Number systems – $\mathbb{Z}/12\mathbb{Z}$, the clock

$$\mathbb{Z}/12\mathbb{Z} = \left\{ 12, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 \right\}$$

$2+12=2$
$3+4=7$
$10+5=3$

The product, or multiplication on $\mathbb{Z}/12\mathbb{Z}$ is given by

$$m \cdot n = \underbrace{m+m+\cdots+m}_{n \text{ times}}$$

For example $5 \cdot 3 = 5+5+5 = 10+5 = 3$.

The multiplication table for $\mathbb{Z}/12\mathbb{Z}$ is

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	2	4	6	8	10	12
3	3	6	9	12	3	6	9	12	3	6	9	12
4	4	8	12	4	8	12	4	8	12	4	8	12
5	5	10	3	8	1	6	11	4	9	2	7	12
6	6	12	6	12	6	12	6	12	6	12	6	12
7	7	2	9	4	11	6	1	8	3	10	5	12
8	8	4	12	8	4	12	8	4	12	8	4	12
9	9	6	3	12	9	6	3	12	9	6	3	12
10	10	8	6	4	2	12	10	8	6	4	2	12
11	11	10	9	8	7	6	5	4	3	2	1	12
12	12	12	12	12	12	12	12	12	12	12	12	12

Let $x \in \mathbb{Z}/12\mathbb{Z}$. The element x is <u>invertible</u> if there exists $y \in \mathbb{Z}/12\mathbb{Z}$ such that

$$y \cdot x = 1.$$

The inverse of 5 is 5, since $5 \cdot 5 = 1$.
The inverse of 2 does not exist.

<u>Theorem</u> Let $m \in \mathbb{Z}_{>0}$. The invertible elements of $\mathbb{Z}/m\mathbb{Z}$ are $x \in \mathbb{Z}_{>0}$ such that

(a) $1 \le x \le m$,
(b) $\gcd(x, m) = 1$.

The invertible elements of $\mathbb{Z}/12\mathbb{Z}$ are $1, 5, 7, 11$

The <u>additive identity</u> is $0 \in \mathbb{Z}/12\mathbb{Z}$ such that if $x \in \mathbb{Z}/12\mathbb{Z}$ then $0 + x = x$ and $x + 0 = x$.

Note that $0 = 12$ in $\mathbb{Z}/12\mathbb{Z}$.

<u>Number systems</u> - $\mathbb{Z}_{>0}$, the free monoid generated by 1.

$$\mathbb{Z}_{>0} = \{1, 1+1, 1+1+1, 1+1+1+1, \ldots\}$$

with addition given by concatenation. For example

$$(1+1) + (1+1+1) = 1+1+1+1+1$$

An example of <u>multiplication</u> in $\mathbb{Z}_{>0}$ is

$$(1+1+1+1)\cdot x = x+x+x+x.$$

Let $x \in \mathbb{Z}_{>0}$. The <u>set of multiples of x</u> is

$$x\cdot\mathbb{Z}_{>0} = \{x, x+x, x+x+x, \ldots\}$$

Let $a, b \in \mathbb{Z}_{>0}$. The element b divides a, $b \mid a$, if

$$a \in b\mathbb{Z}_{>0}.$$

Let $a, b \in \mathbb{Z}_{>0}$. The <u>greatest common divisor of a and b</u>, $\gcd(a,b)$, is

the largest $d \in \mathbb{Z}_{>0}$ such that $d \mid a$ and $d \mid b$.

<u>The order on $\mathbb{Z}_{>0}$</u>: Let $a, b \in \mathbb{Z}_{>0}$. Define

$a < b$ if there exists $x \in \mathbb{Z}_{>0}$ such that $a + x = b$.

A better definition of $\gcd(a,b)$ is:

Let $a, b \in \mathbb{Z}_{>0}$. The <u>greatest</u> <u>common</u> <u>divisor</u> <u>of</u> <u>a</u> <u>and</u> <u>b</u>, $\gcd(a,b)$, is $d \in \mathbb{Z}_{>0}$ such that

(a) $d \mid a$ and $d \mid b$

(b) If $l \in \mathbb{Z}_{>0}$ and $l \mid a$ and $l \mid b$ then $l \leq d$.