Modular Arithmetic

Given integers a and b and a positive number m, we defined that $a \equiv b \bmod m$ in case that m divides $a - b$. That is a and b differ by a multiple of m. If we divide a by m with remainder, that is $a = qm + r, 0 \leq r < m$ then $a - r = qm$ which shows that $a \equiv r$ for a unique r where $0 \leq r < m$.

This shows that the set $\mathbb{Z}$ of integers is divided into m –many classes according to $r = 0, r = 1, \cdots, r - m - 1$. For example, there are three classes of integers modulo $m = 3$:

$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots.\} \ = 3\mathbb{Z}$
$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \ = 3\mathbb{Z} + 1$
$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \ = 3\mathbb{Z} + 2$

The following allows us to add and multiply classes of congruent integers:

$$[a]_m + [b]_m = [a+b]_m, [a]_m \cdot [b]_m = [a \cdot b]_m,$$

Because we use representatives for these operations, one needs to show that the choice of representatives doesn’t matter. If $[a]_m = [a']_m$ and $[b]_m = [b']_m$ then $a - a' = qm, b - b' = q'm$ therefore $(a+b) - (a'+b') = (a-a') + (b-b') = (q-q')m$. Thus $[a+b]_m = [a'+b']_m$. We denote the set of m –many congruence classes as $\mathbb{Z}_m$. On $\mathbb{Z}_m$ an addition and multiplication has been defined which makes $\mathbb{Z}_m$ to a commutative ring with unit $e = [1]_m$.

We list the basic arithmetical properties of $\mathbb{Z}_m$:

$[a] + ([b] + [c]) \ = ([a] + [b]) \ + [c], [a] + [b] = [b] + [a], [a] + [0] = [a], [a] + [-a] = [0];$
$[a] \cdot ([b] \cdot [c]) \ = ([a] \cdot [b]) \ \cdot [c], [a] \cdot [b] = [b] \cdot [a], [a] \cdot [1] = [a]$
$[a] \cdot ([b] + [c]) \ = [a] \cdot [b] + [a] \cdot [c]$

We omitted the subscript n for the classes.

For example $[2]_6 \cdot [3]_6 = [2 \cdot 3]_6 = [6]_6 = [0]_6$ That shows that neither $[2]_6$ nor $[3]_6$ can have a multiplicative inverse. However $[5]_6 \cdot [5]_6 = [25]_6 = [1]_6$ shows that $[5]_6$ has a multiplicative inverse in $\mathbb{Z}_6$.

.

Theorem. Assme that a and m are relatively prime. Then $[a]_m$ has a multiplicative inverse in $\mathbb{Z}_m$.

For the proof we use the fact that the $\gcd(a,m) = 1$ and that for integers s and t we have that $s \cdot a + t \cdot m = 1$. Hence $[s]_m \cdot [a]_m + [t]_m \cdot [m]_m = [1]_m$ This shows $[a]_m$ has a multiplicative inverse, namely $[s]_m$.

If $m = p$ is a prime then $1, 2, \ldots, , p - 1$ are relatively prime to p. That is every congruence class different from $[0]$ has a multiplicative inverse.

Theorem. $\mathbb{Z}_m$ is a field if and only if m is a prime.

In $\mathbb{Z}_p$ we can do linear algebra. For example solve $3x + 2 = 1$ modulo 5. We get

$3x = -1, 3x = 4, [3]_5^{-1} = [2]_5, x = [2]_5 \cdot [4]_5 = [8]_5 = [3]_5$. Check: $3 \cdot 3 + 2 = 11 = 1$ modulo 5√