Notater for forelesning 21/10

Minner om (fra tirsdag):

$$ax \equiv b \,(mod\, n)$$

har løsninger hvis og bare hvis $d = gcd(a, n)|b$. I så fall er det d forskjellige løsninger modulo n. Det kan også formuleres som at det finnes en entydig løsning modulo $\frac{n}{d}$. Hvis $x \equiv x_0 \,(mod\, n)$ er en løsning, er alle løsninger gitt ved $x_0, x_0+\frac{n}{d}, x_0+2\frac{n}{d}, \cdots, x_0+(d-1)\frac{n}{d}$

Den første løsningen kan finnes fra Euklids algoritme. I de likningstypene vi skal se på i dag, vil denne typen likning alltid inngå i utregningen, så vi bør ha dette i bakhodet. Spesielt bør vi huske at det finnes en entydig løsning modulo n dersom $d = 1$.

Teorem 0.1 (Det kinesiske restteoremet)**.** *La $n_1, \cdots, n_r$ være parvis koprimiske heltall, $a_1, \cdots, a_r$ vilkårlige heltall. Da har de simultane (samtidige) likningene*

$$\begin{aligned} x &\equiv a_1 \quad (mod\, n_1) \\ x &\equiv a_2 \quad (mod\, n_2) \\ &\vdots \\ x &\equiv a_r \quad (mod\, n_r) \end{aligned}$$

en løsning, entydig modulo $N = n_1 n_2 \cdots n_r$.

La oss se på beviset i tilfellet $r = 3$; hvis dere forstår dette vil dere også forstå det generelle beviset. Vi har altså tall n_1, n_2, n_3 med $gcd(n_1, n_2) = gcd(n_1, n_3) = gcd(n_2, n_3) = 1$. Se på tallet $N_1 = \frac{N}{n_1} = n_2 n_3$. Vi har $gcd(n_1, N_1) = 1$. Derfor kan vi løse likningen

$$N_1 x \equiv 1 \,(mod\, n_1)$$

og løsningen er entydig modulo n_1. Kall løsningen x_1. På samme måte finner vi at, med $N_2 = \frac{N}{n_2} = n_1 n_3$ ha vi en entydig løsning x_2 modulo n_2 av likningen $N_2 x \equiv 1 \,(mod\, n_2)$. $N_3 = \frac{N}{n_3} = n_1 n_2$ er koprimisk til n_3, og x_3 er den entydige løsningen, modulo n_3, til $N_3 x \equiv 1 \,(mod\, n_3)$. Hold tungen rett i munnen! Det er mange tall i omløp nå. Definer

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$$

Dette gir en løsning av systemet: se først på hva som skjer modulo n_1. Vi har at $N_1 x_1 \equiv 1 \,(mod\, n_1)$, at $N_2 = n_1 n_3 \equiv 0 \,(mod\, n_1)$ og at $N_3 = n_1 n_2 \equiv 0 \,(mod\, n_1)$. Derfor er

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \equiv a_1.1 + a_2.0 + a_3.0 \equiv a_1 \,(mod\, n_1)$$

så den første likningen holder. Modulo n_2 er $N_2 x_2$ kongruent med 1, mens N_1 og N_3 er kongruent med 0, så

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \equiv a_1.0 + a_2.1 + a_3.0 \equiv a_2 \,(mod\, n_2)$$

Til slutt:

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \equiv a_1.0 + a_2.0 + a_3.1 \equiv a_3 \,(mod\, n_3)$$

Dermed løser x alle tre likningene.

For entydigheten modulo N, se boken.

Merk at vi her måtte løse tre hjelpelikninger av typen $ax \equiv b \,(mod\, n)$.

Vi skal også se på to likninger med to ukjente, men med samme modulus:

Teorem 0.2. *La $n \geq 2$ være et helt tall, a, b, c, d, r, s vilkårlige heltall. Se på likningssystemet*

$$ax + by \equiv r \,(mod\, n)$$
$$cx + dy \equiv s \,(mod\, n)$$

Om $gcd(ad - bc, n) = 1$ har dette en entydig løsning modulo n.

For de som har vært borti lineær algebra, er $ad - bc$ determinanten til likningssystemet.

