Modular Arithmetic

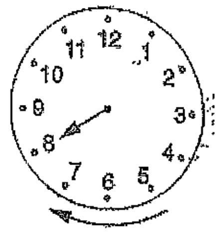
Clock arithmetic and addition

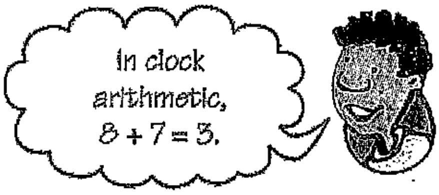
In our counting system, the numbers go on indefinitely: 1, 2, 3, 4, ... This set is an *infinite* one. However, some counting systems are not infinite.

Example 1

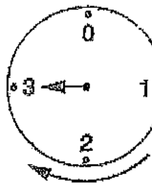
If we count around a clockface, the sequence of numbers is 1, 2, 3, 4, ..., 12. The pattern is repeated after we get to 12. The set is *finite*.

For example, if we start at 8 on a clockface and add 7, we finish at 3.





Example 2

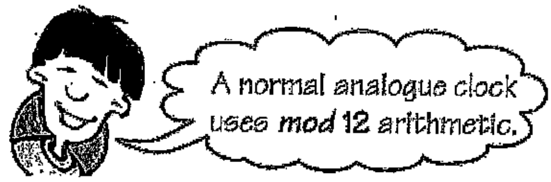


Egg timers work in a similar way. Suppose the indicator on the dial is at 3 minutes. In a further 2 minutes it will be at 1. Thus in this system, $3 + 2 = 1$.

Assuming this indicator keeps going around, in 5 more minutes it will be at 2. That is, $1 + 5 = 2$.

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

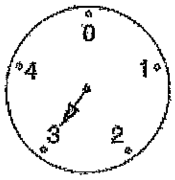
This arithmetic which uses only the numbers 0, 1, 2, 3, is known as **arithmetic modulus 4** or ***mod* 4** arithmetic.

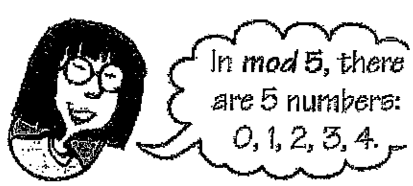


Exercise 17A Clock arithmetic and addition

1 Copy and complete this addition table for a 5 minute clock.

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





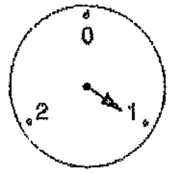
2 Use the *mod* 5 table in question 1 to simplify the following.

(a) $1 + 4$ (b) $3 + 3$ (c) $2 + 4$ (d) $4 + 2$

(e) $1 + 2 + 3$ (f) $3 + 2 + 1$ (g) $4 + 4$ (h) $2 + 2 + 2$

(i) $4 + (3 + 1)$ (j) $(4 + 3) + 1$ (k) $(3 + 2) + 3$ (l) $3 + (2 + 3)$

3 The diagram shows a 3 minute clock. Use it to make an addition table for *mod* 3 arithmetic. Then simplify the following.



(a) $2+1$ (b) $2+2$ (c) $2+1+2$
(d) $1+2+2$ (e) $2+2+2$ (f) $1+2+2+1$
(g) $2+1+2+1+2+1$

4 Construct addition tables for the following modular arithmetics, and keep them for future reference.
(a) *mod* 6 (b) *mod* 7 (c) *mod* 8

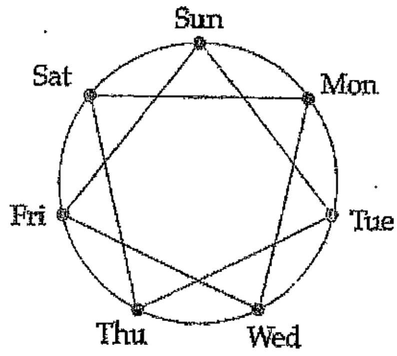
5 Use the tables you have constructed in question 4 to evaluate the following.
(a) $5+3$ (*mod* 7) (b) $5+4$ (*mod* 6) (c) $4+7$ (*mod* 10)
(d) $3+4$ (*mod* 7) (e) $9+8$ (*mod* 11) (f) $7+6$ (*mod* 8)
(g) $4+2+3$ (*mod* 9) (h) $5+6+7$ (*mod* 10) (i) $4+4+4+4$ (*mod* 11)

6 If a 5 minute clock starts at 0, what will the indicator show after:
(a) 11 minutes? (b) 15 minutes? (c) 23 minutes?
(d) 1 hour? (e) 176 minutes? (f) 89 minutes?

7 If a 9 minute clock starts at 0, what will the hand show after the clock has run for:
(a) 20 minutes? (b) 36 minutes? (c) 100 minutes?
(d) 23 minutes? (e) 86 minutes? (f) 2 hours?

8 Suppose the days of the week are placed on a 7 position dial, beginning with Sunday.
(a) What number corresponds to Wednesday?
(b) What number corresponds to Saturday?
(c) What day is 34 days after Sunday?
(d) What day is 59 days after Tuesday?
(e) Anthony planted some tomato seeds on a Thursday, and 32 days later he transplanted them. If he harvested them 54 days after they were transplanted, on what day of the week were they harvested?

