Recall: in $\mathbb{Z}_n$, $a^{-1} \in \mathbb{Z}_n$ is defined to be the number s.t $(a^{-1})(a) = 1$ in $\mathbb{Z}_n$ (if it exists ie if (ie $a^{-1}a \equiv 1 \bmod n$) $\gcd(a,n) = 1$)

E.g. $n = 9$ $\mathbb{Z}_9 = \{0, 1, 2, \cdots, 8\}$

Find 2^{-1} ie find a number in $\mathbb{Z}_9$ s.t (the number) $\times 2 = 1$ in $\mathbb{Z}_9$

Well $5 \times 2 = 10 \equiv 1 \bmod 9$

so $5 \times 2 = 1$ in $\mathbb{Z}_9$

so $5 = 2^{-1}$.

Ex: If $\gcd(a,n) = 1$ then a^{-1} can be found using Euclid's algorithm as we can write for suitable s & t integers, $sa + tn = 1$

But $tn = 0$ in $\mathbb{Z}_n$ (Because it's a multiple of n)

$\Rightarrow sa = 1$ in $\mathbb{Z}_n$

$\Rightarrow s = a^{-1}$ in $\mathbb{Z}_n$.

Ex: Evaluate $3^{-1} \bmod 26$ ie Find 3^{-1} in $\mathbb{Z}_{26}$. By Euclid's Algorithm

$$26 = 3(8) + 2 \quad \cdots (i)$$
$$3 = 2(1) + 1 \quad \cdots (ii)$$

So $\gcd(3, 26) = 1$ so 3^{-1} exists in $\mathbb{Z}_{26}$

By Back substitution we have

$$1 = 3 - 2 \quad \text{(from (ii))}$$
$$\Rightarrow 1 = 3 - [26 - 3(8)] \quad \cdots \text{from (i)}$$
$$= 1 = (-1)26 + (9)3$$
$$= (25)(26) + (9)3$$
$$\overset{11}{0} \text{ in } \mathbb{Z}_{26}$$
$$\Rightarrow 1 = (9)3 \text{ in } \mathbb{Z}_{26} \Rightarrow$$
$$9 = 3^{-1} \text{ in } \mathbb{Z}_{26}$$

§ An Application of Modular Arithmetic ie in $\mathbb{Z}_{11}$.

An ISBN is of the form

$$x_1 - x_2x_3x_4 - x_5x_6x_7x_8x_9 - x_{10}$$

for the no. 10

where $x_i \in \mathbb{Z}_{11} = \{0, 1, 2, \cdots, 9, X\}$

& must have $x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} \equiv 0 \bmod 11$

ie $= 0$ in $\mathbb{Z}_{11}$

e.g. $3-540-22898-5$ is an ISBN.

Because $1(3)+2(5)+3(4)+4(0)+5(2)+6(2)+7(8)$
$+8(9)+9(8)+10(5)$
$=297 \equiv 0 \bmod 11.$

Find The Missing digit in the ISBN

$0-19-850714-?$

$1(0)+2(1)+3(9)+4(8)+5(5)+6(0)+7(7)+8(1)+$
$9(4)+10(?)$

must Be $\equiv 0 \bmod 11$ (OR $=0$ in $\mathbb{Z}_{11}$)

$\Rightarrow 179+10(?)=0$ in $\mathbb{Z}_{11}$

$\Rightarrow 3+10(?)=0$ in $\mathbb{Z}_{11}$

$\Rightarrow 10(?)=-3$ in $\mathbb{Z}_{11}$

$\Rightarrow 10(?)=8$ (as $8+3=11=0$ in $\mathbb{Z}_{11}$)

multiply Both Sides By 10^{-1}

$\Rightarrow (10^{-1})(10)(?) = 10^{-1}(8)$

$\Rightarrow 1(?) = ? = 10^{-1}(8)$

But $10^{-1}=10$ in $\mathbb{Z}_{11}$ as

$10 \times 10 = 100 \equiv 1 \bmod 11$

$\Rightarrow 10^{-1}=10$ in $\mathbb{Z}_{11}$

So $? = 10^{-1}(8) = 10(8) = 80$

$\Rightarrow ? = 3$ in $\mathbb{Z}_{11}$

ie Missing digit $= 3$

$(80 = 11(7)+3)$

Ex: Find the missing digit in the ISBN

0-19-85071 ? 3

We must have:

$$1(0) + 2(1) + 3(9) + 4(8) + 5(5) + 6(0) + 7(7) + 8(1) + 9(?) + 10(3) \equiv 0 \mod 11$$

OR $= 0$ in $\mathbb{Z}_{11}$

$$\Rightarrow \quad 173 + 9(?) = 0 \text{ in } \mathbb{Z}_{11}$$

$$\Rightarrow \quad 8 + 9(?) = 0 \text{ in } \mathbb{Z}_{11}$$

(as $173 = 11(15) + \underline{8}$)

$$\Rightarrow \quad 9(?) = -8 \text{ in } \mathbb{Z}_{11}$$

$$\Rightarrow \quad 9(?) = 3 \text{ in } \mathbb{Z}_{11}$$

(as $3 + 8 = 11 = 0$ in $\mathbb{Z}_{11}$)

$$\Rightarrow \quad \underbrace{9^{-1}9}_{1}(?) = (9^{-1})3 \text{ in } \mathbb{Z}_{11}$$

But $\Rightarrow \quad 1(?) = (5)3$ in $\mathbb{Z}_{11}$

(as $5 \times 9 = 45 \equiv 1 \mod 11 \Rightarrow 5 \times 9 = 1$ in $\mathbb{Z}_{11}$)

($45 = 11(4) + \underline{1}$)

So $5 = 9^{-1}$

So $? = 15 = 4$ in $\mathbb{Z}_{11}$

($15 = 11(1) + 4$)

Ex: Find $29^{-1} \bmod 167$ ie find 29^{-1} in $\mathbb{Z}_{167}$. Recall 29^{-1} will exist if $\gcd(29, 167) = 1$.

$$167 = 29(5) + 22 \quad \cdots (i)$$
$$29 = 22(1) + 7 \quad \cdots (ii)$$
$$22 = 7(3) + 1 \quad \cdots (iii)$$

So $\gcd(29, 167) = 1$ So 29^{-1} exists & is computed as follows: (By Back Substitution)

From eqn (iii) we have

$$1 = 22 - (3)7$$

From eqn (ii) $\Rightarrow$ $1 = 22 - 3[29 - 22]$

$$= (-3)29 + (4)22$$

From eqn (i) $\Rightarrow$

$$1 = (-3)29 + 4[167 - (5)29]$$

$$\Rightarrow \quad 1 = (4)167 + (-23)29$$

But $(4)167 = 0$ in $\mathbb{Z}_{167}$ (a multiple of 167)

$$\Rightarrow \quad 1 = \underbrace{(144)}_{29^{-1}} 29$$

(Because $23 + 144 = 167 = 0$ in $\mathbb{Z}_{167}$ So $-3 = 144$ in $\mathbb{Z}_{167}$)

So $29^{-1} = 144$ in $\mathbb{Z}_{167}$