Chapter 10

Combinatorial Designs

A *combinatorial design*, or simply a *design*, is an arrangement of the objects of a set into subsets satisfying certain prescribed properties. This is a very general definition and includes a vast amount of combinatorial theory. Many of the examples introduced in Chapter 1 can be viewed as designs: (1) perfect covers by dominoes of boards with forbidden positions, where we arrange the allowed squares into pairs so that each pair can be covered by one domino; (2) magic squares, where we arrange the integers from 1 to n^2 in an n-by-n array so that certain sums are identical; and (3) Latin squares, where we arrange the integers from 1 to n in an n-by-n array so that each integer occurs once in each row and once in each column. We shall treat Latin squares and the notion of orthogonality, briefly introduced in Chapter 1, more thoroughly in this chapter.

The area of combinatorial designs is highly developed, yet many interesting and fundamental questions remain unanswered. Many of the methods for constructing designs rely on the algebraic structure called a finite field and more general systems of arithmetic. In Section 1 we give a brief introduction to these "finite arithmetics," concentrating mainly on modular arithmetic. Our discussion will not be comprehensive but should be sufficient to enable us to do arithmetic comfortably in these systems.

10.1 Modular Arithmetic

Let Z denote the set of integers

$$\{\ldots, -2, -1, 0, 1, 2, \ldots\},$$

and let $+$ and $\times$ denote ordinary addition and multiplication of integers. The reason for being so cautious in pointing out the usual notations for addition and multiplication is that we are going to introduce new additions and new multiplications on certain

subsets of the set Z of integers, and we don't want the reader to confuse them with ordinary addition and multiplication.

Let n be a positive integer with $n \geq 2$, and let

$$Z_n = \{0, 1, \ldots, n-1\}$$

be the set of nonnegative integers that are less than n. We can think of the integers in Z_n as the possible remainders when *any* integer is divided by n:

> If m is an integer, then there exist unique integers q (the quotient) and r (the remainder) such that
>
> $$m = q \times n + r, \quad 0 \leq r \leq n-1.$$

With this in mind, we define an addition, denoted $\oplus$, and a multiplication, denoted $\otimes$, on Z_n as follows:

> For any two integers a and b in Z_n, $a \oplus b$ is the (unique) remainder when the ordinary sum $a+b$ is divided by n, and $a \otimes b$ is the (unique) remainder when the ordinary product $a \times b$ is divided by n.

This addition and multiplication depend on the chosen integer n, and we should be writing something like $\oplus_n$ and $\otimes_n$, but such notation gets a little cumbersome.[1] So we just caution the reader that $\oplus$ and $\otimes$ depend on n, and we call them *addition mod n* and *multiplication mod n*, and with this addition and multiplication we get the *system of integers mod n*.[2] We usually denote the arithmetic system of the integers mod n with the same symbol Z_n that we use for its set of elements.

Example. The simplest case is $n = 2$. We have $Z_2 = \{0, 1\}$, and addition and multiplication mod 2 are given in the following tables:

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Notice that mod 2 arithmetic is just like ordinary arithmetic except that $1 \oplus 1 = 0$. This is because $1 + 1 = 2$ and subtracting 2 lands us back at 0 in Z_2. □

[1] Shortly, after the reader has gotten familiar with these new additions and multiplications, we shall replace the notations $\oplus$ and $\otimes$ by the ordinary notations $+$ and $\times$ and preface our calculations with the statement that they are being done mod n.

[2] *Mod* is short for *modulo*, which means *with respect to a modulus* (a quantity, which in our case is the quantity n). For instance, to compute $a \otimes b$, we perform the usual multiplication $a \times b$ and then subtract enough multiples of n from $a \times b$ in order to get an integer in Z_n. The latter is sometimes referred to as "modding out" n.

Example. The addition and multiplication tables for the integers mod 3 are as follows:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

In particular, $2 \otimes 2 = 1$ since $2 \times 2 = 4$ and $4 = 1 \times 3 + 1$. □

Example. Some instances of addition and multiplication in the system of integers modulo 6 are

$$4 \oplus 5 = 3,$$
$$2 \oplus 3 = 5,$$
$$2 \otimes 2 = 4,$$
$$3 \otimes 5 = 3,$$
$$3 \otimes 2 = 0,$$
$$5 \otimes 5 = 1.$$

□

As these examples indicate, sometimes addition or multiplication mod n is like ordinary addition or multiplication (this happens when the ordinary result is an integer in Z_n). Other times, addition or multiplication modulo n is quite different from ordinary addition and multiplication, and the results can seem quite odd. For instance, as displayed in the preceding example, in the integers mod 6 we have $5 \otimes 5 = 1$, which suggests that the reciprocal of 5 is itself; that is, the number which, when multiplied by 5, gives 1, is 5 itself! We also have $3 \otimes 2 = 0$ in the integers mod 6, which should suggest caution, since, in ordinary multiplication, nonzero numbers never multiply to zero.

Before proceeding, we recall some basic notions of arithmetic and algebra as they relate to the integers mod n. First, we observe[3] that addition and multiplication mod n satisfy the usual laws of commutativity, associativity, and distributivity. An *additive inverse* of an integer a in Z_n is an integer b in Z_n such that $a \oplus b = 0$. There is an obvious candidate for the additive inverse for a: If $a = 0$, then it's 0; if $a \neq 0$, then $n - a$ is between 1 and $n - 1$, and $n - a$ is an additive inverse of a, since

$$a + (n - a) = n = 1 \times n + 0 \text{ implying } a \oplus (n - a) = 0.$$

In all cases, the additive inverse is uniquely determined. Following usual conventions, the additive inverse of a is denoted by $-a$, but keep in mind that $-a$ *denotes*[4] one

[3] Actually, it's more than an observation, but it is elementary, if not tedious, to check that these properties hold. Implicit in the word *observation* is that we don't want to bother to check these properties. A student who has never done this before probably should check at least some of them.

[4] If we were to follow our defined notation, we should probably be denoting the additive inverse of a by $\ominus a$

of the integers in $\{0, 1, 2 \ldots, n-1\}$. The fact that all integers in Z_n have additive inverses means that we can always subtract in Z_n, since subtracting b from a is the same as adding $-b$ to a: $a \ominus b = a \oplus (-b)$.

A *multiplicative inverse* of an integer a in Z_n is an integer b in Z_n such that $a \otimes b = 1$. In contrast to additive inverses, there is no obvious candidate for the multiplicative inverse of a. In fact, it should come as no surprise that some nonzero a's may not have multiplicative inverses. In the system Z of integers, the integer 2 does not have a multiplicative inverse since there is no integer b such that $2 \times b = 1$.[5] Indeed, in Z the only numbers that have multiplicative inverses are 1 and -1. Following usual conventions, we denote a multiplicative inverse of an integer a in Z_n by a^{-1}, *if there is one.*

Example. In the integers modulo 10, the additive inverses are as follows:

$$\begin{array}{lllll} -0 = 0 & -1 = 9 & -2 = 8 & -3 = 7 & -4 = 6 \\ -5 = 5 & -9 = 1 & -8 = 2 & -7 = 3 & -6 = 4 \end{array}$$

Note that we have the unusual circumstance whereby $-5 = 5$, but remember that -5 denotes the integer in Z_{10} which, when added (mod 10) to 5, gives 0, and 5 does have this property: $5 \oplus 5 = 0$. Notice also that, if $-a = b$, then $-b = a$; put another way $-(-a) = a$.

By simply checking all possibilities, we can see that the situation with multiplicative inverses in Z_{10} is the following:

$$\begin{array}{ll} 1^{-1} = 1 & \text{(the multiplicative inverse of 1 is always 1)} \\ 3^{-1} = 7 & (3 \otimes 7 = 1) \\ 7^{-1} = 3 & (7 \otimes 3 = 1) \\ 9^{-1} = 9 & (9 \otimes 9 = 1). \end{array}$$

None of $0, 2, 4, 5, 6$, and 8 has a multiplicative inverse in Z_{10}. We thus see that four of the integers in Z_{10} have multiplicative inverses and six do not. □

In general, integers in Z_n may or may not have multiplicative inverses. Of course, 0 never has a multiplicative inverse since $0 \times b = 0$ for all b in Z_n. Theorem 10.1.2 characterizes those integers in Z_n which have multiplicative inverses and, when this characterizing condition is satisfied, its proof points to a method for finding a multiplicative inverse. This method relies on the next simple algorithm for computing the greatest common divisor (GCD) of two positive integers a and b.

Algorithm to compute the GCD of a and b

Set $A = a$ and $B = b$.
While $A \times B \neq 0$, do the following:

[5] Of course, 2 has a multiplicative inverse in the system of rational numbers, namely 1/2, but 1/2 is not an integer.

If $A \geq B$, then replace A by $A - B$.
Else, replace B by $B - A$.

Set GCD $= B$.

In words, we subtract the smaller of the current A and B from the larger and continue until one of A and B is 0 (it will be A because, in the case of a tie, we subtract B from A). We then let GCD equal the terminal value of B. We prove in the next lemma that the algorithm terminates and computes the GCD of a and b correctly.

Lemma 10.1.1 *The preceding algorithm terminates and computes the* GCD *of a and b correctly.*

Proof. We first observe that the algorithm does terminate with the value of A equal to 0. This is so since A and B are always nonnegative integers and at each step one of them decreases. Since we subtract B from A when $A = B$, A achieves the value 0 before B does. We next observe that, given two positive integers m and n with $m \geq n$, we have

$$\text{GCD}\{m, n\} = \text{GCD}\{m - n, n\}.$$

This is because any common divisor of m and n is also a common divisor of $m - n$ and n (if p divides both m and n, then p divides their difference $m - n$); and, conversely, any common divisor of $m - n$ and n is also a common divisor of m and n (if p divides both $m - n$ and n, then p divides their sum $(m - n) + n = m$). Hence, it follows that throughout the algorithm, even though the values of A and B are changing, their GCD is a constant d. Since initially $A = a$ and $B = b$, we see that d is the GCD of a and b. At the termination of the algorithm, we have $A = 0$ and $B > 0$. Since the GCD of two integers, one of which is 0 and one of which is positive, is the positive one, it follows that upon termination the GCD of a and b is the value of B. □

The GCD algorithm is a remarkably simple algorithm for computing the GCD of two nonnegative integers a and b and entails nothing more than repeated subtraction. As illustrated in the next example, it is a consequence of this algorithm that *the GCD, d, of a and b can be written as a linear combination of a and b with integral coefficients: integers x and y exist such that*

$$d = a \times x + b \times y.$$

Example. Compute the GCD of 48 and 126.

We apply the algorithm and display the results in tabular form:

A	B
48	126
48	78
48	30
18	30
18	12
6	12
6	6
0	6

We conclude that the GCD of 48 and 126 is the terminal value $d = 6$ of B.

If, in applying the algorithm to compute the GCD of two positive integers a and b, we subtract A several times consecutively from B or B several times consecutively from A, as just occurred, then we can combine these consecutive steps and treat them as a division.[6] When using the algorithm to compute the GCD by hand, it is generally more efficient to apply the algorithm in this way. The results for computing the GCD of 48 and 126 are displayed in the following table.

A	B	
48	126	$126 = 2 \times 48 + 30$
48	30	$48 = 1 \times 30 + 18$
30	18	$30 = 1 \times 18 + 12$
12	18	$18 = 1 \times 12 + 6$
12	6	$12 = 2 \times 6 + 0$
0	6	$d = 6$

The last nonzero remainder in these divisions is the GCD $d = 6$ of 48 and 126.

We now use the equations in the preceding table to write 6 as a linear combination of 48 and 126:

$$6 = 18 - 1 \times 12$$
$$6 = 18 - 1 \times (30 - 1 \times 18) = 2 \times 18 - 1 \times 30$$
$$6 = 2 \times (48 - 1 \times 30) - 1 \times 30 = 2 \times 48 - 3 \times 30$$
$$6 = 2 \times 48 - 3 \times (126 - 2 \times 48) = 8 \times 48 - 3 \times 126.$$

The final equation, $6 = 8 \times 48 - 3 \times 126$, expresses 6 as an integral linear combination of 48 and 126. □

We next show how to determine which integers in Z_n have multiplicative inverses.

[6] Division of one positive integer by another is, after all, just successive subtraction. For example, when we divide 23 by 5, we get a quotient of 4 and a remainder of 3. This can be displayed as $23 = 4 \times 5 + 3$, which means we can subtract four (and no more) 5s from 23 without getting a negative number.

Theorem 10.1.2 *Let n be an integer with $n \geq 2$ and let a be a nonzero integer in $Z_n = \{0, 1, \ldots, n-1\}$. Then a has a multiplicative inverse in Z_n if and only if the GCD of a and n is 1. If a has a multiplicative inverse, then it is unique.*

Proof. We first show that there can be, at most, one multiplicative inverse for an integer a in Z_n. We shall make use of the rules for addition and multiplication mod n that we have already pointed out, namely, commutativity and associativity. We let b and c be multiplicative inverses of a, and show that $b = c$. Thus, suppose that $a \otimes b = 1$ and $a \otimes c = 1$. Then

$$\begin{array}{rcccccl} c \otimes (a \otimes b) & = & c \otimes 1 & & = & c & \\ c \otimes (a \otimes b) & = & (c \otimes a) \otimes b & = & 1 \otimes b & = & b. \end{array}$$

We thus conclude that $b = c$, and each integer a in Z_n has, at most, one multiplicative inverse.

We next show that, if the GCD of a and n is not 1, then a does not have a multiplicative inverse. Let $m > 1$ be the GCD of a and n. Then n/m is a nonzero integer in Z_n, and since $a \times (n/m)$ is a multiple of n (because there is a factor of m in a), we have

$$a \otimes (n/m) = 0.$$

Suppose there is a multiplicative inverse a^{-1}. Then, using the associative law again,[7] we see that

$$\begin{array}{rcccccl} a^{-1} \otimes (a \otimes (n/m)) & = & a^{-1} \otimes 0 & & = & 0 & \\ a^{-1} \otimes (a \otimes (n/m)) & = & (a^{-1} \otimes a) \otimes (n/m) & = & 1 \otimes n/m & = & n/m. \end{array}$$

Hence, we have $n/m = 0$, which is a contradiction since $1 \leq n/m < n$. Therefore, a does not have a multiplicative inverse.

We lastly suppose that the GCD of a and n is 1 and show that a has a multiplicative inverse. It is a consequence of the GCD algorithm that there exist integers x and y in Z such that

$$a \times x + n \times y = 1. \tag{10.1}$$

The integer x cannot be a multiple of n, for otherwise equation (10.1) would imply that 1 is a multiple of n, contradicting our assumption that $n \geq 2$. Therefore, x has a nonzero remainder when divided by n. That is, there exist integers q and r with $1 \leq r \leq n-1$ such that

$$x = q \times n + r.$$

Substituting into (10.1), we get

$$a \times (q \times n + r) + n \times y = 1,$$

[7] For those students who might have thought that the associative law of arithmetic was not of much consequence and maybe even a nuisance, we now have seen two important applications of it. And there are more to come!

which, upon rewriting, becomes

$$a \times r = 1 - (a \times q + y) \times n.$$

Thus, $a \times r$ differs from 1 by a multiple of n, and it follows that

$$a \otimes r = 1,$$

so r is a (and therefore the unique, by what we have already proved) multiplicative inverse of a in Z_n. □

Corollary 10.1.3 *Let n be a prime number. Then each nonzero integer in Z_n has a multiplicative inverse.*

Proof. Since n is a prime number, the GCD of n and any integer a between 1 and $n - 1$, inclusively, is 1. We now apply Theorem 10.1.2 to complete the proof. □

It is common to call two integers whose GCD is 1 *relatively prime.* Thus, by Theorem 10.1.2, the number of integers in Z_n that have multiplicative inverses equals the number of integers between 1 and $n - 1$ that are relatively prime to n.

