Modulus Arithmetic

1 Congruences Modulo m.

Given an integer $m \geq 2$, we say that a is congruent to ~~b~~ modulo m, written $a \equiv b \pmod{m}$, if m divides $a - b$. Note that the following conditions are equivalent

(1) $a \equiv b \pmod{m}$

(2) $a = b + km$ for some integer k.

(3) a and b have the same remainder when divided by m.

For instance 6 and 21 are congruent modulo 5 because when divided by 5 both have the same remainder of 1.

$$[x] = [x]_m = \{ x + km \mid k \in \mathbb{Z} \}$$

Remark: when writing "$\bar{r}$" as a notation for the class of r we may stress the fact that "r" represent the class of r rather than the integer r by including "(mod p)" at some point. For instance $8 \equiv 3 \pmod p$.
Note that in "$a \equiv b \pmod m$", a and b represent integers, while in "$a = b \pmod m$" they represent elements of $\mathbb{Z}_m$.

Reduction Modulo m: Once a set of representatives has been chosen for the elements of $\mathbb{Z}_m$, we will call "r reduced modulo m", written "r mod m", the chosen representitive for the class of r. For instance, if we choose the representatives in the interval from 0 to 4 for the elements of $\mathbb{Z}_5$ ($\mathbb{Z}_5 = \{0,1,2,3,4\}$), then 9 mod 5 = 4.

$$[x] + [y] = [x+y] \qquad [x].[y] = [x.y]$$

Let say Turkish
modların sonuçları 4 işlem olarak yapılır
ve tekrardan modları alınır. pozitif ve Doğal
Sayı olacak şekilde modlar uygulanır,

$x \cdot x^{-1} = x^{-1} \cdot x = 1$

In general

(1) The elements of $\mathbb{Z}_m$ can be classified into two classes:

(a) Units: elements with multiplicative inverse.

(b) Divisors of zero: elements that multiplied by some other non-zero element give product zero.

(2) An element $[a] \in \mathbb{Z}_m$ is a unit (has a multiplicative inverse) if and only if $\gcd(a, m) = 1$.

(3) All non-zero elements of $\mathbb{Z}_m$ are units if and only if m is a prime number.

The set of units in $\mathbb{Z}_m$ is denoted $\mathbb{Z}_m^*$. For instance

$\mathbb{Z}_2^* = \{1\}$

$\mathbb{Z}_3^* = \{1,2\}$

$\mathbb{Z}_4^* = \{1,3\}$

$\mathbb{Z}_5^* = \{1,2,3,4\}$

$\mathbb{Z}_6^* = \{1,5\}$

$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$\mathbb{Z}_8^* = \{1,3,5,7\}$

$\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$