) yields twelve 3-element sets: three rows, three columns, and six diagonals. Thus, we have 9 objects arranged in 12 blocks with each object in four blocks, each block containing three objects and each pair of objects in one block–in short, a $(12, 9, 4, 3, 1)$ design. Here are the blocks:

$$123, 456, 789, 147, 258, 369, 168, 249, 357, 159, 267, 348.$$

Now we have already seen that the seven additive shifts (mod 7) of our $(7, 3, 1)$ difference set form the blocks of a $(7, 3, 1)$ symmetric design. In addition, the eleven additive shifts (mod 11) of our $(11, 5, 2)$ difference are the blocks of a symmetric $(11, 5, 2)$ design (see for yourself). It turns out that this is the case in general, and we can prove it.

THEOREM 2. *Let $D = \{x_1, x_2, \ldots, x_k\}$ be a (v, k, λ) difference set. Let $B_i := \{x_1 + i, \ldots, x_k + i\}$ where addition is mod v. Then the v sets $B_0, \ldots, B_{v-1}$ are the blocks of a (v, k, λ) symmetric design.*

Proof. By definition, there are v blocks and v varieties. By construction, there are k varieties in each block. In addition, since $y = x_j + (y - x_j)$ for $1 \le j \le k$, each $y \in [0..v-1]$ appears in blocks $B_{y-x_1}, \ldots, B_{y-x_k}$. Hence each variety appears in k blocks. Finally, let $y, z \in [0..v-1]$; then y and z are in B_t if and only if $t = y - x_i = z - x_j$ for distinct $i, j \in [1..k]$. This happens if and only if $y - z = x_i - x_j$; since D is a (v, k, λ) difference set, this happens for exactly λ pairs (x_i, x_j). Thus, there are exactly λ values of t for which $t = y - x_i = z - x_j$ for distinct $i, j \in [1..k]$, and for these values, y and z appear together in a block. ∎

You may wonder whether the converse of this theorem is also true—that is, does every (v, k, λ) symmetric design give rise to a (v, k, λ) difference set? Interesting question: we'll come back to it later.

Finally, a class of block designs that has attracted considerable interest over the years is the one for which $k = 3$ and $\lambda = 1$. Such a design is called a *Steiner triple system* on v varieties, or STS(v) for short. Since $(7, 3, 1)$ certainly has $k = 3$, it is also an STS—in fact, the smallest nontrivial Steiner triple system. Now if an STS(v) exists, then $v \equiv 1$ or $3 \pmod 6$, which follows from the fact that a $(b, v, r, 3, 1)$ design is really a $(\lambda v(v-1)/(3 \cdot 2), v, (v-1)/2, 3, 1)$ design. (You can work this one out!)

Steiner posed the problem of showing that triple systems exist for all such $v \ge 3$, but he did not solve it. In fact, the problem had been solved more than a decade earlier

by the Reverend Thomas A. Kirkman [**11**]—see Doyen's survey article [**5**] for a great deal more about these triple systems. (Perhaps they should be renamed in honor of Kirkman, about whom more later.)

Steiner triple systems turn up in some unlikely places, such as subfield diagrams in algebraic number theory—but that's another story.

Since the 3×3 magic square is a (12, 9, 4, 3, 1) design, it is also an STS(9). But it is more than that: the words *magic square* suggest some connection with geometry. Curiously enough, it turns out that (7, 3, 1) has geometric connections as well. So, let's talk about finite geometries.

Finite geometries

The 3×3 magic square we met in the previous section (FIGURE 2 on the left) is an example of a finite geometry. For, if by a *line*, we mean a set of points—not necessarily connected, straight, or infinite—then the 3×3 magic square obeys some fairly simple rules:

(1) Each pair of points lies on a unique line.

(2) Each pair of lines intersects in at most one point.

(3) There exist four points with no three on a line.

The first two rules are reminiscent of Euclidean plane geometry, and the third ensures that the object at hand is nontrivial. Arrangements that satisfy these three rules are called *finite affine planes*, and the number of points on each line is called the *order* of the plane. Thus, the 3×3 magic square gives rise to a finite affine plane (FAP) of order 3.

We cannot draw a picture of this in the plane without two pairs of lines crossing unnecessarily, but we can draw it on a torus—the surface of a doughnut—by wrapping the diagonals. See FIGURE 3, where solid lines represent the lines of this finite plane, and dotted lines indicate wrapping on the torus.