Applying the algorithm for computing the GCD of two numbers to the nonzero number a in Z_n and n, we obtain an algorithm for determining whether a has a multiplicative inverse in Z_n. By Theorem 10.1.2, a has a multiplicative inverse if and only if this GCD equals 1. As in the proof of Theorem 10.1.2, we can use the results of this algorithm to determine the multiplicative inverse of a when it exists. We illustrate this technique in the next example.

Example. Determine whether 11 has a multiplicative inverse in Z_{30}, and, if so, calculate the multiplicative inverse.

We apply the algorithm for computing the GCD to 11 and $n = 30$ and display the results in the following table.

A	B	
30	11	$30 = 2 \times 11 + 8$
8	11	$11 = 1 \times 8 + 3$
8	3	$8 = 2 \times 3 + 2$
2	3	$3 = 1 \times 2 + 1$
2	1	$2 = 2 \times 1 + 0$
0	1	$d = 1$

Thus, the GCD of 11 and 30 is $d = 1$, and by Theorem 10.1.2, 11 has a multiplicative inverse in Z_{30}. We use the equations in the preceding table to obtain an equation of the form (10.1) in the proof of Theorem 10.1.2:

$$\begin{aligned}
1 &= 3 - 1 \times 2 \\
1 &= 3 - 1 \times (8 - 2 \times 3) = 3 \times 3 - 1 \times 8 \\
1 &= 3 \times (11 - 1 \times 8) - 1 \times 8 = 3 \times 11 - 4 \times 8 \\
1 &= 3 \times 11 - 4 \times (30 - 2 \times 11) = 11 \times 11 - 4 \times 30.
\end{aligned}$$

The final equation expressing the GCD 1 as a linear combination of 11 and 30, namely,

$$1 = 11 \times 11 - 4 \times 30,$$

tells us that, in Z_{30},

$$1 = 11 \otimes 11.$$

Hence,

$$11^{-1} = 11.$$

Of course, now that we know this fact we can check: $11 \times 11 = 121$, and 121 has remainder 1 when divided by 30. □

Example. Find the multiplicative inverse of 16 in Z_{45}.

We display our calculations in the following table:

A	B	
45	16	$45 = 2 \times 16 + 13$
13	16	$16 = 1 \times 13 + 3$
13	3	$13 = 4 \times 3 + 1$
1	3	$3 = 3 \times 1 + 0$
1	0	$d = 1$

Note that, contrary to the rules for our algorithm to compute GCDs, we made B equal to 0. The reason we set up the algorithm the way we did is (for a computer program) to know where to look for the GCD. But if we are doing the calculations by hand, we can make either A or B equal to 0 (and then choose the other as the GCD).

Since the GCD is 1, we conclude that 16 has a multiplicative inverse in Z_{45}. The resulting equations yield

$$\begin{aligned} 1 &= 13 - 4 \times 3 \\ 1 &= 13 - 4 \times (16 - 1 \times 13) = 5 \times 13 - 4 \times 16 \\ 1 &= 5 \times (45 - 2 \times 16) - 4 \times 16 = 5 \times 45 - 14 \times 16. \end{aligned}$$

We conclude that $16^{-1} = -14 = 31$ in Z_{45}. □

Let n be a prime number. By Corollary 10.1.3, each nonzero integer in Z_n has a multiplicative inverse. This implies that, not only can we add, subtract, and multiply in Z_n, but we can also divide by any nonzero integer in Z_n:

$$a \div b = a \times b^{-1}, \quad (b \neq 0).$$

In addition, multiplicative inverses imply that the following properties hold in Z_n if n is a prime:

(1) (Cancellation rule 1) $a \otimes b = 0$ implies $a = 0$ or $b = 0$.

[If $a \neq 0$, then, multiplying by a^{-1}, we obtain

$$0 = a^{-1} \otimes (a \otimes b) = (a^{-1} \otimes a) \otimes b = 1 \otimes b = b.]$$

(2) (Cancellation rule 2) $a \otimes b = a \otimes c$, $a \neq 0$ implies $b = c$.

[We apply Cancellation rule 1 to $a \otimes (b - c) = 0$.]

(3) (Solutions of linear equations) If $a \neq 0$, the equation

$$a \otimes x = b$$

has the unique solution $x = a^{-1} \otimes b$.

[Multiplying the equation by a^{-1} and using the associative law once again shows that the only possible solution is $x = a^{-1} \otimes b$. Then, substituting $x = a^{-1} \otimes b$ into the equation, we see that

$$a \otimes (a^{-1} \otimes b) = (a^{-1} \otimes a) \otimes b = 1 \otimes b = b.]$$

The conclusion that we draw from this discussion is that the usual laws of arithmetic that we are accustomed to taking for granted in the arithmetic systems of real numbers or rational numbers also hold for Z_n, *provided n is a prime number.* If n is not a prime, then, as we have seen, many but not all of the usual laws of arithmetic hold in Z_n. For example, if n has the nontrivial factorization $n = a \times b$, $(1 < a, b < n)$, then, in Z_n, $a \otimes b = 0$, and neither a nor b has a multiplicative inverse. What is unusual about these arithmetical systems is that they have only a finite number of elements (in contrast to the infinite number of rational, real, and complex numbers).

At this point, we stop using the more cumbersome notation $\oplus$ and $\otimes$ for addition and multiplication mod n and use instead $+$ and $\times$, respectively.

There are other methods, however, to obtain finite arithmetical systems which satisfy the laws of arithmetic that we are accustomed to. The name given to these systems, like Z_n for n a prime number, is a *field.*[8] The method is a generalization of that used to obtain the complex numbers from the real numbers and can be summarized as follows:

Recall that the polynomial $x^2 + 1$ (with real coefficients) has no root in the system of real numbers.[9] The complex numbers are obtained from the real numbers by "adjoining" a root, usually denoted by i, of $x^2 + 1 = 0$. The system of complex numbers

[8]The properties that an arithmetical system must satisfy in order to be labeled a field can be found in most books on abstract algebra.

[9]Because the square of a real number can never be the negative number -1. We hasten to point out that this is *not* one of the usual laws of arithmetic to which we have referred. For example, in Z_5 we have $2^2 = 4 = -1$; in fact, the notion of *negative* number has no significance here because $-1 = 4$, $-2 = 3$, $-3 = 2$, and $-4 = 1$. We should not think of the additive inverse as a negative number.

consists of all numbers of the form $a + bi$, where a and b are real numbers, for which the usual laws of arithmetic hold and where $i^2 + 1 = 0$ (i.e., $i^2 = -1$). For instance,

$$(2 + 3i) \times (4 + i) = 8 + 2i + 12i + 3i^2 = 8 + 14i - 3 = 5 + 14i.$$

This method can be used to construct fields with p^k elements for every prime p and integer $k \geq 2$, starting from the field Z_p. We illustrate the method by constructing fields with 4 and 27 elements, respectively.

Example. *Construction of a field of* 4 *elements.* We start with Z_2 and the polynomial $x^2 + x + 1$ with coefficients in Z_2. This polynomial has no root in Z_2, since the only possibilities are 0 and 1 and $0^2 + 0 + 1 = 1$ and $1^2 + 1 + 1 = 1$. Because this polynomial has degree 2, we conclude that it cannot be factored in any nontrivial way. We adjoin a root i of this polynomial[10] to Z_2, getting $i^2 + i + 1 = 0$, or, equivalently,

$$i^2 = -i - 1 = i + 1.$$

(Recall that in Z_2, we have $-1 = 1$.) The elements of the resulting field are the four elements

$$\{0, 1, i, 1 + i\},$$

with addition table and multiplication tables as follows:

$+$	0	1	i	$1+i$
0	0	1	i	$1+i$
1	1	0	$1+i$	i
i	i	$1+i$	0	1
$1+i$	$1+i$	i	1	0

$\times$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	$1+i$	1
$1+i$	0	$1+i$	1	i

Thus, $i^{-1} = 1 + i$, since $i \times (1 + i) = i + i^2 = i + (1 + i) = 1$. □

Example. *Construction of a field of* $3^3 = 27$ *elements.* We start with $Z_3 = \{0, 1, 2\}$, the integers mod 3. We look for a polynomial of degree 3 with coefficients in Z_3 that cannot be factored in a nontrivial way. A polynomial of degree 3 will have this property if and only if it has no root in Z_3.[11] The polynomial $x^3 + 2x + 1$ with coefficients in

[10] We use i as a symbol for the root to stress the *analogy* with the complex numbers. It is not true that $i^2 = -1$.

[11] This is not a general rule. If a polynomial of degree 2 or 3 is factored nontrivially, one of the factors is linear and the polynomial has a root. But, for instance, a polynomial of degree 4 may be factorable into two polynomials of degree 2, neither of which has a root.

Z_3 does not have a root in Z_3 (we need only test the three elements $0, 1$, and 2 of Z_3). Thus, we adjoin a root i of this polynomial, getting $i^3 + 2i + 1 = 0$ or, equivalently,

$$i^3 = -1 - 2i = 2 + i.$$

(Recall that, in Z_3, we have $-1 = 2$ and $-2 = 1$.) Now use the usual rules of arithmetic, but whenever an i^3 appears, replace it by $2 + i$. The elements of the resulting field are the 27 elements

$$\{a + bi + ci^2 : a, b \text{ and } c \text{ in } Z_3\}.$$

Since there are 27 elements, it is no longer practical to write out the addition and multiplication tables. But we illustrate some of the arithmetic in this system as follows:

$$(2 + i + 2i^2) + (1 + i + i^2) = (2 + 1) + (1 + 1)i + (2 + 1)i^2 = 0 + 2i + 0i^2 = 2i;$$

$$\begin{aligned} (1 + i)(2 + i^2) &= 1 \times 2 + i^2 + 2i + i \times i^2 \\ &= 1 + i^2; \end{aligned}$$

$$\begin{aligned} (1 + 2i^2)(1 + i + 2i^2) &= 1 + i + 2i^2 + 2i^2 + 2i^3 + 2 \times 2i^4 \\ &= 1 + i + 2i^2 + 2i^2 + 2(2 + i) + (i \times i^3) \\ &= 1 + i + i^2 + (1 + 2i) + i \times (2 + i) \\ &= 1 + i + i^2 + 1 + 2i + 2i + i^2 \\ &= 2 + 2i + 2i^2. \end{aligned}$$

It is straightforward to check that

$$i^{-1} = 1 + 2i^2 \text{ and } (2 + i + 2i^2)^{-1} = 1 + i^2.$$

□

We conclude this section with the following remarks: For each prime p and each integer $k \geq 2$ there exists a polynomial of degree k with coefficients in Z_p that does not have a nontrivial factorization. Thus, in the manner illustrated in the preceding two examples, we can construct a field with p^k elements. Conversely, it can be proved that, if there is a field with a finite number m elements—that is, a finite system satisfying the usual rules of arithmetic—then $m = p^k$ for some positive integer k and some prime number p, and it can be obtained from Z_p in the manner previously described (or is Z_p if $k = 1$). Thus, *only for a prime power number of elements do finite fields exist.*

10.2 Block Designs

We begin this section with a simplified motivating example from the design of experiments for statistical analysis.

Example. Suppose there are seven varieties of a product to be tested for acceptability among consumers. The manufacturer plans to ask some random (or typical) consumers to compare the different varieties. One way to do this is for each of the consumers involved in the testing to do a complete test by comparing all of the seven varieties. However, the manufacturer, fully aware of the time required for the comparisons and the possible reluctance of individuals to get involved, decides to have each consumer do an incomplete test by comparing only some of the varieties. Thus, the manufacturer asks each person to compare a certain three of the varieties. To draw meaningful conclusions based on statistical analysis of the results, the test must have the property that each pair of the seven varieties is compared by exactly one person. Can such a testing experiment be designed?

We label the different varieties $0, 1, 2, 3, 4, 5$ and 6.[12] There are $\binom{7}{2} = 21$ pairs of the seven varieties. Each tester gets three varieties and thus makes $\binom{3}{2} = 3$ comparisons. Since each pair is to be compared exactly once, the number of testers must equal

$$\frac{21}{3} = 7.$$

Thus, in this case, the number of individuals involved in the experiment is the same as the number of varieties being tested. Fortunately, the preceding quotient turned out to be an integer, for otherwise we would have to conclude that it is impossible to design an experiment with the constraints as given. What we now seek is seven (one for each person involved in the test) subsets $B_1, B_2, \ldots, B_7$ of the seven varieties, which we shall call *blocks*, with the property that each pair of varieties is together in exactly one block. Such a collection of 7 blocks is the following:

$$B_1 = \{0, 1, 3\}, B_2 = \{1, 2, 4\}, B_3 = \{2, 3, 5\}, B_4 = \{3, 4, 6\},$$

$$B_5 = \{0, 4, 5\}, B_6 = \{1, 5, 6\}, B_7 = \{0, 2, 6\}.$$

Another way to present this experimental design is given in the array that follows: In this array, we have one column for each of the seven varieties and one row for each of the seven blocks. A 1 in row i and column j ($i = 1, 2, \ldots, 7; j = 0, 1, \ldots, 6$) means that variety j belongs to block B_i, and a 0 means that variety j does not belong to block B_i. The fact that each block contains three varieties is reflected in the table by the fact that each row contains three 1s. The fact that each pair of varieties is together in one block is equivalent to the property of the table that each pair of columns has

[12] Of course, we are free to *label* the varieties in any way we choose. The reason we choose $0, 1, 2, 3, 4, 5, 6$ is that we can think of the varieties as the numbers in Z_7, the integers mod 7.

1s in exactly one common row. As is evident from the table, each variety occurs in three blocks. This array is the incidence array of the experimental design.

	0	1	2	3	4	5	6
B_1	1	1	0	1	0	0	0
B_2	0	1	1	0	1	0	0
B_3	0	0	1	1	0	1	0
B_4	0	0	0	1	1	0	1
B_5	1	0	0	0	1	1	0
B_6	0	1	0	0	0	1	1
B_7	1	0	1	0	0	0	1

□

Before discussing more examples, we define some terms and discuss some elementary properties of designs. Let k, λ, and v be positive integers with

$$2 \leq k \leq v.$$

Let X be any set of v elements, called *varieties*, and let $\mathcal{B}$ be a collection $B_1, B_2, \ldots, B_b$ of k-element subsets of X called *blocks*.[13] Then $\mathcal{B}$ is a *balanced block design* on X, provided that each pair of elements of X occurs together in exactly λ blocks. The number λ is called the *index of the design*. The foregoing assumption that k is at least 2 is to prevent trivial solutions: If $k = 1$, then a block contains no pairs and $\lambda = 0$.

