(Diskret matte D, ht13: F10, fr 20 sep 2013)

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 $y \in \mathbb{Z}$.

Lite om kvadratiska kongruenser:

Ekvationer som $x^2 + c_1 x + c_2 \equiv_m 0$ kan (om m är udda) med kvadratkomplettering skrivas som $(x + a)^2 \equiv_m b$ och har då lösningar precis om $y^2 \equiv_m b$ har det, dvs om $b \in \mathbb{Z}_m$ är en kvadrat.
Om p är ett udda primtal är precis $\frac{p+1}{2}$ av de p elementen i $\mathbb{Z}_p$ kvadrater.

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
$F : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ 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 $f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ given av $f([a]_m) = ([a]_{m_1}, \ldots, [a]_{m_k})$ är (väldefinierad och) **1 till 1** (dvs $a \neq b \Rightarrow f(a) \neq f(b)$).

$|\mathbb{Z}_m| = |\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}|$, så f är **på** (den antar alla värden i $\mathbb{Z}_{m_1} \times \ldots$).

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 $m_1, \ldots, m_k \in \mathbb{N}$, $\text{sgd}(m_i, m_j) = 1$ 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 $a_1, \ldots, a_k$.