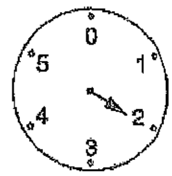
9 Cheryl goes to the gymnasium every second day. The diagram gives a geometric pattern that illustrates her program.
(a) If she trains on Monday, what time will elapse before she trains on Monday again?
(b) How many lines are found in this pattern?
(c) How many times do you move around the clock before arriving back at the starting point?



10 Draw a pattern similar to the pattern in question 9 for a person who goes to the gymnasium:
A every day *B* every third day
C every fourth day *D* every fifth day
For each pattern, answer the following questions.
(a) If the person trains on Monday, what time will elapse before training on Monday again?
(b) How many lines are found in the pattern?
(c) How many times do you move around the clock before arriving back at the starting point?

11 State the modulus of the following.
(a) the months of the year
(b) a 3 minute egg timer
(c) the days of the week
(d) an analogue clock

Residues and congruent integers



This clock uses *mod* 6 arithmetic. No matter how many times the pointer moves around the dial, only the numbers 0, 1, 2, 3, 4, 5 will be indicated.

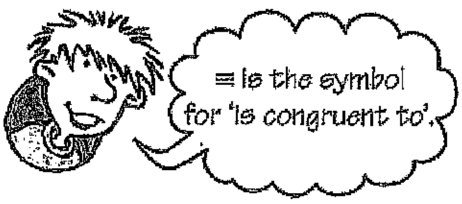
For example, if we set the clock at 0, after 49 minutes the pointer will be at 1. That is,

$$49 = 6 \times 8 + \textcircled{1}$$ **The remainder is 1 when we divide 49 by 6.**

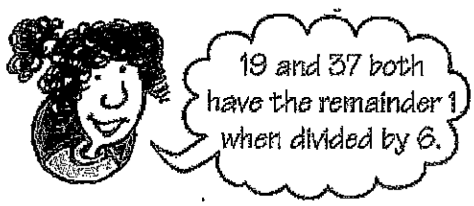
The remainder is known as the **residue.**

> **Residue**
> The residue of an integer n *mod* m is the remainder when n is divided by m.

All integers in *mod* 6 with the same remainder are said to be **congruent** in *mod* 6 arithmetic. For example,



$19 \equiv 37$ (*mod* 6)



> **Congruence**
> The integers x and y are said to be congruent *mod* m if they have the same residue *mod* m. In this case we write $x \equiv y$ (*mod* m).

Exercise 17B Residues and congruent integers

1 (a) Write down the residues in *mod* 5 arithmetic.
(b) Write down the residues in *mod* 7 arithmetic.

2 Write down the residues *mod* 5 for the following numbers.
(a) 26 (b) 100 (c) 17 (d) 0 (e) 11
(f) 83 (g) 264 (h) 81 (i) 4 (j) 3217

3 Write the residues of the following in *mod* 7.
(a) 34 (b) 21 (c) 88 (d) 94 (e) 5
(f) 170 (g) 131 (h) 0 (i) 4 (j) 4316

4 What are the residues of 50 in the following arithmetics?
(a) *mod* 7 (b) *mod* 5 (c) *mod* 6 (d) *mod* 11

5 Write 4 numbers congruent to:
(a) 1 (*mod* 7) (b) 3 (*mod* 5) (c) 4 (*mod* 6)

6 Write true (T) or false (F) for the following statements.

(a) $5 \equiv 3$ (*mod* 2) (b) $17 \equiv 2$ (*mod* 3) (c) $49 \equiv 37$ (*mod* 12)
(d) $16 \equiv 3$ (*mod* 7) (e) $32 \equiv 0$ (*mod* 5) (f) $1233 \equiv 1914$ (*mod* 11)

7 Find the smallest value for the pronumeral in each of:

(a) $17 \equiv x$ (*mod* 5) (b) $20 \equiv y$ (*mod* 7) (c) $33 \equiv a$ (*mod* 6)
(d) $65 \equiv b$ (*mod* 3) (e) $47 \equiv a$ (*mod* 4) (f) $101 \equiv c$ (*mod* 11)

Notation

The set of residues in *mod* 5 arithmetic is {0, 1, 2, 3, 4}. This set is often referred to as $\mathbb{Z}_5$.

Similarly, in *mod* 7 the residues are given by $\mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$.

8 Write each of the following as a set.

(a) $\mathbb{Z}_3$ (b) $\mathbb{Z}_4$ (c) $\mathbb{Z}_9$

9 Write each of the numbers below as congruent to *a* (*mod* 5), where *a* is an element of $\mathbb{Z}_5$.

(a) 46 (b) 83 (c) 109 (d) 153 (e) 550

10 Find the smallest value of *m* in the following.

(a) $7 \equiv 2$ (*mod m*) (b) $7 \equiv 3$ (*mod m*) (c) $27 \equiv 5$ (*mod m*)
(d) $27 \equiv 2$ (*mod m*) (e) $81 \equiv 0$ (*mod m*) (f) $586 \equiv 5$ (*mod m*)

11 Consider the question $22 + 34$ (*mod* 5).

Approach 1: $22 + 34$ (*mod* 5) $= 2 + 4$ (*mod* 5)
$\equiv 1$ (*mod* 5)

Approach 2: $22 + 34$ (*mod* 5) $= 56$ (*mod* 5)
$\equiv 1$ (*mod* 5)

Use both approaches to answer the following.