Let $\mathcal{B}$ be a balanced block design. If $k = v$ (that is, the complete set of varieties occurs in each block), then the design $\mathcal{B}$ is called a *complete* block design. If $k < v$, then $\mathcal{B}$ is a balanced *incomplete* block design, or *BIBD*[14] for short. A complete design corresponds to a testing experiment in which each individual compares each pair of varieties. From a combinatorial point of view, they are trivial, forming a collection of sets all equal to X, and we henceforth deal with incomplete designs—that is, designs for which $k < v$.

Let $\mathcal{B}$ be a BIBD on X. As in the preceding example, we associate with $\mathcal{B}$ an *incidence matrix* or *incidence array* A. The array A has b rows, one corresponding to each of the blocks $B_1, B_2, \ldots, B_b$, and v columns, one corresponding to each of the varieties $x_1, x_2, \ldots, x_v$ in X. The entry a_{ij} at the intersection of row i and column j is 0 or 1:

$$a_{ij} = 1 \text{ if } x_j \text{ is in } B_i,$$

$$a_{ij} = 0 \text{ if } x_j \text{ is not in } B_i.$$

[13] We do not rule out the possibility that some of the blocks may be identical, although it is more challenging to find designs all of whose blocks are different. Thus, the collection of blocks is, in general, a multiset of blocks.

[14] BIBDs were introduced by F. Yates, Complex Experiments (with Discussion), *J. Royal Statistical Society*, Suppl. 2, (1935), 181–247.

We talk about *the* incidence matrix of $\mathcal{B}$, even though it depends on the order in which we list the blocks and the order in which we list the varieties. The rows of the incidence matrix display the varieties contained in each of the blocks. The columns of the incidence matrix display the blocks containing each of the varieties. Except for the labeling of the varieties and of the blocks, the incidence matrix A contains full information about the BIBD. Since each block contains k varieties, each row of the incidence matrix A contains k 1s. Since there are b blocks, the total number of 1s in A equals bk. We now show that each variety is contained in the same number of blocks; that is, each column of A contains the same number of 1s.

Lemma 10.2.1 *In a BIBD, each variety is contained in*

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks.

Proof. We use the important technique of counting in two ways and then equating the two counts. Let x_i be any one of the varieties, and suppose that x_i is contained in r blocks

$$B_{i_1}, B_{i_2}, \ldots, B_{i_r}. \tag{10.2}$$

Since each block contains k elements, each of these blocks contains $k-1$ varieties other than x_i. We now consider each of the $v-1$ pairs $\{x_i, y\}$, where y is a variety different from x_i, and for each such pair, we count the number of blocks in which both varieties are contained. Each pair $\{x_i, y\}$ is contained in λ blocks (these blocks must be λ of the blocks in (10.2) since they are all the blocks containing x_i). Adding, we get

$$\lambda(v-1).$$

On the other hand, each of the blocks in (10.2) contains $k-1$ pairs, one element of which is x_i. Adding, we now get

$$(k-1)r.$$

Equating these two counts, we obtain

$$\lambda(v-1) = (k-1)r.$$

Hence, x_i is contained in $\lambda(v-1)/(k-1)$ blocks. This is true for each variety x_i, and thus each variety is contained in $r = \lambda(v-1)/(k-1)$ blocks. □

Corollary 10.2.2 *In a BIBD, we have*

$$bk = vr.$$

Proof. We have already observed that counting by rows, the number of 1s in the incidence matrix A of a BIBD is bk. By Lemma 10.2.1, we know that each column of A contains r 1s. Thus, counting by columns, the number of 1s in A equals vr. Equating the two counts, we obtain $bk = vr$. □

Corollary 10.2.3 *In a BIBD, we have*

$$\lambda < r.$$

Proof. In a BIBD, we have, by definition, $k < v$; hence, $k - 1 < v - 1$. Using Lemma 10.2.1, we conclude that $\lambda < r$. □

As a consequence of Lemma 10.2.1, we now have five parameters, not all independent, that are associated with a BIBD:

b: the number of blocks;

v: the number of varieties;

k: the number of varieties in each block;

r: the number of blocks containing each variety;

λ: the number of blocks containing each pair of varieties.

We call b, v, k, r, λ the *parameters* of the BIBD. The parameters of the design in our introductory example are: $b = 7, v = 7, k = 3, r = 3,$ and $\lambda = 1$.

Example. Is there a BIBD with parameters $b = 12, k = 4, v = 16,$ and $r = 3$ (the parameter λ is not specified)?

The equation $bk = vr$ in Corollary 10.2.2 holds, since both sides have the value 48. By Lemma 10.2.1, if there is such a design, its index λ satisfies

$$\lambda = \frac{r(k-1)}{v-1} = \frac{3(3)}{15} = \frac{9}{15}.$$

Since this is not an integer, there can be no such design with four of its parameters as given. □

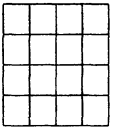
Example. In this example, we display a design with parameters $b = 12, v = 9, k = 3, r = 4,$ and $\lambda = 1$. It is most convenient to define the design by its 12-by-9 incidence

matrix:

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

It is straightforward to check that this matrix defines a BIBD with parameters as given. □

Example. Consider the squares of a 4-by-4 board:



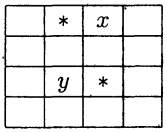
Let the varieties be the 16 squares of the board. We define blocks as follows: For each given square, we take the 6 other squares that are either in its row or in its column (so not the given square itself).[15] Therefore, each of the 16 squares on the board determines a block in this way. We thus have $b = 16, v = 16$, and $k = 6$. Each square belongs to six blocks, since each square lies in a row with three other squares and in a column with three more squares. Thus, we also have $r = 6$. But we haven't yet shown we have a BIBD. So let's take a pair of squares x and y. There are three possibilities:

1. x and y are in the same row. Then x and y are together in the two blocks determined by the other two squares in their row.

2. x and y are in the same column. Then x and y are together in the two blocks determined by the other two squares in their column.

3. x and y are in different rows and in different columns. Then x and y are together in two blocks, one determined by the square at the intersection of the row of x and the column of y, the other determined by the intersection of the column of x and the row of y. The following array, where the blocks are those determined by the squares marked with an asterisk (*), is illustrative:

[15] We can think of the varieties as a rook on the 4-by-4 board and the blocks as all the squares that a rook on the board can attack.



Since each pair of varieties is together in two blocks, we have a BIBD with $\lambda = 2$. □

The basic property of designs presented in the next theorem says that, in a BIBD, the number of blocks must be at least as large as the number of varieties and is known as Fisher's inequality.[16]

Theorem 10.2.4 *In a BIBD, $b \geq v$.*

Proof. We outline a linear algebraic proof for those familiar with the ideas it uses. Let A be the b-by-v incidence matrix of a BIBD. Since each variety is in r blocks and since each pair of varieties is in λ blocks, the v-by-v matrix A^TA, obtained by multiplying[17] the transpose[18] A^T of A by A, has each main diagonal entry equal to r and each off-diagonal element equal to λ:

$$A^TA = \begin{bmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{bmatrix}.$$

Since $\lambda < r$, by Corollary 10.2.3, the matrix A^TA can be shown to have a nonzero determinant[19] and hence is invertible. Thus, A^TA has rank equal to v. Therefore A has rank at least v, and since A is a b-by-v matrix, we have $b \geq v$.[20] □

A BIBD for which equality holds in Theorem 10.2.4, that is, for which the number b of blocks equals the number v of varieties, is called *symmetric,*[21] and this is shortened

[16]R.A. Fisher, An Examination of the Different Possible Solutions of a Problem in Incomplete Blocks, *Annals of Eugenics*, 10(1940), 52–75.

[17]The product of an m-by-n matrix X with typical entry x_{ij} and an n-by-p matrix Y with typical entry y_{jk} is the m-by-p matrix Z whose typical entry is $z_{ik} = \sum_{j=1}^{n} x_{ij}y_{jk}$.

[18]The transpose of an m-by-n matrix X is the n-by-m matrix X^T obtained by letting the rows of X "become" the columns of X^T and the columns of X "become" the rows of X^T. If, as the matrix A in the proof of the theorem, the entries of X are 0s and 1s, then the typical entry of X^TX in row i and column j (by the definition of product, it is determined by column i and column j of X) equals the number of rows in which *both* column i and column j have a 1.

[19]The value of the determinant is $(r - \lambda)^{v-1}(r + (v - 1)\lambda)$, which is nonzero by Corollary 10.2.3.

[20]If you didn't understand this proof because you never studied elementary linear algebra, I hope you will now do so. Only then can you appreciate what an elegant and simple proof has just been shown you.

[21]The symmetry has to do with the parameters satisfying $b = v$ and, as shown in the next few lines, $k = r$.

to SBIBD. Since a BIBD satisfies $bk = vr$, we conclude by cancellation that, for an SBIBD, we also have $k = r$. By Lemma 10.2.1, the index λ for an SBIBD is determined by v and k by

$$\lambda = \frac{k(k-1)}{v-1}. \tag{10.3}$$

Thus, the parameters associated with an SBIBD are as follows:

v: the number of blocks;

v: the number of varieties;

k: the number of varieties in each block;

k: the number of blocks containing each variety;

λ: the number of blocks containing each pair of varieties, where λ is given by (10.3).

Some of our examples have been SBIBDs.

We now discuss a method for constructing SBIBDs that uses the arithmetic of the integers mod n. In this method, the varieties are the integers in Z_n, so, to agree with our notation, we use v instead of n.

Thus, let $v \geq 2$ be an integer, and consider the set of integers mod v:

$$Z_v = \{0, 1, 2, \ldots, v-1\}.$$

Note that addition and multiplication in Z_v are denoted by the usual symbols $+$ and $\times$. Let $B = \{i_1, i_2, \ldots, i_k\}$ be a subset of Z_v consisting of k integers. For each integer j in Z_v, we define

$$B + j = \{i_1 + j, i_2 + j, \ldots, i_k + j\}$$

to be the subset of Z_v obtained by adding mod v the integer j to each of the integers in B. The set $B + j$ also contains k integers. This is because if

$$i_p + j = i_q + j \quad (\text{in } Z_v),$$

then cancelling j (by adding the additive inverse $-j$ to both sides) we get $i_p = i_q$. The v sets

$$B = B + 0, B + 1, \ldots, B + v - 1$$

so obtained are called the *blocks developed from the block* B, and B is called the *starter block*.

Example. Let $v = 7$ and consider

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

Now consider the starter block

$$B = \{0, 1, 3\}.$$

Then we have

$$\begin{aligned} B + 0 &= \{0, 1, 3\} \\ B + 1 &= \{1, 2, 4\} \\ B + 2 &= \{2, 3, 5\} \\ B + 3 &= \{3, 4, 6\} \\ B + 4 &= \{4, 5, 0\} \\ B + 5 &= \{5, 6, 1\} \\ B + 6 &= \{6, 0, 2\}. \end{aligned}$$

(Each set in this list, other than the first, is obtained by adding 1 mod 7 to the previous set. In addition, the first set B on the list can be gotten from the last by adding 1 mod 7.) This is a BIBD, indeed, the same one in the introductory example of this section. Since $b = v$, we have an SBIBD with $b = v = 7$, $k = r = 3$, and $\lambda = 1$. □

Example. Let $v = 7$ as in the previous example, but now let the starter block be

$$B = \{0, 1, 4\}.$$

Then we have

$$\begin{aligned} B + 0 &= \{0, 1, 4\} \\ B + 1 &= \{1, 2, 5\} \\ B + 2 &= \{2, 3, 6\} \\ B + 3 &= \{3, 4, 0\} \\ B + 4 &= \{4, 5, 1\} \\ B + 5 &= \{5, 6, 2\} \\ B + 6 &= \{6, 0, 3\}. \end{aligned}$$

In this case, we do not obtain a BIBD because, for instance, the varieties 1 and 2 occur together in one block, while the varieties 1 and 5 are together in two blocks. □

It follows from these two examples that sometimes, but not always, the blocks developed from a starter block are the blocks of an SBIBD. The property that we need in order to obtain an SBIBD in this way is contained in the next definition. Let B be a subset of k integers in Z_v. Then B is called a *difference set mod* v, provided that each nonzero integer in Z_v occurs the same number λ of times among the $k(k-1)$ differences among distinct elements of B (in both orders):

$$x - y \quad (x, y \text{ in } B; x \neq y).$$

Since there are $v - 1$ nonzero integers in Z_v, each nonzero integer in Z_v must occur

$$\lambda = \frac{k(k-1)}{v-1}$$

times as a difference in a difference set.

Example. Let $v = 7$ and $k = 3$ and consider $B = \{0, 1, 3\}$. We compute the subtraction table for the integers in B, ignoring the 0's in the diagonal positions:

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

Examining this table, we see that the nonzero integers 1, 2, 3, 4, 5, 6 in Z_7 each occur exactly once in the off-diagonal positions and hence exactly once as a difference. Hence, B is a difference set mod 7. □

Example. Again, let $v = 7$ and $k = 3$, but now let $B = \{0, 1, 4\}$. Computing the subtraction table, we now get

$-$	0	1	4
0	0	6	3
1	1	0	4
4	4	3	0

We see that 1 and 6 each occur once as a difference, 3 and 4 each occur twice, and 2 and 5 do not occur at all. Thus, B is not a difference set in this case. □

Theorem 10.2.5 *Let B be a subset of $k < v$ elements of Z_v that forms a difference set mod v. Then the blocks developed from B as a starter block form an SBIBD with index*

$$\lambda = \frac{k(k-1)}{v-1}.$$

Proof. Since $k < v$, the blocks are not complete. Each block contains k elements. Moreover, the number of blocks is the same as the number v of varieties. Thus, it remains to be shown that each pair of elements of Z_v is together in the same number of blocks. Since B is a difference set, each nonzero integer in Z_v occurs as a difference exactly $\lambda = k(k-1)/(v-1)$ times. We show that each pair of elements of Z_v is in λ blocks and hence λ is the index of the SBIBD.

Let p and q be distinct integers in Z_v. Then $p - q \neq 0$, and since B is a difference set mod v, the equation

$$x - y = p - q$$

has λ solutions with x and y in B. For each such solution x and y, let $j = p - x$. Then

$$p = x + j \text{ and } q = y - x + p = y + j.$$

Thus, p and q are together in the block $B + j$ for each of the λ j's. Hence, p and q are together in λ blocks. Since

$$v(v-1)\lambda = v(v-1)\frac{k(k-1)}{v-1} = vk(k-1),$$

it follows that each pair of distinct integers in Z_v is together in exactly λ blocks. □

Example. Find a difference set of size 5 in Z_{11}, and use it as a starter block in order to construct an SBIBD.

