Notater for forelesning 14/10

Vi så sist at vi kan plusse og gange, men ikke dele når vi holder på med kongruensregning. I dag skal vi først se på hvilke ekstra betingelser vi trenger for å kunne dele. I vanlige tall er den eneste restriksjonen at vi ikke kan dele på null. I kongruensregningen kan vi heller ikke dele på null, men det er flere betingelser. Når vi holder på med divisjon av heltall, er en måte å se på det å dele på et tall at følgende holder: om $ca = cb$, og $c \neq 0$, så er $a = b$. Vi sier at vi kan *forkorte* c på begge sider av likhetstegnet; denne egenskapen kan vi undersøke også for kongruensregningen.

Teorem 0.1. *Om* $ca \equiv cb \,(mod\, n)$ *er* $a \equiv b \,(mod\, n/d)$, *der* $d = gcd(c, n)$.
Særskilt har vi: Om $ca \equiv cb \,(mod\, n)$ *og* $gcd(c, n) = 1$ *er* $a \equiv b \,(mod\, n)$.
Hvis $n = p$ *er et primtall, er kravet* $ca \equiv cb \,(mod\, p)$ *og* $p \not| c$ *gir* $a \equiv b \,(mod\, p)$.

Beviset er ganske greit, og vi vil følge boken tett (side 67-68).

Neste tema er delbarhetstester, som er en anvendelse av teorien. F.eks. er et tall delelig på 3 hvis og bare hvis tverrsummen av tallet er delelig på 3. 213452151 har tverrsum $1 + 2 + 3 + 4 + 5 + 2 + 1 + 5 + 1 = 24 = 8.3$, og kan derfor deles på 3. Vi kommer frem til enkle kriterier for deling på $2, 3, 4, 5, 9, 11, 25$, og kanskje litt mer kompliserte for deling på $7, 13$.

Det viktigste hjelperesultatet er at vi kan evaluere polynomer i kongruensregningen, det vil si:

Lemma 0.2. *La* $P(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ *være et polynom med heltallige koeffisienter (dvs. at alle* a_i *er hele tall). Om* $a \equiv b \,(mod\, n)$ *så er også* $P(a) \equiv P(b) \,(mod\, n)$.

Hvordan kan vi bruke dette? La oss tenke på å dele med 3 igjen. Siden $10 = 3.3 + 1$ er $10 \equiv 1 \,(mod\, 3)$, og derfor er også $10^2 \equiv 1^2 \equiv 1 \,(mod\, 3)$, og generelt $10^t \equiv 1 \,(mod\, 3)$. Men et tall abcd (med fire siffer, a, b, c, d er tall større enn eller lik null og mindre enn ti) er en forkortelse for $a1000 + b100 + c10 + d$. Modulo 3 er dette derfor

$$a1000 + b100 + c10 + d \equiv a.1 + b.1 + c.1 + d.1 \equiv a + b + c + d \,(mod\, 3)$$

Vi får dermed et marginalt sterkere resultat: et tall har samme rest som sin tverrsum når det deles på 3. Lignende resonnementer vil gi tester for delbarhet på andre tall.

Oppgave: Sjekk om hvert tall du ser i dag (f.eks. på bilers registreringsskilter) er delelig på 3!

Jon Eivind Vatne