Notater for forelesning 18/10

Nå begynner vi på likningsteorien for kongruenser. Den enkleste typen er

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

Her er $n \geq 2$, a og b hele tall. Det finnes 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 ene løsningen kan finnes fra Euklids algoritme, som i dette eksemplet: $9x \equiv 6 \,(mod\, 24)$. Euklids algoritme brukt på 24 og 9 gir

$$24 = 2.9 + 6,\ 9 = 1.6 + 3,\ 6 = 2.3 + 0$$

Dermed er $gcd(24, 9) = 3$, som deler $6 = 2.3$. Som vanlig går vi baklengs gjennom algoritmen, og finner

$$3 = 9 - 6 = 9 - (24 - 2.9) = 3.9 - 1.24$$

Den foreløpige konklusjonen er at

$$9.3 \equiv 3 \,(mod\, 24)$$

Vi ganger så med $2 = \frac{6}{3}$ og ser at

$$9.6 \equiv 6 \,(mod\, 24)$$

så $x_0 \equiv 6$ (prøve: $9.6 = 54 = 2.24 + 6$ OK.). De andre $d - 1 = 2$ løsningene får vi ved å legge til $24/3 = 8$ og $2.24/3 = 16$, så hele løsningsmengden er

$$x \equiv 6,\ x \equiv 14,\ x \equiv 22 \,(mod\, 24)$$

Eventuelt kan vi si at løsningene er gitt ved

$$x \equiv 6 \,(mod\, 8)$$

I den spesielle situasjonen at $n = p$ er et primtall, kan vi løse $ax \equiv b \,(mod\, p)$ entydig så sant $a \not\equiv 0 \,(mod\, p)$. Dette utnyttes f.eks. i ISBN-nummer. Disse tallene er gitt modulo 11, som er et primtall. Lærebokens ISBN-nummer er 0071243259. Her er alle sifrene unntatt det siste valgt for å identifisere boken (land, forlag og boknummer ligger innbakt.), mens det siste sifferet er et *kontrollsiffer*. Det beregnes på denne måten: ta de ni første sifrene, og gang dem med $1, 2, 3, \cdots, 9$, og legg sammen resultatet.

$$1.0 + 2.0 + 3.7 + 4.1 + 5.2 + 6.4 + 7.3 + 8.2 + 9.5 = 141$$

Løs så ligningen

$$10x = -141 \,(mod 11)$$

Her kan vi faktisk forenkle litt, siden $10 \equiv -1 \, (mod \, 11)$:

$$x \equiv 141 \equiv 9 \, (mod \, 11)$$

Så kontrollsifferet er 9. Siden 11 er et primtall, har dette alltid en entydig løsning, og kontrollsifferet kan alltid beregnes entydig. Resultatet blir at i det endelige ISBN-nummeret, hvis vi ganger sifrene med tallene $1, 2, 3, \cdots, 9, 10$ henholdsvis, så kan svaret deles på 11.

Det hender at den entydige løsningen er 10, f.eks. om de første sifrene er 080213467 (Conversations with Pinter / Mel Gussow. - New York : Grove Press , 1996) blir kontrolsifferet 10; dette skrives x. Bokens fullstendige ISBN-nummer er derfor $080213467X$.

Vi kunne også forklart de norske personnumrene nå, men det virker mer naturlig å ta det på fredag (i forbindelse med to likninger med to ukjente).

Jon Eivind Vatne