Forelesning 14/10

Thm 3.8 Ligningen $ax \equiv b \mod t$ har løsning hvis og bare hvis $(a,t) \mid b$

største felles divisor

$(6,2) = 2$

$(24,18) = 6$

$\vdots$

Eks 1

$\overset{a}{2}x \equiv \overset{b}{5} \mod \overset{t}{7}$

Har løsning: fordi $(2,7) = 1$.

Finner løsning v/ utprøving:

$2 \cdot 0 \equiv 0$ $2 \cdot 4 \equiv 1$

$2 \cdot 1 \equiv 2$ $2 \cdot 5 \equiv 3$

$2 \cdot 2 \equiv 4$ $\boxed{2 \cdot 6 \equiv 5} \mod 7$

Eks 2 $2x \equiv 6 \mod 10$

$(2,10) = 2$ og $2 \mid 6$ så ok!

Kan skrive alle ~~...~~ kombinasjoner opp.

- $2 \cdot 3 \equiv 6 \mod 10$
- $2 \cdot 8 \equiv 6 \mod 10$

(lekse: sjekk at dette er alle)

Eks 3 $2x \equiv 3 \mod 4$??

$2 \cdot 0 \equiv 0$

$2 \cdot 1 \equiv 2$

$2 \cdot 2 \equiv 0$

$2 \cdot 3 \equiv 2$

Ingen løsning fordi $2 \nmid 3$.

<u>Korollar</u> Anta $(a,t) = d$. Og $d|b$. Da er det nøyaktig d løsninger til $ax \equiv b \mod t$. Gitt én løsning x_0 finner vi de andre ved

$$x = x_0 + k\frac{t}{d} \quad \text{for } k = 0, \dots, d-1.$$

<u>Bevis</u> En løsning $ax \equiv b \mod t$ er det samme som at

$$ax - b = yt \text{ for } y \in \mathbb{Z}.$$

$$\Leftrightarrow \quad ax - yt = b.$$

Gitt én løsning av en slik er, så er de andre gitt ved

$$x_0 + k\frac{t}{d} \quad \text{og} \quad y_0 + k\frac{a}{d} \quad \text{for } k \in \mathbb{Z}$$

Dette gir d forskjellige løsninger siden

$$x_0 + (k+d)\frac{t}{d} = x_0 + k\frac{t}{d} + d\frac{t}{d} = x_0 + k\frac{t}{d} + t$$

Så modulo t er $x_0 + (k+d)\frac{t}{d} \equiv x_0 + k\frac{t}{d}$,

så vi får d forskjellige løsninger. $\blacksquare$

Eks $\quad 9x \equiv 6 \mod 24 \quad$ Løs denne.

$(9,24) = 3$

$3^2 \quad 3\cdot 2^3$

Denne skal ha $\underline{3}$ løsninger.

Bruk Euklids algoritme på 9 og 24.

$$24 : 9 = 2$$
$$\frac{18}{6}$$

Så $24 = 2\cdot 9 + 6$

$-2\cdot 9 + 24 = 6$

Så mod 24 er $\boxed{9(-2) \equiv 6 \mod 24}$

Vi har at $-2 \equiv 22 \mod 24$. Så en løsning er $x_0 = 22$.

Da er de andre gitt v/ $22 + k\frac{24}{3} = 22 + 8k$ for $k = 0,1,2$

Så $22,\ \underset{30 \mod 24}{\overset{}{6}}$ og $14 \mod 24$.

$6 \equiv 30 \mod 24$

□

Eks 2 $\qquad 11x \equiv 3 \mod 37$ Denne skal ha én løsning.

$37 : 11 = 3 \qquad 37 = 3\cdot 11 + 4$

$\underline{33}$

4

$11 : 4 = 2 \qquad 11 = 2\cdot 4 + 3$ ✓ samme m/ 11 og 4.

