

# Magic Squares and Modular Arithmetic

Jim Carlson

November 7, 2001

## 1 Introduction

Recall that a *magic square* is a square array of consecutive distinct numbers such that all row and column sums are the same. Here is an example, a magic square of *order* three:

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

Fig. 1

The common row (or column) sum is called the *magic sum*. In Figure 1 above, the magic sum is 15. This is the first known example of a magic square, taken from *Loh-Shu* scroll in China. Some scholars date it to the mythical founder of Chinese civilization, *Fuh-Shi*, 2858-2736 BC. In any case, it is very, very old.

Below is another magic square of order three which uses nine consecutive numbers starting with zero. Notice how it is related to the *Loh-Shu* square. What is its magic sum?

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

Fig. 2

In these notes we will, except for historical examples and those directly related to them, use magic squares which “start” with zero.

## Introductory problems

1. Find a magic square of order three whose first row is

0 8 4

2. Find a magic square of order three whose first row is

1 8 3

3. Find a magic squares of order three which is different from all the previous ones.
4. Are there magic squares of order one and two?
5. Are there ways to construct new magic squares from old ones that do not change the magic sum?
6. Consider a  $4 \times 4$  magic square with elements 0, 1, ..., 15. What is the magic sum?
7. Consider an  $n \times n$  magic square with elements 0, 1, ...,  $n^2 - 1$ . What is the magic sum?
8. There are  $4 \times 4$  magic squares. The one illustrated in Figure 3, below comes from the engraving *Melancholia*, dated 1514, by the artist Albrecht Dürer. Like the *Loh-Shuh* square, it starts with the number 1.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Fig. 3

What is the magic sum of the Dürer square? How does it relate to the magic sum of the previous two problems? See if you can construct a  $4 \times 4$  magic square using the same numbers as the Dürer square which completes the figure below:

1	14	8	11
15			
12			
6			

Problems like this are much harder than the  $3 \times 3$  case without some kind of theory or method as a guide (see 10 and reflect upon it). You may want to try this problem for, say, ten, fifteen, thirty minutes, then come back to it later, or after reading the next section.

9. Find a magic square with first row

1 15 14 4

Again: such problems are hard without a theory or a method.

10. How many ways are there of filling an  $n \times n$  square with the numbers 0, 1, ...,  $n - 1$ ? Make a table of this number, which we will call  $F(n)$ , for  $n = 1, 2, 3, 4, 5$ . Let  $M(n)$  be the number of magic squares of order  $n$ . Any guesses about how large this number is?

## Notes

Consider the following  $5 \times 5$  array of 5 symbols, which we call  $X$ :

```
a b c d e
b c d e a
c d e a b
d e a b c
e a b c d
```

It has the property that in each symbol occurs once and only once in each row, and also in each column. Such a square is called a *Latin*. What is the rule used in its construction?

Here another Latin square, which we call  $Y$ :

```
a b c d e
e a b c d
d e a b c
c d e a b
b c d e a
```

What is its rule of construction? Now superimpose the two Latin squares to get the following array, which we call  $XY$ :

```

aa bb cc dd ee
be ca db ec ad
cd de ea ab bc
dc ed ae ba cb
eb ac bd ce da

```

Notice that each pair of symbols occurs once and only once. When  $XY$  has this property, we call  $X$  and  $Y$  *orthogonal* Latin squares. The square  $XY$  is called a *Greco-Latin* squares.

**Questions for contemplation:** Is there a connection between Latin squares and magic squares? Investigate and comment. How many Latin squares of order  $n$  are there? How many Greco-Latin squares? Is there a way to systematically construct all Latin squares? All Greco-Latin squares? Are the Latin (or Greco-Latin) squares of all orders?

## 2 Modular arithmetic

We're now going to learn how to construct magic squares using *modular arithmetic*. This is something we know, even if we don't know the name: if it is now 7 o'clock, and if a friend calls to say "please meet me at the airport in 8 hours," then we go to the airport at 3 o'clock. This is because  $7 + 8 = 15$ , but when we subtract 12, we get 3. If we were told to meet at the airport in 39 hours, we would compute  $7 + 39 = 46 = 3 \times 12 + 10$ . Our appointment is at 10 PM one day later.