(a) $7 + 12$ (*mod* 5) (b) $14 + 11$ (*mod* 7) (c) $20 + 19$ (*mod* 7)
(d) $16 + 23$ (*mod* 6) (e) $5 + 4 + 6$ (*mod* 3) (f) $21 + 23 + 25$ (*mod* 4)

Riddle When visitors knock on your door, what is the polite thing to do?

Match the letters with the answers to solve the riddle.

A: $6 + 11$ (*mod* 12) M: $24 + 27$ (*mod* 5)
I: $3 + 4 + 5$ (*mod* 6) N: $22 + 15$ (*mod* 7)
T: The number of elements in $\mathbb{Z}_7$
V: The number of elements in $\mathbb{Z}_6$

6	0	7	5	1	0	2

Challenging problem   Operation $\circledast$

The operation $\circledast$ is defined as

$$a \circledast b = 2a - b$$

where a, b are integers.

For example, $5 \circledast 4 = 2 \times 5 - 4$
$= 10 - 4$
$= 6$

Answer the following.

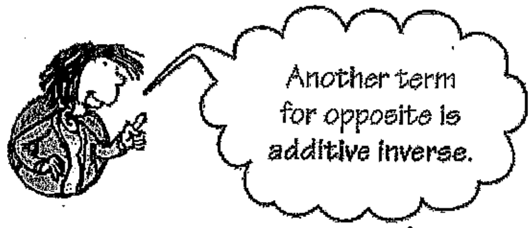
(a) Find:

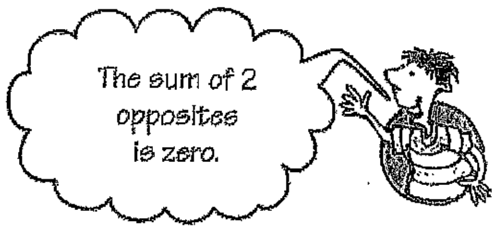
(i) $4 \circledast 3$ (ii) $6 \circledast 8$ (iii) $-4 \circledast 2$

(b) Is $6 \circledast 5$ the same as $5 \circledast 6$?

Opposites and subtraction

In normal arithmetic, the opposite of the integer 6 is the integer −6; that is, $6 + (-6) = 0$. And the opposite of −3 is 3; again, $-3 + 3 = 0$.





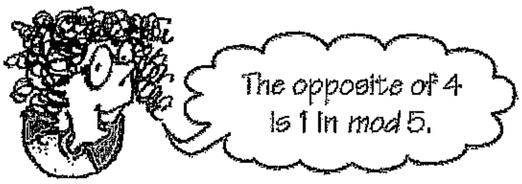
Opposites exist in modular arithmetic also. For example, $3 + 2 \equiv 0$ (*mod* 5). Thus 3 is the opposite of 2, and 2 is the opposite of 3, in *mod* 5.

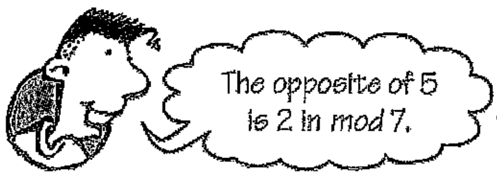
Subtraction is an operation where we 'add the opposite'.

Examples

1 $3 - 4 = 3 + 1$ (*mod* 5)
$= 4$ (*mod* 5)

2 $1 - 5 = 1 + 2$ (*mod* 7)
$= 3$ (*mod* 7)





Exercise 17C Opposites and subtraction

1 Write down the opposites of the following in *mod* 3.
(a) 1   (b) 2   (c) 0

2 Write down the following in $\mathbb{Z}_5$
(a) −3   (b) −4   (c) −1   (d) −2

3 What numbers in $\mathbb{Z}_8$ are represented by:

(a) –6? (b) –3? (c) –7? (d) –2?

(e) –1? (f) –9? (g) –27? (h) –16?

4 Simplify.

(a) 2 – 3 (*mod* 7)
(b) 2 – 4 (*mod* 5)
(c) 4 – 1 (*mod* 5)
(d) 9 – 2 (*mod* 10)
(e) (3 – 5) (*mod* 10)
(f) 2 + 1 – 4 (*mod* 5)
(g) 3 – 2 – 3 (*mod* 4)
(h) 1 – 4 – 3 (*mod* 6)
(i) 1 – (2 – 4) (*mod* 5)
(j) 4 – 7 – 9 (*mod* 11)

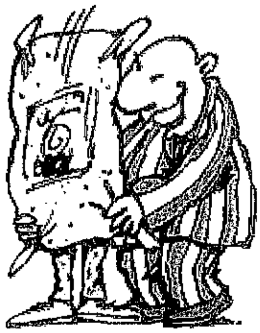
5 In *mod* 4, simplify the following.