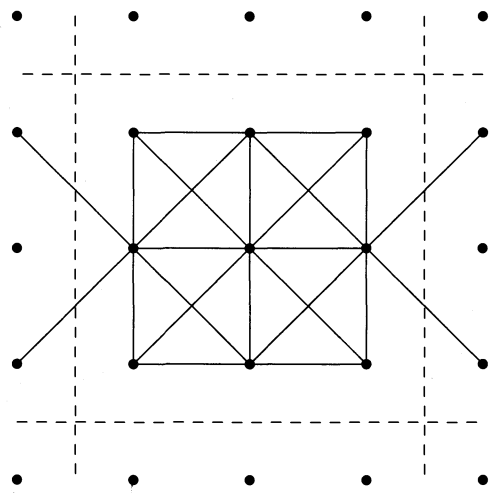

Figure 3 The finite affine plane of order 3

Here's a question: What is the smallest possible finite plane? We need at least four points with no three on a line; if we call the points A, B, C, and D, then the six lines AB, AC, AD, BC, BD, and CD form a perfectly good finite plane. Now in our affine planes, some of the lines intersect and some of them do not.

But what if we insisted that the plane be *projective*, that is, that every pair of lines have a unique point in common? What is the smallest possible finite projective plane (FPP)?

Let's add some points to the plane above. Clearly, AB and CD must meet in some point X, AC and BD meet in some point Y, and AD and BC meet in some point Z. If $X = Y$, then A, B, and X are on a line, and B, D, and $X(= Y)$ are on a line. But B and X determine a unique line, so that A, B, and D are on a line—contrary to assumption. Hence, $X \neq Y$. For the same reason, $X \neq Z$ and $Y \neq Z$.

We know that an FPP contains at least seven points, and so far, it contains the six lines ABX, CDX, ACY, BDY, ADZ, and BCZ. There must be a line through X and Y. To keep things small, we add the line XYZ (represented by the circle on the left in FIGURE 4); then each pair of lines intersects in a unique point. The resulting seven-point FPP is known as the *Fano plane*; here it is on the left in FIGURE 4:

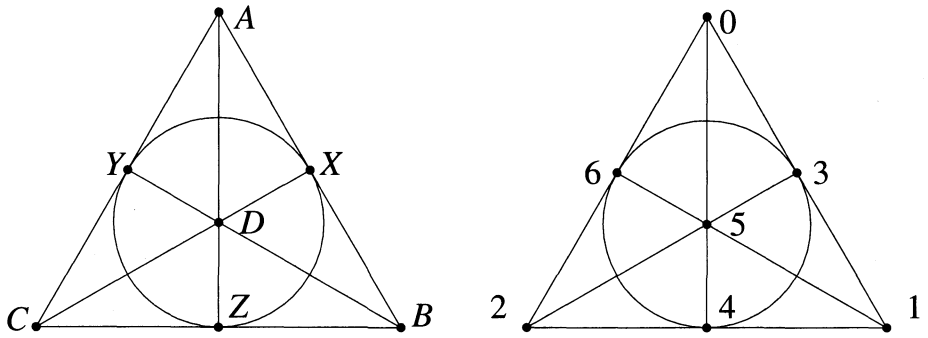

Figure 4 The Fano plane

Notice that the Fano plane has seven points and seven lines; each line contains three points, each point is on three lines and each pair of points is on exactly one line. Sound suspiciously familiar? It should, for if we replace A, B, C, D, X, Y, and Z with 0, 1, 2, 5, 3, 6, and 4, respectively, the lines look like this:

$$124, \quad 235, \quad 346, \quad 450, \quad 561, \quad 602, \quad \text{and} \quad 013,$$

and (7, 3, 1) has reappeared—on the right in FIGURE 4—as the Fano plane. This configuration was named for G. Fano, who described it in 1892 [**6**]. In another twist of fate, however, he was anticipated by Woolhouse in 1844 [**20**] and, yes, by Kirkman in 1850 [**12**].

More generally, a *finite projective plane of order n*, abbreviated FPP(n), is an FPP containing $n^2 + n + 1$ points and $n^2 + n + 1$ lines, such that every point is on $n + 1$ lines, every line contains $n + 1$ points, and every pair of points is on a unique line. Thus, an FPP(n) is an $(n^2 + n + 1, n + 1, 1)$ symmetric design; conversely, every $(v, k, 1)$ design is a finite projective plane of order $n = k - 1$ with $v = n^2 + n + 1$.

