Lecture 7 and 8: Congruence

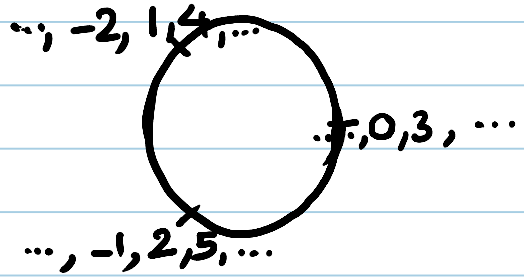
Monday, October 20, 2014
11:53 PM

Def. Let $n \in \mathbb{Z}^{>1}$. We say a and b are congruent modulo n and write $a \equiv b \pmod{n}$ or $a \overset{n}{\equiv} b$ if $n \mid a-b$.

There are various ways to interpret this property:

Covering Space

wind around the circle of length n.



$a \overset{n}{\equiv} b \iff$ after a or b steps on the circle we end up with the same end point.

This way we are looking at integers as "time", and we are moving counter-clockwise with constant

speed. Now $a \overset{n}{\equiv} b \iff$ if after a seconds and b seconds we are at the same place.

Now by looking at a point $\underline{P}$ we can gather all the times when we are at $\underline{P}$.

Partition.

• If r is the remainder of a divided by n, then

$$a = nq + r \iff n \mid a - r \implies a \overset{n}{\equiv} r.$$

• $\left.\begin{matrix} 0 \le r_1 \le r_2 < n \\ r_1 \overset{n}{\equiv} r_2 \end{matrix}\right\} \implies \left.\begin{matrix} n \mid r_2 - r_1 \\ 0 \le r_2 - r_1 < n \end{matrix}\right\} \implies r_1 = r_2$

So for any integer $\underline{a}$, there is a unique $0 \le r < n$ s.t. $a \overset{n}{\equiv} r$.

• On the other hand, for an integer a_0

$$\{a \in \mathbb{Z} \mid a \overset{n}{\equiv} a_0\} = \{a_0 + nk \mid k \in \mathbb{Z}\}$$

$$= \{a_0\} + n\mathbb{Z}.$$

$$\{\text{Convention}\} = a_0 + n\mathbb{Z}.$$

Hence overall we have:

(1) $\mathbb{Z} = n\mathbb{Z} \cup n\mathbb{Z}+1 \cup \cdots \cup n\mathbb{Z}+(n-1)$

(2) $(n\mathbb{Z}+i) \cap (n\mathbb{Z}+j) = \emptyset$ if $0 \le i < j \le n-1$.

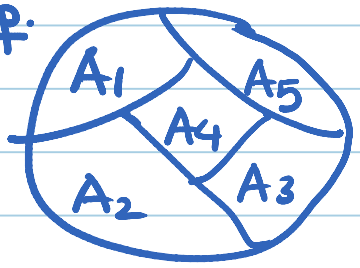
So $\{n\mathbb{Z}, n\mathbb{Z}+1, \cdots, n\mathbb{Z}+(n-1)\}$ is a partition of $\mathbb{Z}$.

Recall. $\{A_0, \cdots, A_{n-1}\}$ is called a partition of the set X if

(1) $X = A_0 \cup \cdots \cup A_{n-1}$ (3) $A_i \neq \emptyset$

(2) $A_i \cap A_j = \emptyset$ if $i \neq j$.

Exp.



; $\{\{1\}, \{2\}\}$ and $\{\{1,2\}\}$ are partitions of $\{1,2\}$.

Exp. If $f: X \to \{0, \cdots, n-1\}$ is an onto function, then $\{f^{-1}(0), \cdots, f^{-1}(n-1)\}$ is a partition of X.

The above interpretations are connected through the covering map:

Let's label the n points on the circle by $P_0, P_1, \dots, P_{n-1}$. Let $f: \mathbb{Z} \to \{P_0, \dots, P_{n-1}\}$ be s.t. $f(a)$ is where we are after a steps starting from P_0. So $f^{-1}(P_i) = i + n\mathbb{Z}$ gives us the following partition of $\mathbb{Z}$ into n sets:

$$\{n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+(n-1)\}$$

. We denote the above set by either $\mathbb{Z}_n$ or $\mathbb{Z}/_{n\mathbb{Z}}$.

. For any integer a, let $[a]_n := a + n\mathbb{Z}$.

So $[a]_n = [b]_n \iff a \overset{n}{\equiv} b$.

. a is called a representative of the set $[a]_n$.