(a) 1 + 3 – 2
(b) 3 – 2 – 3
(c) 1 – (2 – 1)
(d) 2 – (1 – 2)
(e) (1 – 2) + (2 – 3)
(f) (1 – 2) – (2 – 3)

6 In what modular arithmetics would the following be true?

(a) 1 – 3 = 2
(b) 1 – 3 = 5
(c) 5 – 7 = 8
(d) 4 – 5 = 6
(e) 2 – 7 = 3
(f) 6 – 9 = 10

Riddle Who gets the sack every time he goes to work?



Evaluate the following, then match the letters with the answers to solve the riddle:

S: 1 – 4 (*mod* 7)
H: 3 – 4 – 2 (*mod* 11)
M: 5 – 6 (*mod* 7)
O: 3 + 3 + 5 (*mod* 6)
E: –3 (*mod* 5)
P: –36 (*mod* 13)

A: The opposite of 2 in $\mathbb{Z}_{11}$

T: The opposite of 3 in $\mathbb{Z}_{10}$

N: The additive inverse of 6 in $\mathbb{Z}_7$

7	8	2	3	5	4	7	6	9	1

Multiplication in modular arithmetic

Example 1

$\mathbb{Z}_5$

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

Consider the multiplication table in *mod* 5
Each entry belongs to $\mathbb{Z}_5$ For example,

$3 \times 4 = 12 \equiv 2 \ (mod\ 5)$

and $4 \times 2 = 8 \equiv 3 \ (mod\ 5)$

Exercise 17D Multiplication

1 Use the multiplication table in $\mathbb{Z}_5$ above to evaluate the following.

(a) $(3 \times 4) \times 2$ (b) 4×0 (c) $2 \times 2 \times 2$
(d) $(2 \times 3) \times 4$ (e) 4×4 (f) 3^2
(g) 2^3 (h) $1 \times 2 \times 3 \times 0$ (i) 4^3
(j) $(2 \times 3) + (3 \times 4)$ (k) $2 - (3 \times 4)$ (l) $2^2 + 3^2$

2 Make multiplication tables for *mod* 2, *mod* 4, *mod* 6, *mod* 7, *mod* 8, *mod* 9, *mod* 10 and *mod* 12 arithmetics, and keep them for further reference.

3 Compute in *mod* 4.

(a) 2×3 (b) $2 \times 3 \times 2$ (c) 2^2
(d) $3(1+2)$ (e) $3 \times 2 + 1 \times 2$ (f) 3^2
(g) 3×0 (h) $2^2 + 3^2$ (i) 3^3

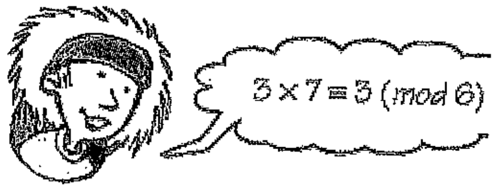
4 Simplify in $\mathbb{Z}_6$

(a) 5×2 (b) $3 \times 2 \times 4$ (c) 5^2
(d) 2^3 (e) $3^2 - 4^2$ (f) $2^3 - 4$
(g) -4×5 (h) 3^4 (i) $3^2 + 4^2$
(j) $2^2 - 3^2$ (k) $-1 \times 3 \times 4$ (l) $(-4)^2$
(m) $(2-3)(3-4)$ (n) $3(2-4)$ (o) 4^4

Example 2

Evaluate $(3 \times 7)^6 \ (mod\ 6)$.

Solution: $(3 \times 7)^6 \equiv 3^6 \ (mod\ 6)$
$\equiv 3 \ (mod\ 6)$



5 Study Example 2, then evaluate.

(a) $(2 \times 3)^4 \ (mod\ 5)$ (b) $(2 \times 3)^6 \ (mod\ 4)$ (c) $5 \times 6 \ (mod\ 7)$
(d) $7 \times 8 \ (mod\ 10)$ (e) $(4 \times 5)^8 \ (mod\ 10)$ (f) $(3 \times 7)^{10} \ (mod\ 10)$
(g) $3 + 4 \times 2 \ (mod\ 8)$ (h) $5^2 + 3^2 + 4^2 \ (mod\ 6)$ (i) $10^3 \ (mod\ 9)$
(j) $10^4 \ (mod\ 12)$

6 Evaluate x^2 if:

(a) $x = 2 \ (mod\ 5)$ (b) $x = 3 \ (mod\ 5)$ (c) $x = 7 \ (mod\ 8)$
(d) $x = 9 \ (mod\ 12)$ (e) $x = 3 \ (mod\ 7)$ (f) $x = 8 \ (mod\ 10)$

7 Evaluate $x^2 + 3x + 2$ if:

(a) $x = 2 \ (mod\ 5)$ (b) $x = 3 \ (mod\ 7)$ (c) $x = 5 \ (mod\ 8)$
(d) $x = 7 \ (mod\ 9)$ (e) $x = 7 \ (mod\ 10)$ (f) $x = 9 \ (mod\ 12)$