$\underline{8}$

$3 \qquad 4 = 1\cdot 3 + 1$ ✓

og $4 : 3 = 1$ Så $1 = 4 - 1\cdot 3$

$\underline{3}$

1

$$= 4 - (11 - 2\cdot 4)$$
$$= 3\cdot 4 - 1\cdot 11$$
$$= 3\cdot(37 - 3\cdot 11) - 1\cdot 11$$
$$= 3\cdot 37 - 9\cdot 11 - 1\cdot 11 = 3\cdot 37 - 10\cdot 11$$

inversen til 11 modulo 37

Så modulo 37 er $1 \equiv (-10)\cdot 11 \mod 37$

ganger m/ 3 på begge sider: $3 \equiv (-30)\cdot 11 \mod 37$, men $-30 \equiv 7 \mod 37$

Så løsningen er $x_0 = 7$.

Merknad: Spesialtilfelle av $ax \equiv b \mod r$ er $ax \equiv 1 \mod r$. Løsning bare hvis a og r ikke har noen felles faktorer. Kaller løsningen for a^{-1}.

„inversen til a"

Strategi for å løse $ax \equiv b \mod t$.

① Bruk Euklid / deling til å skrive (a,t) som lineærkombinasjon av a og t.

Til å få $ax + ct = (a,t)$

② Ta modulo t og få

$$ax \equiv (a,t) \mod t$$

③ Gang m/ passende konstant for å finne løsningen.

Kap. 4: Fermat, Wilson osv.

Fermat's lille Teorem

La p være primtall og $a \not\equiv 0 \mod p$. Da er

$$\boxed{a^{p-1} \equiv 1 \mod p}$$

Bf Se på mengden $\{1, 2, 3, \dots, p-1\}$ i $\mathbb{Z}/(t)$

Gang alle med a. $\{1\cdot a, 2\cdot a, 3\cdot a, \dots, (p-1)a\}$

Så ta produktet

$$1\cdot 2\cdot 3 \cdots (p-1) \equiv 1a \cdot 2a \cdot 3a \cdots (p-1)\cdot a$$

$$\equiv a^{p-1}\, 1\cdot 2\cdot 3 \cdots (p-1)$$

Så v/ å dele på begge sider er $a^{p-1} \equiv 1 \mod p$.

$3a \equiv 6 \mod T$

Har én løsning

Merk hvis $p \nmid a$

$ab \equiv ac \mod p$

gir $a(b-c) \equiv 0 \mod p$

så $b - c \equiv 0 \mod p$

siden $p \nmid a$ så $b \equiv c \mod p$.

https://www.youtube.com/watch?v=XPMzosLWGHo

Pent bevis av Fermats lille

Korollar $a^p \equiv a \mod p$ for alle $a \in \mathbb{Z}/p$.

Bevis Om $a \equiv 0 \mod p$ ok.

Om $a \not\equiv 0 \mod p \Rightarrow a^{p-1} \equiv 1 \mod p$

gang m/a $\Rightarrow a^p \equiv a \mod p$.

Eks 1 $n \nmid 13$. Vis at $7n^{12} + 6 \mid 13$.

Anta

Vi har v/ Fermat at $7 \cdot n^{12} + 6 \equiv 7 \cdot 1 + 6 \equiv 13 \equiv 0 \mod 13$.

Så $7n^{12} + 6 \mid 13$.

Eks 2 Regn ut $7^{1000} \mod 13$.

$76 = 5 \cdot 13 + 11$

$1000 = 76 \cdot 13 + 12$

$$7^{1000} \equiv (7^{13})^{76} 7^{12} \equiv 7^{76} \cdot 7^{12} \equiv 7^{76} \equiv (7^{13})^5 7^{11} \equiv 7^5 7^{11}$$

Potensregler

Korollar

Fermats lille

$\equiv 7^{12} 7^4 \equiv 7^4$

$\equiv 49 \cdot 49 \equiv 10 \cdot 10$

$\equiv (-3) \cdot (-3) \equiv 9 \mod 13.$

okt 14-15:15

Mye går galt om p ikke er primtall.

