Forelesning 14
MER KONGRUENSREGNING

- Diskrete logaritmer
  $$x \equiv \log_a b \pmod m \iff a^x \equiv b \pmod m$$
- Det kinesiske restteoremet og system av kongruensligninger
  $$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$
- Ekvivalensklasser
  $$[a_m] = \{b \mid b \equiv a \pmod m\}$$

Diskrete logaritmer

Vi har en effektiv måte å regne ut
$$x \equiv a^b \pmod m$$

Kan vi gå motsatt vei? Det vil si hvis vi har $a^x \equiv b \pmod m$
kan vi finne $x \equiv \log_a b \pmod m$?

Definisjon

La $a, b, e, m \in \mathbb{Z}$ med $m > 0$

Hvis $b \equiv a^e \pmod m$ så sier vi at e er
den diskrete logaritmen til b, med hensyn til basen a,
modulo m

Eksempel

Modulo 11 har vi

$2^1 \equiv 2$ $2^2 \equiv 4$ $2^3 \equiv 8$ $2^4 \equiv 5$ $2^5 \equiv 10$

$2^6 \equiv 9$ $2^7 \equiv 7$ $2^8 \equiv 3$ $2^9 \equiv 6$

F.eks. er $\log_2 3 \equiv 8 \pmod{11}$ fordi $2^8 \equiv 3$

Merk: Det finnes ikke alltid en x slik at $a^x \equiv b$ (modulo m)
og selv om den finnes, så har vi ingen effektiv
måte å beregne x!!
- ↳ Diskrete logaritmer egner seg godt for kryptografi
- ↳ Kan gjøre det litt bedre enn å gjette (ØF)

Det kinesiske restteoremet

La oss si at vi ønsker å løse et system av kongruensligninger, f.eks.

$$x \equiv 1 \pmod 2$$
$$x \equiv 4 \pmod 5$$

Først: hvis to tall er kongruente mod $2 \cdot 5 = 10$, så er de også kongruente modulo både 2 og 5.

Hvorfor? $a \equiv b \pmod{10}$ gir $10 \mid (a-b)$

Dvs $(a-b) = 10 \cdot q = 2 \cdot (5q) = 5\,(2q)$
Så $5 \mid (a-b)$ og $2 \mid (a-b)$

Eller: $a \equiv b \pmod 5$ og $a \equiv b \pmod 2$

Det motsatte holder også når $m \perp n$
(her $2 \perp 5$)

Så for å sjekke om x er en løsning, holder det å sjekke om x mod 10 er en løsning.

La oss lage en tabell:

x mod 10	0	1	2	3	4	5	6	7	8	9
x mod 2	0	1	0	1	0	1	0	1	0	1
x mod 5	0	1	2	3	4	0	1	2	3	4

Vi får at $x \equiv 1 \pmod 2$ og $x \equiv 4 \pmod 5$ når $x \equiv 9 \pmod{10}$

La oss stokke om litt

x mod 10	0	6	2	8	4	5	1	7	3	9
x mod 2	0	0	0	0	0	1	1	1	1	1
x mod 5	0	1	2	3	4	0	1	2	3	4

Vi kan se at alle

$$\begin{cases} x \equiv a \pmod 2 \\ x \equiv b \pmod 5 \end{cases}$$

har entydig løsning modulo 10.

La oss generalisere, og løse

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases} \quad \text{der } m \perp n \ (\gcd(m,n)=1)$$

Siden $\gcd(m,n)=1$, så finnes det heltall u og v slik at $u \cdot m + v \cdot n = 1$

Vi har da at $u \cdot m \equiv 0 \pmod m$
$u \cdot m \equiv 1 \pmod n$
($n \mid (u \cdot m - 1)$ fordi $u \cdot m - 1 = -v \cdot n$)

Tilsvarende har vi
$v \cdot n \equiv 0 \pmod n$
$v \cdot n \equiv 1 \pmod m$

La nå $x = a \cdot v \cdot n + b \cdot u \cdot m$
Da er x en løsning av systemet!

