

Note 1

Til TØ-gangen i rusugen diskuterede vi forskellige former for notation, som I vil støde på i kurset. Dette er en lille sammenskrivning af hvad vi snakkede om. Jeg har også skrevet en besvarelse ned på gcd-opgaven, hvis gennemgang i mandags ikke var videre heldig. Endelig har jeg til sidst præsenteret et resultat om polynomier, som jeg kraftigt vil opfordre jer til at bide mærke i. I vil højst sandsynligt finde det nyttigt på et eller andet tidspunkt.

Summer

Ofte har man brug for at skrive en sum bestående af et ubestemt, for eksempel n , led. Dette kan gøres på mange måder. Fx er det klart at $\underbrace{a + \dots + a}_n = na$, men udeladelsesprikkerne kan til tider give anledning til forvirring. Hvad er fx $1 + a + \dots + a^{n-1}$? Man har derfor indført en særlig notation, hvor det bliver klart hvad hvert led i summen er. Det store græske bogstav Σ (sigma) svarer til latinsk S (for sum), og hvis man eksempelvis skriver

$$\sum_{k=1}^n a^{k-1}$$

mener man summen af de tal a^{k-1} der fremkommer ved at lade k gennemløbe de hele tal fra 1 til n og lægge sammen. Fx betyder

$$\sum_{k=1}^n k^2$$

summen af de første n kvadrattal (og man kan i øvrigt vise, at denne er $\frac{n(n+1)(2n+1)}{6}$).

Man tillader også en variation af notationen ovenfor. Hvis K er en endelig mængde, og f er en funktion defineret på K som antager talværdier, betyder

$$\sum_{k \in K} f(k)$$

summen af tallene $f(k)$ når k gennemløber elementerne i K . Et måske lidt fjollet eksempel: Lad K være mængden bestående af de tre ord $K = \{\text{hus, bil, matematik}\}$ og lad f være funktionen der til et ord knytter dets

længde (altså antallet af bogstaver). Så er

$$\sum_{k \in K} f(k) = 3 + 3 + 9 = 15.$$

Man bør bemærke, at definitionen af $\sum_{k \in K}$ er uafhængig af hvilken rækkefølge elementerne i K gennemløbes, da $+$ er kommutativ (altså $a + b = b + a$ for alle tal a, b).

Endelig argumenterede jeg for, hvorfor man har valgt at definere den tomme sum $\sum_{k \in \emptyset} f(k)$ til at være 0.

Produkter

I fuldstændig analogi med summerne har man indført en særlig notation for produkter. Det græske bogstav der svarer til P er π , og et stort græsk π ser sådan ud: Π . Man vedtager, at det tomme produkt er 1.

Fra gymnasiet kan I måske huske, at logaritmen til et produkt er summen af logaritmerne (dvs. $\log(ab) = \log a + \log b$ for alle positive tal a, b). Dette faktum kan man (fx ved induktion) generalisere, og jeg overlader det til jer at indse hvorfor

$$\log \left(\prod_{i=1}^n a_i \right) = \sum_{i=1}^n \log(a_i)$$

når a_i er positive tal.

Mængder

En (endelig) mængde kan skrives op på såkaldt *fuldstændig listeform*, hvor man altså opskriver mængdens elementer mellem tuborgparenteser, separeret af kommaer. Rækkefølgen hvori elementerne opskrives er underordnet; således er $\{\pi, 2, 8\}$, $\{2, 8, \pi\}$ og $\{8, 2, \pi\}$ alle den samme mængde. Gentagelse af et element ændrer heller ikke mængden; $\{\pi, 2, 8, 2, 2\} = \{2, 8, \pi\}$. Hvis mængden er uendelig, eller så stor at man ikke kan eller vil skrive alle dens elementer ned, kan man også bruge *ufuldstændig listeform*. Det forudsætter dog, at det fra konteksten er klart hvilke elementer mængden består af. Eksempelvis er det først klart, hvad $\{2, 3, 5, \dots, 997\}$ betyder, når man i ord forklarer at der tales om mængden af primtal mindre end 1000.