For å finne x vil vi kvitte oss med y. Hvis vi ganger den øverste likningen med d og den nederste med b, vil det stå det samme foran y både oppe og nede:

$$adx + bdy \equiv rd \,(mod\, n)$$
$$bcx + bdy \equiv bs \,(mod\, n)$$

Vi kan derfor ta den øverste og trekke fra den nederste; da vil y-leddene oppheve hverandre:

$$adx - bcx \equiv rd - bs \,(mod\, n)$$

Venstresiden er $(ad - bc)x$, og siden $gcd(ad - bc, n) = 1$ har vi en entydig løsning av likningen modulo n.

Tilsvarende kan vi eliminere x ved å gange den øverste likningen med c, og den nederste med a:

$$acx + bcy \equiv cr \,(mod\, n)$$
$$acx + ady \equiv as \,(mod\, n)$$

Om vi så tar den nederste, og trekker fra den øverste, vil x-leddene falle bort, og vi står igjen med

$$ady - bcy \equiv as - cr \,(mod\, n)$$

Venstresiden er $(ad-bc)y$, og siden $gcd(ad-bc,n)=1$ har vi en entydig løsning modulo n også for y.

Merk at vi her trenger å løse to hjelpelikninger av typen $ax \equiv b\,(mod\,n)$. Merk også at vi ikke sier noenting om mulige løsninger når $gcd(ad-bc,n) \neq 1$.

Norske personnummer beregnes ved å løse to likninger med to ukjente modulo 11. Et personnummer er bygget opp som følger: de seks første sifrene viser fødselsdato: ddmmåå. En person som er født 2.juli 1903 vil da ha 020703 som sine seks første sifre. De neste tre sifrene er tildelte sifre, med forholdsvis lite meningsinnhold. De to siste sifrene er kontrollsifre; det er beregningen av disse som er vårt hovedanliggende. Notasjon: skriv et personnumer som

$$d_{10}d_1\, m_{10}m_1\, a_{10}a_1\, n_{100}n_{10}n_1\, xy$$

La

$$\begin{aligned} r &= 3d_{10}+7d_1+6m_{10}+1m_1+8a_{10}+9a_1+4n_{100}+5n_{10}+2n_1 \\ s &= 5d_{10}+4d_1+3m_{10}+2m_1+7a_{10}+6a_1+5n_{100}+4n_{10}+3n_1. \end{aligned}$$

Da er de to kontrollsifrene x og y definert som løsningene til

$$\begin{aligned} 10x &\equiv r\,(mod\,11) \\ 9x+10y &\equiv s\,(mod\,11) \end{aligned}$$

Siden $ad-bc = 10.10-0.9 \equiv 1\,(mod\,11)$, har dette alltid en entydig løsning. Det blir kanskje litt enklere å se på likningene med negative tall, siden vi jobber modulo 11 er et ekvivalent system

$$\begin{aligned} -x &\equiv r\,(mod\,11) \\ -2x-y &\equiv s\,(mod\,11) \end{aligned}$$

Hvis løsningen gir at x eller y blir 10, må personnummeret forkastes.

Eksempel. Kong Olav ble født 2. juli 1903. Det kan være naturlig å velge 005 som de neste tre sifrene, siden han var den femte kong Olav av Norge. Dermed er personnummeret $020703005xy$. Vi ser da at

$$r = 58,\ \ s = 55$$

og vi skal løse

$$\begin{aligned} -x &\equiv 58\,(mod\,11) \\ -2x-y &\equiv 55\,(mod\,11) \end{aligned}$$

Fra den øverste ser vi direkte at $x \equiv -58 \equiv 8\,(mod\,11)$, og vi finner da av den nederste at $y \equiv -55-2x \equiv -55-16 \equiv 6\,(mod\,11)$. Siden begge tallene er $\neq 10$, er altså 02070300586 et gyldig personnummer.

For en beskrivelse av bakgrunnen for dette systemet, se Ernst S. Selmer: "Personnummerering i Norge: Litt anvendet tallteori og psykologi", Nordisk matematisk

tidsskrift 12, 1964, side 36-44.

Jon Eivind Vatne