We show that $B = \{0, 2, 3, 4, 8\}$ is a difference set with $\lambda = 2$. We compute the subtraction table to obtain

−	0	2	3	4	8
0	0	9	8	7	3
2	2	0	10	9	5
3	3	1	0	10	6
4	4	2	1	0	7
8	8	6	5	4	0

Examining all the off-diagonal positions, we see that each nonzero integer in Z_{11} occurs twice as a difference and hence B is a difference set. Using B as a starter block, we obtain the following blocks for an SBIBD with parameters $b = v = 11$, $k = r = 5$, and $\lambda = 2$:

$$\begin{aligned}
B + 0 &= \{0, 2, 3, 4, 8\} \\
B + 1 &= \{1, 3, 4, 5, 9\} \\
B + 2 &= \{2, 4, 5, 6, 10\} \\
B + 3 &= \{0, 3, 5, 6, 7\} \\
B + 4 &= \{1, 4, 6, 7, 8\} \\
B + 5 &= \{2, 5, 7, 8, 9\} \\
B + 6 &= \{3, 6, 8, 9, 10\} \\
B + 7 &= \{0, 4, 7, 9, 10\} \\
B + 8 &= \{0, 1, 5, 8, 10\} \\
B + 9 &= \{0, 1, 2, 6, 9\} \\
B + 10 &= \{1, 2, 3, 7, 10\}.
\end{aligned}$$

□

10.3 Steiner Triple Systems

Let $\mathcal{B}$ be a balanced incomplete block design whose parameters are b, v, k, r, λ. Since $\mathcal{B}$ is incomplete, we know, by definition, that $k < v$; that is, the number of varieties in each block is less than the total number of varieties. Suppose $k = 2$. Then each block in $\mathcal{B}$ contains exactly two varieties. for each pair of varieties to occur in the same number λ of blocks of $\mathcal{B}$, each subset of two varieties must occur as a block exactly λ times. Thus, for BIBDs, with $k = 2$, we have no choice but to take each subset of two varieties and write it down λ times.

Example. A BIBD with $v = 6$, $k = 2$, and $\lambda = 1$ is given by

$$\begin{array}{lll} \{0,1\} & \{0,2\} & \{0,3\} \\ \{0,4\} & \{0,5\} & \{1,2\} \\ \{1,3\} & \{1,4\} & \{1,5\} \\ \{2,3\} & \{2,4\} & \{2,5\} \\ \{3,4\} & \{3,5\} & \{4,5\}. \end{array}$$

To get a BIBD with $\lambda = 2$, simply take each of the blocks twice. To get one with $\lambda = 3$, take each of the blocks three times. □

So BIBDs with block size 2 are trivial. The smallest (in terms of block size) interesting case occurs when $k = 3$. Balanced block designs with block size $k = 3$ are called *Steiner triple systems.*[22] The first example given in Section 10.2 is a Steiner triple system. It has seven varieties and seven blocks of size 3. Also, each pair of varieties is contained in $\lambda = 1$ block. This is the only instance of a Steiner triple system that forms an SBIBD—that is, one for which the number of blocks equals the number of varieties.

Another example of a Steiner triple system is obtained by taking $v = 3$ varieties $0, 1$, and 2 and the one block $\{0, 1, 2\}$. We thus have $b = 1$, and clearly each pair of varieties is contained in $\lambda = 1$ block. This Steiner system is not an incomplete design since $v = k = 3$.[23] Every other Steiner triple system is a BIBD.

Example. The following is an example of a Steiner triple system of index $\lambda = 1$ with nine varieties:

$$\begin{array}{lll} \{0,1,2\} & \{3,4,5\} & \{6,7,8\} \\ \{0,3,6\} & \{1,4,7\} & \{2,5,8\} \\ \{0,4,8\} & \{2,3,7\} & \{1,5,6\} \\ \{0,5,7\} & \{1,3,8\} & \{2,4,6\}. \end{array}$$

□

In the next theorem, we obtain some relationships that must hold among the parameters of a Steiner triple system.

Theorem 10.3.1 *Let $\mathcal{B}$ be a Steiner triple system with parameters $b, v, k = 3, r, \lambda$. Then*

$$r = \frac{\lambda(v-1)}{2} \tag{10.4}$$

and

$$b = \frac{\lambda v(v-1)}{6}. \tag{10.5}$$

[22] After J. Steiner, who was one of the first to consider them: Combinatorische Aufgabe, *Journal für die reine und angewandte Mathematik*, 45 (1853), 181–182.

[23] We consider it as a Steiner triple system since we shall use it to construct Steiner triple systems that are incomplete designs.

If the index is $\lambda = 1$, then there is a nonnegative integer n such that $v = 6n + 1$ or $v = 6n + 3$.

Proof. By Theorem 10.2.1, we have

$$r = \frac{\lambda(v-1)}{k-1}$$

for any BIBD. Since a Steiner triple system is a BIBD with $k = 3$, we get (10.4). For a BIBD, we also have, by Corollary 10.2.2,

$$bk = vr.$$

Substituting the value of r, as given by (10.4), and using $k = 3$ again, we get (10.5).

The equations (10.4) and (10.5) tell us that, if there is a Steiner triple system of index λ with v varieties, then $\lambda(v-1)$ is even and $\lambda v(v-1)$ is divisible by 6. Now assume that $\lambda = 1$. Then $v - 1$ is even and hence v is odd, and $v(v-1)$ is divisible by 6. The latter implies that either v or $v - 1$ is divisible by 3. First, suppose that v is divisible by 3. Since v is odd, this means that v is 3 times an odd number:

$$v = 3 \times (2n + 1) = 6n + 3.$$

Now suppose that $v - 1$ is divisible by 3. Since v is odd, $v - 1$ is even and we find that $v - 1$ is 3 times an even number:

$$v - 1 = 3 \times (2n) = 6n \text{ and so } v = 6n + 1.$$

□

In the remainder of this section we consider only Steiner triple systems of index $\lambda = 1$. By Theorem 10.3.1, the number of varieties in a Steiner triple system of index $\lambda = 1$ is either $v = 6n + 1$ or $v = 6n + 3$, where n is a nonnegative integer. This raises the question as to whether, for all nonnegative integers n, there exist Steiner triple systems with $v = 6n + 1$ and $v = 6n + 3$ varieties. The case $n = 0$ and $v = 6n + 1$ has to be eliminated, since, in that case, $v = 1$ and no triples are possible. For all other cases, it was shown by Kirkman[24] that Steiner triple systems can be constructed. The proof is beyond the scope of this book. We shall be satisfied to give a method for constructing a Steiner triple system from two known (possibly the same) Steiner systems of smaller order.

Theorem 10.3.2 *If there are Steiner triple systems of index $\lambda = 1$ with v and w varieties, respectively, then there is a Steiner triple system of index $\lambda = 1$ with vw varieties.*

[24] T. P. Kirkman, On a Problem in Combinations, *Cambridge and Dublin Mathematics Journal*, 2 (1847), 191–204. This question was also raised later by J. Steiner, who was unaware of Kirkman's work (cf. footnote 22). It was only later that Kirkman's work became known, and this was long after the name *Steiner* (and not *Kirkman*) triple systems had become common.

Proof. Let $\mathcal{B}_1$ be a Steiner triple system of index $\lambda = 1$ with the v varieties $a_1, a_2, \ldots, a_v$ and let $\mathcal{B}_2$ be a Steiner triple system of index $\lambda = 1$ with the w varieties $b_1, b_2, \ldots, b_w$. We consider a set X of vw varieties $c_{ij}, (i = 1, \ldots, v; j = 1, \ldots, w)$, which we may think of as the entries (or positions) of a v-by-w array whose rows correspond to $a_1, a_2, \ldots, a_v$ and whose columns correspond to $b_1, b_2, \ldots, b_w$:[25]

$$\begin{array}{c} \\ a_1 \\ a_2 \\ \vdots \\ a_v \end{array} \begin{array}{c} \begin{array}{cccc} b_1 & b_2 & \cdots & b_w \end{array} \\ \left[\begin{array}{cccc} c_{11} & c_{12} & \cdots & c_{1w} \\ c_{21} & c_{22} & \cdots & c_{2w} \\ \vdots & \vdots & \ddots & \vdots \\ c_{v1} & c_{v2} & \cdots & c_{vw} \end{array}\right] \end{array}. \tag{10.6}$$

We define a set $\mathcal{B}$ of triples of the elements of X. Let $\{c_{ir}, c_{js}, c_{kt}\}$ be a set of three elements of X. Then $\{c_{ir}, c_{js}, c_{kt}\}$ is a triple of $\mathcal{B}$ if and only if one of the following holds:

(1) $r = s = t$, and $\{a_i, a_j, a_k\}$ is a triple in $\mathcal{B}_1$. Put another way, the elements c_{ir}, c_{js}, and c_{kt} are in the same column of the array (10.6), and the rows in which they lie correspond to a triple of $\mathcal{B}_1$.

(2) $i = j = k$, and $\{b_r, b_s, b_t\}$ is a triple of $\mathcal{B}_2$. Put another way, the elements c_{ir}, c_{js}, and c_{kt} are in the same row of the array (10.6), and the columns in which they lie correspond to a triple of $\mathcal{B}_2$.

(3) i, j, and k are all different and $\{a_i, a_j, a_k\}$ is a triple of $\mathcal{B}_1$, *and* r, s, and t are all different and $\{b_r, b_s, b_t\}$ is a triple of $\mathcal{B}_2$. Put another way, the elements c_{ir}, c_{js}, and c_{kt} are in three different rows and three different columns of the array (10.6), and the rows in which they lie correspond to a triple of $\mathcal{B}_1$ and, similarly, the columns in which they lie correspond to a triple of $\mathcal{B}_2$.

For the rest of the proof we shall implicitly use the fact that no triple of $\mathcal{B}$ lies either in exactly two rows or exactly two columns of the array (10.6). We now show that this set $\mathcal{B}$ of triples of X defines a Steiner triple system of index $\lambda = 1$. Thus, let c_{ir}, c_{js} be a pair of distinct elements of X. We need to show that there is exactly one triple of $\mathcal{B}$ containing both c_{ir} and c_{js}; that is, we need to show that there is exactly one element c_{kt} of X such that $\{c_{ir}, c_{js}, c_{kt}\}$ is a triple of $\mathcal{B}$. We consider three cases:

Case 1: $r = s$ *and thus* $i \neq j$. Our pair of elements in this case is c_{ir}, c_{jr} lying in the same column of (10.6). Since $\mathcal{B}_1$ is a Steiner triple system of index $\lambda = 1$, there is a

[25] We could think of c_{ij} as the ordered pair (a_i, b_j) but, since we are going to be discussing unordered pairs and triples, it seems less confusing to invent the new symbols c_{ij}.

unique triple $\{a_i, a_j, a_k\}$ containing the distinct pair a_i, a_j. Hence, $\{c_{ir}, c_{jr}, c_{kr}\}$ is the unique triple of $\mathcal{B}$ containing the pair c_{ir}, c_{jr}.

Case 2: $i = j$ *and thus* $r \neq s$. Our pair of elements is now c_{ir}, c_{is} lying in the same row of (10.6). Since $\mathcal{B}_2$ is a Steiner triple system of index $\lambda = 1$, there is a unique triple $\{b_r, b_s, b_t\}$ containing the distinct pair b_r, b_s. Hence, $\{c_{ir}, c_{is}, c_{it}\}$ is the unique triple of $\mathcal{B}$ containing the pair c_{ir}, c_{is}.

Case 3: $i \neq j$ *and* $r \neq s$. There is a unique triple $\{a_i, a_j, a_k\}$ of $\mathcal{B}_1$ containing the distinct pair a_i, a_j and a unique triple $\{b_r, b_s, b_t\}$ of $\mathcal{B}_2$ containing the distinct pair b_r, b_s. The triple $\{c_{ir}, c_{js}, c_{kt}\}$ is then the unique triple of $\mathcal{B}$ containing the pair c_{ir}, c_{js}.

We have thus shown that $\mathcal{B}$ is a Steiner triple system of index $\lambda = 1$ with vw varieties. □

Example. The simplest instance in which we may apply Theorem 10.3.2 is that obtained by choosing $\mathcal{B}_1$ and $\mathcal{B}_2$ to be Steiner triple systems with three varieties. The result should be a Steiner triple system with $3 \times 3 = 9$ varieties.

Let $\mathcal{B}_1$ be the Steiner triple system with the three varieties a_1, a_2, a_3 and unique triple $\{a_1, a_2, a_3\}$, and let $\mathcal{B}_2$ be the Steiner triple system with the three varieties b_1, b_2, b_3 and unique triple $\{b_1, b_2, b_3\}$. We consider the set X of nine varieties comprising the entries of the following array:

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\ \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix} \end{array}.$$

Following the construction in the proof of Theorem 10.3.2, we obtain the following set of 12 triples, which constitute a Steiner triple system of index 1 with nine varieties:

(1) The entries in each of the three rows:

$$\{c_{11}, c_{12}, c_{13}\}, \{c_{21}, c_{22}, c_{23}\}, \{c_{31}, c_{32}, c_{33}\}$$

(2) The entries in each of the three columns:

$$\{c_{11}, c_{21}, c_{31}\}\{c_{12}, c_{22}, c_{32}\}, \{c_{13}, c_{23}, c_{33}\}.$$

(iii) Three entries, no two from the same row or column:[26]

$$\{c_{11}, c_{22}, c_{33}\}, \{c_{12}, c_{23}, c_{31}\}, \{c_{13}, c_{21}, c_{32}\}$$

$$\{c_{13}, c_{22}, c_{31}\}, \{c_{12}, c_{21}, c_{33}\}, \{c_{11}, c_{23}, c_{32}\}$$

[26]Considering the array as a 3-by-3 board, these correspond to positions for three nonattacking rooks on the board.

If we replace $c_{11}, c_{21}, c_{31}, c_{12}, c_{22}, c_{32}, c_{13}, c_{23}, c_{33}$ by $0, 1, 2, 3, 4, 5, 6, 7, 8$, respectively, we obtain the Steiner triple system $\mathcal{B}$ with nine varieties given earlier in this section:

$$\begin{array}{cccc} \{0,1,2\} & \{0,3,6\} & \{0,4,8\} & \{2,4,6\} \\ \{3,4,5\} & \{1,4,7\} & \{2,3,7\} & \{1,3,8\} \\ \{6,7,8\} & \{2,5,8\} & \{1,5,6\} & \{0,5,7\} \end{array} \tag{10.7}$$

□

The columns of (10.7) partition the triples of $\mathcal{B}$ into parts so that each variety occurs in exactly one triple in each part. A Steiner triple system of index $\lambda = 1$ with this property is called *resolvable*, and each part is called a *resolvability class*. Note that each resolvability class is a partition of the set of varieties into triples. The notion of resolvability of Steiner triple systems arose in the following problem, first posed by Kirkman:[27]

Kirkman's schoolgirl problem: A schoolmistress takes her class of 15 girls on a daily walk. The girls are arranged in five rows, with three girls in each row, so that each girl has two companions. Is it possible to plan a walk for seven consecutive days so that no girl will walk with any of her classmates in a triplet more than once?

A solution to this problem consists of $7 \times 5 = 35$ triples of the 15 girls, with each pair of girls together in exactly one triple. Moreover, it should be possible to partition the 35 triples into 7 groups of 5 triples each so that, in each group, each girl appears in exactly 1 triple. Now, the number of triples of a Steiner triple system of index $\lambda = 1$ with $v = 15$ varieties is

$$b = \frac{v(v-1)}{6} = 35.$$

Thus, Kirkman's schoolgirl problem asks for a resolvable Steiner triple system of index $\lambda = 1$ with $v = 15$ varieties. The preceding example contains a solution for the Kirkman's schoolgirls problem in the case of ninr girls. In this case, there are nine girls and arrangements for a daily walk for four days with each girl having different companions on all four days.