One of the major unsolved problems in combinatorics is determining the values of n for which an FPP(n) exists. Their existence is equivalent to the existence of certain families of designs called Latin squares, designs that got mixed up with one of the

most famous false conjectures in the history of mathematics. So let's talk briefly about them now.

A *Latin square of order n* is an $n \times n$ array with entries from the set $[1..n]$ such that each element of $[1..n]$ appears in each row and each column of the array exactly once. Two Latin squares $A = [a_{ij}]$ and $B = [b_{ij}]$ of order n are said to be *orthogonal* if the n^2 ordered pairs (a_{ij}, b_{ij}) are distinct. (A good reference for the general subject of Latin squares is a text by Dénes and Keedwell [**4**].) Here are three Latin squares of order 4; you can check that (a) they are Latin squares and (b) they are orthogonal in pairs:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 4 & 2 & 3 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \end{bmatrix}$$

It turns out that the existence of this trio of pairwise orthogonal Latin squares of size 4 is equivalent to the existence of a finite projective plane of order 4; in fact, this is true in general:

THEOREM 3. *Let n be an integer greater than 1. Then there exists a finite projective plane of order n if and only if there exists a set of* $n - 1$ *Latin squares of size n that are pairwise orthogonal.*

An outline of the proof is given in a text by Roberts [**16**]—who also shows that if n is a prime power, then there exists a set of $n - 1$ Latin squares of size n that are pairwise orthogonal. Hence, FPP's exist for orders 2, 3, 4, 5, 7, 8, and 9. In particular, (7, 3, 1) is a FPP(2) and so there must be a corresponding set of $n - 1$ pairwise orthogonal Latin squares of size $n = 2$. And what is that set? You can figure it out, or I'll tell you later.

So 2, 3, 4, 5, 7, 8, and 9 are all just fine. But what about order 6?

The great Leonhard Euler wondered about 6, too. That prodigious mathematical mind from the eighteenth century made a study of Latin squares, showed how to construct a pair of size n if n is not of the form $4k + 2$, and saw immediately that it is impossible to construct a pair of orthogonal Latin squares of size 2 (try it). He then attempted to construct a pair of size 6; failing to do so, he made the following bold conjecture:

EULER'S CONJECTURE (1782). For each nonnegative integer k, there does not exist a pair of orthogonal Latin squares of size $4k + 2$.

For over 100 years, nothing happened. Then, in 1900, G. Tarry wrote two papers [**19**] proving that Euler was right about 6. But as Bose, Shrikhande, and Parker [**3**] showed in 1960, he was spectacularly wrong for all other values of $4k + 2$ greater than 6:

THEOREM 4. *There exists a pair of orthogonal Latin squares of order n for all* $n > 6$.

It is now known (the details are in a nice survey by Lam [**13**]) that an FPP(10) does not exist; the smallest unknown case is for $n = 12$. So we see that (7, 3, 1) is connected with one of the rare instances in which Euler was almost totally wrong!

It happens that (7, 3, 1) has connections, not only with combinatorics, but also with that other major branch of discrete mathematics: graph theory. So let's talk about graph theory.

Graph theory connections

A *graph* G is a set of points (or vertices) $V(G)$ together with a set of lines (or edges) $E(G)$ joining some (perhaps all, perhaps none) of the points. We say that the vertices a and b are *adjacent* if the edge ab is in the graph. A graph is *complete* if there is an edge between every pair of points. Graphs can be *directed*, that is, each edge is assigned a direction: we write (a, b) if there is an edge directed from a to b. Graphs model an amazing number of problems, from simple word puzzles (the Wolf-Goat-Cabbage problem) and games (Tic–Tac–Toe and chess) to such complex systems as the continental power grid and the internet. Directed graphs can model the play of teams in a league, and that is where (7, 3, 1) comes in.

In many sports leagues, each team plays every other team exactly once, and there are no ties. We can model this scenario with a graph as follows. The teams are the vertices, and for each pair of teams u and v, include the edge (u, v) directed from u to v if u beats v, and include the edge (v, u) if v beats u. We call such a graph a *(round–robin) tournament*; thus, a tournament is a complete graph with a direction assigned to each edge. (A good reference on tournaments is Moon's book [**14**].) The score of a vertex u is the number of edges (u, v) in the tournament. A tournament is called *transitive* if every team has a different score, and *regular* if every team has the same score. Naturally, the higher the score, the higher the team's rank. Thus, in a transitive tournament, the scores determine the ranking unambiguously, and in a regular tournament, the scores don't give any information. (A transitive tournament is so named because it has the property that if u beats v and v beats w, then u beats w.)

