Math Circle–November 2 and 9
Division Algorithm and Remainder Arithmetic

Part I: Introduction – Relations

In the study of mathematics, two concepts we often face are *operations* and *relations*. For example, if we are given two numbers a and b, we can perform the operations $a+b,\ a-b,\ a\times b$ and $a\div b$. These operations yield numerical answers.

On the other hand, a *relation* between two objects means that they share something special with each other. We are familiar with the relation $=$ in that we say that $a = b$ if a and b have the same value. For example, if $a = 3 + 5$ and $b = 12 - 4$, we say that $a = b$.

A relation need not be a mathematical expression. We can say two people are "related" if they have the same eye color.

If we define the meaning of the symbol $<$ by: *$a < b$ if there exists a positive number k such that $a + k = b$* and if we are given two numbers a and b and ask the question, "is $a < b$?", the answer is either "yes" or "no." The symbol $<$ describes a special property "relating" a to b. This property is the relationship *is less than*.

There are many important relations in mathematics. In number theory an important relation is the *divides* relation. This should not be confused with the operation *division*. We ask the question "does *a divide b*?" and we expect an answer of "yes" or "no." However, if we ask the question "what is $a \div b$?" we expect to get an answer involving numbers (a quotient and a remainder). We will be making use of this relation in our later work.

> **Definition.** An integer a, not zero, is said to **divide** an integer b, which we will denote by $a \mid b$, if there exists an integer k such that $b = a \times k$. If a does not divide b, we write $a \nmid b$.

For example, $3 \mid 15$ since there exists an integer 5 such that $15 = 3 \times 5$. On the other hand, $3 \nmid 7$ since we cannot find an integer k such that $7 = 3 \times k$.

In mathematics, most relations are defined on sets of numbers. The relation given by $a < b$ can be defined on the set of whole numbers, the set of integers, the set of rational numbers, or on the set of all real numbers. However, our relation $a \mid b$ is restricted to the set of integers.

There are three properties that a relation *might have*, whether the relation is mathematical or not. If we let the symbol $\mathcal{R}$ represent any relation then then three properties are:

- The **reflexive** property: $a\mathcal{R}a$. That is, when a is related to itself.
- The **symmetric** property: If $a\mathcal{R}b$, then $b\mathcal{R}a$. That is, if a is related to b, then b is related to a.
- The **transitive** property: If $a\mathcal{R}b$ and $b\mathcal{R}c$, then $a\mathcal{R}c$.

Exercise 1. Answer each of the following.

(a) For the non-mathematical relation ***is taller than*** defined on a set of people, which of the above three properties does this relation satisfy?

(b) For the relation ***has the same eye color*** defined on a set of people, which of the above three properties does this relation satisfy?

(c) For the relation $=$, which of the above three properties does this relation satisfy?

(d) For the relation $<$, which of the above three properties does this relation satisfy?

(e) For the relation $\mid$, which of the above three properties does this relation satisfy?

If a relation satisfies all three properties (reflexive, symmetric and transitive), then we call it an **equivalence relation**. Did you find any of the relations in the above exercise to be an equivalence relation? We will talk more about equivalence relations later.

Some properties of the divides relation.

1. $a \mid 0,\ 1 \mid a,\ a \mid a$.
2. If $a \mid b$, then $a \mid -b$.
3. If $a \mid b$, then $a \mid bn$, for any integer n.
4. If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$. In fact $a \mid (bx+cy)$ where x and y are any integers.
5. If $a \mid b$ and $b \mid c$, then $a \mid c$.
6. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
7. If $a \mid b$, then $a^2 \mid b^2$. In fact, $a^n \mid b^n$ for all whole numbers n.

You can convince yourself of the truth of the above statements by using the definition of the divides relation. Look at the following examples and see if you can verify the other parts of the above.

For example, in item (2) we have that if $a \mid b$, then by the definition of divides, $b = a \cdot k$ for some integer k. If $b = a \cdot k$, then $-b = -a \cdot k = a \cdot (-k)$. But if $-b = a(-k)$ then $a \mid -b$.

