(F18, on 15 mar 2006)

$$x \equiv y \pmod{m}, \quad \text{eller} \quad x \equiv_m y$$

betyder $m|(x-y)$ och läses "x är kongruent med y modulo m".

Det är en **ekvivalensrelation** på $\mathbb{Z}$, med m st ekvivalensklasser:

$$[0]_m = \{0, \pm m, \pm 2m, \dots\},$$
$$[1]_m = \{1, \pm m + 1, \pm 2m + 1, \dots\},$$
$$\vdots$$
$$[m-1]_m = \{-1, \pm m - 1, \pm 2m - 1, \dots\}.$$

Mängden av dessa ("heltalen modulo m"): $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$.

Sats: $x_1 \equiv_m x_2,\ y_1 \equiv_m y_2 \ \Rightarrow\ x_1 + y_1 \equiv_m x_2 + y_2,\ x_1 y_1 \equiv_m x_2 y_2$.

Så vi kan **definiera** $+$ och $\cdot$ på $\mathbb{Z}_m$:

$$[a]_m \circ [b]_m = [a \circ b]_m \quad \text{för} \quad \circ = +, \cdot$$

Vi skriver oftast $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ och räknar $+$ och $\cdot$ "som vanligt men med rest mod m".

Definition: $r \in \mathbb{Z}_m$ är **inverterbart** om det finns $x \in \mathbb{Z}_m$ med $rx = 1$ i $\mathbb{Z}_m$. Detta x kallas r^{-1}, r:s **invers**.

Sats: $r \in \mathbb{Z}_m$ är inverterbart omm $sgd(r, m) = 1$ (i $\mathbb{Z}$).

U_m: mängden av inverterbara element i $\mathbb{Z}_m$, $|U_m| = \phi(m)$

Sats: $y \in U_m \ \Rightarrow y^{\phi(m)} = 1$ i $\mathbb{Z}_m$,

dvs uttryckt i $\mathbb{Z}$ (**Eulers sats**): $sgd(y, m) = 1 \Rightarrow y^{\phi(m)} \equiv_m 1$.

Speciellt om **p primtal**: $y \neq 0 \Rightarrow y^{p-1} = 1$ i $\mathbb{Z}_p$,

dvs i $\mathbb{Z}$ (**Fermats lilla sats**): $p \not| y \Rightarrow y^{p-1} \equiv_p 1$,

så $y^p = y$, alla $y \in \mathbb{Z}_p$ och $y^p \equiv_p y$, alla $y \in \mathbb{Z}$.