Now, the high schools of Auburn, Blacksburg, Christiansburg, EastMont, Giles, Newman, and Radford make up the Riverside League. In most years, one or two schools dominate, but last year the results of the league's round-robin play were quite different:

Team	**Victories Over**
Auburn	Blacksburg, Giles, Radford
Blacksburg	Christiansburg, Giles, Newman
Christiansburg	Auburn, Newman, Radford
EastMont	Auburn, Blacksburg, Christiansburg
Giles	Christiansburg, EastMont, Radford
Newman	Auburn, Giles, EastMont
Radford	Blacksburg, EastMont, Newman

Each team had the same score of 3, so this was a regular tournament. But the league was even more balanced than that: each pair of teams was victorious over exactly one common opponent. (Such a tournament is called *doubly regular*.) Let us look at this a little more carefully, assigning numbers to the teams as follows: $A = 3$, $B = 0$, $C = 1$, $E = 6$, $G = 4$, $N = 2$, and $R = 5$. If we now rewrite the results in numerical order, the table of victories begins to look somewhat familiar:

Team	Victories Over
0	1, 2, 4
1	2, 3, 5
2	3, 4, 6
3	4, 5, 0
4	5, 6, 1
5	6, 0, 2
6	0, 1, 3

Our old friend (7, 3, 1) has reappeared: the sets of teams defeated by each member of the league are the blocks of a (7, 3, 1) symmetric design, and the teams defeated by Team 0 form a (7, 3, 1) difference set.

Of course, this is no accident—and we can prove it.

THEOREM 5. *Let $p = 4n + 3$ be a prime. Define the tournament T by $V(T) = [0..p-1]$ and $E(T) = \{(x, x+r)$: r is a square mod $p\}$. Then T is a doubly regular tournament with $4n + 3$ vertices, in which every vertex has a score of $2n + 1$ and every pair of vertices defeats n common opponents.*

Proof. Since there are $(p-1)/2 = 2n + 1$ squares mod p, each vertex has a score of $2n + 1$. Now let x, y be distinct vertices. Then (x, z) and (y, z) are both edges of T if and only if there exist distinct squares r and s such that $z - x = r$ and $z - y = s$. Hence, the number of such z is equal to the number of pairs of distinct squares r, s such that $r - s = x - y$. But the squares form a $(4n + 3, 2n + 1, n)$ difference set, and so the nonzero number $x - y$ can be written as a difference $r - s$ in exactly n distinct ways. Hence, there are n vertices z such that both (x, z) and (y, z) are edges of T, that is, T is doubly regular. ∎

In short, (7, 3, 1) is a doubly regular tournament.

Now, the adjacency matrix of a tournament T on v vertices $x_1, \ldots, x_v$ is a $v \times v$ matrix $A = [A_{ij}]$ such that $A_{ij} = 1$ if there is an edge from x_i to x_j, and $A_{ij} = 0$ otherwise. Thus, the (7, 3, 1) doubly regular tournament has the following adjacency matrix A:

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}$$

If we replace all the 0s in A with -1s and border the resulting matrix top and left with a row and column of 1s, we obtain the above matrix H. If we multiply H by its transpose H^T, it turns out that $HH^T = 8I$, where I is the 8×8 identity matrix. An $n \times n$ matrix H of 0s and 1s for which $HH^T = nI$ is called a *Hadamard matrix* of order n—not a property enjoyed by very many $(-1, 1)$-matrices. It turns out that the adjacency matrix of every doubly regular tournament can be transformed into a skew–Hadamard matrix (one for which $H + H^T = 2I$), and every skew–Hadamard matrix gives rise to a doubly regular tournament [**15**].

Hadamard matrices are very useful in constructing error–correcting codes and other combinatorial designs. You can show that if H is a Hadamard matrix of order $n > 1$, then either $n = 2$ or $n \equiv 0 \bmod 4$. Whether the converse is true is an unsolved problem.

More graph theory connections

The final two (7, 3, 1) connections turned up in my course in Galois theory, that beautiful subject in which Évariste Galois (1811–1832) related the roots of polynomials to number fields and finite groups. One basic idea is that if $p(x)$ is a polynomial with rational coefficients, then there is a smallest subfield $L(p)$ of the complex numbers $\mathbb{C}$ containing both the rationals $\mathbb{Q}$ and all the roots of $p(x)$. This is the *splitting field* of p over $\mathbb{Q}$. If $a, b, \ldots \in \mathbb{C}$ and if K is a subfield of $\mathbb{C}$, write $K(a, b, \ldots)$ to mean the smallest subfield of $\mathbb{C}$ containing K and $a, b, \ldots$.

