Notater for forelesning 8/11

Dagens forelesning er ved Thomas Gregersen, som har sagt seg villig til å dekke for meg mens jeg lever livet på konferanse i kongens by (København).

Vi starter med å repetere to definisjoner fra sist:

Definisjon 0.1. La $n > 1$ være et heltall, og a et tall med $gcd(a, n) = 1$. Da definerer vi *as orden* modulo n som det minste tallet $k \geq 1$ slik at $a^k \equiv 1 \, (mod \, n)$.

Definisjon 0.2. Vi sier at a er en *primitiv rot* modulo n dersom ordenen til a er $\phi(n)$.

Målet i dag er å vise følgende teorem:

Teorem 0.3. *La p være et primtall. Da finnes det en primitiv rot modulo p.*

Mer presist får vi ut at det finnes $\phi(p-1)$ forskjellige primitive røtter modulo p. For å finne dette resultatet, trenger vi noen hjelperesultater. Det første er svært interessant i seg selv, og sier at polynomer i kongruensteori modulo primtall har en viktig egenskap til felles med polynomer over de reelle tallene:

Teorem 0.4. *La $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ være et polynom med heltallige koeffisienter, og la p være et primtall. Anta $a_n \not\equiv 0 \, (mod \, p)$. Da har likningen*

$$f(x) \equiv 0 \, (mod \, p)$$

høyst n forskjellige løsninger modulo p.

Dette er ikke sant om vi arbeider modulo et tall som ikke er et primtall. F.eks. har $x^2 - 1 \equiv 0 \, (mod \, 12)$ de fire løsningene $1, 5, 7, 11$.

Videre skal vi se at $x^d - 1 \equiv 0 \, (mod \, p)$, der $d | p-1$, har nøyaktig d løsninger, og så at det er nøyaktig $\phi(d)$ forskjellige tall modulo p som har orden akkurat d modulo p. Da blir vårt hovedresultat tilfellet $d = p - 1$ av dette utsagnet.

Jon Eivind Vatne