Example 3

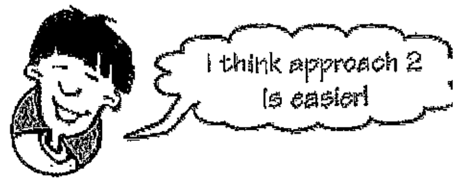
Evaluate $17 \times 29 \equiv a \ (mod\ 7)$, where a is in $\mathbb{Z}_7$

Approach 1: $17 \times 29 = 493 \ (mod\ 7)$

$\equiv 3 \ (mod\ 7)$

Approach 2: $17 \times 29 = 3 \times 1 \ (mod\ 7)$

$\equiv 3 \ (mod\ 7)$



8 Study Example 3, then evaluate the following where a is in $\mathbb{Z}_7$

(a) $9 \times 11 \equiv a \ (mod\ 7)$ (b) $13 \times 15 \equiv a \ (mod\ 7)$ (c) $28 \times 16 \equiv a \ (mod\ 7)$

(d) $36 \times 50 \equiv a \ (mod\ 7)$ (e) $5 \times 8 \times 11 \equiv a \ (mod\ 7)$ (f) $22^2 \equiv a \ (mod\ 7)$

9 Simplify the following in *mod* 5.

(a) 24×27 (b) $31 \times 32 \times 33$ (c) 104×216

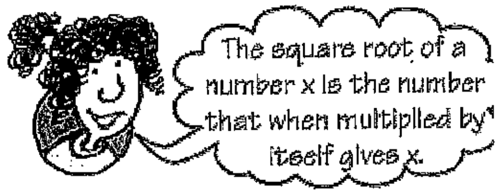
(d) 16^4 (e) 101×203 (f) 6^{10}

Example 4

Consider this example in *mod* 5:

$1 \times 1 = 1 \ (mod\ 5)$ and $4 \times 4 = 1 \ (mod\ 5)$

We can conclude that the square root of 1 in *mod* 5 is either 1 or 4.



10 (a) By considering the multiplication table in *mod* 5, find the square root(s) of 4.

(b) Does every element of $\mathbb{Z}_5$ have a square root? If not, which ones do?

11 Consider $\mathbb{Z}_7$

(a) Indicate which numbers have a square root or roots, and write them down.

(b) Which numbers do not have a square root?

12 Investigate square roots in $\mathbb{Z}_3$, $\mathbb{Z}_4$ and $\mathbb{Z}_9$. Write down your conclusions.

Challenging problem **Remainders**

(a) Find the remainder when 7^4 is divided by 100.

(b) Hence or otherwise, find the remainder when 7^{1999} is divided by 100.

Riddle **How can you build a sandcastle in 10 seconds?**

Evaluate the following, then match the letters with the answers to solve the riddle.

N: $4^2 \ (mod\ 9)$ D: $3 \times 7 \ (mod\ 11)$

K: $5 \times 4 \ (mod\ 7)$ A: $3 \times 8 \ (mod\ 10)$

S: $2 \times 3 \times 5 \ (mod\ 7)$ I: $5 \times 3 \ (mod\ 12)$

E: $2^3 \ (mod\ 9)$ U: $7 \times 5 \ (mod\ 10)$

C: $6 \times 3 \ (mod\ 9)$ Q: $5 \times 2 \ (mod\ 9)$

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

Challenging problem Is it true?

We can show that:

$2^3 \equiv 2 \ (mod\ 3)$ $2^5 \equiv 2 \ (mod\ 5)$ $2^7 \equiv 2 \ (mod\ 7)$

$3^5 \equiv 3 \ (mod\ 5)$ $3^7 \equiv 3 \ (mod\ 7)$ $4^5 \equiv 4 \ (mod\ 5)$

(a) Is it true in general that

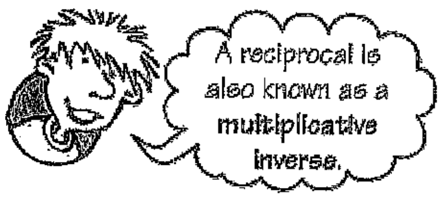
$$x^m \equiv x \ (mod\ m)$$

for x in $\mathbb{Z}_m$?

(b) For what values of m does the result hold?

Reciprocals and division

If 2 numbers have a product of 1, then they are said to be **reciprocals** of each other.

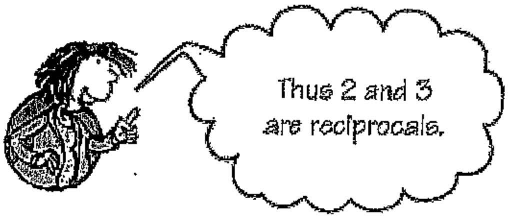


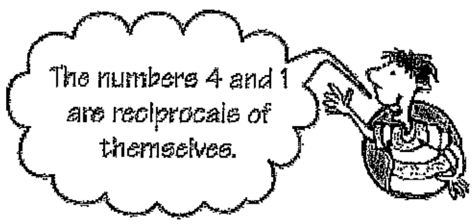
$\mathbb{Z}_5$

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

If we look at the multiplication table for *mod* 5 arithmetic, we observe that:

$2 \times 3 = 1$
$4 \times 4 = 1$
$1 \times 1 = 1$
$3 \times 2 = 1$





$\mathbb{Z}_4$

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

Consider multiplication in *mod* 4.