Mængden uden elementer kan man således skrive $\{\}$, men da dette let kan give anledning til forvirring har man indført det særlige symbol \emptyset for den tomme mængde.

Oftentimes har man brug for at betragte mængden af de elementer som har en eller anden foreskrevet egenskab. Helt generelt skal udtryk of formen

$$\{x \in A \mid P(x)\}$$

læses som “de x i A for hvilke udsagnet $P(x)$ er sandt”. Eksempler på dette kunne være

$$\begin{aligned} \{x \in \mathbb{N} \mid x \text{ er et ulige primtal}\} &= \{3, 5, 7, 11, \dots\} \\ \{x \in \mathbb{Z} \mid x^2 < 10\} &= \{-3, -2, -1, 0, 1, 2, 3\} \\ \{x \in \mathbb{N} \mid x \mid 56\} &= \{1, 2, 4, 7, 8, 14, 28, 56\}. \end{aligned}$$

Dette sidste eksempel tjener to formål. Dels kaldes mængden for “mængden af divisorer i 56”, og man bruger nogle gange notationen $\text{Div}(56)$ om den. Dels skal det illustrere den lidt uheldige dobbeltstreg, som den lodrette streg \mid har. Den første skal læses “for hvilke” eller “således at”, mens den anden skal læses “går op i” eller “er divisor i”. Den lodrette streg bruges også nogle gange i par til at betyde absolutværdi eller norm; fx er intervallet $[-2, 2]$ det samme som mængden $\{x \in \mathbb{R} \mid |x| \leq 2\}$.

Man kan godt støde på bøger og lignende som benytter et kolon i stedet for en lodret streg; i visse sammenhænge har det oplagte fordele; fx er $\{x \in \mathbb{R} : |x| \leq 2\}$ lidt mindre forvirrende.

En TØ-opgave

Mandag efter rusturen var jeg åbenbart ikke helt frisk. Det følgende er en (forhåbentlig) bedre besvarelse af opgave 5 på Ugeseddel 3.

Vi har altså givet to naturlige tal a og b sammen med deres primtalsfaktoriseringer

$$a = \prod_{i=1}^N p_i^{k_i} \qquad b = \prod_{i=1}^N p_i^{l_i}$$

hvor $\{p_1, p_2, \dots, p_N\}$ er foreningsmængden af primdivisorerne i a og b (altså alle de primtal der skal bruges for at faktorisere a og b), og $k_i, l_i \in \mathbb{N} \cup \{0\}$. Vi har desuden navngivet p_i 'erne sådan at $p_i \neq p_j$ når $i \neq j$ [hvis det samme primtal $p_i = p_j$ optrådte to steder i faktoriseringen af a , kunne vi blot erstatte $p_i^{k_i} p_j^{k_j}$ med $p_i^{k_i+k_j}$].

For hvert i mellem 1 og N lader vi nu m_i betegne den mindste af de to eksponenter k_i og l_i ; altså $m_i = \min(k_i, l_i)$. Opgaven er at vise, at det tal c

der fremkommer ved fastsættelsen

$$c = \prod_{i=1}^N p_i^{m_i}$$

er den største fælles divisor i a og b .

Bevis. Vi starter med at kontrollere, at c faktisk er en fælles divisor. Da $m_i \leq k_i$ for alle i , er $p_i^{k_i - m_i}$ et naturligt tal for alle $i = 1, \dots, N$. Derfor er

$$\begin{aligned} a &= \prod_{i=1}^N p_i^{k_i} = \prod_{i=1}^N p_i^{m_i} p_i^{k_i - m_i} \\ &= \left(\prod_{i=1}^N p_i^{m_i} \right) \cdot \left(\prod_{i=1}^N p_i^{k_i - m_i} \right) = c \cdot \prod_{i=1}^N p_i^{k_i - m_i} \end{aligned}$$

så c er en divisor i a . På tilsvarende måde finder man, at c er en divisor i b .