For the polynomial $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$, it turns out that $L(p) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Now this field contains, besides itself and $\mathbb{Q}$, fourteen other subfields which—to my great delight—form a (7, 3, 1) design. For this particular incarnation of (7, 3, 1), the varieties are the seven quadratic subfields $\mathbb{Q}(\sqrt{d})$, where $d \in \{2, 3, 5, 6, 10, 15, 30\}$, and the blocks are the seven biquadratic subfields $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ (where $d_1 d_2$ is not a perfect square). See for yourself:

Biquadratic Field	**Contains $\mathbb{Q}(\sqrt{d})$ for these d**
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	2, 3, 6
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	3, 5, 15
$\mathbb{Q}(\sqrt{5}, \sqrt{6})$	5, 6, 30
$\mathbb{Q}(\sqrt{6}, \sqrt{15})$	6, 15, 10
$\mathbb{Q}(\sqrt{15}, \sqrt{30})$	15, 30, 2
$\mathbb{Q}(\sqrt{30}, \sqrt{10})$	30, 10, 3
$\mathbb{Q}(\sqrt{10}, \sqrt{2})$	10, 2, 5

In short, (7, 3, 1) appears in the subfields of the splitting field of a polynomial.

But there's one more connection. If we join two subfields of L by a line if one contains the other and there is no intermediate field, we get the lattice of subfields of L. For our field $L(p)$, if we do this and ignore $L(p)$ and $\mathbb{Q}$, the left side of FIGURE 5 shows what we get.

This is the (3, 6) cage: every vertex has degree 3, the shortest cycle has length 6, and no graph with fewer vertices has these properties. The (3, 6) cage cannot be drawn in the plane without edges crossing. It can, however, be drawn on the torus, and the right side of FIGURE 5 shows what *that* looks like.

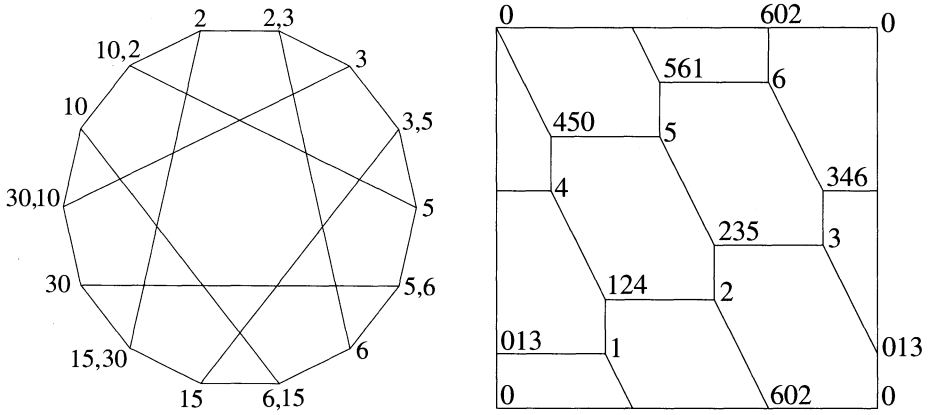

Figure 5 The Heawood graph

This toroidal embedding is what gives the graph its common name: the Heawood graph. For, in 1890, Percy J. Heawood proved that every graph that can be drawn on the torus without edges crossing requires at most seven colors to color its regions with neighboring regions having different colors. The Heawood graph was his example of a toroidal graph requiring seven colors, for it consists of seven mutually adjacent hexagons.

With that, we see how (7, 3, 1) has a connection with Heawood's 7–Color Theorem for toroidal graphs, and with the Heawood graph—just one more of the many names of (7, 3, 1).

Questions

Does (7, 3, 1) have any other names? Yes, it does. There is a combinatorial design called a (3, 4, 7, 2) *configuration of size 14*; it consists of fourteen 3-element subsets of [1..7], no more than two of which lie in a common 4-element subset of [1..7]. The incidence graph of this design (two 3-sets are joined if and only if they lie in a common 4-set) is the Heawood graph. To find more names, Richard Guy's paper [**9**] is an excellent place to start.

