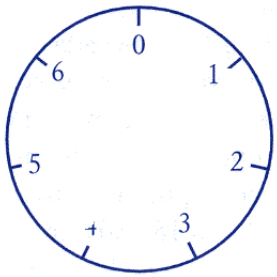
Modular arithmetic (self-study notes)
Informal disquisition: "clock arithmetic"

1. Packing non-negative integers

For a natural number n, let us consider the elements of the set $\{0, 1, 2, 3, \ldots, n\}$ drawn in a circle (like an "n-hours clock"). For example, the following figure shows a clock with only 7 subdivisions ("hours") which are labelled with the numbers from 0 to 6 (a modulo 7-clock).



Using this picture we will see a way, different from the usual one, for "summing" the elements in the set $\{0, 1, 2, 3, 4, 5, 6\}$.

To compute $2+3$ we imagine a "clock hand" pointing, initially, to position 0; then it turns 3 positions right ("clockwise") and, after it, 3 positions right again. The final position of the clock hand is 5. Then, we say that 2+3 is 5 (that coincides, in this case, with the usual arithmetic).

However, in order to compute $2+6$, the clock hand turns 2 positions clockwise and, then, 6 positions clockwise. Its final position is 1, and we say that "$2+6$ is 1" (the results differs from the usual arithmetic, this time). To represent this type of operation, it is convenient to use the following notation:

- $2 + 3 \equiv 5 \ (mod\ 7)$, and we read "2+3 is congruent to 5 modulo 7"

- $2 + 6 \equiv 1 \ (mod \ 7)$, and we read "2+6 is congruent to 1 modulo 7"

The word "modulo 7" indicates that we are summing using a modulo 7-clock (that is, a clock with 7 positions).

Two non-negative integers a and b are called congruent modulo 7 if, starting at the 0-position in a modulo 7-clock, turning it (clockwise) a positions, the clock hand reaches the same location than turning it (clockwise) b positions. For example: $8 \equiv 1 \ (mod \ 7)$, $8 \equiv 15 \ (mod \ 7)$, $9 \equiv 2 \ (mod \ 7)$, $9 \equiv 23 \ (mod \ 7)$ and also $7 \equiv 0 \ (mod \ 7)$.

But... why are two non-negative integers congruent modulo 7? What have they in common? Take, for example, 9 and 23, which are congruent modulo 7 (check it!).

- If the clock hand turns 9 positions (starting at "0"), we see that it completes one revolution **plus 2 positions**.
- If the clock hand turns 23 positions (starting at "0"), we see that it completes 3 revolutions **plus 2 positions**.

You can see that both numbers have the following element in common: **the remainder of the divisions $9 \div 7$ and $23 \div 7$ coincide**. This is the key:

Two non-negative integers are congruent modulo 7 if and only if the remainders of the corresponding divisions by 7 coincide.

Exercise 1. Determine if the following pairs of numbers are congruent modulo 7. In the affirmative cases, compute an integer number between 0 and 6 (including both) that is congruent (modulo 7) to them.

(a) 59 and 38.

(b) 69 and 41.

(c) 82 abd 71.

Look at the following fact:

Given a non-negative integer a, **there is a unique integer between 0 and 6 that is congruent to a modulo 7** (it is the number of "extra" positions after given a number of complete revolutions to the clock, that is, it is the **remainder** of the division $a \div 7$).

For each non-negative integer a we will denote (for the moment) by $\overline{a}$ (or $[a]$) to the set of all non-negative integers that are congruent to a modulo 7. These sets are called congruence classes modulo 7.

Example 1. Compute the **class of 12**, that is, $\overline{12}$. The remainder of the division $12 \div 7$ is 5. Therefore, the elements of $\overline{12}$ are all the non-negative integers whose remainder (when we divide them by 7) is 5, that is, $5, 12, 19, 26, 33, \ldots$. or,

$$5 + 0 \cdot 7, 5 + 1 \cdot 7, 5 + 2 \cdot 7, 5 + 3 \cdot 7, 5 + 4 \cdot 7, \ldots.$$

Hence:

$$\overline{12} = \{5 + k \cdot 7 \mid k \text{ es is a non-negative integer}\} = \{5, 12, 19, 26, 33, \ldots\}.$$

What is the congruence class of an element in $\overline{12}$ (for example, 19)? Its class, $\overline{19}$ is the set of all the non-negative integers whose remainders (when they are divided by 7) **coincide with the one of the division** $19 \div 7$. Since this remainder is 5 it is clear that: **the elements in the class** $\overline{19}$ **are exactly the same as those in the class** $\overline{12}$. Therefore $\overline{19} = \overline{12}$. Of course, by the same reason:

$$\overline{5} = \overline{12} = \overline{19} = \overline{26} = \overline{33} = \cdots .$$

All the numbers in $\{\mathbf{5}, 12, 19, 26, 33, \ldots\}$ **have the same congruence class** (modulo 7). We have put all these numbers in a "package" (the congruence class). Observe that **only one of the elements in the class is between 0 and 6**: 5 (the remainder). We are going to call, to this number, the **main representative** of the class.

