Notater for forelesning 25/10

I dag dreier det seg om Fermats (lille) teorem. La oss begynne med utsagnet:

Teorem 0.1 (Fermat)**.** *La p være et primtall, a et heltall slik at $p \not| a$. Da er*

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

F.eks. er $3^6 \equiv 729 \equiv 1 \, (mod \, 7)$; det kan vi lett sjekke direkte ($729 = 104.7 + 1$).

Hvis $p|a$, er $a \equiv 0 \, (mod \, p)$. Hvis vi kombinerer dette med tilfellet $p \not| a$ fra teoremet (og ganger med a på begge sider av kongruenstegnet) får vi at $a^p \equiv a \, (mod \, p)$ for alle tall a.

Et annet poeng som dukker opp i dette avsnittet, som det er vel verdt å legge merke til, er et delingsresultat for binomialkoeffisienter. Om p er et primtall, og $1 \leq k \leq p-1$, har vi at $p|\binom{p}{k}$. F.eks. vil $7|\binom{7}{4} = 35$. Dette er ikke sant for tall som ikke er primtall, f.eks. $4 \not| \binom{4}{2} = 6$.

Tall som tilfredsstiller egenskaper "nær" konklusjonen i Fermats teorem, kalles pseudoprimtall. Dette står godt forklart i boken. Spesielt finnes det tall n, f.eks. 1729, som er slik at $a^n \equiv a \, (mod \, n)$ for alle tall a, uten at n er et primtall.

Jon Eivind Vatne