We can verify the first part of item (4) in the following way. If $a \mid b$, the $b = a \cdot k$ for some integer k. If $a \mid c$, then $c = a \cdot n$ for some integer n. Now $b + c = a \cdot k + a \cdot n = a(k+n)$. Since k and n are integers, $k + n = m$, an integer. Therefore, $b+c = a \cdot m$ and $a \mid (b+c)$ by the definition of the divides relation.

Part II: The Division Algorithm

You should all be familiar with the division algorithm, whether you call it that or not. For example, if you divide 17 by 7, you would get a quotient of 2 and a remainder of 3. We will write this as

$$17 = 7 \times 2 + 3 \quad \text{or} \quad 17 = 7 \cdot 2 + 3.$$

The Division Algorithm. For any integers a and b, with $a > 0$, there exist unique integers q and r such that

$$b = a \cdot q + r, \quad \text{with} \quad 0 \leq r < a.$$

[By *unique* we mean that if we all correctly divide 23 by 7, we will all get a quotient of 3 and a remainder of 2.]

When you perform the operation of division and a remainder is obtained, that remainder must be bigger than 0 and less than the number you are dividing by. *If we divide* 37 *by* 4 *and get a remainder larger than* 4*, we have made a mistake in our division.* Here are some examples.

$12 \div 7$ yields $12 = 7 \cdot 1 + 5$

$38 \div 13$ yields $38 = 13 \cdot 2 + 12$

$48 \div 12$ yields $48 = 12 \cdot 4$ we normally do not write a remainder of 0

Notice that this is just a different way of writing

$$\frac{12}{7} = 1 + \frac{5}{7} \quad \text{or} \quad 12 \div 7 = 1 \text{ with a remainder of } 5$$

$$\frac{38}{13} = 2 + \frac{12}{13} \quad \text{or} \quad 38 \div 13 = 2 \text{ with a remainder of } 12$$

$$\frac{48}{12} = 4 \quad \text{or} \quad 48 \div 12 = 4 \text{ with a remainder of } 0$$

The form used for the division algorithm is very useful in that it conveniently displays the remainder. Let us define a relation, $\mathcal{R}_3$, on the integers as "*has the same remainder when divide by* 3." That is, $a \,\mathcal{R}_3\, b$ if the remainder

we get when a is divided by 3 is exactly the same as the remainder we get when we divide b by 3. For example, if $a = 7$ and $b = 22$, division by 3 gives $7 = 3 \cdot 2 + 1$ and $22 = 3 \cdot 7 + 1$ and hence, since $1 = 1$, we have $7\ \mathcal{R}_3\ 22$. However if $a = 7$ and $b = 14$, $7\ \not\mathcal{R}_3\ 14$, since $7 = 3 \cdot 2 + 1$ but $14 = 3 \cdot 4 + 2$ and the remainders are not equal. Note that we are using $a\ \not\mathcal{R}_3\ b$ to mean that a is not related to b by the relation $\mathcal{R}_3$.

Exercise 2.

(a) Find six integers that have the property that they **have the same remainder, 2, when divided by 4**.

(b) Find six integers that have the property that they **have the same remainder, 5, when divided by 7**.

(c) Find six integers that have the property that they **have the same remainder, 1, when divided by 5**.

(d) Find six integers that have the property that they **have the same remainder, 3, when divided by 11**.

(e) Which of the properties of a relation does $\mathcal{R}_3$ satisfy?

Suppose we divide the integers a and b by m and get the same remainder. The division algorithm might look like this

$$a = m \cdot q_1 + r \quad \text{with} \quad 0 \leq r < m \tag{1}$$

$$b = m \cdot q_2 + r \quad \text{with} \quad 0 \leq r < m \tag{2}$$

If we subtract equation (2) from equation (1) we get

$$a - b = m(q_1 - q_2).$$

Since the remainders were equal they subtract out and since q_1 and q_2 are integers, their difference $q_1 - q_2$ is an integer, say $q_1 - q_2 = k$. We then have $a - b = m \cdot k$. By the definition of the divides relation, we have that $m \mid (a - b)$. We have just shown that if two integers have the same remainder when divided by m, their difference is divisible by m. We can then more easily check the relation "*has the same remainder when divide by m*" by merely checking to see if $m \mid (a - b)$.