If you think about this, you will realize that, with a modulo 7-clock, we can make **7 different congruence classes**: those corresponding to all possible **main representatives** (0, 1, 2 ,3, 4, 5 and 6):

$$\overline{0} = \{0, 7, 14, 21, \ldots\}$$
$$\overline{1} = \{1, 8, 15, 22, \ldots\}$$
$$\overline{2} = \{2, 9, 16, 23, \ldots\}$$
$$\overline{3} = \{3, 10, 17, 24, \ldots\}$$
$$\overline{4} = \{4, 11, 18, 25, \ldots\}$$
$$\overline{5} = \{5, 12, 19, 26, \ldots\}$$
$$\overline{6} = \{6, 13, 20, 27, \ldots\}$$

Observe that the union of these classes is the set of non-negative integers and, moreover, they are pairwise disjoint. That is, they form a **partition** of the set of non-negative integers. In other words:

Every non-negative integer belongs to one, and only one congruence class (modulo 7).

Exercise 2. Compute the main representatives of the following congruence classes (modulo 7): $\overline{123}, \overline{56}, \overline{49}, \overline{111}, \overline{82}$.

2. Generalization: "Packing" integers (negative and non-negative)

At this moment, we have divided the set of non-negative integers into "packages" (which are the congruence classes (modulo 7)). But... instead of considering only the non-negative integers, we can consider the whole set of integers. This generalization is not difficult, as we will see:

> We interpret that, when we have a negative integer $-a$, we turn a positions in the clock, **but counter-clockwise.**

For example, if we turn -8 positions (that is, 8 positions counter-clockwise starting at "0") we will finish at position 6. Therefore, we say that **-8 is congruente to 6 (modulo 7)**, that is, $-8 \equiv 6\ (mod\ 7)$.

With this generalization of the concept of congruence, we can put **all the integers** (not only the non-negative ones) into the congruence classes:

> Two **arbitrary integers** a and b are *congruent modulo 7*, written $a \equiv b\ (mod\ 7)$, if the location of the clock hand of a modulo 7-clock, after turning it a positions, coincides with the location after turning it b positions (clockwise or counter-clockwise depending on the signs of a and b).

Example 2. We know that the non-negative integers in the congruence class of 2 are: $2, 9, 16, 23, \ldots$ but, now, we must also add $2 - 7 = -5,\ 2 - 2 \cdot 7 = -12,\ 2 - 3 \cdot 7 = -19, \ldots$. That is, with this generalization, we have that:

$$\overline{2} = \{2 + k \cdot 7 \mid k \text{ is an integer}\} = \{\ldots, -19, -12, -5, 2, 9, 16, 23, \ldots\}.$$

Observe that **there is only one main representative** in each class.

Exercise 3. Complete the gaps in the following congruence classes (modulo 7):

$$\overline{0} = \{\ldots, \_, \_, \_, 0, 7, 14, 21, \ldots\}$$
$$\overline{1} = \{\ldots, \_, \_, \_, 1, 8, 15, 22, \ldots\}$$
$$\overline{2} = \{\ldots, \_, \_, \_, 2, 9, 16, 23, \ldots\}$$
$$\overline{3} = \{\ldots, \_, \_, \_, 3, 10, 17, 24, \ldots\}$$
$$\overline{4} = \{\ldots, \_, \_, \_, 4, 11, 18, 25, \ldots\}$$
$$\overline{5} = \{\ldots, \_, \_, \_, 5, 12, 19, 26, \ldots\}$$
$$\overline{6} = \{\ldots, \_, \_, \_, 6, 13, 20, 27, \ldots\}$$

Observation: The "trick" of dividing by 7 and taking the remainder to compute the main representative of a class $\overline{a}$ is not valid if $a < 0$. For example, $-8 \equiv \underline{6}\ (mod\ 7)$ and the remainder of the division $8 \div 7$ is $\underline{1}$.

The following property (that is easy to deduce from the preceding examples) gives an easy criterium to determine whether two integers are congruent modulo 7. It is valid for any pair of integers (negative or non-negative).

Proposition 1. Two integers a and b are congruent modulo 7 if and only if $a - b$ is multiple of 7.

Therefore:

to determine whether two integers a and b are congruent modulo 7, it is enough to study whether the difference $a - b$ is a multiple of 7 or not.

For example: -1236 y 47673 are congruent modulo 7 because$-1236 - 47673 = -48909 = 7 \cdot (-6987)$.

Although we have studied the congruence modulo 7, adapted to a "modulo 7-clock", we can consider also a modulo 2-clock, or a modulo 3-clock, or a modulo 22-clock,... or, in general, a modulo n-clock, for any natural number $n > 1$. Everything is working similarly! (replacing 7 by n).

Exercise 4. Consider a "modulo 4-clock".

(b) Write all the congruence classes modulo 4.

(a) Are true of false the following assertioins? $5 \equiv 17\ (mod\ 4)$, $19 \equiv 43\ (mod\ 4)$, $-9 \equiv 7\ (mod\ 4)$?