Clock arithmetic is modular arithmetic with *modulus* 12. The basic idea is "do the usual arithmetic, then add or subtract multiples of 12" to get a number in range. "In range means in the range 1 to 12 (or 0 to 11). Of course, one can do this with any number as modulus, not just 12. Here are some examples.

$$\begin{aligned} 7 + 8 &\equiv 3 \pmod{12} \\ 7 \times 8 &\equiv 8 \pmod{12} \\ 4 - 9 &\equiv 7 \pmod{12} \end{aligned}$$

$$\begin{aligned} 4 + 3 &\equiv 2 \pmod{5} \\ 4 - 3 &\equiv 1 \pmod{5} \\ 3 - 4 &\equiv 4 \pmod{5} \\ 3 \times 4 &\equiv 2 \pmod{5} \end{aligned}$$

Note that  $3 - 4 = -1$ , but  $-1 + 5 = 4$ , so that  $3 - 4$  is the same as 4 modulo 5. Again, two numbers  $a$  and  $b$  are considered to be the same modulo  $n$  if they

differ by a multiple of  $n$ . Thus one can consider the numbers  $0, 1, \dots, n - 1$  to form a finite system of arithmetic.

1. Make addition and multiplication tables for arithmetic modulo 5.
2. Let  $f(x, y) = 3x + y \pmod{5}$ . Compute  $f(1, 2)$ .
3. Make a table of values  $f(x, y)$  where  $x = 0, 1, 2, 3, 4$  and  $y = 0, 1, 2, 3, 4$ . Study the row and column sums of this table. Can you describe in a non-technical way the pattern of zeroes, the pattern of ones, etc.?
4. Make a table of values  $g(x, y) = 3x + 4y \pmod{5}$  where  $x = 0, 1, 2, 3, 4$  and  $y = 0, 1, 2, 3, 4$ . Study the row and column sums of this table. Can you describe in a non-technical way the pattern of zeroes, the pattern of ones, etc.?
5. Now make a table of for the values of  $h(x, y) = f(x, y) + 5g(x, y)$ , where the arithmetic used is the ordinary one. Study the row and column sums of this table.
6. Rewrite the entries of the table you just made in base 5 notation. Describe any significant properties you notice.

### 3 Constructing Magic Squares

In the last section you noticed something quite remarkable about the tables that you constructed using modular arithmetic. Here are some ideas to use in thinking about such tables and in constructing magic squares.

- A square is *row magic* if all its row sums are the same.
- A square is *column magic* if all its column sums are the same.
- A square is *magic* if all its row and column sums are the same.
- A square is *simple* if all of its entries are distinct.

Which terms applies to the tables for  $f$ ,  $g$ , and  $h$ ? Notice that what we called a magic square in the introduction is a square that is both magic and simple.

1. Construct a  $7 \times 7$  magic square.
2. Construct a  $6 \times 6$  magic square. This is harder than the previous problem.

3. Suppose given two functions  $f(x, y) = ax + by + c \pmod n$  and  $g(x, y) = dx + ey + f \pmod n$ . Let  $h(x, y) = f(x, y) + ng(x, y)$ . Use  $h$  to make an  $n \times n$  table. What are the conditions on  $(a, b, c)$  and  $(d, e, f)$  that ensure that (i) the square is row magic, (ii) the square is column magic, (iii) the square is simple? Partial answers are welcome.
4. What is the effect on the Latin squares of changing the constant term in  $f(x, y)$ , that is, of changing  $c$ ? What is the effect on the magic square of changing the constant terms in both  $f(x, y)$  and  $g(x, y)$ ?
5. What orders of magic squares can we construct using functions like  $h(x, y)$ ? Partial answers are welcome.
6. Can you find any other interesting properties of the magic squares constructed? Can you prove that these properties hold? Can you prove that they hold for a general class of magic squares?
7. Are magic squares used for anything besides fun and games?

Enjoy working on the problems. You *don't* have to do them all!! But try some of them between this time and next.

This document, including improvements and corrections, is available in pdf form at

<http://www.math.utah.edu/~carlson/mathcircles/magic.pdf>

## 4 Why does it work?

In the last section we noticed several remarkable things. The first is that we can use certain modular functions to make Latin squares. In fact one of the functions that works is  $f(x, y) = x + y \pmod n$ , which gives the addition table modulo  $n$ . (Remember that in an  $n \times n$  Latin square, the  $n$  symbols appear exactly once in each row and in each column, like this:

a	b	c	d	e
b	c	d	e	a
c	d	e	a	b
d	e	a	b	c
e	a	b	c	d

The Latin square below is the same, but with a different set of symbols. Do you recognize it?

