Notater for forelesning 1/11

Hsuk at vi sist definerte Eulers ϕ-funksjon ved at $\phi(n)$ = antall tall a slik at $1 \leq a \leq n$ og $gcd(a, n) = 1$.

Om n er faktorisert så vi at vi kan beregne $\phi(n)$:

Teorem 0.1 (Beregning av $\phi(n)$)**.** *La $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} > 1$. Da er*

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

Jeg minner også om Fermats teorem:

Teorem 0.2 (Fermat)**.** *Om p er et primtall, og a et heltall slik at $p \not| a$, er*

$$a^{p-1} \equiv 1 \, (mod \, p)$$

Vi skal i dag se på Eulers generalisering av dette resultatet:

Teorem 0.3 (Euler)**.** *La $n \geq 1$ være et heltall, a et heltall med $gcd(a, n) = 1$. Da er*

$$a^{\phi(n)} \equiv 1 \, (mod \, n)$$

Beviset går som følger: Siden $gcd(a, n) = 1$ ser vi at om a ganges med alle tallene lavere enn n, som er relativt primiske til n, vil resultatet bli en samling av $\phi(n)$ tall som er kongruente til de samme $\phi(n)$ tallene. Dermed får vi samme produkt modulo n, og om vi så forkorter alt bortsett fra de $\phi(n)$ kopiene av a, står vi igjen med resultatet.

Fermats teorem er spesialtilfellet $n = p$ er et primtall.

Som en pussig konsekvens, nærmest et lite stykke kuriosa, kan vi nevne at om et tall er relativt primisk til 10 (altså et oddetall som ikke kan deles på 5), så vil tallet dele et tall skrevet med kun enere.

Jon Eivind Vatne