Hvorfor?
$x = a \cdot v \cdot n + b \cdot u \cdot m \equiv a \cdot v \cdot n \equiv a \pmod m$ og
$x = a \cdot v \cdot n + b \cdot u \cdot m \equiv b \cdot u\, m \equiv b \pmod n$

Oppsummert

Løsningen av $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$
er gitt ved $x \equiv c \cdot v \cdot n = b \cdot u \cdot m \pmod{m \cdot n}$
der u og v er heltall slik at $u \cdot m + v \cdot n = 1$

(Det vi egentlig trenger er bare at u er en invers til m modulo n og v er en invers til n modulo m)

La oss generalisere til et vilkårlig antall ligninger

La $m_1, m_2, \dots m_r$ være parvis relativt primiske
Det vil si at $m_i \perp m_j$ når $i \neq j$

La så $m = m_1 \cdot m_2 \cdot \dots \cdot m_r$

Da er $a \equiv b \pmod m \iff \begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \\ \vdots \\ a \equiv b \pmod{m_r} \end{cases}$

Vi ønsker å løse følgende system

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

La $M_i = \frac{M}{m_i}$ og la $k_i \equiv M_i^{-1} \pmod{m_i}$

↑ Denne eksisterer fordi $M_i \perp m_i$

Sett $x \equiv \sum_{i=1}^{r} a_i M_i k_i \pmod{M}$

Hvis vi regner modulo m_j får vi

$$x \equiv \sum_{i=1}^{r} a_i M_i k_i \equiv a_j M_j k_j \equiv a_j M_j M_j^{-1} \equiv a_j \pmod{m_j}$$

for alle $j = 1, \dots, r$

For eksempelet fra i stad får vi

$$x \equiv 1 \pmod 2$$
$$x \equiv 4 \pmod 5$$

$$x \equiv \sum_{i=1}^{r} a_i M_i k_i = {}_1M_1k_1 = a_2M_2k_2 \pmod M$$

Vi har $a_1 = 1$, $a_2 = 4$, $m_1 = 2$, $m_2 = 5$

Det gir

$$M = 2 \cdot 5 = 10$$
$$M_1 = \frac{10}{2} = 5$$
$$M_2 = \frac{10}{5} = 2$$

Videre skal vi ha k_1 slik at $k_1 \cdot M_1 \equiv 1 \pmod{m_1}$

$$k_1 \cdot 5 \equiv 1 \pmod 2$$

$$\Rightarrow \boxed{k_1 = 1}$$

Og vi skal ha $k_2 \cdot M_2 \equiv 1 \pmod 5$

$$k_2 \cdot 2 \equiv 1 \pmod 5$$

$$\Rightarrow \boxed{k_2 = 3}$$

Til sammen får vi

$$x = a_1M_1k_1 + a_2M_2k_2 = 1 \cdot 5 \cdot 1 + 4 \cdot 2 \cdot 3$$
$$= 29 \equiv 9 \pmod{10}$$

↑ Samme som i sted!

Hva om m_i-ene <u>ikke</u> er parvis relativt primiske?

↳ Det <u>kan</u> finnes en løsning, men ikke nødvendigvis

↳ Mer om dette i ØF!

Ekvivalensklasser (Antonsen kap 17)

La oss definere en relasjon $\equiv_m$ som er slik at $a \equiv_m b$ hvis og bare hvis $a \equiv b \pmod m$

Da har vi

- $\equiv_m$ er refleksiv: $a \equiv a \pmod m$
- $\equiv_m$ er symmetrisk:
  $a \equiv b \pmod m \iff b \equiv a \pmod m$
- $\equiv_m$ er transitiv
  $a \equiv b \pmod m$, $b \equiv c \pmod m$ $\} \Rightarrow a \equiv c \pmod m$

Så $\equiv_m$ er en <u>ekvivalensrelasjon</u>!

Dette lar oss definere <u>ekvivalensklasser</u>

$$[a]_m = \{b \mid b \equiv_m a\}$$

Eksempel

$[3]_5 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$ (+5, +5)

$[0]_2 = \{$alle tall som er kongruent med 0 mod 2$\}$

$= \{a \mid a$ er et partall$\}$

Mengden av ekvivalensklasser for m kalles <u>kvotientmengden</u> og er lik $\{[a]_m \mid a \in \mathbb{Z}\}$

Denne betegnes med

$$\mathbb{Z}/\equiv_m \text{ eller } \mathbb{Z}/m\cdot\mathbb{Z} \text{ eller } \mathbb{Z}_m$$

For $m = 3$:

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$

↑ Kan tenke på denne som "heltallene modulo 3"