Notater for forelesning 23/9

På tirsdag beviste vi

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

I dag vil vi begynne med å vise

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.

Hvordan kan man så finne disse primtallene? Et svar er *Eratosthenes' såld*. Tankegangen bak denne metoden er som følger. Hvis a, b er to tall, begge større enn $\sqrt{n}$, vil nødvendigvis $ab > \sqrt{n}\sqrt{n} = n$. Hvis vi er interessert i å sjekke om n er et primtall, er det derfor nok å lete etter faktorer mindre enn $\sqrt{n}$. For eksempel må 53 være et primtall, siden det ikke kan deles på $2, 3, 4, 5, 6, 7$ og $7 < \sqrt{53} < 8$. Det er også nok å sjekke for primtallene under $\sqrt{n}$, så for 53 sin del hadde det vært nok å se at 53 ikke kan deles på $2, 3, 5, 7$.

Hvis man vil finne alle primtallene under n, er det nok å sjekke om ting kan deles på $2, 3, 5, \cdots, p$ der p er det største primtallet under $\sqrt{n}$. Det er enklest å forstå prosedyren ved å se på et eksempel; ta $n = 100$. Skriv opp alle tallene under 100 (ikke ta med 1).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Start med det første tallet (altså 2), og fjern alle tallene som kan skrives som et multiplum av 2, men ikke 2 selv:

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

Det laveste tallet over 2 som ikke er fjernet, er 3, og vi fjerner så alle multipler av det (unntatt 3 selv) som ikke allerede er fjernet.

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

Så gjør vi det samme med 5.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

Så 7.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

Siden det ikke er noen nye tall igjen under $\sqrt{100}$, har vi fjernet alle multipler av alle primtall under $\sqrt{100}$, så alle tallene som står igjen må være primtall. Dette er altså listen over primtall under 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Med en enkel endring av tankegangen, kan vi også bruke dette for å finne primtall i et gitt intervall.

Neste spørsmål: Hvor fort vokser primtallene? Hvis vi ordner primtallene i stigende rekkefølge $p_1 < p_2 < p_3 < \cdots$, kan vi finne en begrensning på p_n? Her er for eksempel $p_1 = 2, p_2 = 3, p_3 = 5, p_{20} = 71$. Med elementære metoder kan vi bevise (vi bruker bare estimatet $p_{n+1} < p_1 p_2 \cdots p_n + 1$ som dukket opp i beviset for at det finnes uendelig mange primtall) at $p_n \leq 2^{2^{n-1}}$. Dette er et ganske grovt estimat. For eksempel sier det at

$$71 = p_{20} \leq 2^{2^{19}} = 2^{524288}$$

som er et latterlig dårlig anslag ($2 = p_1 \leq 2, 3 = p_2 \leq 4, 5 \leq 16, 7 \leq 256, 11 \leq 65536$).

I tillegg vil jeg fortelle litt om andre estimater og beregningsmetoder, som vi ikke har utviklet maskineri for å bevise, men som gir mer presis informasjon om primtallenes fordeling utover blant alle tall.

Jon Eivind Vatne