$1 \times 1 = 1$ and $3 \times 3 = 1$ $\therefore$ 1 and 3 have reciprocals

We can conclude that in *mod* 4 the number 2 does not have a reciprocal.

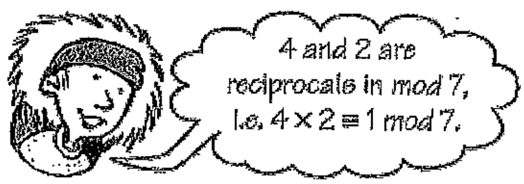
If p is *prime*, then in *mod* p arithmetic every *non-zero* number has a unique reciprocal.

As in the case of real numbers, division is regarded as the inverse of multiplication. That is, when 'dividing' we 'multiply by the reciprocal'.

Examples

1 $4 \div 3 = 4 \times 2 \ (mod\ 5)$
$\quad \equiv 3 \ (mod\ 5)$

2 $1 \div 4 = 1 \times 2 \ (mod\ 7)$
$\quad \equiv 2 \ (mod\ 7)$



Exercise 17E Reciprocals and division

1 (a) Do all non-zero numbers in *mod* 3 arithmetic have reciprocals?
(b) Write down the reciprocals of each number.

2 Which numbers have reciprocals in *mod* 7? List them.

3 (a) Which numbers have reciprocals in *mod* 6?
(b) Which do not have reciprocals?

4 Evaluate in *mod* 7.

(a) $3 \div 2$ (b) $2 \div 3$ (c) $1 \div 2$
(d) $5 \div 2$ (e) $2 \div 6$ (f) $4 \div 3$
(g) $6 \div 5$ (h) $4 \div 2$ (i) $\frac{3 \times 2}{4 \times 5}$
(j) $3 + 6 \div 4$ (k) $(2 - 3) \div 2$ (l) $(5 \times 2) \div 6$

5 Evaluate in *mod* 5.

(a) $1 \div 2$ (b) $3 \div 2$ (c) $4 \div 3$
(d) $(2 \div 3) \times 4$ (e) $(1 \div 3)^2$ (f) $\frac{2 \div 3}{3 \div 4}$
(g) $4 \div 2 \div 3$ (h) $3 - 1 \div 2$ (i) $4 \div 3 \times 2$

6 Evaluate in *mod* 11

(a) $4 \div 3$ (b) $2 \div 9$ (c) $5 \div 6$
(d) $10 \div 7$ (e) $6 \div 5$ (f) $7 \div 10$
(g) $\frac{4 \times 3}{6 \times 7}$ (h) $\frac{2 \times 5}{3 \times 7}$ (i) $\frac{3 \div 7}{4 \div 9}$

Challenging problem *Mod* primes

1 Show that $1 + 3 + 5 + 7 + 9 \equiv 0$ (*mod* 5).

2 Find $2 + 4 + 6 + 8 + 10 + 12 + 14$ (*mod* 7).

3 (Harder) Find $1 + 4 + 7 + \ldots$ (22 terms) (*mod* 5).

4 $3 + 3^2 + 3^3 + 3^4 + \ldots + 3^{24}$ (*mod* 7).

Solving equations

The normal rules apply when solving equations in modular arithmetic.

Examples

1 $3x = 4$ (*mod* 5)
$x = 4 \div 3$ (*mod* 5) Divide both sides by 3.
$= 4 \times 2$ (*mod* 5)
$= 3$ (*mod* 5)

2 $a - 3 = 4 \pmod 5$
$a = 4 + 3 \pmod 5$. Add 3 to both sides.
$= 2 \pmod 5$

3 $2a + 6 = 1 \pmod 7$
$2a = 1 - 6 \pmod 7$ Take 6 from both sides.
$= 1 + 1 \pmod 7$ Add the opposite.
$= 2 \pmod 7$
$a = 1 \pmod 7$ Divide both sides by 2.

Exercise 17F Solving equations

1 Solve the following in *mod* 5.

(a) $2x = 1$ (b) $x + 4 = 3$ (c) $\frac{x}{2} = 3$
(d) $x - 4 = 1$ (e) $3a = 1$ (f) $3 - y = 2$
(g) $1 - c = 4$ (h) $4x = 3$

2 Solve the following in *mod* 7.

(a) $3a = 2$ (b) $\frac{c}{4} = 3$ (c) $a + 6 = 3$
(d) $5 + y = 0$ (e) $c + 6 = 4$ (f) $y - 6 = 3$
(g) $5x = 4$ (h) $x^2 = 1$

3 Solve in the modulus indicated.
(a) $x + 3 = 1 \pmod 6$ (b) $2a - 3 = 7 \pmod 9$ (c) $5 - d = 3 \pmod 7$
(d) $5 - 2c = 1 \pmod 6$ (e) $3a - 2 = 4 \pmod 5$ (f) $2x + 5 = 2 \pmod 7$
(g) $5x + 6 = 7 \pmod{11}$ (h) $3x + 1 = x + 6 \pmod 7$ (i) $2x + 1 = 3 - x \pmod 5$
(j) $3(x - 1) = 2 \pmod 5$ (k) $\frac{2a}{3} = 4 \pmod 5$ (l) $3x - 5 = 6 + x \pmod 7$

Riddle What do you have if you are holding 7 oranges in your left hand and 8 apples in your right hand?

