Why is $\mathbb{Z}_p$ a field?

Because

$\forall \; a \in \mathbb{Z}_p \setminus \{0\}$

there exists a^{-1}.

How to calculate a^{-1} ?

use extended Euclidean algorithm !

(輾轉相除法)

$\because \gcd(a, p) = 1$

use extended Euclidean algo

to find $ax + py = 1$

then $a^{-1} = x$!

why?

$$ax + py = 1$$

$$ax = 1 - py$$

$$= 1 \mod p$$

$$\therefore x = a^{-1}$$

Eg 1: $7^{-1} = ?$ mod 101

$$\begin{array}{r|l} 2 & \begin{array}{r|l} 7 & \begin{array}{r|l} 101 & 14 \\ 98 & \\ \hline 3 & \end{array} \\ \hline 6 & \\ \hline 1 & \end{array} \\ \hline \end{array}$$

$1 = 7 - 6$

$= 7 - 2 \cdot 3$

$= 7 - 2(101 - 98)$

$= 7 - 2(101 - 14 \cdot 7)$

$= 29 \cdot 7 - 2 \cdot 101$

x y

$\therefore 7^{-1} = 29$

Eg 2: $25^{-1} = ?$ mod 911

	25	911	
	22	900	36
2	3	11	3
1	2	9	
	1	2	

$1 = 3 - 2$

$= 3 - (11 - 3 \cdot 3)$

$= 4 \cdot 3 - 11$

$= 4(25 - 2 \cdot 11) - 11$

$= 4 \cdot 25 - 9 \cdot 11$

$= 4 \cdot 25 - 9(911 - 36 \cdot 25)$

$= 328 \cdot 25 - 9 \cdot 911$

$\therefore 25^{-1} = 328 \mod 911$