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

As noted in the last section that some functions  $f(x, y) = ax + by + c \pmod n$  produce Latin squares. In problem 3 of that section we asked when functions like these can be used to make magic squares. Let's think about that problem some more, and see if we can solve it.

**Problem 1** *What are the conditions on  $a$ ,  $b$ ,  $c$ , and  $n$  that guarantee that  $f(x, y) = ax + by + c \pmod n$  generates a Latin square? What kind of magic properties does the resulting Latin square have?*

Once we have solved problem 1, we can do a more one:

**Problem 2** *What are the conditions on  $a$ ,  $b$ ,  $c$ , on  $d$ ,  $e$ ,  $f$ , and also on  $n$  that guarantee that  $f(x, y) = ax + by + c \pmod n$  and  $h(x, y) = dx + ey + f \pmod n$  are orthogonal Latin squares?*

Recall that given two Latin squares  $U$  and  $V$  we can make a new square with entries  $(u, v)$ , in the  $(i, j)$  position, where  $u$  comes from the  $(i, j)$  position of  $U$  and  $v$  from the  $(i, j)$  position of  $V$ . We call the new square  $UV$ . Then  $U$  and  $V$  are *orthogonal* if each pair  $(u, v)$  occurs exactly once.

**Problem 3** *What are the conditions on  $a$ ,  $b$ , etc. for  $f(x, y)$  and  $g(x, y)$  to form a magic square according to the rule  $h(x, y) = f(x, y) + ng(x, y)$ ? Note that the  $h(x, y)$  is formed using the rules of ordinary arithmetic. We'll call such a square an  $(f, g)$  magic square.*

By solving the above three problems, you will understand a lot about the theory of magic squares. In particular, you will be able to generate many magic squares for many orders  $n$ . Below are some more problems.

## Problems

1. How many  $(f, g)$  magic squares of order three are there? How does this number compare with the total number of ways of filling a  $3 \times 3$  square by the numbers  $0, \dots, 8$ ? (This problem, stated for  $n = 3$ , can be generalized).

2. Can you make an  $(f, g)$  magic square of order 4?
3. Find an  $(f, g)$  magic square of order ten. Then color it according to the rules discussed in class.

## 5 More about modular arithmetic

Modular arithmetic is good for many things other besides making Latin, Greco-Latin, and magic squares. We are going to end this session by seeing how to compute and think about big powers mod  $n$ . Here is an example:

**Problem 4** *What is  $3^{100} \pmod{101}$  ?*

Raising huge numbers to huge powers modulo a huge number is the kind of mathematics that makes the famous RSA code work. (That's the encryption algorithm used by web browsers to transmit credit card information, etc. Number theory is applied math!)

We are going to solve this problem in two ways, but before we do, we are going to do a warm up exercise. What is

$$5^{13} \pmod{17}?$$

Here is a hint on how to do problems like this. First,

$$13 = 8 + 4 + 1.$$

This is equivalent to the statement that the binary expansion of 13 is 1101:

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

Do you see why? Now

$$5^{13} = 5^{8+4+1}.$$

But we can easily compute  $5^2$ ,  $5^4$ ,  $5^8$ , etc. modulo 17 by successive squaring:

$$\begin{aligned} 5^2 &= 25 \equiv 8 \pmod{17} \\ 5^4 &\equiv 8^2 \equiv 13 \pmod{17} \\ 5^8 &\equiv 13^2 \equiv 16 \pmod{17} \end{aligned}$$

Thus

$$5^{13} \equiv 5 \cdot 13 \cdot 16 \equiv 1040 \equiv 3 \pmod{17}.$$

Now you can easily solve Problem 4.



## Problems

1. Compute  $23^{113} \bmod 129$ .
2. Explore the expressions  $2^k \bmod p$ , where  $p$  is a prime. Are there any values of  $(k, p)$  for which one notices interesting patterns? Can you prove these patterns to be correct?

## 6 Notes

Magic square:

1	14	8	11
15	4	10	5
12	7	13	2
6	9	3	16

Magic square:

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16