Examples. Note that if $m \mid (a-b)$, then $m \mid (b-a)$, since $b-a = -(a-b)$.

- 8 and 5 have the same remainder when divided by 3 since $8-5=3$ and $3 \mid 3$, so $3 \mid (8-5)$.
- 13 and 25 have the same remainder when divided by 6 since $13-25 = -12$ and $6 \mid -12$, so $6 \mid (13-25)$.
- 27 and -25 have the same remainder when divided by 13 since $27-(-25)=52$ and $13 \mid 52$, so $13 \mid (27-(-25))$.

Note. The division algorithm requires that the divisor a be positive and that the remainder r be an integer between 0 and a; however, there are no restrictions on the integer b. For example, if $b=-17$ and $a=5$, we must find a quotient q and a remainder r such that $-17 = 5 \cdot q + r$ with $0 \leq r < 5$. To satisfy the condition $0 \leq r < 5$, we must let $q=-4$ so that $-17 = 5(-4)+3$.

Exercise 3.

(a) Find six integers that have the property that they have the same remainder as 7 does when divided by 4.

(b) Find six integers that have the property that they have the same remainder as 17 does when divided by 7.

(c) Find six integers that have the property that they have the same remainder as 36 does when divided by 11.

(d) Find six integers that have the property that they have the same remainder as $^{-}14$ when divided by 6.

(e) List all integers that have a remainder of 0 when divided by 3. [See the hint below.]

(f) List all integers that have a remainder of 1 when divided by 3.

(g) List all integers that have a remainder of 2 when divided by 3.

Hint for doing parts (e), (f) and (g). All integers that have a remainder of 1 when divided by 4 would be represented by

$$\{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, \ldots\}.$$

Part III: The Congruence Relation

We have found that we simplified our work in finding integers that had the same remainder when divided by a given integer by introducing the property that that the integers a and b had the same remainder when divided by m is $m \mid (a - b)$. That is, instead of having to divide a and b each by m and then comparing the remainders, all we had to do was see if m divided the difference $a - b$. We will use this information to define a new relation.

> **Definition.** The two integers a and b are said to be **congruent mod** m, where $m > 0$, if $m \mid (a - b)$. We denote this relation as $a \equiv b (\text{mod } m)$. If a is not congruent to b mod m, we write $a \not\equiv b (\text{mod } m)$.

Examples.

- $7 \equiv 2 (\text{mod } 5)$, since $7 - 2 = 5$ and $5 \mid 5$.
- $28 \equiv 2 (\text{mod } 13)$, since $28 - 2 = 26$ and $13 \mid 26$.
- $-8 \equiv 6 (\text{mod } 7)$, since $-8 - 6 = -14$ and $7 \mid -14$.
- $19 \equiv 1 (\text{mod } 3)$, since $19 - 1 = 18$ and $3 \mid 18$.
- $723 \equiv 3 (\text{mod } 5)$, since $723 - 3 = 720$ and $5 \mid 720$.

Exercises.

4. Fill in each blank with an integer between 0 and 2.

   (a) $34 \equiv$ (mod 3).

   (b) $26 \equiv$ (mod 3).

   (c) $-4 \equiv$ (mod 3).

   (d) $268 \equiv$ (mod 3).

   (e) $5462 \equiv$ (mod 3).

5. Fill in each blank with an integer between 0 and 9.

   (a) $34 \equiv \quad \pmod{10}$.

   (b) $26 \equiv \quad \pmod{10}$.

   (c) $-4 \equiv \quad \pmod{10}$.

   (d) $268 \equiv \quad \pmod{10}$.