Example. *Solution of Kirkman's schoolgirl problem.* What is required is a resolvable Steiner triple system of index $\lambda = 1$ with 15 varieties. Such a Steiner system, along with its resolution into seven parts (one corresponding to each of the seven days), is

[27] T. P. Kirkman, Note on an Unanswered Prize Question, *Cambridge and Dublin Mathematics Journal*, 5 (1850), 255–262, and Query VI, *Lady's and Gentleman's Diary* No. 147, 48.

as follows:

$$\begin{array}{llll} \{0,1,2\} & \{0,3,4\} & \{0,5,6\} & \{0,7,8\} \\ \{3,7,11\} & \{1,7,9\} & \{1,8,10\} & \{1,11,13\} \\ \{4,9,14\} & \{2,12,13\} & \{2,11,14\} & \{2,4,5\} \\ \{5,10,12\} & \{5,8,14\} & \{3,9,13\} & \{3,10,14\} \\ \{6,8,13\} & \{6,10,11\} & \{4,7,12\} & \{6,9,12\} \end{array}$$

$$\begin{array}{lll} \{0,9,10\} & \{0,11,12\} & \{0,13,14\} \\ \{1,12,14\} & \{1,3,5\} & \{1,4,6\} \\ \{2,3,6\} & \{2,8,9\} & \{2,7,10\} \\ \{4,8,11\} & \{4,10,13\} & \{3,8,12\} \\ \{5,7,13\} & \{6,7,10\} & \{5,9,11\}. \end{array}$$

□

A resolvable Steiner triple system of index $\lambda = 1$ is also called a *Kirkman triple system*. Suppose $\mathcal{B}$ is a Kirkman triple system with v varieties. Since we must be able to partition the v varieties into triples, v must be divisible by 3. Hence, by Theorem 10.3.1, in order for a Kirkman system with v varieties to exist, v must be of the form $6n + 3$. The parameters of a Kirkman system are thus of the form

$$\begin{aligned} v &= 6n + 3, \\ b &= v(v-1)/6 = (2n+1)(3n+1), \\ k &= 3, \\ r &= (v-1)/2 = 3n+1, \\ \lambda &= 1. \end{aligned}$$

The number of triples in each resolvability class is

$$\frac{v}{3} = 2n + 1,$$

which fortunately is an integer. (If this number were not an integer for some n, then we would have to conclude that, for such n, a Kirkman triple system with $v = 6n + 3$ could not exist.) For over a hundred years, no one knew whether, for each nonnegative integer n, there is a Kirkman triple system with $v = 6n + 3$ varieties; in 1971, Ray-Chaudhuri and Wilson[28] showed how to construct such a system for all n.

10.4 Latin Squares

Latin squares were introduced in Section 1.4 in connection with Euler's problem of the 36 officers, and you may wish to review that section before proceeding. A formal

[28] D. K. Ray-Chaudhuri and R. M. Wilson, Solution of Kirkman's Schoolgirl Problem, *American Mathematical Society Proceedings, Symposium on Pure Mathematics*, 19 (1971), 187–204.

definition is the following: Let n be a positive integer and let S be a set of n distinct elements. A *Latin square of order n*, based on the set S, is an n-by-n array, each of whose entries is an element of S such that each of the n elements of S occurs once (and hence exactly once) in each row and once in each column. Thus each of the rows and each of the columns of a Latin square is a permutation of the elements of S. It follows from the pigeonhole principle that we can check in either of two ways whether an n-by-n array based on a set S of n elements is a Latin square: (1) Check that each element of S occurs at least once in each row and at least once in each column, or (2) Check that no element of S occurs more than once in each row and no more than once in each column.

The actual nature of the elements of S is of no importance and usually we take S to be $Z_n = \{0, 1, \ldots, n-1\}$. In this case, we number the rows and the columns of the Latin square as $0, 1, \ldots, n-1$, rather than the more conventional $1, 2, \ldots, n$. A 1-by-1 array is always a Latin square based on the set consisting of its unique element. Other examples of Latin squares are the following:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}. \tag{10.8}$$

To confirm our stated convention, row 0 of the last square is the permutation $0, 1, 2, 3$, and row 2 is the permutation $2, 3, 0, 1$.

Consider a Latin square of order n based on Z_n, and let k be any element of Z_n. Then k occurs n times in A, once in each row and once in each column. Thinking of an n-by-n array as n-by-n board, the positions occupied by k are positions for n nonattacking rooks on an n-by-n board. Let $A(k)$ be the set of positions occupied by k's, $(k = 0, 1, \ldots, n-1)$. Then $A(0), A(1), \ldots, A(n-1)$ is a partition of the set of n^2 positions of the board. Thus, a Latin square of order n corresponds to a partition of the positions of an n-by-n array into n sets

$$A(0), A(1), \ldots, A(n-1),$$

each consisting of n positions for nonattacking rooks. This observation is readily verified in the preceding examples. Note that, if, in a Latin square, we replace, say, all the 1s with 2s and all the 2s with 1s, the result is a Latin square. The resulting partition previously described is the same, except that now the set $A(1)$ has become $A(2)$ and $A(2)$ has become $A(1)$. More generally, we can interchange $A(0), A(1), \ldots, A(n-1)$ at will and the result will always be a Latin square. There are $n!$ Latin squares that result in this way. For instance, consider the 4-by-4 Latin square A in (10.8). For this A, we have

$$A(0) = \{(0,0), (1,3), (2,2), (3,1)\} \quad A(1) = \{(0,1), (1,0), (2,3), (3,2)\}$$

$$A(2) = \{(0,2),(1,1),(2,0),(3,3)\} \quad A(3) = \{(0,3),(1,2),(2,1),(3,0)\}.$$

We obtain a new Latin square A' by letting

$$A'(0) = A(2),\ A'(1) = A(3),\ A'(2) = A(0),\ A'(3) = A(1).$$

The result is

$$A' = \begin{bmatrix} 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{bmatrix}.$$

Using this idea of interchanging the positions occupied by the various elements $0, 1, \ldots, n-1$, we can always bring a Latin square to *standard form*, whereby in row 0 the integers $0, 1, \ldots, n-1$ occur in their natural order. The three Latin squares in (10.8) are in standard form.

The three examples of Latin squares in (10.8) are instances of a general construction of a Latin square of order n coming from the addition table of the integers mod n.

Theorem 10.4.1 *Let n be a positive integer. Let A be the n-by-n array whose entry a_{ij} in row i and column j is*

$$a_{ij} = i + j \text{ (addition mod } n), \ (i, j = 0, 1, \ldots, n-1).$$

Then A is a Latin square of order n based on Z_n.

Proof. The Latin property of this array is a consequence of the properties of addition in Z_n. Suppose, for some row i of the array, the elements in positions in row i, column j and row i, column k are identical; that is,

$$i + j = i + k.$$

Then, adding the additive inverse $-i$ of i in Z_n to both sides, we get $j = k$, showing that there is no element repeated in row i. In a similar way, w show that there is no element repeated in any column. □

The Latin square of order n constructed in Theorem 10.4.1 is nothing but the addition table of Z_n. There is a more general construction using the integers mod n that produces a wider class of Latin squares. It rests on the existence of multiplicative inverses of some elements of Z_n. (See Theorem 10.1.2.)

Example. We consider Z_5, the integers mod 5. By Theorem 10.1.2, 3 has a multiplicative inverse in Z_5; in fact, $3 \times 2 = 1$ in Z_5. Using the arithmetic of Z_5, we

construct a 5-by-5 array whose entry in row i and column j is $a_{ij} = 3 \times i + j$. The result is

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{array}\right] \end{array}. \tag{10.9}$$

Inspection reveals that we have a Latin square of order 5. □

Theorem 10.4.2 *Let n be a positive integer and let r be a nonzero integer in Z_n such that the GCD of r and n is 1. Let A be the n-by-n array whose entry a_{ij} in row i and column j is*

$$a_{ij} = r \times i + j \text{ (arithmetic mod } n), \ (i, j = 0, 1, \ldots, n-1).$$

Then A is a Latin square of order n based on Z_n.

Proof. The Latin property of this array follows from the properties of addition and multiplication in Z_n. Suppose, for some row i of the array, the elements in positions (i, j) and (i, k) are identical; that is,

$$r \times i + j = r \times i + k.$$

In a manner similar to that used in the proof of Theorem 10.4.1, by adding the additive inverse of $r \times i$ to both sides, we conclude that $j = k$ and there is no repeated element in row i. To show that there is no repeated element in any column, we also must use the fact that the GCD of r and n is 1. By Theorem 10.1.2, r has a multiplicative inverse r^{-1} in Z_n. Suppose that the elements in positions row i, column j and row k, column j are identical; that is,

$$r \times i + j = r \times k + j.$$

Subtracting j from both sides and rewriting, we get

$$r \times (i - k) = 0.$$

Multiplying by r^{-1}, we get $i = k$, implying that there is no repeated element in column j. Hence, A is a Latin square. □

Theorem 10.4.1 is the special case of Theorem 10.4.2 obtained by taking $r = 1$.

The Latin square of order n constructed in Theorem 10.4.2, using an integer r with a multiplicative inverse in Z_n, will be denoted by L_n^r. Thus, the Latin square in (10.9)

is L_5^3. If r does not have a multiplicative inverse, then the resulting array L_n^r will not be a Latin square. (See Exercise 39.)

There is another way to think of the Latin property of a Latin square. Let

$$R_n = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \cdots & \vdots \\ n-1 & n-1 & \cdots & n-1 \end{bmatrix} \tag{10.10}$$

and

$$S_n = \begin{bmatrix} 0 & 1 & \cdots & n-1 \\ 0 & 1 & \cdots & n-1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & n-1 \end{bmatrix} \tag{10.11}$$

be two n-by-n arrays based on Z_n with identical columns and rows, respectively, as shown. Let A be any n-by-n array based on Z_n. Then A is a Latin square if and only if the following conditions are satisfied:

(1) When the arrays R_n and A are juxtaposed[29] to form an array $R_n \times A$, the set of ordered pairs thus obtained equals the set of *all* ordered pairs (i, j) that can be formed using the elements of Z_n;

(2) When the arrays S_n and A are juxtaposed to form an array $S_n \times A$, the set of ordered pairs thus obtained equals the set of *all* ordered pairs (i, j) that can be formed using the elements of Z_n.

Since the juxtaposed arrays contain n^2 ordered pairs, which is exactly the number of ordered pairs that can be formed using the elements of Z_n, it follows from the pigeonhole principle that the preceding properties can be expressed by saying that the ordered pairs in $R_n \times A$ are all distinct, and the ordered pairs in $S_n \times A$ are all distinct.

Example. We illustrate the foregoing discussion with a Latin square of order 3:

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (0,0) & (0,1) & (0,2) \\ (1,1) & (1,2) & (1,0) \\ (2,2) & (2,0) & (2,1) \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (0,0) & (1,1) & (2,2) \\ (0,1) & (1,2) & (2,0) \\ (0,2) & (1,0) & (2,1) \end{bmatrix}.$$

In each of the two juxtaposed arrays, each ordered pair occurs exactly once. ∎

[29] Corresponding entries side by side.

We now apply the preceding ideas to two Latin squares. Let A and B be Latin squares based, for instance, on the integers in Z_n.[30] Then A and B are called *orthogonal*, provided that in the juxtaposed array $A \times B$, each of the ordered pairs (i, j) of integers in Z_n occurs exactly once.[31] This notion of orthogonality was introduced in Section 1.5 in connection with Euler's problem of the 36 officers, where two orthogonal Latin squares of order 3 were given. It is simple to check that there do not exist two orthogonal Latin squares of order 2.

Example. The following two Latin squares of order 4 are orthogonal, as is seen by examining their juxtaposed array:

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{bmatrix}.$$

□

Orthogonal Latin squares have application to the design of experiments in which variational differences need to be kept at a minimum to draw meaningful conclusions. We illustrate their use with an example from agriculture.

Example. It is desired to test the effects of various quantities of water and various types (or quantities) of fertilizer on the yield of wheat on a certain type of soil. Suppose there are n quantities of water and n types of fertilizer to be tested, so that there are n^2 possible combinations of water and fertilizer. We have at our disposal a rectangular field that is subdivided into n^2 plots, one for each of the n^2 possible water–fertilizer combinations. There is no reason to expect that soil fertility is the same throughout the field. Thus, it may very well be that the first row is of high fertility, and therefore a higher yield of wheat will occur, which is not due solely to the quantity of water and the type of fertilizer used on it. We are likely to minimize the influence of soil fertility on the yield of wheat if we insist that each quantity of water occur no more than once in any row and in any column, and similarly that each type of fertilizer occur no more than once in any row and in any column. Thus, the application of the n quantities of water on the n^2 plots should determine a Latin square A of order n, and also the application of the n types of fertilizer should determine a Latin square B of order n. Since all n^2 possible water–fertilizer combinations are to be treated, when the two Latin squares A and B are juxtaposed, all n^2 combinations should occur once. Thus, the Latin squares A and B are to be orthogonal. Two orthogonal Latin squares of order n, one for the application of the n quantities of water and one for the n types of fertilizer, determine a design for an experiment to test the effects of water and

[30] It is not necessary that the two Latin squares be based on the same set of elements. The choice makes for convenience in the exposition.

[31] For emphasis, we repeat that, by the pigeonhole principle, we can instead say that each ordered pair occurs *at most* once.

fertilizer on the production of wheat. The two orthogonal Latin squares of order 4 in the previous example give us a design for four quantities of water (labeled 0, 1, 2, and 3) and four types of fertilzer (also labeled 0, 1, 2, and 3). □.

We now extend our notion of orthogonality from two Latin squares to any number of Latin squares. Let $A_1, A_2, \ldots, A_k$ be Latin squares of order n. Without loss of generality, we assume that each of these Latin squares is based on Z_n. We say that $A_1, A_2, \ldots, A_k$ are *mutually orthogonal*, provided that each pair A_i, A_j $(i \neq j)$ of them is orthogonal. We refer to mutually orthogonal Latin squares as *MOLS*. If n is a prime number, we can construct a set of $n-1$ MOLS of order n.

Theorem 10.4.3 *Let n be a prime number. Then $L_n^1, L_n^2, \ldots, L_n^{n-1}$ are $n-1$ MOLS of order n.*

Proof. By Corollary 10.1.3, since n is prime, each nonzero integer in Z_n has a multiplicative inverse. By Theorem 10.4.2, the arrays $L_n^1, L_n^2, \ldots, L_n^{n-1}$ are Latin squares of order n. Let r and s be distinct nonzero integers in Z_n. We show that L_n^r and L_n^s are orthogonal. Suppose that in the juxtaposed array, $L_n^r \times L_n^s$ some ordered pair occurs twice—say, the pair in row i and column j and the pair in row k and column l are the same. Recalling the definition of the Latin squares L_n^r and L_n^s, we see that this means that

$$r \times i + j = r \times k + l \text{ and } s \times i + j = s \times k + l.$$

We rewrite these equations, obtaining

$$r \times (i - k) = (l - j) \text{ and } s \times (i - k) = (l - j);$$

hence

$$r \times (i - k) = s \times (i - k).$$

Suppose that $i \neq k$. Then $(i - k) \neq 0$ and hence has a multiplicative inverse in Z_n. Multiplying the preceding equation by $(i - k)^{-1}$—that is, cancelling $(i - k)$—we get $r = s$, a contradiction. Thus, we must have $i = k$, and then, substituting into the first equation, we get $j = l$. It follows that the only way two positions in $L_n^r \times L_n^s$ can contain the same ordered pair is for the two positions to be the same position. This means that L_n^r and L_n^s are orthogonal for all $r \neq s$ and hence $L_n^1, L_n^2, \ldots, L_n^{n-1}$ are MOLS. □

At the end of Section 10.1, we discussed briefy the arithmetical system called a field, which satisfies the usual laws of arithmetic. We remarked that, for each prime number p and each positive integer k, there exists a field with the finite number p^k of elements (and the number of elements in a finite field is always a power of a prime). Theorems 10.4.2 and 10.4.3 generalize to each finite field. We briefly discuss this now.

