

4.20.8 Elementene relativt primiske til p^2 er alle np , hvor $n \in \mathbb{Z}$.

For elementer mindre end p^2 blir dette

$$\{np \mid 0 < n \leq p\}, \text{ altså er } \phi(p^2) = p^2 - p = \underline{\underline{p(p-1)}}$$

4.20.14

$$45x \equiv 15 \pmod{24}$$

$$\gcd(45, 24) = 3$$

$3 \mid 15$, så fra Corollary 20.13 eksisterer det 3 løsninger

$$15x \equiv 5 \pmod{8}$$

$$-x \equiv 5 \pmod{8}$$

$$x = -5 \equiv 3 \pmod{8}$$

$$\begin{aligned} \text{Løsninger: } & 3 + 24\mathbb{Z} \\ & 11 + 24\mathbb{Z} \\ & 19 + 24\mathbb{Z} \end{aligned}$$

4.20.27

$$\text{Antag } x^2 = 1$$

$$\text{Da er } x^2 - 1 = 0$$

$$(x+1)(x-1) = 0$$

Siden $\mathbb{Z}_p$ er en kropp, så har den ingen null-divisorer,

$$\text{så } x = 1 \text{ eller } x = -1 = p-1$$

$$1^2 = 1 \quad (p-1)^2 = p^2 - 2p + 1 = 1 \quad \text{i } \mathbb{Z}_p,$$

så både 1 og $p-1$ er egne inverser, og disse er de eneste.

4.20.28

p prim

$$(p-1)! = (p-1)(p-2) \cdots 3 \cdot 2 \cdot 1$$

For alle $x \in \{2, 3, \dots, p-2\}$ eksisterer $x^{-1} \in \{2, 3, \dots, p-2\}$,
derfor vil $(p-2) \cdots 3 \cdot 2 = 1$ i $\mathbb{Z}_p$.

Det gir

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

$$\text{så } (p-1)! \equiv -1 \pmod{p}.$$