GTLA Lecture 04.08.2020

The clock $\mathbb{Z}/12\mathbb{Z}$

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

$12 + 2 = 2$

$11 + 7 = 6$

$5 \cdot 3 = 5 + 5 + 5 = 12 + 3 = 3$

+	12	1	2	3	4	5	6	7	8	9	10	11
12	12	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	3	4	5	6	7	8	9	10	11	12	1
3	3	4	5	6	7	8	9	10	11	12	1	2
4	4	5	6	7	8	9	10	11	12	1	2	3
5	5	6	7	8	9	10	11	12	1	2	3	4
6	6	7	8	9	10	11	12	1	2	3	4	5
7	7	8	9	10	11	12	1	2	3	4	5	6
8	8	9	10	11	12	1	2	3	4	5	6	7
9	9	10	11	12	1	2	3	4	5	6	7	8
10	10	11	12	1	2	3	4	5	6	7	8	9
11	11	12	1	2	3	4	5	6	7	8	9	10

$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$ addition

$(a, b) \longmapsto a + b$

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

$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ multiplication

$(a, b) \longmapsto ab$

$1 \cdot 1 = 1$, $5 \cdot 5 = 1$, $7 \cdot 7 = 1$, $11 \cdot 11 = 1$.

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

Write $(\mathbb{Z}/12\mathbb{Z})^{\times} = \{1, 5, 7, 11\}$. not a field

Yes a commutative ring.

$12 = 0$, so $\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \ldots, 11\}$

The relation between $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

$$15 = 12 + 3$$

$$49 = 4 \cdot 12 + 1 \longrightarrow \begin{cases} a = 49 \\ q = 4, \ r = 1 \end{cases}$$

<u>Theorem</u> <u>Euclidean algorithm</u>

Let $m \in \mathbb{Z}_{>0}$ and consider

$$\left.\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}\right\} \text{clock}$$

Let $a \in \mathbb{Z}$. Then there exist unique $q \in \mathbb{Z}$ and $r \in \{0, \ldots, m-1\}$ such that

$$a = qm + r$$

The 7-clock $\mathbb{Z}/7\mathbb{Z}$

$$\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$$

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

The invertible elements in $\mathbb{Z}/7\mathbb{Z}$.

$$\left(\mathbb{Z}/7\mathbb{Z}\right)^{\times} = \{1, 2, 3, 4, 5, 6\}.$$

Only 0 is not invertible in $\mathbb{Z}/7\mathbb{Z}$

number system

A **field** is a commutative ring F such that

if $r \in F$ and $r \neq 0$ then r is invertible.

The clock $\mathbb{Z}/p\mathbb{Z}$ when p is prime.

Main result:

Theorem If $p \in \mathbb{Z}_{>0}$ and p is prime then

$$\mathbb{Z}/p\mathbb{Z} \text{ is a field.}$$

Extended Theorem If $p \in \mathbb{Z}_{>0}$ and p is prime.

(a) If $n \in \mathbb{Z}/p\mathbb{Z}$ and $n \neq 0$ then there exists $y \in \mathbb{Z}/p\mathbb{Z}$ such that

$$y \cdot n = 1 \quad \text{in } \mathbb{Z}/p\mathbb{Z}.$$

(c) If $n \in \mathbb{Z}/p\mathbb{Z}$ and $n \neq 0$ then

$$n^{p-1} = 1 \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

Fermat's little theorem

$0^{p-1} \neq 1$

(b) If $n \in \mathbb{Z}/p\mathbb{Z}$ then

$$\boxed{n^p = n} \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

$0^p = 0$

(d) If $x, y \in \mathbb{Z}/p\mathbb{Z}$ then

$$(x+y)^p = x^p + y^p$$

$x^2 + y^2 \stackrel{?}{=} (x+y)^2$

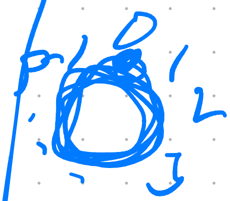
YES in $\mathbb{Z}/2\mathbb{Z}$

(e) $\binom{p}{0} = \frac{p!}{0!(p-0)!} = \frac{p!}{1\cdot p!} = 1.$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots 2\cdot 1}{k(k-1)\cdots 2\cdot 1\,(p-k)(p-k-1)\cdots 2\cdot 1}$$

$$\binom{p}{p} = \frac{p!}{p!(p-p)!} = \frac{p!}{p!\,0!} = \frac{p!}{p!\cdot 1} = 1.$$

$\boxed{\text{If } k \notin \{0,p\} \text{ then } \binom{p}{k} \text{ is divisible by } p.}$



i.e. $\binom{p}{k} = 0$ in $\mathbb{Z}/p\mathbb{Z}$ if $k \notin \{0,p\}$

If you believe

$$(x+y)^p = \binom{p}{0}x^0y^p + \binom{p}{1}x^1y^{p-1} + \binom{p}{2}x^2y^{p-2} + \cdots + \binom{p}{p-1}x^{p-1}y + \binom{p}{p}x^py^0$$

then in $\mathbb{Z}/p\mathbb{Z}$,

$$(x+y)^p = 1\cdot x^0y^p + 0\cdot x^1y^{p-1} + 0\cdot x^2y^{p-2} + \cdots + 0x^{p-1}y + 1\cdot x^py^0$$

$$= y^p + x^p = x^p + y^p.$$

If you believe $n^p = n$ then

$(n+1)^p = n^p + 1^p = n+1$

So if $1^p = 1$ then $2^p = 2$

and $3^p = 3$

and $4^p = 4$

and ....

RSA. It is hard for computers to factor.

?

Let p_1, p_2 be prime. Let

$m = p_1 p_2$.

Can the computer factor m?

If p_1 and p_2 have 100 digits then the computer takes more that 2^{100} microseconds.

exponential time.

enc: $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$

$x \longmapsto x^e$

(m, e) public

dec: $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$

$y \longmapsto y^d$

d is private.

We <u>need</u>

$$dec(enc(x)) = x.$$

i.e.

$$(x^e)^d = x.$$

i.e.

$$\boxed{x^{ed} = x.}$$

not necessarily prime

A	R	U	N
1	17	24	13
1^{31}	17^{31}	24^{31}	13^{31}
	$=6$	$=72$	$=26$

If $e = 31$