   (e) $5462 \equiv \quad \pmod{10}$.

6. Fill in each blank with an integer between 0 and 4.

   (a) $27 \equiv \quad \pmod{5}$.

   (b) $46 \equiv \quad \pmod{5}$.

   (c) $-14 \equiv \quad \pmod{5}$.

   (d) $308 \equiv \quad \pmod{5}$.

   (e) $1462 \equiv \quad \pmod{5}$.

Some properties of the congruence relation:

Let a, b, c, d, x, y denote integers. Then:

(a) $a \equiv a \pmod{m}$,

(b) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements,

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$,

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ax + cy \equiv bx + dy \pmod{m}$ and $ac \equiv bd \pmod{m}$,

(e) If $a \equiv b \pmod{m}$ then $ax + cy \equiv bx + cy \pmod{m}$ and $ac \equiv bc \pmod{m}$, (Special case of (d).)

(f) If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for any positive integer n,

(g) If $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$, then $a \equiv b \pmod{d}$,

---

Recall that an equivalence relation is a relation for which the reflexive, symmetric and transitive properties all hold.

The congruence relation is an equivalence relation.

1. It is **reflexive** because $a \equiv a \pmod{m}$ is true since $m \mid (a - a)$.
2. It is **symmetric** since if $a \equiv b \pmod{m}$, then $m \mid (a - b)$; and, if $m \mid (a - b)$, then $m \mid (b - a)$ and $b \equiv a \pmod{m}$.
3. It is **transitive** since if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, $m \mid (a - b)$ and $m \mid (b - c)$. By the properties of the divide relation $m \mid (a - b) + (b - c)$, so $m \mid (a - c)$ and therefore $a \equiv c \pmod{m}$.

The reason we are interested in equivalence relations is that they separate (partition) the set of numbers we are working with into sets in which all the elements in each set are related. We call these sets **equivalence classes**. Equivalence classes partition the set on which the equivalence relation is defined into a collection of sets that have the following properties.

1. No two of the equivalence classes have members in common. (We call such sets disjoint sets.)
2. Every member in the set on which the equivalence relation is defined has to appear in one and only one of the equivalence classes.

Exercise 7. Is the relation we described earlier, $\mathcal{R}_3$, an equivalence relation? What are the equivalence classes?

The congruence relation can be used to partition the integers into equivalence classes according to the remainders one gets when dividing by m.

Example. If we let $m = 4$, the remainders we get upon division by 4 are 0, 1, 2, 3. Thus, if we look at the set of all integers with the congruence $n \equiv 0(\text{mod } 4)$, we will have all integers that have a remainder of 0 when divided by 4; that is, all multiples of 4. Thus,

$$\underline{0}_4 = \{n | n \equiv 0(\text{mod } 4)\} = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}.$$

When we write $\underline{0}_4 = \{n | n \equiv 0(\text{ mod } 4)\}$ we mean "$\underline{0}_4$ is the set of all integers n such that $n \equiv 0(\text{ mod } 4)$." We use $\underline{0}_4$ to mean this is not the number 0, but represents a set of numbers.

Now all integers with a remainder of 1 when divided by 4 would be given by $n \equiv 1(\text{mod } 4)$ and

$$\underline{1}_4 = \{n | n \equiv 1(\text{mod } 4)\} = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}.$$

Now all integers with a remainder of 2 when divided by 4 would be given by $n \equiv 2(\text{mod } 4)$ and

$$\underline{2}_4 = \{n | n \equiv 2(\text{mod } 4)\} = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}.$$

Now all integers with a remainder of 3 when divided by 4 would be given by $n \equiv 3(\text{mod } 4)$ and

$$\underline{3}_4 = \{n | n \equiv 3(\text{mod } 4)\} = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}.$$

By the division algorithm, if we divide an integer by 4 we get a unique quotient and **remainder**. Thus, since each of the above sets contain all integers with the same remainder, no two sets have a member in common. Also, every integer must have a quotient and a remainder when divided by 4, so all the integers are contained in the above sets.

