Repetisjon: høydepunkter fra første del av MA1301-tallteori.

- Matematisk induksjon
- Binomialteoremet
- Divisjonsalgoritmen
- Euklids algoritme
- Lineære diofantiske ligninger
- Aritmetikkens fundamentalteorem
- Euklid: uendelig mange primtall

La oss se tilbake på disse punktene etter tur.

Matematisk induksjon

Dette ligger i bunnen for svært mye av det vi gjør i dette kurset.

Se på et utsagn som avhenger av et positivt heltall n, f.eks. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Hvis vi kan vise at utsagnet er sant for $n = 1$, og at om det er sant for et tall $n = k$, vil det også være sant for det neste ($n = k + 1$), så er det sant for alle tall.

$n = 1$ $1 = 1.2/2$; OK

$n = k$ Anta $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

$n = k + 1$ $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k + 1)$. Vi bruker antagelsen:

$$\sum_{i=1}^{k} i + (k + 1) = \frac{k(k + 1)}{2} + \frac{2(k + 1)}{2}$$

Ekspander telleren, og observer at den er lik $(k+1)(k+2)$, så vi får til slutt

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

som ønsket.

Konkl.: Dermed er utsagnet sant for alle positive heltall n.

En annen, men logisk ekvivalent, variant av induksjon går ut på å vise utsagnet for $n = 1$, og så anta at det er sant for alle tall $n \leq k$ (ikke bare $n = k$), og bruke denne antagelsen til å vise utsagnet for $n = k+1$.

Binomialteoremet

Binomialkoeffisientene definerte vi ved

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$$

Her antar vi at $0 \leq k \leq n$ er heltall, og $i! = 1.2.3.\cdots.i$ for $i > 0$, $0! = 1$.

Nå sier binomialteoremet

$$(a+b)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^k$$

For $n = 2$ er dette den velkjente kvadratsetningen $(a+b)^2 = a^2 + 2ab + b^2$. Vi så at binomialkoeffisientene kan beregnes ved

$$\left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k-1 \end{array} \right) = \left(\begin{array}{c} n+1 \\ k \end{array} \right)$$

Beviset for binomialteoremet gikk som følger: Det er sant for $n = 1$, for da står det samme uttrykket på begge sider av likhetstegnet. Siden $(a+b)^{k+1} = a(a+b)^k + b(a+b)^k$ kan vi bruke induksjonsantagelsen på $(a+b)^k$. Derfra kan vi regne oss fram til formelen for $n = k+1$, og vi trengte da rekursjonen over.

Dette viser også at alle binomialkoeffisientene er heltall. Eksempler på sammenhenger mellom disse koeffisientene:

$$2^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right)$$

som er teoremet med $a = b = 1$

$$0 = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) (-1)^k$$

som er teoremet med $a = 1, b = -1$.

Divisjonsalgoritmen

Divisjon av positive heltall virker som følger. Hvis vi ønsker å dele a på b skriver vi $a = qb + r$ der $0 \leq r < b$. Dette kan gjøres på en og bare en måte, så q og r er entydig bestemt av a og b.

Beviset for at dette virker, er basert på velordningsprinsippet, som sier at alle mengder positive heltall (med minst et element i seg) har et minste element. Dermed kan vi definere r som det minste tallet i mengden $\{a - xb \geq 0 \,|x \text{ heltall}\}$.

Vi bruker denne formuleringen av divisjon til å dele opp spørsmål om alle heltall i biter, avhengig av hvilken rest de har ved divisjon på et fast tall. For eksempel så vi at alle kvadrattall har rest 0 eller 1 ved divisjon på 3, altså at de er på formen $3k$ eller $3k + 1$.

Euklids algoritme

$x|y$ betyr at $\frac{y}{x}$ er et heltall.

Største felles divisor av to heltall (ikke begge 0) er definert ved

$gcd(a,b) = d$ om $d|a\,, d|b,$ og om $c|a$, $c|b$ er $c \leq d$

Dette tallet kan vi beregne ved hjelp av Euklids algoritme. Først deler vi a på b, så deler vi b på resten, så deler vi resten på den nye resten, osv:

$$\begin{aligned} a &= q_1 b + r_1 && \leftarrow \text{def. av } q_1, r_1 \\ b &= q_2 r_1 + r_2 && \leftarrow \text{def. av } q_2, r_2 \\ r_1 &= q_3 r_2 + r_3 && \leftarrow \text{def. av } q_3, r_3 \\ &\vdots && \vdots \end{aligned}$$

Dette stopper når en rest blir null, altså ved at $r_{n+1}|r_n$. De siste skrittene av algoritmen ser da slik ut:

$$
\begin{array}{rl}
\vdots & \vdots \\
r_{n-3} = q_{n-1}r_{n-2} + r_{n-1} & \leftarrow \text{def. av } q_{n-1}, r_{n-1} \\
r_{n-2} = q_n r_{n-1} + r_n & \leftarrow \text{def. av } q_n, r_n \\
r_{n-1} = q_{n+1}r_n + 0 & \leftarrow \text{def. av } q_{n+1}
\end{array}
$$

Den siste resten som er ulik 0, r_n, er den største felles divisoren til a og b, $r_n = gcd(a, b)$.