Let F be a finite field with $n = p^k$ elements for some prime p and positive integer k. Let

$$\alpha_0 = 0, \alpha_1, \ldots, \alpha_{n-1}$$

be the elements of F with α_0, as indicated, the zero element of F. Consider any nonzero element α_r, $(r \neq 0)$ of F, and define an n-by-n array A such that the element a_{ij} in row i and column j of A is

$$a_{ij} = \alpha_r \times \alpha_i + \alpha_j, \quad (i, j = 0, 1, \ldots, n-1),$$

where the arithmetic is that of the field F. Then a proof like that given for Theorem 10.4.2 (using only the usual laws of arithmetic, which, since F is a field, are satisfied) shows that A is a Latin square of order n based on the elements of F. Denote the Latin square A constructed in this way by $L_n^{\alpha_r}$. Then, following the proof of Theorem 10.4.3,[32] we find that

$$L_n^{\alpha_1}, L_n^{\alpha_2}, \ldots, L_n^{\alpha_{n-1}} \tag{10.12}$$

are $n-1$ MOLS of order n. We summarize these facts in the next theorem.

Theorem 10.4.4 *Let $n = p^k$ be an integer that is a power of a prime number p. Then there exist $n-1$ MOLS of order n. In fact, the $n-1$ Latin squares* (10.12) *of order n constructed from a finite field with $n = p^k$ elements are $n-1$ MOLS of order n.* □

Example. We illustrate the preceding construction by obtaining three MOLS of order 4. In Section 10.1 we constructed a field with four elements. The elements of this field are

$$\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = i, \alpha_3 = 1 + i.$$

Using the arithmetic of this field (the addition and multiplication tables are given in Section 10.1), we obtain the following Latin squares:

$$L_4^1 = \begin{bmatrix} 0 & 1 & i & 1+i \\ 1 & 0 & 1+i & i \\ i & 1+i & 0 & 1 \\ 1+i & i & 1 & 0 \end{bmatrix}$$

$$L_4^i = \begin{bmatrix} 0 & 1 & i & 1+i \\ i & 1+i & 0 & 1 \\ 1+i & i & 1 & 0 \\ 1 & 0 & 1+i & i \end{bmatrix}$$

$$L_4^{1+i} = \begin{bmatrix} 0 & 1 & i & 1+i \\ 1+i & i & 1 & 0 \\ 1 & 0 & 1+i & i \\ i & 1+i & 0 & 1 \end{bmatrix}.$$

[32] Again, only the usual laws of arithmetic were used.

L_4^1 is just the addition table of F. It is straightforward to check that L_4^1, L_4^i, L_4^{1+i} are three MOLS of order 4 based on F. □

By Theorem 10.4.4, there exist $n-1$ MOLS of order n whenever n is a prime power. Is it possible to have a collection of more than $n-1$ MOLS of order n? The negative answer to this question is given in the next theorem.

Theorem 10.4.5 *Let $n \geq 2$ be an integer, and let $A_1, A_2, \ldots, A_k$ be k MOLS of order n. Then $k \leq n-1$; that is, the largest number of MOLS of order n is at most $n-1$.*

Proof. We may assume without loss of generality that each of the given Latin squares is based on the elements of Z_n. We first observe the following: Each of the Latin squares $A_1, A_2, \ldots, A_k$ can be brought to standard form, and this does not affect their mutual orthogonality. This latter fact is easy to check for: If, after bringing two Latin squares to standard form, their juxtaposed array had a repeated ordered pair, then the juxtaposed array must have had a repeated ordered pair to begin with. Thus, we may assume that each of $A_1, A_2, \ldots, A_k$ is in standard form. Then, for each pair A_i, A_j, the juxtaposed array $A_i \times A_j$ has first row equal to $(0,0),(1,1),\ldots,(n-1,n-1)$. Now consider the entry in the position of row 1, column 0 of each A_i. None of these entries can equal 0, since 0 is already occurring in the position directly above it in column 0. Therefore, in each of $A_1, A_2, \ldots, A_k$, the entry in row 1, column 0 is one of $1, 2, \ldots, n-1$. Moreover, no two of $A_1, A_2, \ldots, A_k$ can have the same integer in this position. For if A_i and A_j both had, say, r in this position, then the juxtaposed array $A_i \times A_j$ would contain the pair (r,r) twice, since it is already occurring in row 0. Thus, each of $A_1, A_2, \ldots, A_k$ contains one of the integers $1, 2, \ldots, n-1$ in the row 1, column 0 position, and no two of them contain the same integer in this position. By the pigeonhole principle, we have $k \leq n-1$, and the theorem is proved. □

For n a positive integer, let $N(n)$ denote the largest number of MOLS of order n. We have $N(1) = 2$ because a Latin square of order 1 is orthogonal to itself.[33] Since no two Latin squares of order 2 are orthogonal, we have $N(2) = 1$. It follows from Theorems 10.4.4 and and 10.4.5 that

$$N(n) = n-1 \text{ if } n \text{ is a prime power.}$$

It is natural to wonder whether $N(n) = n-1$ for all integers $n \geq 2$. Unfortunately, $N(n)$ may be less than $n-1$. (By Theorem 10.4.4, n cannot be a prime power if this happens.) The smallest integer that is not a prime power is $n = 6$, and not only do we have $N(6) \neq 5$, but we also have $N(6) = 1$; that is, there do not even exist two orthogonal Latin squares of order 6! This was verified[34] by Tarry[35] around 1900. We

[33] A Latin square of order $n \geq 2$ can never be orthogonal to itself.

[34] Not a trivial verification indeed!

[35] G. Tarry, Le problème de 36 Officiers, *Comptes Rendu de l'Association Française pour l'Avancement de Science Naturel*, 1 (1900), 122–123 and 2 (1901), 170–203.

can use the integers mod n to show that for each odd integer n there exists a pair of MOLS of order n.

Theorem 10.4.6 *$N(n) \geq 2$ for each odd integer n.*

Proof. Let n be an odd integer. We shall show that the addition table A and the subtraction table B of Z_n are MOLS. The entry a_{ij} in row i and column j of A is $a_{ij} = i + j$ (addition mod n), and we know by Theorem 10.4.1 that A is a Latin square of order n. The entry b_{ij} in row i and column j of B is $b_{ij} = i - j$ (subtraction mod n), and we first show that B is a Latin square. This is straighforward and is like the proof of Theorem 10.4.1. Suppose that the integers in row i of B and columns j and k are the same. This means that

$$i - j = i - k.$$

Adding $-i$ to both sides, we obtain $-j = -k$ and hence $j = k$. Hence, there are no repeated elements in a row and, in a similar way, we show that there are no repeated elements in a column. Thus, B is a Latin square.

We now show that A and B are orthogonal. Suppose that in the juxtaposed array $A \times B$, some ordered pair occurs twice, say,

$$(a_{ij}, b_{ij}) = (a_{kl}, b_{kl}).$$

This means that

$$i + j = k + l \text{ and } i - j = k - l.$$

Adding and subtracting these two equations, we get

$$2i = 2k \text{ and } 2j = 2l.$$

Now, remembering that n is odd, we observe that the GCD of 2 and n is 1, and hence by Theorem 10.1.2, 2 has a multiplicative inverse 2^{-1} in Z_n. Cancelling the 2 in the preceding equations, we get $i = k$ and $j = l$. Hence, the only way $A \times B$ can have the same ordered pair in two positions is for the positions to be the same. We thus conclude that A and B are orthogonal. □

There is a way to combine MOLS in order to get MOLS of larger order. The notation for carrying out and verifying this construction is a little cumbersome since we must deal with ordered pairs of ordered pairs. But the idea of the construction is very simple. We illustrate it by obtaining two MOLS of order 12 from two MOLS of order 3 and two MOLS of order 4. Consider the two MOLS of order 3 given by

$$A_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}.$$

These are the addition table and subtraction table of Z_3, respectively. Consider also the two MOLS of order 4 given by

$$B_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad B_2 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix}.$$

These are the first two MOLS of order 4 constructed following Theorem 10.4.4 with i replaced by 2 and $1+i$ replaced by 3. We now form the 12-by-12 arrays $A_1 \otimes B_1$ and $A_2 \otimes B_2$, which are defined as follows: First we replace each entry a_{ij}^1 of A_1 by the 4-by-4 array

$$(a_{ij}^1, B_1) = \begin{bmatrix} (a_{ij}^1, b_{00}^1) & (a_{ij}^1, b_{01}^1) & (a_{ij}^1, b_{02}^1) & (a_{ij}^1, b_{03}^1) \\ (a_{ij}^1, b_{10}^1) & (a_{ij}^1, b_{11}^1) & (a_{ij}^1, b_{12}^1) & (a_{ij}^1, b_{13}^1) \\ (a_{ij}^1, b_{20}^1) & (a_{ij}^1, b_{21}^1) & (a_{ij}^1, b_{22}^1) & (a_{ij}^1, b_{23}^1) \\ (a_{ij}^1, b_{30}^1) & (a_{ij}^1, b_{31}^1) & (a_{ij}^1, b_{32}^1) & (a_{ij}^1, b_{33}^1) \end{bmatrix}.$$

The result is the 12-by-12 array $A_1 \otimes B_1$ based on the 12 ordered pairs of integers (p, q) with p in Z_3 and q in Z_4. We obtain the 12-by-12 array $A_2 \otimes B_2$ in a similar way from A_2 and B_2. It is elementary to check that $A_1 \otimes B_1$ and $A_2 \otimes B_2$ are Latin squares, based on the set of 12 ordered pairs and that they are orthogonal. We leave this verification for the exercises. Now, in order to have these 12-by-12 arrays based on Z_{12},[36] we set up a one-to-one correspondence between Z_{12} and the ordered pairs (p, q). Any of the 12! such correspondences will do. One is the following (the one obtained by taking the ordered pairs in lexicographic order):

$$(0,0) \to 0, \quad (0,1) \to 1, \quad (0,2) \to 2, \quad (0,3) \to 3,$$

$$(1,0) \to 4, \quad (1,1) \to 5, \quad (1,2) \to 6, \quad (1,3) \to 7,$$

$$(2,0) \to 8, \quad (2,1) \to 9, \quad (2,2) \to 10, \quad (2,3) \to 11.$$

[36] This is, of course, not necessary. We do it only to avoid having Latin squares based on a set of elements that are ordered pairs.

The two MOLS of order 12 obtained in this way are as follows:

$$\begin{bmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 \\
2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 \\
3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 \\
4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 \\
5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 & 1 & 0 & 3 & 2 \\
6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 & 2 & 3 & 0 & 1 \\
7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 & 3 & 2 & 1 & 0 \\
8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
9 & 8 & 11 & 10 & 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\
10 & 11 & 8 & 9 & 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\
11 & 10 & 9 & 8 & 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4
\end{bmatrix}$$

$$\begin{bmatrix}
0 & 1 & 2 & 3 & 8 & 9 & 10 & 11 & 4 & 5 & 6 & 7 \\
2 & 3 & 0 & 1 & 10 & 11 & 8 & 9 & 6 & 7 & 4 & 5 \\
3 & 2 & 1 & 0 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 \\
1 & 0 & 3 & 2 & 9 & 8 & 11 & 10 & 5 & 4 & 7 & 6 \\
4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 & 8 & 9 & 10 & 11 \\
6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 & 10 & 11 & 8 & 9 \\
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 11 & 10 & 9 & 8 \\
5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 & 9 & 8 & 11 & 10 \\
8 & 9 & 10 & 11 & 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\
10 & 11 & 8 & 9 & 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
9 & 8 & 11 & 10 & 5 & 4 & 7 & 6 & 1 & 0 & 3 & 2
\end{bmatrix}.$$

The preceding construction works in general, and it yields the following result.

Theorem 10.4.7 *If there is a pair of MOLS of order m and there is a pair of MOLS of order k, then there is a pair of MOLS of order mk. More generally,*

$$N(mk) \geq \min\{N(m), N(k)\}.$$

□

We can combine Theorem 10.4.7 with Theorem 10.4.4 to obtain the next result.

Theorem 10.4.8 *Let $n \geq 2$ be an integer and let*

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$$

be the factorization of n into distinct prime numbers $p_1, p_2, \ldots, p_k$. Then

$$N(n) \geq \min\{p_i^{e_i} - 1 : i = 1, 2, \ldots, k\}.$$

Proof. Using Theorem 10.4.7 and a simple induction argument on the number k of distinct prime factors of n, we get

$$N(n) \geq \min\{N(p_i^{e_i}) : i = 1, 2, \ldots, k\}.$$

By Theorem 10.4.4, we have

$$N(p_i^{e_i}) = p_i^{e_i} - 1$$

and the theorem follows. □

Corollary 10.4.9 *Let $n \geq 2$ be an integer that is not twice an odd number. Then there exists a pair of orthogonal Latin squares of order n.*

Proof. If p is a prime number and e is a positive integer, we have $p^e - 1 \geq 2$ unless $p = 2$ and $e = 1$. Hence, by Theorem 10.4.8, we have $N(n) \geq 2$, provided that the prime factorization of n does not contain exactly one 2; that is, provided n is not twice an odd number. □

The integers n for which Corollary 10.4.9 does *not* guarantee the existence of a pair of MOLS of order n are the integers

$$2, 6, 10, 14, 18, \ldots, 4k + 2, \ldots. \tag{10.13}$$

We have already remarked that there do not exist pairs of MOLS of order 2 and of order 6. Thus, the first undecided n is $n = 10$. It was conjectured by Euler in 1782 that for *no* integer n in the sequence (10.13) does there exist a pair of MOLS of order n. The combined efforts of Bose, Shrikhande, and Parker[37] succeeded in showing that Euler's conjecture holds only for $n = 2$ and $n = 6$; that is, except for 2 and 6 for each integer n in the sequence (10.13), there exists a pair of MOLS of order n. We do not prove this result, but the following is a pair of MOLS of order 10 constructed by Parker[38] in 1959:

$$\begin{bmatrix}
0 & 6 & 5 & 4 & 7 & 8 & 9 & 1 & 2 & 3 \\
9 & 1 & 0 & 6 & 5 & 7 & 8 & 2 & 3 & 4 \\
8 & 9 & 2 & 1 & 0 & 6 & 7 & 3 & 4 & 5 \\
7 & 8 & 9 & 3 & 2 & 1 & 0 & 4 & 5 & 6 \\
1 & 7 & 8 & 9 & 4 & 3 & 2 & 5 & 6 & 0 \\
3 & 2 & 7 & 8 & 9 & 5 & 4 & 6 & 0 & 1 \\
5 & 4 & 3 & 7 & 8 & 9 & 6 & 0 & 1 & 2 \\
2 & 3 & 4 & 5 & 6 & 0 & 1 & 7 & 8 & 9 \\
4 & 5 & 6 & 0 & 1 & 2 & 3 & 9 & 7 & 8 \\
6 & 0 & 1 & 2 & 3 & 4 & 5 & 8 & 9 & 7
\end{bmatrix}$$

[37] R. C. Bose, S. S. Shrikhande, and E. T. Parker: Further Results on the Construction of Mutually orthogonal Latin Squares and the Falsity of Euler's Conjecture, *Canadian J. Math.*, 12 (1960), 189–203. See also the account written by Martin Gardner in his Mathematical Games column in the *Scientific American* (November, 1959).