Note. If n is a member of the set

$$\underline{3}_4 = \{n | n \equiv 3(\text{mod } 4)\} = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\},$$

then, by the Division Algorithm, n is of the form $n = 4k+3$. That is, when n is divided by 4, we get a quotient k and a remainder of 3. Thus, any integer,

when divided by 4, must have one of the forms: $4k,\ 4k+1,\ 4k+2$, or $4k+3$. Therefore, we have that

$$\underline{3}_4 = \{n | n \equiv 3 (\text{mod } 4)\} = \{n | n = 4k+3,\ k = 0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

Exercise 8.

(a) Find the equivalence classes for $m = 5$. That is, find the sets corresponding to the following and list out the elements, as was done in the previous example.

- $n \equiv 0 (\text{mod } 5)$,
- $n \equiv 1 (\text{mod } 5)$,
- $n \equiv 2 (\text{mod } 5)$,
- $n \equiv 3 (\text{mod } 5)$,
- $n \equiv 4 (\text{mod } 5)$.

(b) For some integers m and n, is it true that $6m + 5 = 6n - 1$? Can you explain why it is true or why it is not true? If it in not true, can you change it to a true statement?

(c) For some integers m and n, is it true that $5m + 2 = 5n - 2$? Can you explain why it is true or why it is not true? If it in not true, can you change it to a true statement?

(d) For some integers m and n, is it true that $4m + 2 = 4n - 2$? Can you explain why it is true or why it is not true? If it in not true, can you change it to a true statement?

Remainder Arithmetic

In our previous discussion we represented all numbers that had the same remainder when divided by 4, to be in one of the following sets.

$\underline{0}_4 = \{n | n \equiv 0 (\text{mod } 4)\} = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}.$

$\underline{1}_4 = \{n | n \equiv 1 (\text{mod } 4)\} = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}.$

$\underline{2}_4 = \{n | n \equiv 2 (\text{mod } 4)\} = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}.$

$\underline{3}_4 = \{n | n \equiv 3 (\text{mod } 4)\} = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}.$

Suppose we pick two numbers out of the set $\underline{1}_4$, say we choose 17 and 9. If we multiply these together, what do you think will be the remainder if we divide the product by 4? Well, the product is $17 \cdot 9 = 153$ and by the Division Algorithm we have $153 = 4 \cdot 38 + 1$, so the remainder is 1. Would this be true for any two numbers selected from $\underline{1}_4$? We can use the congruence relation to make the task must quicker and easier. We will use the property (d) of congruences: If $a \equiv b \,(\text{mod } m)$ and $c \equiv d \,(\text{mod } m)$ then $ac \equiv bd \,(\text{mod } m)$.

If a and b are both in $\underline{1}_4$, then $a \equiv 1 \,(\text{mod } 4)$ and $b \equiv 1 \,(\text{mod } 4)$. By property (d), we have that $a \cdot b \equiv 1 \cdot 1 \,(\text{mod } 4)$ and the product $a \cdot b$ has a remainder of 1 when divided by 4. Since a and b we any numbers we wanted to pick from $\underline{1}_4$ it follows that the product of any two numbers that each have a remainder of 1 when divided by 4 will also have a remainder of 1 when divided by 4.

If we wanted to establish that the product of any two numbers that each have a remainder of 1 when divided by 4 will also have a remainder of 1 when divided by 4 without using congruences, we would have to do the following.

> If a is a number in $\underline{1}_4$, then by the Division algorithm, we can write $a = 4q_1 + 1$. And if b is also in $\underline{1}_4$, then $b = 4q_2 + 1$. The product

is then

$$ab = (4q_1 + 1)(4q_2 + 1).$$

We then have to perform the multiplication to get

$$\begin{aligned} ab &= (4q_1 + 1)(4q_2 + 1) \\ &= (4q_1)(4q_2) + 4q_1 + 4q_2 + 1 \\ &= 16q_1q_2 + 4q_1 + 4q_2 + 1 \\ &= 4(4q_1q_2 + q_1 + q_2) + 1 \\ &= 4k + 1, \quad \text{where} \quad k = 4q_1q_2 + q_1 + q_2 \end{aligned}$$

Therefore, by the Division Algorithm, ab has a remainder of 1 when divided by 4.

