(Diskret matte D, ht17: F14, on 27 sep 2017)

Modulär aritmetik

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

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

Mängden av alla heltal, $\mathbb{Z}$, delas in i m st klasser av kongruenta tal:

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

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

$rx = 1$ i $\mathbb{Z}_m$ omm $rx - km = 1$ för något $k \in \mathbb{Z}$, så r^{-1} kan bestämmas med Euklides algoritm.

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

Linjära kongruenser = linjära ekvationer i $\mathbb{Z}_m$:

$ax \equiv b \pmod{m} \ \Leftrightarrow\ ax = b$ i $\mathbb{Z}_m \ \Leftrightarrow\ ax - km = b$ för något $k \in \mathbb{Z}$,
så ekvationen är lösbar omm $d = \text{sgd}(a, m) \mid b$.
Då finns d olika lösningar $\pmod{m}$, dvs d olika lösningar i $\mathbb{Z}_m$.

$ax \equiv ay \pmod{m} \ \Leftrightarrow\ x \equiv y \pmod{m}$ **om** $\text{sgd}(a, m) = 1$

$ax \equiv ay \pmod{an} \ \Leftrightarrow\ x \equiv y \pmod{n}$

$a \nmid y \ \Rightarrow\ ax \not\equiv y \pmod{an}$.

Kongruenser med flera moduler:

Låt $m_1, \ldots, m_k \in \mathbb{N}$, $\text{sgd}(m_i, m_j) = 1$ om $i \neq j$ och funktionen $F : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$ ges av $F(a) = ([a]_{m_1}, \ldots, [a]_{m_k})$. Då gäller

$$F(a) = F(b) \;\Leftrightarrow\; a \equiv_m b, \;\; m = m_1 \ldots m_k,$$

så funktionen $f\colon \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$ given av $f([a]_m) = ([a]_{m_1}, \ldots, [a]_{m_k})$ är (väldefinierad och) **injektiv**.

$|\mathbb{Z}_m| = |\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}|$, så f är **surjektiv**.

Det gäller

$$f([a+b]_m) = ([a]_{m_1} + [b]_{m_1}, \ldots, [a]_{m_k} + [b]_{m_k}) = f([a]_m) + f([b]_m)$$
$$f([ab]_m) = ([a]_{m_1}[b]_{m_1}, \ldots, [a]_{m_k}[b]_{m_k}) = f([a]_m) f([b]_m)$$

(komponentvisa operationer i HL), dvs f är en **isomorfi**.

Det ger

$$f^{-1}([a_1]_{m_1}, \ldots, [a_k]_{m_k}) = [y_1 a_1 + \cdots + y_k a_k]_m,$$

där $y_i = f^{-1}(0, 0, \ldots, 1, \ldots, 0)$ (1 i pos. i), dvs $[y_i]_{m_j} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$

Kinesiska restsatsen: Om $m_1, \ldots, m_k \in \{2, 3, \ldots\}$ och $\text{sgd}(m_i, m_j) = 1$ då $i \neq j$, har systemet

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \\ \vdots \\ x \equiv_{m_k} a_k \end{cases}$$

för alla $a_1, \ldots, a_k \in \mathbb{Z}$ en lösning, unik mod $m = m_1 \ldots m_k$,

$$x \equiv_m y_1 a_1 + \cdots + y_k a_k$$

för vissa $y_1, \ldots, y_k$, oberoende av $a_1, \ldots, a_k$.

Eulers sats, Fermats lilla sats

U_m: mängden av inverterbara element i $\mathbb{Z}_m$.
$x, y \in U_m \;\Rightarrow\; xy, x^{-1} \in U_m$
$|U_m| = \phi(m) = |\{x \in \mathbb{Z} \mid 1 \leq x \leq m, \; \text{sgd}(x, m) = 1\}|$.
ϕ kallas **Eulers ϕ-funktion**.

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

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

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

dvs i $\mathbb{Z}$ (**Fermats lilla sats**): $p \nmid y \Rightarrow y^{p-1} \equiv_p 1$,

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

$$(\mathbb{Z}_{mn}, +, \cdot) \approx (\mathbb{Z}_m \times \mathbb{Z}_n, +, \cdot) \textbf{ om } \mathbf{sgd}(m, n) = 1,$$

$$\text{ty} \quad x \equiv_{mn} y \quad \Leftrightarrow \quad \begin{cases} x \equiv_m y \\ x \equiv_n y \end{cases}$$

ger

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,$$

$$f([x]_{mn}) = ([x]_m, [x]_n).$$

f är **1-1** och (således) **på** (dvs en bijektion).

Dessutom gäller

$$f(a + b) = f(a) + f(b), \; f(a \cdot b) = f(a) \cdot f(b),$$

(komponentvisa operationer i HL) så **f är en isomorfi**.

Exempel ($m = 3,\ n = 5$):

$\mathbf{0 \mapsto (0,0)}$	$\mathbf{5 \mapsto (2,0)}$	$\mathbf{10 \mapsto (1,0)}$
$\mathbf{1 \mapsto (1,1)}$	$\mathbf{6 \mapsto (0,1)}$	$\mathbf{11 \mapsto (2,1)}$
$\mathbf{2 \mapsto (2,2)}$	$\mathbf{7 \mapsto (1,2)}$	$\mathbf{12 \mapsto (0,2)}$
$\mathbf{3 \mapsto (0,3)}$	$\mathbf{8 \mapsto (2,3)}$	$\mathbf{13 \mapsto (1,3)}$
$\mathbf{4 \mapsto (1,4)}$	$\mathbf{9 \mapsto (0,4)}$	$\mathbf{14 \mapsto (2,4)}$

$f(8) = (2,3),\ f(11) = (2,1)$ och

$(2,3) + (2,1) = (1,4) = f(4)$ i $\mathbb{Z}_3 \times \mathbb{Z}_5$, **så** $8 + 11 = 4$ i $\mathbb{Z}_{15}$

$(2,3) \cdot (2,1) = (1,3) = f(13)$ i $\mathbb{Z}_3 \times \mathbb{Z}_5$, **så** $8 \cdot 11 = 13$ i $\mathbb{Z}_{15}$

$(2,3)^{-1} = (2^{-1}, 3^{-1}) = (2,2) = f(2)$ i $\mathbb{Z}_3 \times \mathbb{Z}_5$, **så** $8^{-1} = 2$ i $\mathbb{Z}_{15}$

$$\begin{array}{ccc} \mathbb{Z}_{15} & \xrightarrow{f} & \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \circ \downarrow & & \downarrow \quad \downarrow \circ \\ \mathbb{Z}_{15} & \xleftarrow[f^{-1}]{} & \mathbb{Z}_3 \times \mathbb{Z}_5 \end{array}$$

$\circ = +, \cdot$ eller $^{-1}$

$f(10) = (1,0),\ f(6) = (0,1)$ så $f(a \cdot 10 + b \cdot 6) = ([a]_3, [b]_5)$ och

$$f^{-1}((a,b)) = [ay_1 + by_2]_{15}, \qquad y_1 = 10,\ y_2 = 6.$$