Where can I find out more about difference sets? One of the best places to begin is with H. J. Ryser's beautifully written book [**17**], which will take you a fair way into the subject. Two others are the more recent book by Beth, Jungnickel, and Lenz [**1**] and Marshall Hall's classic [**10**], both of which will take you as far as you want to go into the subject. All three of these also give good introductions to the other combinatorial designs talked about here.

Do all (v, k, λ) symmetric designs give rise to (v, k, λ) difference sets? In fact, they don't—but the smallest example is $(v, k, \lambda) = (25, 9, 3)$. Exercise: Find it.

How did Tarry prove that there does not exist a pair of orthogonal Latin squares of size 6? Brute force. He used symmetry arguments to reduce the number of cases to about six thousand—then eliminated them, one by one. (Don't try this at home.)

What is the complete set of orthogonal Latin squares that corresponds to (7, 3, 1)? We know that (7, 3, 1) is also an FPP of order $n = 2$, so the corresponding set of $n - 1 = 1$ orthogonal Latin square(s) of size 2 is just

$$A = \left\{ \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \right\}.$$

Did the Reverend Thomas Kirkman ever get credit for anything? Yes, he did. In 1850, he posed what is known as Kirkman's Schoolgirls Problem. Fifteen schoolgirls take daily walks, arranged in five rows of three each; arrange the girls so that for seven consecutive days, no girl is in a row with the same companion more than once. The solution to this problem is a particularly interesting Steiner triple system on 15 varieties, with parameters (35, 15, 7, 3, 1)—but that's another story.

Speaking of Steiner triple systems: are there Steiner quadruple systems? In fact, the idea generalizes to a Steiner system $S(k, m, n)$, which is a collection C of m-element subsets of an n−element set B, such that every k-element subset of B is contained in exactly one of the sets in C. An $S(2, 3, n)$ is a Steiner triple system, and an $S(2, n + 1, n^2 + n + 1)$ is a finite projective plane. Not too many of these are known with $k > 3$. One of these is known as $S(5, 8, 24)$; it has many extraordinary properties, as well as connections with—ahh, but *that's* another story!

REFERENCES

1. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory, 2nd Edition*, Cambridge University Press, Cambridge, 1999.
2. R. C.Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939), 353–399.
3. R. C. Bose, S. Shrikhande, and E. T. Parker, Further results on the construction of sets of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* **12** (1960), 189–203.
4. Jozsef Dénes and Donald Keedwell, *Latin Squares and their Applications*, Academic Press, New York, 1974.
5. Jean Doyen, Recent developments in the theory of Steiner systems, *Atti dei Conv. Lincei* **17** (1976), 277–285.
6. G. Fano, Sui postulati fondamentali della geometria proiettiva, *Giorn. Mat.* **30** (1892), 114–124.
7. R. A. Fisher, *The Design of Experiments*, Oliver and Boyd, Edinburgh, 1935.
8. R. A. Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics* **10** (1940), 52–57.
9. Richard K. Guy, The unity of combinatorics, in C. J. Colburn and E. S. Mahmoodian (eds) *Combinatorics Advances*, Kluwer, 1995, 129–159.
10. Marshall Hall, Jr., *Combinatorial Theory* (9th edition), Blaisdell Publishing Company, Waltham, MA, 1967.
11. T. A. Kirkman, On a problem in combinations, *Camb. Dublin Math. J.* **2** (1847), 191–204.
12. T. A. Kirkman, Note on an unanswered prize question, *Camb. Dublin Math. J.* **5** (1850), 255–262.
13. Clement W. H. Lam, The search for a finite projective plane of order 10, *Amer. Math. Monthly* **98** (1991), 305–318.
14. J. W. Moon, *Topics on Tournaments*, Holt, Rinehart and Winston, New York, 1968.
15. K. B. Reid and E. Brown, Doubly regular tournaments are equivalent to skew–Hadamard matrices, *J. Combinatorial Theory, Series A* **12** (1972), 332–338.
16. Fred S. Roberts, *Applied Combinatorics*, Prentice–Hall, 1984.
17. H. J. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monograph No. 14, Mathematical Association of America, Washington, DC, 1963.
18. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.
19. G. Tarry, Le Problème de 36 officiers, *C. R. Assoc. Fr. Avance. Sci. Nat* **1** (1900), 122–123; **2** (1901), 170–203.
20. W. S. B. Woolhouse, Prize question 1733, *Lady's and Gentleman's Diary*, 1844.