[38] E. T. Parker: Orthogonal Latin Squares, *Proc. Nat. Acad. Sciences*, 45 (1959), 859–862.

$$\begin{bmatrix} 0 & 9 & 8 & 7 & 1 & 3 & 5 & 2 & 4 & 6 \\ 6 & 1 & 9 & 8 & 7 & 2 & 4 & 3 & 5 & 0 \\ 5 & 0 & 2 & 9 & 8 & 7 & 3 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 9 & 8 & 7 & 5 & 0 & 2 \\ 7 & 5 & 0 & 2 & 4 & 9 & 8 & 6 & 1 & 3 \\ 8 & 7 & 6 & 1 & 3 & 5 & 9 & 0 & 2 & 4 \\ 9 & 8 & 7 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 8 & 9 & 7 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 & 9 & 7 & 8 \end{bmatrix}.$$

For nearly 200 years, 10 was the smallest undecided case of Euler's conjecture.

By Theorem 10.4.5, for each integer $n \geq 2$, we have $N(n) \leq n-1$, and by Theorem 10.4.4, we have equality if n is a power of a prime. There are no other known values of n for which $N(n) = n-1$. We establish a connection between $n-1$ MOLS of order n and the block designs of Section 10.2. Let $A_1, A_2, \ldots, A_{n-1}$ denote $n-1$ MOLS of order n. We use the $n+1$ arrays

$$R_n,\ S_n,\ A_1,\ A_2,\ \ldots,\ A_{n-1}, \tag{10.14}$$

where R_n and S_n are defined in (10.10) and (10.11), to construct a block design $\mathcal{B}$ with parameters

$$b = n^2 + n,\ v = n^2,\ k = n,\ r = n+1,\ \lambda = 1.$$

Recall that $A_i(k)$ denotes the set of positions of A_i occupied by k, $(k = 0, 1, \ldots, n-1)$. Since A_i is a Latin square, $A_i(k)$ contains one position from each row and each column; in particular, no two positions in $A_i(k)$ belong to the same row or to the same column. We also use this notation for R_n and S_n. For instance, $R_n(0)$ denotes the set of positions of R_n that are occupied by 0s, and this set is the set of positions of row 0, and $S_n(1)$ denotes the set of positions of S_n that are occupied by 1s and this is the set of positions of column 1.

We take the set X of varieties to be the set of $v = n^2$ positions of an n-by-n array; that is,

$$X = \{(i,j) : i = 0, 1, \ldots, n-1; j = 0, 1, \ldots, n-1\}.$$

Each of the $n+1$ arrays in (10.14) determines n blocks:

$$R_n(0)\quad R_n(1)\quad \ldots\quad R_n(n-1) \tag{10.15}$$

$$S_n(0)\quad S_n(1)\quad \ldots\quad S_n(n-1) \tag{10.16}$$

$$\begin{matrix} A_1(0) & A_1(1) & \dots & A_1(n-1) \\ \vdots & \vdots & \dots & \vdots \\ A_{n-1}(0) & A_{n-1}(1) & \dots & A_{n-1}(n-1). \end{matrix} \tag{10.17}$$

Thus, we have $b = n \times (n+1) = n^2 + n$ blocks, each containing $k = n$ varieties. Let $\mathcal{B}$ denote this collection of blocks. To conclude that $\mathcal{B}$ is a BIBD with the specified parameters, we need only check that each pair of varieties occur together in exactly $\lambda = 1$ block. There are three possibilities to consider:

(1) *Two varieties in the same row*: These are together in precisely one of the blocks in (10.15) and in no other blocks.

(2) *Two varieties in the same column*: These are together in precisely one of the blocks in (10.16) and in no other blocks.

(3) *Two varieties (i,j) and (p,q) belonging to different rows and to different columns*: These two varieties are not together in any of the blocks in (10.15) and (10.16). Suppose that they are together in blocks $A_r(e)$ and $A_s(f)$. This means that there is an e in positions row i, column j and row p, column q of A_r and an f in the same positions of A_s. If $r \neq s$, then, in the juxtaposed array $A_r \times A_s$, the ordered pair (e,f) appears twice, contradicting the orthogonality of A_r and A_s. Thus, $r = s$, which implies that A_r has both an e and an f in positions row i, column j and row p, column q. We also conclude that $e = f$. Hence, $A_r(e)$ and $A_s(f)$ are the same block, and we now conclude that (i,j) and (p,q) are together in *at most* one block.

At this point, we know that each pair of varieties is together in, at most, one block. This is now enough for us to conclude that each pair of varieties is together in exactly one block. This follows by a counting argument similar to one we have made in Section 10.2: There are n^2 varieties, we can form $n^2(n^2-1)/2$ pairs of them, and we know that each pair is in, at most, one of the n^2+n blocks. Each block has n varieties and thus contains $n(n-1)/2$ pairs. For all blocks, this gives a total of

$$(n^2+n) \times \frac{n(n-1)}{2} = \frac{n^2(n^2-1)}{2}$$

pairs, which is exactly the total number of pairs of varieties. Hence, by the pigeonhole principle, each pair of varieties must be in exactly one block. Thus, $\mathcal{B}$ is a BIBD of index $\lambda = 1$.

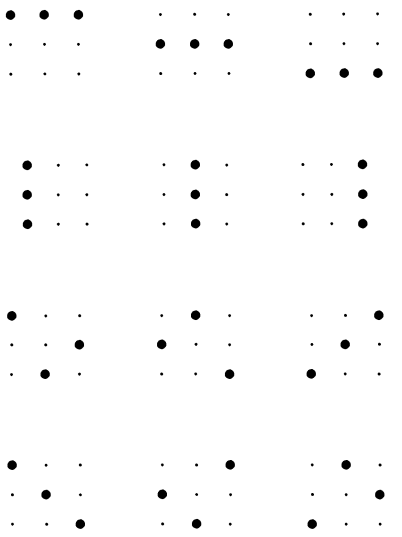
We note that the design $\mathcal{B}$ constructed is *resolvable* in the sense used in Section 10.2 for Steiner systems. The collection of n^2+n blocks is partitioned into $n+1$ parts (*resolvability classes*) of n blocks each (see (10.15), (10.16), and (10.17)), and each resolvability class is a partition of the n^2 varieties.

Example. We illustrate the preceding construction of a BIBD using the two Latin

squares of order 3:

$$A_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}.$$

The varieties are the nine positions of a 9-by-9 array, and the blocks are pictured geometrically by resolvability classes as follows:



If we think of the varieties as *points* and the blocks as *lines*, and, as usual, call two lines *parallel*, provided that they have no point in common, then each of the preceding displays (the resolvability classes) consists of three parallel lines. Each pair of varieties being together in exactly one block translates to two points determining exactly one line. The resolvability of the design also translates to the property that, given a line and a point not on it, there is exactly one line parallel to the first containing the given point. This is the so-called *parallel postulate* of Euclidean geometry.

Theorem 10.4.10 *Let $n \geq 2$ be an integer. If there exist $n-1$ MOLS of order n, then there exists a resolvable BIBD with parameters*

$$b = n^2 + n, v = n^2,\ k = n,\ r = n+1,\ \lambda = 1. \tag{10.18}$$

Conversely, if there exists a resolvable BIBD with parameters (10.18)*, then there exist $n-1$ MOLS of order n.*

Proof. Previously, we showed how to construct a resolvable BIBD with parameters (10.18) from $n-1$ MOLS of order n. This process can be reversed. We outline how and leave some of the details for the Exercises. Suppose we have a resolvable BIBD $\mathcal{B}$ with parameters (10.18). Since there are n^2 varieties and each block contains n varieties, each resolvability class contains n blocks. Moreover, since there are n^2+n blocks, there are $n+1$ resolvability classes

$$\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_{n+1}.$$

We use two of the resolvability classes $\mathcal{B}_n$ and $\mathcal{B}_{n+1}$ in order to "coordinatize" the varieties. Let the blocks in $\mathcal{B}_n$ be

$$H_0, H_1, \ldots, H_{n-1}$$

and let the blocks in $\mathcal{B}_{n+1}$ be

$$V_0, V_1, \ldots, V_{n-1}.$$

(H is for *horizontal* and V is for *vertical*.) Given any variety x, there is a unique i between 0 and $n-1$ such that x is in H_i and a unique j between 0 and $n-1$ such that x is in V_j. This gives an ordered pair of coordinates (i,j) to each variety x. Moreover, since the index λ equals 1, two different varieties do not get the same coordinates (if x and y both had coordinates (i,j), then x and y would be together in the two blocks H_i and V_j). We may now think of the set X of varieties as the coordinate pairs themselves:[39]

$$X = \{(i,j) : i = 0,1,\ldots,n-1; j = 0,1,\ldots,n-1\}.$$

Now consider any other resolvability class $\mathcal{B}_p$, $(p = 0,1,\ldots,n-1)$. Let the blocks in $\mathcal{B}_p$ be labeled

$$A_p(0),\ A_p(1),\ \ldots,\ A_p(n-1).$$

These blocks partition X into n sets of size n. Also, as the notation suggests, let A_p be the n-by-n array that has a k in each position of $A_p(k)$. If, for instance, there were two k's in row i of A_p, this would imply that there are two varieties (i,a) and (i,b) that are in both of the blocks H_i and $A_i(k)$. Thus, A_p is a Latin square. Moreover, for $p \neq q$, A_p and A_q are orthogonal: If the juxtaposed array $A_p \times A_q$ contained the same ordered pair in both positions row i, column j and row u, column v, then the two varieties (i,j) and (u,v) would be in two blocks. Hence, $A_1, A_2, \ldots, A_{n-1}$ are MOLS of order n. □

We conclude this section with some questions that naturally arise when we attempt to construct a Latin square.

There are three natural ways to construct a Latin square of order n:

[39] We make a similar identification in analytic geometry when we give the points of the plane coordinates and the coordinates "become" the points.

1. row by row,
2. column by column, and
3. element by element.

The first two ways are quite similar, and we consider only the first.

To construct a Latin square row by row means to put in one complete row at a time. Thus, we can construct a Latin square of order 3 by first choosing a permutation of $\{0,1,2\}$ for row 0, say, 2, 1, 0, then a permutation for row 1 (which doesn't give a repeated integer in any column), say, 0, 2, 1, and then a permutation for row 2, say, 1, 0, 2 (actually, if we know all but the last row of a Latin square, then the last row can be filled in uniquely because we must put in each column the integer that is not yet there). The result is

$$\begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix}.$$

Will we ever get stuck if we construct a Latin square in this way, at each step choosing an allowable permutation for the next row?

To construct a Latin square element by element means to put in all the occurrences of each of the elements, one element at a time. Thus, we could have constructed the preceding Latin square of order 3 by first choosing three positions for the 0s (three positions for nonattacking rooks), then three positions for the 1s, and finally three positions for the 2s, (as in the row by row construction, the last step is uniquely determined). *Will we ever get stuck if we construct a Latin square in this way, at each step choosing the set of positions for the next integer?*

We show that Theorem 9.2.2 of Chapter 9 allows us to answer both of these questions.[40] First, we make a definition that is suggested by the first question.

Let m and n be integers with $m \leq n$. An m-by-n *Latin rectangle*, based on the integers in Z_n, is an m-by-n array such that no integer is repeated in any row or in any column. Each of the rows of an m-by-n Latin rectangle is a permutation of $\{0,1,\ldots,n-1\}$ and no column contains a repeated integer. If $m = n$, then our definition of a Latin rectangle is equivalent to that of a Latin square.[41] An example of a 3-by-5 Latin rectangle is

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 3 & 2 & 1 \end{bmatrix}.$$

We say that an m-by-n Latin rectangle L can be *completed*, provided it is possible to attach $n-m$ rows to L and obtain a Latin square L^* of order n. Such a Latin

[40] Letting the "cat out of the bag," we never get stuck.

[41] The pigeonhole principle again!

square L^* is called a *completion* of L. For example, a completion of the previous Latin rectangle L is

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 3 & 2 & 1 \\ 2 & 3 & 1 & 4 & 0 \\ 1 & 2 & 4 & 0 & 3 \end{bmatrix}.$$

The answer to our first question is a consequence of the next theorem.

Theorem 10.4.11 *Let L be an m-by-n Latin rectangle based on Z_n with $m < n$. Then L has a completion.*

Proof. It suffices to show that we can adjoin one new row to L to get an $(m+1)$-by-n Latin rectangle because then we can proceed inductively until we obtain a Latin square of order n. We define a family $\mathcal{A} = (A_1, A_2, \ldots, A_n)$ of subsets of the set $Z_n = \{0, 1, \ldots, n-1\}$ by defining each A_i to bet the set of integers in Z_n that are *missing* in column i. Since L is an m-by-n Latin rectangle, each A_i contains exactly $n-m$ elements. Moreover, since each integer in Z_n occurs once in each of the m rows of L and in different columns, each integer in Z_n occurs in exactly $n-m$ of the sets of $\mathcal{A}$.

Suppose there is an SDR $(a_1, a_2, \ldots, a_n)$ of $\mathcal{A}$. Then $a_1, a_2, \ldots, a_n$ are the integers $0, 1, \ldots, n-1$ in some order and, since for each i, a_i is in A_i, a_i does not occur in column i of L. We can then adjoin a_1, a_2, $\cdots$, a_n as a new row (row $m+1$) of L and obtain, as desired, an $(m+1)$-by-n Latin rectangle. So we have only to show that $\mathcal{A}$ does indeed have an SDR. By Theorem 9.2.2, we have only to show that $\mathcal{A}$ satisfies the marriage condition MC (cf. Exercise 15 of Chapter 9).

