6 Congruences

Fix an integer $m > 1$. We say that two integers a, b are **congruent modulo** m iff $m|(a-b)$.

Remark: If we had done this for $m = 1$, then any pair a, b would be congruent mod 1.

If a, b are congruent mod m, we write

$$a = b \pmod{m}$$

Modular arithmetic:

If a is any integer, we can use the Euclidean algorithm to write

$$a = mq + r, \text{ with } 0 \leq r < m$$

Then $m|(a-r)$, so $a \equiv r \pmod{m}$.

Consequently, we can partition $\mathbb{Z}$ into m blocks, one for each integer r, with $0 \leq r < m$. Suppose B_r is the block corresponding to r. Then, for **any** a in B_r, $a \equiv r \pmod{m}$. Note: $B_0 = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$, $B_1 = \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots\}$, etc.

If $m = 2$, this partition will yield even and odd integers; the even integers are $\equiv 0 \pmod{2}$ and the odd integers are $\equiv 1 \pmod{2}$.

m=3:	a	r	(mod 3)
	0	0	
	1	1	
	2	2	
	3	0	
	4	1	
	5	2	
	6	0	

These blocks are called **congruence classes modulo** m. There are exactly m classes. We write $\mathbb{Z}/m$ for $\{B_0, B_1, \ldots B_{m-1}\}$.

Definition: A **set of representatives** for $\mathbb{Z}/m$ is a subset $S = \{x_0, x_1, \ldots, x_{n-1}\}$ of $\mathbb{Z}$ such that $x_r \in B_r$ for each $r = 0, 1, \ldots, m-1$.

Note: There is a **natural choice** for S, namely $S_0 = \{0, 1, \ldots, m-1\}$, called the **standard** or **usual** set of representatives.

So for $m = 3$, we can use

$$S_0 = \{0, 1, 2\}$$

or

$$S_1 = \{9, 16, -1\}$$

as a set of representatives.

Claim:

One has addition, subtraction, 0, and multiplication in $\mathbb{Z}/m$, just like in $\mathbb{Z}$.

Proof. Consider B_i, B_j. Look at $i + j$. By Euclidean algorithm,

$$i + j = qm + r_{i+j},$$

for some r_{i+j} with $0 \leq r_{i+j} < m$. We put

$$B_i + B_j = B_{r_{i+j}}$$

Similarly, $B_i - B_j = B_{r_{i-j}}$, if $i - j = q'm + r_{i-j}$, with $0 \leq r_{i-j} < m$. B_0 is the "zero" of $\mathbb{Z}/m$, because

$$B_0 + B_i = B_i = B_i + B_0$$

Multiplication

$$B_i B_j = ?$$

Write $ij = bm + r_{ij}$, $0 \leq r_{ij} < m$. Put $B_i B_j = B_{r_{ij}}$. Note that

$$B_1 B_j = B_j, \text{ for any } j.$$

So B_1 is the "one" element. Also have distributive and associative laws just like in $\mathbb{Z}$.

Definition: If $a \in \mathbb{Z}$, write $a \pmod{m}$ to denote the block it belongs to. If $a, b \in \mathbb{Z}$, we write $a + b \pmod{m}$ for any element of $B_i + B_j$, if $a \in B_i,\ b \in B_j$. Similarly, $ab \pmod{m}$ is defined.

Remark. In $\mathbb{Z}$ the only numbers we can divide by, i.e., which have "multiplicative inverses", are ± 1. The situation is better in $\mathbb{Z}/m$. In fact, when m is a prime p, all the non-zero elements of $\mathbb{Z}/m$ are invertible $\pmod{m}$.