For instance any even number is a representative of $[0]_2$.

"Group action" and the space of orbits.

We introduced groups as "symmetries" of objects.

For instance we can view $\mathbb{Z}$ as group of

translations which send the integer grid to itself. Clearly 0 can be send to any other integer point via "the $\mathbb{Z}$-action" (i.e. an integer translation). So there is only one orbit under "the $\mathbb{Z}$-action".

What happens if we just look at $n\mathbb{Z}$, i.e. translations that are multiples of n ?

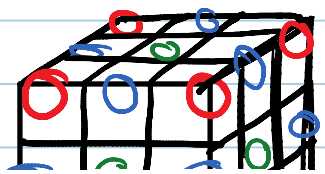
. Under "the action of $n\mathbb{Z}$", where does a point is mapped?

. How many orbits do we get?

For instance under the movements of Rubik Cube:

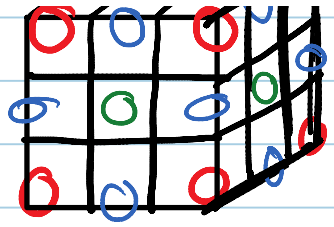
What is the size of the orbit of a corner?

8 : it can be sent to all the corners



to all the corners

(and only corners)



What is the size of the orbit of a middle cube?

12 : it can be sent to all the middle cubes (and only middle cubes).

What is the size of the orbit of a center cube?

6 : it can be sent to all the center cubes and only to them.

What is "the space of orbits", i.e. the set consisting of all the orbits.

Any cube belongs to one of the above orbits. So there are precisely 3 orbits.

When $X \curvearrowleft G$ (G acts on X), the space of orbits is denoted by X/G.

In the case of $\mathbb{Z} \curvearrowright n\mathbb{Z}$ we get back $\mathbb{Z}/_{n\mathbb{Z}} = \{n\mathbb{Z}, n\mathbb{Z}+1, \cdots, n\mathbb{Z}+(n-1)\}$.

Why do we care about $\overset{n}{\equiv}$?

The main reason is the following:

Lemma $\left.\begin{array}{l} x_1 \overset{n}{\equiv} x_2 \\ y_1 \overset{n}{\equiv} y_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x_1+y_1 \overset{n}{\equiv} x_2+y_2 \\ x_1 y_1 \overset{n}{\equiv} x_2 y_2 \end{array}\right.$

This implies that $\left\{\begin{array}{l} [x]_n + [y]_n := [x+y]_n \\ [x]_n \cdot [y]_n := [x \cdot y]_n \end{array}\right.$

are well-defined operations.

Cor. $\overline{a_k a_{k-1} \cdots a_0} \overset{9}{\equiv} \sum_{i=0}^{k} a_i$ where a_i's are digits of $\overline{a_k \cdots a_0}$.

Pf. $\overline{a_k \cdots a_0} = \sum_{i=0}^{k} 10^i a_i \overset{9}{\equiv} \sum_{i=0}^{k} (1)^i a_i = \sum_{i=0}^{k} a_i$. ∎

Cor. $\overline{a_k a_{k-1} \cdots a_0} \overset{11}{\equiv} \sum_{i=0}^{k} (-1)^i a_i$.

Pf. $\overline{a_k \cdots a_0} = \sum_{i=0}^{k} 10^i a_i \overset{11}{\equiv} \sum_{i=0}^{k} (-1)^i a_i$. ∎

Pf. $\overline{a_k \cdots a_0} = \sum_{i=0}^{k} 10^i a_i \overset{11}{\equiv} \sum_{i=0}^{k} (-1)^i a_i$. ∎

Cor. Let a be an odd number. Then $a^2 \overset{8}{\equiv} 1$.

Pf 1 $a = 2k+1 \Rightarrow a^2 = 4k^2+4k+1$

$= 4k(k+1)+1$

either k is even or $k+1$ is even. So

$2 \mid k(k+1)$.

$\Rightarrow 8 \mid 4k(k+1) \Rightarrow a^2 \overset{8}{\equiv} 1$. ∎

Pf 2. $2 \nmid a \Rightarrow a \overset{8}{\equiv} 1, 3, 5, 7$

$\Rightarrow a^2 \overset{8}{\equiv} 1$ or $9 \overset{8}{\equiv} 1$ or $25 \overset{8}{\equiv} 1$ or

$49 \overset{8}{\equiv} 1$

$\Rightarrow a^2 \overset{8}{\equiv} 1$. ∎