# Notater for forelesning 28/10

Vi har to temaer i dag; Wilsons teorem og Eulers $\phi-$funksjon. Den greske bokstaven $\phi$ uttales "fi".

**Teorem 0.1** (Wilson)**.** *La $p$ være et primtall. Da er*

$$(p-1)! \equiv -1 \,(mod\, p)$$

Dette er et interessant resultat i seg selv, men det viktigste for oss er at beviset ligner veldig på beviset for Fermats teorem (og Eulers teorem, som vi kommer til neste gang). Å se flere bevis med samme grunntanke bør være med å hjelpe på forståelsen av teknikkene.

Beviset står godt forklart i boken, la meg her bare forklare hvordan tankegangen vil være i tilfellet $p = 7$. Da skal vi altså vise at $1.2.3.4.5.6 \equiv -1 \,(mod\, 7)$. Men

$$\begin{aligned} 2.4 &\equiv 8 \equiv 1 \,(mod\, 7 \\ 3.5 &\equiv 15 \equiv 1 \,(mod\, 7) \\ 6 &\equiv -1 \,(mod\, 7) \end{aligned}$$

Derfor er

$$1.2.3.4.5.6 \equiv (2.4).(3.5).6 \equiv 1.1.(-1) \equiv 1 \,(mod\, 7)$$

En interessant konsekvens av Wilsons teorem er at likningen $x^2 \equiv -1 \,(mod\, p)$, for $p$ et odde primtall, har løsning hvis og bare hvis $p \equiv 1 \,(mod\, 4)$.

Eulers $\phi$-funksjon er definert på heltallene $\geq 1$ ved at $\phi(n) =$ antall tall $a$ slik at $1 \leq a \leq n$ og $gcd(a, n) = 1$. F.eks. er

$$\begin{array}{llll} \phi(1) = 1 & \phi(2) = 1 & \phi(3) = 2 & \phi(4) = 2 \\ \phi(5) = 4 & \phi(6) = 2 & \phi(30) = 8 & \phi(100) = 40 \end{array}$$

Denne funksjonen kan beregnes dersom vi klarer å faktorisere $n$, for vi har dette teoremet:

**Teorem 0.2** (Beregning av $\phi(n)$)**.** *La $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} > 1$. Da er*

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

F.eks. er, for $n = 64144128 = 2^8.3.17^4$,

$$\phi(2^8.3.17^4) = (2^8 - 2^7)(3^1 - 3^0)(17^4 - 17^3) = 128.2.78608 = 20123648$$

Vi kommer til å følge beviset i boken. Det vanskelige punktet er å vise at om to tall $m$ og $n$ er slik at $gcd(m, n) = 1$, så er $\phi(mn) = \phi(m)\phi(n)$ (det betyr at $\phi$ er en *multiplikativ funksjon*). I resonnementet for denne egenskapen vil vi utføre omtrent det samme som vi gjorde i første del av beviset for Fermats teorem, nemlig vise at en mengde på $n$ hele tall, som er inkongruente modulo $n$, som mengde er kongruent til mengden av tall $\{0, 1, 2, 3, \cdots, n-1\}$. Derfor vil det måtte være nøyaktig $\phi(n)$

blant dem som er relativt primiske til $n$, siden det per definisjon er så mange blant $\{0, 1, 2, 3, \cdots, n-1\}$ som er det.

Jon Eivind Vatne