Suppose a and b are numbers in $\underline{3}_4$. What would the remainder be if we divide the product ab by 4. We know that if a and b are numbers in $\underline{3}_4$, then $a \equiv 3 \pmod 4$ and $b \equiv 3 \pmod 4$. Therefore $ab \equiv 9 \pmod 4$, but $9 \equiv 1 \pmod 4$, so $ab \equiv 1 \pmod 4$ [by the transitive property for the congruence relation we have that if $ab \equiv 9 \pmod 4$ and $9 \equiv 1 \pmod 4$, then $ab \equiv 1 \pmod 4$.] and the remainder when ab is divided by 4 is 1.

Using congruence, we can create an arithmetic for adding and multiplying remainders. Let's create addition and multiplication tables for the remainders of numbers when we divide by 4.

$\oplus$	$\underline{0}_4$	$\underline{1}_4$	$\underline{2}_4$	$\underline{3}_4$
$\underline{0}_4$	$\underline{0}_4$	$\underline{1}_4$	$\underline{2}_4$	$\underline{3}_4$
$\underline{1}_4$	$\underline{1}_4$	$\underline{2}_4$	$\underline{3}_4$	$\underline{0}_4$
$\underline{2}_4$	$\underline{2}_4$	$\underline{3}_4$	$\underline{0}_4$	$\underline{1}_4$
$\underline{3}_4$	$\underline{3}_4$	$\underline{0}_4$	$\underline{1}_4$	$\underline{2}_4$

$\otimes$	$\underline{0}_4$	$\underline{1}_4$	$\underline{2}_4$	$\underline{3}_4$
$\underline{0}_4$	$\underline{0}_4$	$\underline{0}_4$	$\underline{0}_4$	$\underline{0}_4$
$\underline{1}_4$	$\underline{0}_4$	$\underline{1}_4$	$\underline{2}_4$	$\underline{3}_4$
$\underline{2}_4$	$\underline{0}_4$	$\underline{2}_4$	$\underline{0}_4$	$\underline{2}_4$
$\underline{3}_4$	$\underline{0}_4$	$\underline{3}_4$	$\underline{2}_4$	$\underline{1}_4$

The tables look a little crowded with the numbers underlined and with subscripts. From now on we will use regular integers 0, 1, 2, 3, etc. to represent the remainders and we will designate what number we are dividing by by putting a subscript on the operation symbol.

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

In the above we are doing addition using the property of congruences: *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$ *then* $a + c \equiv b + d \pmod{m}$. And for multiplication we are using: *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$ *then* $ac \equiv bd \pmod{m}$.

However, we can actually make it simpler by just doing the normal arithmetic and then reducing, if necessary, mod 4. For example, in the addition table, $2 + 2 = 4 \equiv 0 (\text{mod } 4)$–since 4 is too big to be a remainder when dividing by 4, we must reduce it mod 4. For multiplication, we have that $3 \cdot 2 = 6 \equiv 2 (\text{mod } 4)$—since 6 is bigger than our divisor 4, we reduce it mod 4. It is important to realize that when we are adding or multiplying, the answer must be a legitimate remainder. If our divisor is some integer m, then the answer has to be one of the numbers 0, 1, 2, 3, ..., $m - 1$. If it isn't, we reduce it mod m.

Exercise 9. We know that when dividing by 5, the remainders are 0,1,2,3, and 4. Complete the following tables for adding and multiplying the remainders for division by 5.