Ved å gå baklengs gjennom denne utregningen, finner vi to hele tall x og y slik at

$$gcd(a, b) = ax + by$$

Lineære diofantiske ligninger

Vi er interessert i å løse ligninger på formen

$$ax + by = c$$

der a, b, c er hele tall, og løsningene vi ønsker er i heltall x, y.

Ligningen kan løses hvis og bare hvis $d = gcd(a, b)|c$. I så fall bruker vi først metoden med å gå baklengs gjennom Euklids algoritme for å finne d som en lineærkombinasjon av a og b, og så ganger vi med c/d, som jo er et heltall. Dermed har vi funnet *en* løsning, kall den $x = x_0, y = y_0$. Når vi har en løsning, vil alle løsningene være gitt ved

$$x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t,\ t \text{ heltall}$$

Det var flere ting å sjekke i beviset for dette resultatet. I dag har vi allerede sett at betingelsen $d|c$ er tilstrekkelig til at det finnes en løsning. Vi måtte også sjekke det motsatte, altså at hvis det finnes en løsning, må $d|c$. Videre må vi kontrollere at den generelle formelen $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ løser ligningen. Det vanskeligste punktet var å vise at en vilkårlig løsning nødvendigvis må være på denne formen.

Hvis vi stiller en slik ligning sammen med ulikheter, for eksempel kravet at x og y skal være positive, kan denne tankegangen brukes til å løse klassiske oppgaver, for eksempel frimerkeproblemet. Når vi har funnet den generelle løsningen, kan vi bruke ulikhetene til å få betingelser på parameteren t, og dermed få en liste over mulige løsninger.

Aritmetikkens fundamentalteorem

Ethvert heltall $n > 1$ kan skrives entydig som et produkt av primtall. Dette utsagnet er så viktig at det har fått navnet *Aritmetikkens fundamentalteorem*.

Vi beviste at et tall *kan* skrives som et produkt ved en induktiv tankegang, ved at vi først viste at den minste divisoren (større enn 1) til et heltall nødvendigvis er et primtall. Ved å dele på dette primtallet får vi et lavere tall, og dette tallets minste divisor er igjen et primtall, og så videre.

For å vise entydighet, brukte vi en induktiv tankegang som over, kombinert med et hjelperesultat. Det sier at om et primtall deler et produkt, må det dele en av faktorene. Dette er en konsekvens av det som kalles Euklids lemma.

Dette gir at tall kan skrives på *kanonisk form*,

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_s} \cdots$$

Produkt er gitt ved å ta sum av eksponenter, divisjon ved å ta differanse. Videre er $gcd(a, b)$ gitt ved å ta minimum i eksponentene, som er en svært enkel og rask prosedyre. Tilsvarende kan vi finne minste felles multiplum ved å ta maksimum i hver eksponent. Siden $x + y = min(x, y) + max(x, y)$ ser vi direkte at

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

Dette er en av grunnene til at vi som regel nøyer oss med å se på gcd.

Euklid: uendelig mange primtall

Euklids bevis for at det finnes uendelig mange forskjellige primtall går på denne måten: Anta det motsatte, altså at det bare finnes endelig mange primtall. Da vil vi komme fram til en selvmotsigelse. Dermed kan det ikke være sant at det bare finnes endelig mange primtall, så det må være uendelig mange.

Anta bare endelig mange, $p_1, p_2, \cdots, p_n$. Bruk aritmetikkens fundamentalteorem på $N = p_1 p_2 \cdots p_n + 1 = q_1 q_2 \cdots q_r$. Siden q_1 er et primtall, og $p_1, \cdots, p_n$ er *alle* primtallene, må $q_1 = p_j$ for en av $p-$ene. Men da har vi $q_1 | N$ og $q_1 | p_1 \cdots p_j \cdots p_n$, så $q_1 | N - p_1 \cdots p_n = 1$. Men ingen primtall kan dele 1, og vi har en selvmotsigelse.

Et lignende resonnement viste at det finnes uendelig mange primtall på formen $4n + 3$.

En konsekvens av tankegangen i beviset, er at om vi har en hvilken som helst endelig liste primtall, kan vi finne et nytt ved å se på faktoriseringen av produktet av disse primtallene pluss 1. I noen tilfeller kan dette tallet være et primtall selv, i andre tilfeller kan det ha flere faktorer.

$$2.3.5 + 1 = 31 \text{ er et primtall}$$

$$3.7 + 1 = 22 = 2.11 \text{ er ikke primtall}$$

Metoden Eratosthenes' såld lot oss beregne alle primtall i et intervall, ved å fjerne de tallene som kan deles på primtallene opp til roten av det høyeste tallet i intervallet.

Vi har ingen praktisk gjennomførbar metode for å beregne vilkårlig store primtall.

Midtsemesterprøven vil teste dere både i teoretiske og praktiske ferdigheter i dette stoffet. Hvis dere forstår og kan fylle ut detaljene i de punktene som har blitt presentert her, vil dere være godt rustet til å klare den teoretiske delen. For den praktiske delen vil dere trenge å kunne regne med de metodene vi har innført, så for eksempel Euklids algoritme må sitte i fingrene.

Jeg håper denne raske gjennomgangen vil være til hjelp i forberedelsene, og en hjelp til å prioritere blant stoffet i boken!

Les boken! Regn oppgaver! Still spørsmål til foreleser og øvingslærer, enten ved oppmøte på trefftidene eller ved e-post!

Jon Eivind Vatne