Eks $2^4 \equiv 0 \mod 4$

Så $2^4 \not\equiv 2 \mod 4$ ← 4 ikke primtall

Vi trenger Eulers ϕ-funksjon $\phi: \mathbb{N} \to \mathbb{N}$

$$\phi(n) = \#\{m \in \mathbb{N} \mid m \leq n \text{ og } (m,n) = 1\}$$

Eks $\phi(6) = \#\{1,5\} = 2$

$\phi(10) = \#\{1,3,7,9\} = 4$

$\phi(7) = \#\{1,2,3,4,5,6\} = 6$

$\phi(p) = p-1$

$\phi(pq) = (p-1)(q-1)$

Eulers teorem Anta at $(a,t) = 1$. (ikke har noen felles faktorer)

Da er $a^{\phi(t)} \equiv 1 \mod t$.

Bevis Nesten samme. La $\{a_1, a_2, \ldots, a_{\phi(t)}\}$ være alle tall $\leq t$ med ingen faktorer felles m/ t.

Siden $(a,t) = 1$ kan vi gange m/ a:

$\{a_1 a, a_2 a, \ldots, a_{\phi(t)} a\}$.

Har de samme elementene, bare stokket om (fordi $ax \equiv b \mod t$ har én løsning)

Så vi får $a_1 a_2 \cdots a_{\phi(t)} \equiv a^{\phi(t)} a_1 \cdots a_{\phi(t)} \mod t$.

Kan dele på a_i siden de ikke har noen felles faktor m/ t.

$1 \equiv a^{\phi(t)} \mod t$.

Eks $5^{\phi(6)} \equiv 5^2 \equiv 25 \equiv 1 \mod 6$. ok

Wilsons teorem $(p-1)! \equiv -1 \mod p$

for p primtall.

Eksempel $p=5$

$1 \cdot 2 \cdot 3 \cdot 4 = 24 \equiv -1 \mod 5$

Pf observasjon ligningen $x^2 \equiv 1 \mod p$

har kun ± 1 som løsninger fordi

$$x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \mod p$$

så enten $x-1 \mid p$ eller $x+1 \mid p$. Så x er $pk+1$ eller $pk-1$ for en $k \in \mathbb{Z}$.

Altså $x \equiv \pm 1 \mod p$.

Med andre ord: de eneste tallene my seg selv som inverse $(x \cdot x \equiv 1 \mod p)$ er ± 1.

Så kan gruppere tallene $\{1, -1, 2, 3, \ldots, p-2\}$ fordi $p-1 \equiv -1 \mod p$

i grupper på to: $\{x_1, x_1^{-1}\} \cup \{x_2, x_2^{-1}\} \cup \ldots \cup \{x_{\frac{p-3}{2}}, x_{\frac{p-3}{2}}^{-1}\} \cup \{1\} \cup \{-1\}$

Ganger sammen: $x_1 \cdot x_1^{-1} \cdot x_2 \cdot x_2^{-1} \cdot \ldots \cdot 1 \cdot -1 = 1 \cdot 1 \cdot \ldots \cdot 1 \cdot 1 \cdot (-1)$

$= -1 \mod p$. ∎

For $p=5$, hva er 2^{-1}?

$2x \equiv 1 \mod 5$ så siden $2 \cdot 3 = 6 \equiv 1 \mod 5$

er $2^{-1} \equiv 3 \mod 5$

2^{-1}

$\{1\} \cup \{-1\} \cup \{2, 3\}$

$\{-1\} = \{4\}$

$p = 7$ $\{1\} \cup \{-1\} \cup \{2, 4\} \cup \{3, 5\} \mod 7$

$-1 = 6$

$(7-1)! = 1 \cdot -1 \cdot 2 \cdot 4 \cdot 3 \cdot 5 = -1$

Inversen til a $\boxed{ax = 1 \mod p}$ har unik løsning hvis $(a, p) = 1$.

er gitt v.