Solve the following equations in *mod* 11, then match the letters with the answers to solve the riddle.

H: $4x - 5 = 7$ S: $x + x = 1$
D: $x + 7 = 3$ A: $\frac{c}{5} = 4$
I: $3 - c = 10$ B: $9y = 7$
G: $2x + 5 = 3$ N: $5d = 7$

2	4	10	3	9	8	7	6

Answers

Exercise 17A

1 *mod* 5

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

2 (a) 0 (b) 1 (c) 1 (d) 1 (e) 1 (f) 1 (g) 3 (h) 1 (i) 3 (j) 3 (k) 3 (l) 3

3 *mod* 3

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

(a) 0 (b) 1 (c) 2 (d) 2 (e) 0 (f) 0 (g) 0

4 (a) *mod* 6

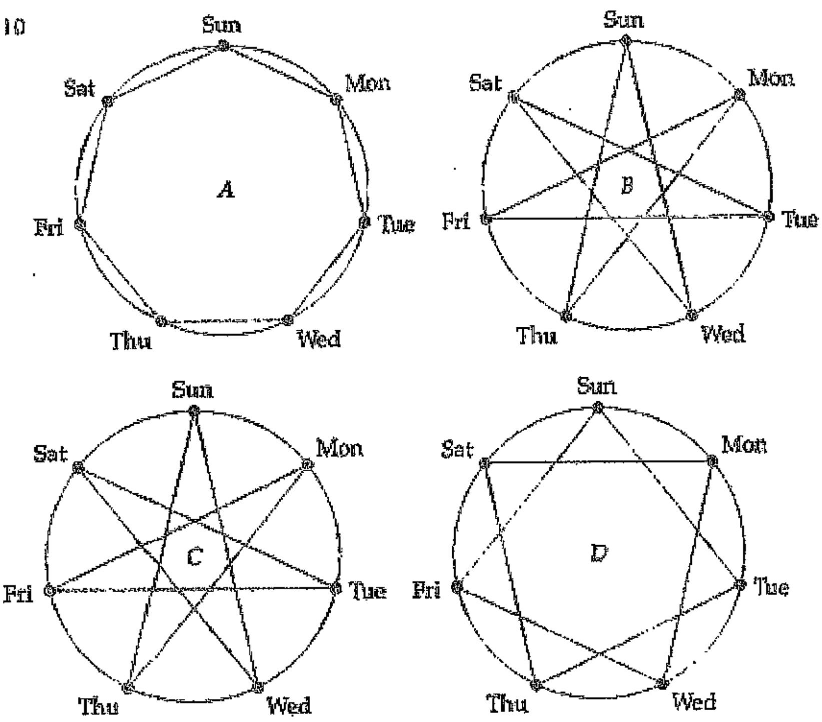
+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) *mod* 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

5 (a) 1 (b) 3 (c) 1 (d) 0 (e) 6 (f) 5 (g) 0 (h) 8 (i) 5 6 (a) 1 (b) 0 (c) 3 (d) 0 (e) 1 (f) 4
7 (a) 2 (b) 0 (c) 1 (d) 5 (e) 5 (f) 3 8 (a) 3 (b) [illegible] (c) Saturday (d) Friday (e) Saturday
9 (a) 2 weeks (b) 7 lines (c) 2 times

10



(a) *A* 7 days, *B* 3 weeks, *C* 4 weeks, *D* 5 weeks
(b) All 7 lines (c) *A* 1 time, *B* 3 times, *C* 4 times, *D* 5 times
11 (a) *mod* 12 (b) *mod* 3 (c) *mod* 7 (d) *mod* 12 (e) *mod* 6 (f) *mod* 24

Exercise 17B

1 (a) 0, 1, 2, 3, 4 (b) 0, 1, 2, 3, 4, 5, 6 2 (a) 1 (b) 0 (c) 2 (d) 0 (e) 1 (f) 3 (g) 4 (h) 1 (i) 4 (j) 2
3 (a) 6 (b) 0 (c) 4 (d) 3 (e) 5 (f) 2 (g) 5 (h) 0 (i) 4 (j) 4 4 (a) 1 (b) 0 (c) 2 (d) 6
5 (a) 8, 15, 22, 29 (b) 8, 13, 18, 23 (c) 10, 16, 22, 28 6 (a) T (b) T (c) T (d) F (e) F (f) F
7 (a) 2 (b) 6 (c) 3 (d) 2 (e) 3 (f) 2 8 (a) {0, 1, 2} (b) {0, 1, 2, 3} (c) {0, 1, 2, 3, 4, 5, 6, 7, 8}
9 (a) $46 \equiv 1$ (*mod* 5) (b) $83 \equiv 3$ (*mod* 5) (c) $109 \equiv 4$ (*mod* 5) (d) $153 \equiv 3$ (*mod* 5) (e) $550 \equiv 0$ (*mod* 5)
10 (a) 5 (b) 2 (c) 2 (d) 5 (e) 3 (f) 7 11 (a) 4 (*mod* 5) (b) 4 (*mod* 7) (c) 4 (*mod* 7) (d) 3 (*mod* 6)
(e) 0 (*mod* 3) (f) 1 (*mod* 4)

