

$$\begin{cases} 3x + y = 2 \\ 2x - 3y = 0 \end{cases}$$

i $\mathbb{Q}$:

från ekv. 1 får vi:

$$y = 2 - 3x,$$

insättning i den andra ekv.

ger

$$2x - 3(2 - 3x) = 0$$

$$11x - 6 = 0; \quad x = \frac{6}{11} \quad y = \frac{4}{11}$$

i $\mathbb{Z}_9$

— " —

— " —

ger

$$2x - 6 = 0$$

$$\boxed{x=3} \quad \boxed{y=2}$$

$$\begin{array}{l}
 1^2 = 1 \equiv 1 \pmod{p} \\
 p-1 \equiv -1 \pmod{p} \\
 (p-1)^2 \equiv (-1)^2 = 1 \pmod{p}
 \end{array}
 \left. \vphantom{\begin{array}{l} 1^2 = 1 \equiv 1 \pmod{p} \\ p-1 \equiv -1 \pmod{p} \\ (p-1)^2 \equiv (-1)^2 = 1 \pmod{p} \end{array}} \right\} \begin{array}{l} 1 \text{ och } p-1 \\ \text{är verkligen} \\ \text{lösningar.} \end{array}$$

Finns det andra lösningar?

nej! $x^2 - 1 = (x+1)(x-1)$

ingen annan faktorisering
finns pga multiplikations-
tabellen i $\mathbb{Z}_p$

Så det är bara 1 och $p-1$ som
är sina egna inverser:

$$1 \cdot 1 = (p-1) \cdot (p-1) = 1 \quad \text{i } \mathbb{Z}_p.$$

Betrakta nu $(p-1)! =$

$$= 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2)(p-1) = p-1 \equiv -1 \pmod{p}$$

$\underbrace{\hspace{10em}}_{1 \text{ i } \mathbb{Z}_p}$

i produkten $2 \cdot 3 \cdot \dots \cdot (p-2)$ ingår restklasserna
tillsammans med sina inverser precis en gång.