Notater for forelesning 4/11

Fra bokens avsnitt 7.4 har vi bare med det første resultatet, nemlig

Teorem 0.1 (Gauss). *La $n \geq 1$ være et heltall. Da er*

$$n = \sum_{d|n} \phi(d)$$

Dette betyr altså at n er summen av $\phi(d)$, der d gjennomløper alle divisorene til n. F.eks. er

$$14 = 6 + 6 + 1 + 1 = \phi(14) + \phi(7) + \phi(2) + \phi(1)$$

Beviset står fint forklart i boken, og gjennomgås på forelesning.

Neste tema er *ordenen* til et tall modulo et tall. Vi vet at $a^{\phi(n)} \equiv 1\,(mod\,n)$, når $gcd(a,n) = 1$. Men det kan også godt hende at $a^k \equiv 1\,(mod\,n)$ for et tall k som er mindre enn $\phi(n)$. F.eks. er $7^2 \equiv 1\,(mod\,12)$, mens $\phi(12) = 4$.

Definisjon 0.2. 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 $a^k \equiv 1\,(mod\,n)$.

Så 7s orden modulo 12 er 2. Merk at det virkelig er nødvendig å kreve $gcd(a,n) = 1$ her. Siden $1 \equiv a^k \equiv a.a^{k-1}\,(mod\,n)$, finnes det en løsning til $ax \equiv 1\,(mod\,n)$. Vi vet at en slik løsning finnes hvis og bare hvis $gcd(a,n)|1$, som er ekvivalent med $gcd(a,n) = 1$. Merk også at siden $\phi(n)$ er et positivt tall med $a^{\phi(n)} \equiv 1\,(mod\,n)$, så finnes det et minste tall k med denne egenskapen (velordningsprinsippet).

Vi har noen interessante egenskaper med dette begrepet:

Teorem 0.3. *La a være et tall med orden k modulo n. Da har vi*

i) $a^h \equiv 1\,(mod\,n)$ *hvis og bare hvis* $k|h$.
ii) $k|\phi(n)$
iii) $a^i \equiv a^j\,(mod\,n)$ *hvis og bare hvis* $i \equiv j\,(mod\,k)$.
iv) $a, a^2, a^3, \cdots, a^k$ *er inkongruente modulo* n.
v) *Ordenen til* a^h *modulo* n *er* $k/gcd(k,h)$

Definisjon 0.4. Vi sier at a er en *primitiv rot* modulo n dersom ordenen til a er $\phi(n)$.

I så fall er alle tall som er relativt primiske til n kongruente med en potens av a. Multiplikasjon av slike tall modulo n kan derfor beskrives ved hjelp av addisjon modulo $\phi(n)$ (i eksponentene til a). F.eks. er $\phi(14) = 6$, og tallene $3, 3^2 \equiv 9, 3^3 \equiv 13, 3^4 \equiv 11, 3^5 \equiv 5, 3^6 \equiv 1\,(mod\,14)$ er alle restene modulo 14 som er relativt primiske til 14. Så 3 er en primitiv rot modulo 14. Derfor ser vi at $11.5 \equiv 3^4.3^5 \equiv 3^{4+5} \equiv 3^3 \equiv 13\,(mod\,14)$. Uformelt kan vi si at en primitiv rot gir oss en metode for å regne "logaritmisk" modulo n.

Primitive røtter finnes ikke alltid: f.eks. er $\phi(12) = 4$, men $1, 5, 7, 11$ har orden $1, 2, 2, 2$ henholdsvis, så det finnes ingen primitiv rot modulo 12. Derimot vil vi se på tirsdag at det alltid finnes en primitiv rot modulo p, når p er et primtall. Og punkt v) i teoremet gir spesielt at om det finnes en primitiv rot a, så vil a^h være en ny primitiv rot dersom $gcd(h, \phi(n)) = 1$, så vi vet hvor mange som finnes om det først finnes en.

Jon Eivind Vatne