Challenging problem Operation ⊛ (a) (i) 5 (ii) 4 (iii) −10 (b) No

Exercise 17C

1 (a) 2 (b) 1 (c) 0 2 (a) 2 (b) 1 (c) 4 (d) 3 3 (a) 2 (b) 5 (c) 1 (d) 6 (e) 7 (f) 7 (g) 5 (h) 0
4 (a) 6 (*mod* 7) (b) 3 (*mod* 5) (c) 3 (*mod* 5) (d) 7 (*mod* 10) (e) 8 (*mod* 10) (f) 4 (*mod* 5) (g) 2 (*mod* 4)
(h) 0 (*mod* 6) (i) 3 (*mod* 5) (j) 10 (*mod* 11) 5 (a) 2 (b) 2 (c) 0 (d) 3 (e) 2 (f) 0 6 (a) *mod* 4 (b) *mod* 7
(c) *mod* 10 (d) *mod* 7 (e) *mod* 8 (f) *mod* 3

Exercise 17D

1 (a) 4 (b) 0 (c) 3 (d) 4 (e) 1 (f) 4 (g) 3 (h) 0 (i) 4 (j) 3 (k) 0 (l) 3

2 *mod* 2

×	0	1
0	0	0
1	0	1

mod 4

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

mod 6

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

3 (a) 2 (b) 0 (c) 0 (d) 1 (e) 0 (f) 1 (g) 0 (h) 1 (i) 3 4 (a) 4 (b) 0 (c) 1 (d) 2 (e) 5 (f) 4 (g) 4
(h) 3 (i) 1 (j) 1 (k) 0 (l) 4 (m) 1 (n) 2 (o) 4 5 (a) 1 (*mod* 5) (b) 0 (*mod* 4) (c) 2 (*mod* 7) (d) 6 (*mod* 10)
(e) 0 (*mod* 10) (f) 1 (*mod* 10) (g) 3 (*mod* 8) (h) 2 (*mod* 6) (i) 1 (*mod* 9) (j) 4 (*mod* 12) 6 (a) 4 (*mod* 5)
(b) 4 (*mod* 5) (c) 1 (*mod* 8) (d) 9 (*mod* 12) (e) 2 (*mod* 7) (f) 4 (*mod* 10) 7 (a) 2 (*mod* 5) (b) 6 (*mod* 7)
(c) 2 (*mod* 8) (d) 0 (*mod* 9) (e) 2 (*mod* 10) (f) 2 (*mod* 12) 8 (a) 1 (b) 6 (c) 0 (d) 1 (e) 6 (f) 1 9 (a) 3
(b) 1 (c) 4 (d) 1 (e) 3 (f) 1 10 (a) 2 or 3 (b) No. 0, 1, 4 do. 11 (a) 0, 1, 2, 4 (b) 3, 5, 6
12 J_3 and J_4: 0, 1 have square root(s).
J_9: 0, 1, 4, 7 have square root(s).
Challenging problem Remainders (a) 1 (b) 43
Challenging problem Is it true? (a) No (b) When m is a prime

Exercise 17E

1 (a) Yes (b) The reciprocal of 1 is itself. The reciprocal of 2 is itself. 2 1, 2, 3, 4, 5, 6 3 (a) 1, 5 (b) 0, 2, 3, 4
4 (a) 5 (b) 3 (c) 4 (d) 6 (e) 5 (f) 6 (g) 4 (h) 2 (i) 1 (j) 8 (k) 3 (l) 4 5 (a) 3 (b) 4 (c) 3 (d) 1
(e) 4 (f) 2 (g) 3 (h) 0 (i) 1 6 (a) 5 (b) 10 (c) 10 (d) 3 (e) 10 (f) 4 (g) 5 (h) 1 (i) 10
Challenging problem *Mod* prime 1 $1+3+5+7+9=25\equiv 0$ (*mod* 5) 2 0 (*mod* 7) 3 0 (*mod* 5) 4 0 (*mod* 7)

Exercise 17F

1 (a) $x=3$ (b) $x=4$ (c) $x=1$ (d) $x=0$ (e) $a=2$ (f) $y=1$ (g) $c=2$ (h) $x=2$ 2 (a) $a=3$ (b) $c=5$ (c) $a=4$
(d) $y=2$ (e) $c=5$ (f) $y=2$ (g) $x=5$ (h) $x=1, 6$ 3 (a) $x=4$ (*mod* 6) (b) $a=5$ (*mod* 9) (c) $d=2$ (*mod* 7)
(d) $c=2$ (*mod* 6) (e) $a=2$ (*mod* 5) (f) $x=2$ (*mod* 7) (g) $x=9$ (*mod* 11) (h) $x=6$ (*mod* 7) (i) $x=4$ (*mod* 5)
(j) $x=0$ (*mod* 5) (k) $a=1$ (*mod* 5) (l) $x=2$ (*mod* 7)