Consider k distinct integers $i_1, i_2, \ldots, i_k$ from $\{1, 2, \ldots, n\}$, and let

$$q = |A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}|.$$

We evaluate

$$\alpha = |A_{i_1}| + |A_{i_2}| + \cdots + |A_{i_k}|$$

in two ways. On the one hand, since each set in $\mathcal{A}$ contains exactly $n-m$ integers, $\alpha = k(n-m)$. On the other hand, each integer in Z_n occurs in exactly $n-m$ of the sets of $\mathcal{A}$, and hence each of the q integers in $A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}$ occurs in at most $n-m$ of the sets $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$. Thus $\alpha \leq q(n-m)$. Thus we have

$$k(n-m) = \alpha \leq q(n-m).$$

Cancelling $n - m \geq 1$, we get $k \leq q$, that is,

$$|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}| \geq k.$$

Thus MC is satisfied and $\mathcal{A}$ has an SDR. Since $\mathcal{A}$ has an SDR, we conclude that the Latin rectangle L has a completion. □

The following definition is motivated by our second question. Consider an n-by-n array L in which some positions are unoccupied and other positions are occupied by one of the integers $\{0, 1, \ldots, n-1\}$. Suppose that, if an integer k occurs in L, then it occurs n times and no two k's belong to the same row or column. Then we call L a *semi-Latin square.* If m different integers occur in L, then we say L has *index* m. A semi-Latin square of order n and index m has exactly mn occupied positions. An example of a semi-Latin square of order 5 and index 3 is

1		0		2
	2	1		0
0	1		2	
2	0		1	
		2	0	1

We can think of this example as a 5-by-5 board (and we have illustrated it as such) on which there are five red nonattacking rooks (the 0s), five white nonattacking rooks (the 1s), and five blue nonattacking rooks (the 2s). What we seek are positions for five green nonattacking rooks and five yellow nonattacking rooks on this board. If we think of 3 as green and 4 as yellow, then a solution is given by

$$\begin{bmatrix} 1 & 4 & 0 & 3 & 2 \\ 3 & 2 & 1 & 4 & 0 \\ 0 & 1 & 4 & 2 & 3 \\ 2 & 0 & 3 & 1 & 4 \\ 4 & 3 & 2 & 0 & 1 \end{bmatrix}.$$

We say that a semi-Latin square L of order n can be *completed* to a Latin square, provided that it is possible to fill in the unoccupied positions to obtain a Latin square $L^{\#}$ of order n. Such a Latin square $L^{\#}$ is called a *completion* of L. The answer to our second question is a consequence of the final theorem of this chapter.

Theorem 10.4.12 *Let L be a semi-Latin square of order n and index m, where $m < n$. Then L has a completion.*

Proof. Suppose the integers that occur in L are $0, 1, \ldots, m-1$. It suffices to show that we can find n unoccupied positions in which to put m to get a Latin square of order n of index $m+1$, because then we can proceed inductively.

As in the proof of Theorem 10.4.11, a family $\mathcal{A} = (A_1, A_2, \ldots, A_n)$ of subsets of the set $Z_n = \{0, 1, \ldots, n-1\}$ is defined where for each i, A_i consists of all those positions j in row i that are unoccupied. Then $|A_i| = n - m$ for each i and each integer in Z_n occurs in exactly $n - m$ of the sets in $\mathcal{A}$. As in the proof of Theorem 10.4.11, the

family $\mathcal{A}$ has an SDR. The SDR tells us where to put the integer $m+1$ in each row so as to obtain a semi-Latin square of index m. □

The similarity between Theorems 10.4.11 and 10.4.12 is not accidental. There is a one-to-one correspondence between m-by-n Latin rectangles and semi-Latin squares of order n and index m that transforms the proof of Theorem 10.4.11 into that of Theorem 10.4.12 and vice versa. This correspondence is the following: Let L be an m-by-n Latin rectangle (based on Z_n) and let the entry in position row i, column j be denoted by a_{ij}. We define an n-by-n array B by letting the entry b_{ij} in position row i, column j be k, provided that i occurs in column j of row k of L. Thus,

$$b_{ij} = k \text{ if and only if } a_{kj} = i.$$

Some positions in B are unoccupied since, if $m < n$, some integers are missing in the columns of L. We leave it as an exercise to show that the array B constructed from L in this way is a semi-Latin square of index m.

Example. Consider the 3-by-5 Latin rectangle

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 0 & 2 \\ 1 & 0 & 4 & 2 & 3 \end{bmatrix}.$$

Then, following the preceding construction, we obtain the semi-Latin square B of order 5 and index 3:

$$B = \begin{array}{|c|c|c|c|c|} \hline 0 & 2 & & 1 & \\ \hline 2 & 0 & 1 & & \\ \hline & & 0 & 2 & 1 \\ \hline 1 & & & 0 & 2 \\ \hline & 1 & 2 & & 0 \\ \hline \end{array}$$

□

10.5 Exercises

1. Compute the addition table and the multiplication table for the integers mod 4.
2. Compute the subtraction table for the integers mod 4. How does it compare with the addition table computed in Exercise 1?
3. Compute the addition table and the multiplication table for the integers mod 5.
4. Compute the subtraction table of the integers mod 5. How does it compare with the addition table computed in Exercise 3?

5. Prove that no two integers in Z_n, arithmetic mod n, have the same additive inverse. Conclude from the pigeonhole principle that

$$\{-0, -1, -2, \ldots, -(n-1)\} = \{0, 1, 2, \ldots, n-1\}.$$

(Remember that $-a$ is the integer which, when added to a in Z_n, gives 0.)

6. Prove that the columns of the subtraction table of Z_n are a rearrangement of the columns of the addition table of Z_n (cf. Exercises 2 and 4).

7. Compute the addition table and multiplication table for the integers mod 6.

8. Determine the additive inverses of the integers in Z_8, with arithmetic mod 8.

9. Determine the additive inverses of 3, 7, 8, and 19 in the integers mod 20.

10. Determine which integers in Z_{12} have multiplicative inverses, and find the multiplicative inverses when they exist.

11. For each of the following integers in Z_{24}, determine the multiplicative inverse if a multiplicative inverse exists:

$$4, \quad 9, \quad 11, \quad 15, \quad 17, \quad 23.$$

12. Prove that $n-1$ always has a multiplicative inverse in Z_n, $(n \geq 2)$.

13. Let $n = 2m + 1$ be an odd integer with $m \geq 2$. Prove that the multiplicative inverse of $m + 1$ in Z_n is 2.

14. Use the algorithm in Section 10.1 to find the GCD of the following pairs of integers:

    (a) 12 and 31

    (b) 24 and 82

    (c) 26 and 97

    (d) 186 and 334

    (e) 423 and 618

15. For each of the pairs of integers in Exercise 14, let m denote the first integer and let n denote the second integer of the pair. When it exists, determine the multiplicative inverse of m in Z_n.

16. Apply the algorithm for the GCD in Section 10.1 to 15 and 46, and then use the results to determine the multiplicative inverse of 15 in Z_{46}.

17. Start with the field Z_2 and show that x^3+x+1 cannot be factored in a nontrivial way (into polynomials with coefficients in Z_2), and then use this polynomial to construct a field with $2^3 = 8$ elements. Let i be the root of this polynomial adjoined to Z_2, and then do the following computations:

    (a) $(1+i)+(1+i+i^2)$
    (b) $(1+i^2)+(1+i^2)$
    (c) i^{-1}
    (d) $i^2 \times (1+i+i^2)$
    (e) $(1+i)(1+i+i^2)$
    (f) $(1+i)^{-1}$

18. Does there exist a BIBD with parameters $b = 10$, $v = 8$ $r = 5$, and $k = 4$?

19. Does there exist a BIBD whose parameters satisfy $b = 20$, $v = 18$, $k = 9$, and $r = 10$?

20. Let $\mathcal{B}$ be a BIBD with parameters b, v, k, r, λ whose set of varieties is $X = \{x_1, x_2, \ldots, x_v\}$ and whose blocks are $B_1, B_2, \ldots, B_b$. For each block B_i, let $\overline{B_i}$ denote the set of varieties which do *not* belong to B_i. Let $\mathcal{B}^c$ be the collection of subsets $\overline{B_1}, \overline{B_2}, \ldots, \overline{B_b}$ of X. Prove that $\mathcal{B}^c$ is a block design with parameters

$$b' = b,\ v' = v,\ k' = v-k,\ r' = b-r,\ \lambda' = b-2r+\lambda,$$

    provided that we have $b-2r+\lambda > 0$. The BIBD $\mathcal{B}^c$ is called the *complementary design* of $\mathcal{B}$.

21. Determine the complementary design of the BIBD with parameters $b = v = 7, k = r = 3, \lambda = 1$ in Section 10.2.

22. Determine the complementary design of the BIBD with parameters $b = v = 16, k = r = 6, \lambda = 2$ given in Section 10.2.

23. How are the incidence matrices of a BIBD and its complement related?

24. Show that a BIBD, with v varieties whose block size k equals $v-1$, does not have a complementary design.

25. Prove that a BIBD with parameters b, v, k, r, λ has a complementary design if and only if $2 \leq k \leq v-2$ (Cf. Exercises 20 and 24).

26. Let B be a difference set in Z_n. Show that, for each integer k in Z_n, $B+k$ is also a difference set. (This implies that we can always assume without loss of generality that a difference set contains 0 for, if it did not, we can replace it by $B+k$, where k is the additive inverse of any integer in B.)

27. Prove that Z_v is itself a difference set in Z_v. (These are *trivial* difference sets.)

28. Show that $B = \{0, 1, 3, 9\}$ is a difference set in Z_{13}, and use this difference set as a starter block to construct an SBIBD. Identify the parameters of the block design.

29. Is $B = \{0, 2, 5, 11\}$ a difference set in Z_{12}?

30. Show that $B = \{0, 2, 3, 4, 8\}$ is a difference set in Z_{11}. What are the parameters of the SBIBD developed from B?

31. Prove that $B = \{0, 3, 4, 9, 11\}$ is a difference set in Z_{21}.

32. Use Theorem 10.3.2 to construct a Steiner triple system of index 1 having 21 varieties.

33. Let t be a positive integer. Use Theorem 10.3.2 to prove that there exists a Steiner triple system of index 1 having 3^t varieties.

34. Let t be a positive integer. Prove that, if there exists a Steiner triple system of index 1 having v varieties, then there exists a Steiner triple system having v^t varieties (cf. Exercise 33).

35. Assume a Steiner triple system exists with parameters b, v, k, r, λ, where $k = 3$. Let a be the remainder when λ is divided by 6. Use Theorem 10.3.1 to show the following:

    (1) If $a = 1$ or 5, then v has remainder 1 or 3 when divided by 6.

    (2) If $a = 2$ or 4, then v has remainder 0 or 1 when divided by 3.

    (3) If $a = 3$, then v is odd.

36. Verify that the following three steps construct a Steiner triple system of index 1 with 13 varieties (we begin with Z_{13}).

    (1) Each of the integers $1, 3, 4, 9, 10, 12$ occurs exactly once as a difference of two integers in $B_1 = \{0, 1, 4\}$.

    (2) Each of the integers $2, 5, 6, 7, 8, 11$ occurs exactly once as a difference of two integers in $B_2 = \{0, 2, 7\}$.

    (3) The 12 blocks developed from B_1 together with the 12 blocks developed from B_2 are the blocks of a Steiner triple system of index 1 with 13 varieties.

37. Prove that, if we interchange the rows of a Latin square in any way and interchange the columns in any way, the result is always a Latin square.

38. Use the method in Theorem 10.4.2 with $n = 6$ and $r = 5$ to construct a Latin square of order 6.

39. Let n be a positive integer and let r be a nonzero integer in Z_n such that the GCD of r and n is not 1. Prove that the array constructed using the prescription in Theorem 10.4.2 is not a Latin square.

40. Let n be a positive integer and let r and r' be distinct nonzero integers in Z_n such that the GCD of r and n is 1 and the GCD of r' and n is 1. Show that the Latin squares constructed by using Theorem 10.4.2 need not be orthogonal.

41. Use the method in Theorem 10.4.2 with $n = 8$ and $r = 3$ to construct a Latin square of order 8.

42. Construct four MOLS of order 5.

43. Construct three MOLS of order 7.

44. Construct two MOLS of order 9.

45. Construct two MOLS of order 15.

46. Construct two MOLS of order 8.

47. Let A be a Latin square of order n for which there exists a Latin square B of order n such that A and B are orthogonal. B is called an *orthogonal mate* of A. Think of the 0s in A as rooks of color red, the 1s as rooks of color white, the 2s as rooks of color blue, and so on. Prove that there are n nonattacking rooks in A, no two of which have the same color. Indeed, prove that the entire set of n^2 rooks can be partitioned into n sets of n nonattacking rooks each, with no two rooks in the same set having the same color.

48. Prove that the addition table of Z_4 is a Latin square without an orthogonal mate (cf. Exercise 47).

49. First construct 4 MOLS of order 5, and then construct the resolvable BIBD corresponding to them as given in Theorem 10.4.10.

50. Let A_1 and A_2 be MOLS of order m and let B_1 and B_2 be MOLS of order n. Prove that $A_1 \otimes B_1$ and $A_2 \otimes B_2$ are MOLS of order mn.

51. Fill in the details in the proof of Theorem 10.4.10.

52. Construct a completion of the 3-by-6 Latin rectangle

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 & 0 \\ 5 & 4 & 3 & 0 & 1 & 2 \end{bmatrix}.$$

53. Construct a completion of the 3-by-7 Latin rectangle

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 0 & 6 & 5 & 4 & 1 \\ 1 & 4 & 6 & 0 & 2 & 3 & 5 \end{bmatrix}.$$

54. How many 2-by-n Latin rectangles have first row equal to

$$0 \quad 1 \quad 2 \quad \cdots \quad n-1 \ ?$$

55. Construct a completion of the semi-Latin square

$$\begin{bmatrix} & 2 & 0 & & & 1 \\ 2 & 0 & & & 1 & \\ 0 & & 2 & 1 & & \\ & & 1 & 2 & & 0 \\ & 1 & & & 0 & 2 \\ 1 & & & 0 & 2 & \end{bmatrix}.$$

56. Construct a completion of the semi-Latin square

$$\begin{bmatrix} 0 & 2 & 1 & & & & 3 \\ 2 & 0 & & 1 & & 3 & \\ 3 & & 0 & 2 & 1 & & \\ & 3 & 2 & 0 & & 1 & \\ & & 3 & & 0 & 2 & 1 \\ 1 & & & & 3 & 0 & 2 \\ & 1 & & 3 & 2 & & 0 \end{bmatrix}.$$

57. Let $n \geq 2$ be an integer. Prove that an $(n-2)$-by-n Latin rectangle has at least two completions, and, for each n, find an example that has exactly two completions.

58. A Latin square A of order n is *symmetric*, provided the entry a_{ij} at row i, column j equals the entry a_{ji} at column j, row i for all $i \neq j$. Prove that the addition table of Z_n is a symmetric Latin square.

59. A Latin square of order n (based on Z_n) is *idempotent*, provided that its entries on the diagonal running from upper left to lower right are $0, 1, 2, \ldots, n-1$.

    (1) Construct an example of an idempotent Latin square of order 5.

    (2) Construct an example of a symmetric, idempotent Latin square of order 5.

60. Prove that a symmetric, idempotent Latin square has odd order.

61. Let $n = 2m + 1$, where m is a positive integer. Prove that the n-by-n array A whose entry a_{ij} in row i, column j satisfies

$$a_{ij} = (m + 1) \times (i + j) \text{ (arithmetic mod } n)$$

is a symmetric, idempotent Latin square of order n. (*Remark*: The integer $m + 1$ is the multiplicative inverse of 2 in Z_n. Thus, our prescription for a_{ij} is to "average" i and j.)

62. Let L be an m-by-n Latin rectangle (based on Z_n) and let the entry in row i, column j be denoted by a_{ij}. We define an n-by-n array B whose entry b_{ij} in position row i, column j satisfies

$$b_{ij} = k, \text{ provided } a_{kj} = i$$

and is blank otherwise. Prove that B is a semi-Latin square of order n and index m. In particular, if A is a Latin square of order n, so is B.