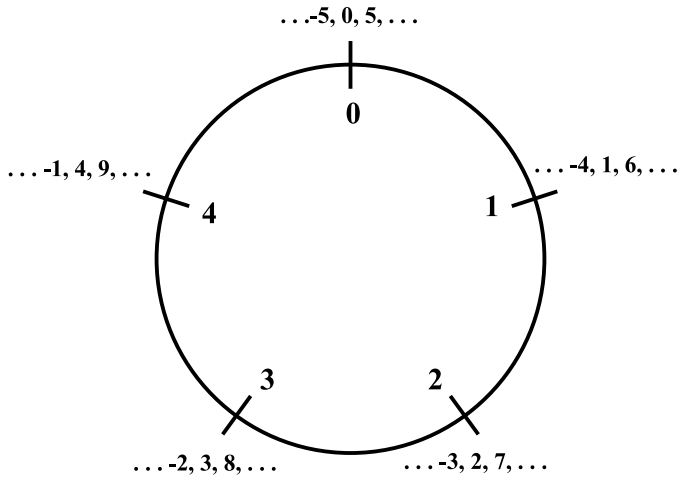
$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1			4	
2	2	3		0	
3			0	1	2
4	4		1		

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1			
2	0				3
3	0		1		
4	0			2	

In remainder arithmetic (also called modular arithmetic[1]), one can also think of the integers arranged around a circle, like the hours on a clock, instead of along an infinite straight line. We must to decide how many "hours"

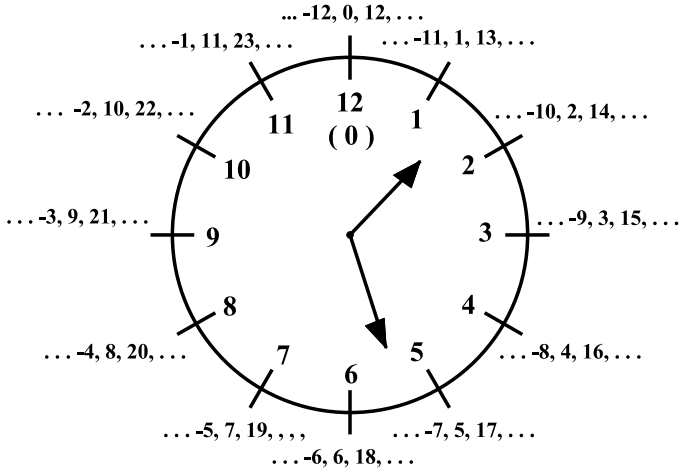
[1]We called this *remainder arithmetic* because the term *remainder* is familiar to us and *modular* is not.

our clock is going to have. It can be any number, not necessarily 12. Let us look at one having 5 "hours."



To add 4 and 3 mod 5, we start at 0, count 4 clockwise, and then a further 3 clockwise, this time ending on 2. To multiply 4 by 3 mod 5, we start at 0 and count 4 clockwise 3 times, again ending up at 2. We would write $4 + 3 \equiv 2 \pmod{5}$ and $4 \cdot 3 \equiv 2 \pmod{5}$.

One can use a normal analog clock to do arithmetic mod 12. If you go on a 4-hour trip starting at 10 o'clock, you will arrive at your destination at 2 o'clock. That is, $10 + 4 = 14 \equiv 2 \pmod{12}$.



Remainder arithmetic on the clock (with any number of "hours") also allows us to do subtraction very easily — we just move in the counter-

clockwise direction. For example, to compute $3 - 8$, we start at 3 then count back 8 to end on 7. We verify can verify this using congruences: $3 - 8 = -5 \equiv 7 \pmod{12}$. Since one can, in theory, wind the number line around the clock face, we turn usual arithmetic into remainder (or modular) arithmetic.

Exercise 10. Make up addition and multiplication tables for remainders when dividing by 6.

Exercise 11. Make up addition and multiplication tables for remainders when dividing by 7.

Exercise 12. Make a clock with 6 "hours" and label the positions on the clock face. Using this model, find the following.

(a) What is $4 + 4$?

(b) What is $5 \cdot 3$?

(c) What is $2 - 5$?

(d) What is $5 + 4$?

(e) Verify your answers to the above problems using the tables you made in Exercise 10.