Notater for forelesning 20/9

Vi skal nå begynne å studere primtall. Det viktigste resultatet er det såkalte *fundamentalteoremet*.

Teorem 0.1 (Aritmetikkens fundamentalteorem)**.** *Ethvert heltall, større enn 1, kan skrives entydig som et produkt av primtall (opp til rekkefølgen av primtallene).*

For å gjøre det helt klart: entydigheten sier at $6 = 3.2 = 2.3$ skal betraktes som samme måte å faktorisere 6 på, det er bare rekkefølgen på primtallene som er endret.

Beviset, som blir gjennomgått på forelesning, vil følge boken. Spesielt vil vi trenge et delresultater som står i boken på side 41: hvis et primtall deler et produkt, må det dele en av faktorene.

La oss se på en konsekvens, som er et resultat vi har sett på tidligere også. Legg først merke til at vi kan ordne primfaktorene til et tall i stigende rekkefølge. Så vi kan skrive et tall som

$$a = 2^{a_2}.3^{a_3}.5^{a_5}.\cdots$$

Vi sier at tallet er skrevet på *kanonisk form*. For eksempel er $48 = 2.2.2.2.3 = 2^4.3^1.5^0.\cdots$ (alle de videre eksponentene er null). Se på et annet tall $b = 2^{b_2}.3^{b_3}.5^{b_5}.\cdots$. Da har vi

1. $ab = 2^{a_2+b_2}.3^{a_3+b_3}.5^{a_5+b_5}.\cdots$
2. $a|b$ hvis og bare hvis $a_p \leq b_p$ for alle primtall p. I så fall er $\frac{b}{a} = 2^{b_2-a_2}.3^{b_3-a_3}.5^{b_5-a_5}.$ (Hvis $a \not| b$ gir denne formelen allikevel *brøken* b/a)
3. $gcd(a,b) = 2^{min(a_2,b_2)}.3^{min(a_3,b_3)}.\cdots$
4. $lcm(a,b) = 2^{max(a_2,b_2)}.3^{max(a_3,b_3)}.\cdots$

For eksempel er $gcd(2^7.3^{232}.17^4, 2^{124}.3^4.5^7) = 2^7.3^4$ og $lcm(2^7.3^{232}.17^4, 2^{124}.3^4.5^7) = 2^{124}.3^{232}.5^7.17^4$.

Siden $a_p + b_p = min(a_p, b_p) + max(a_p, b_p)$ ser vi at vi får et enklere bevis for at

$$lcm(a,b)gcd(a,b) = ab$$

fra punktene 1,3 og 4 over. I forhold til Euklids algoritme ser vi at det er veldig enkelt å finne største felles divisor av to tall skrevet på kanonisk form. Derimot er det veldig arbeidskrevende å finne primtallsfaktoriseringen av et gitt tall, og det er derfor vi trenger Euklids algoritme.

En annen konsekvens er at vi kan bevise at forskjellige tall, for eksempel $\sqrt{2}$, ikke kan skrives som brøk.

Når vi først har fundamentalteoremet, er det neste spørsmålet hvordan man kan finne primtall, og hvordan de fordeler seg utover blant alle tall. Det første skrittet i denne retningen er å se at det finnes uendelig mange primtall:

Teorem 0.2 (Euklid)**.** *Det finnes uendelig mange forskjellige primtall.*

Beviset går ut på å anta at dette ikke er sant, og så finne en selvmotsigelse. Det står på side 47 i boken, og vil presenteres på forelesning.

I enkelte miljøer går det sport i å finne nye beviser for gamle resultater, og dette teoremet er et av de mer yndete objekter for denne sporten. Det står et bevis til i boken, vi kommer til å se på en annen variant på fredag.

Jon Eivind Vatne