Hvis p er et primtal som går op i $\gcd(a, b)$ må vi også have at p går op i a og b . Da alle de primtal der går op i a og b findes i mængden $\{p_1, p_2, \dots, p_N\}$ har vi at p må være et af disse tal. Denne overvejelse viser, at de primtal der skal bruges til at faktorisere $\gcd(a, b)$ er at finde blandt p_1, p_2, \dots, p_N , så vi kan skrive

$$\gcd(a, b) = \prod_{i=1}^N p_i^{g_i}$$

hvor $g_i \in \mathbb{N} \cup \{0\}$. Da c er en fælles divisor for a og b må c være en divisor i $\gcd(a, b)$, men det betyder at $m_i \leq g_i$ for alle i .

På den anden side: Da $\gcd(a, b)$ er en divisor i a og b , må $p_i^{g_i}$ også være en divisor i a og b for alle i . Men $p_i^{g_i}$ kan kun gå op i a hvis den i 'te faktor i a , dvs. $p_i^{k_i}$ er stor nok; altså hvis $g_i \leq k_i$. På samme måde indser man at $g_i \leq l_i$. Men disse to uligheder medfører at $g_i \leq \min(k_i, l_i) = m_i$. Da således $g_i \leq m_i$ og $m_i \leq g_i$ for alle i har vi at $g_i = m_i$ for alle i , men det betyder præcis at $c = \gcd(a, b)$. \square

Ekstraspørgsmålet, hvornår $\gcd(a, b)$ er lig med 1 kan man nu besvare i termer af primfaktoriseringerne af a og b : Tallet c er lig med 1 hvis og kun hvis alle eksponenterne m_i er lig 0; men dette sker hvis og kun hvis det for ethvert i gælder at mindst en af k_i og l_i er lig 0. Med andre ord, hvis og kun hvis der ikke er fælles primfaktorer i a og b .

Polynomier

Mange ting hører med til den almene dannelse; det resultat der præsenteres i dette afsnit er en af disse ting. Lad f være et polynomium, altså

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0. \quad (1)$$

Ofte er man interesseret i at finde rødder i polynomier. Hvis a_0 er 0 er $x = 0$ oplagt en rod i p .

Antag nu, at koefficienterne a_i alle er heltal. Vi taber ikke megen generalitet ved yderligere at antage, at a_n og a_0 er forskellige fra 0. Påstanden er nu følgende:

Lemma 1. *Hvis $x = \frac{p}{q}$ er en rationel rod i f , og $\frac{p}{q}$ er uforkortelig (altså $\text{gcd}(p, q) = 1$), så er p divisor i a_0 og q er divisor i a_n .*

Nytten af denne påstand er følgende: *Der er kun endeligt mange potentielle rationelle rødder i et givet polynomium med heltallige koefficienter!* Med andre ord: Hvis man leder efter alle rødderne i et polynomium med heltallige koefficienter, kan man starte med at afprøve om nogen af de rationelle kandidater er rødder. Hvis man er heldig finder man en rod, og så kan man udføre polynomiers division og få et polynomium af grad en mindre.

Bevis for lemmaet. Vi antager altså at

$$a_n \left(\frac{p}{q}\right)^n + \cdots + a_1 \frac{p}{q} + a_0 = 0.$$

Ganger vi denne ligning igennem med q^n og flytter en smule om finder vi, at

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} = -a_0 q^n.$$

Bemærk at denne identitet kun involverer heltal. Man ser, at p er divisor i venstresiden, men det betyder at $p \mid a_0 q^n$. Da vi har antaget at p og q er indbyrdes primiske, må vi have at $p \mid a_0$.

På tilsvarende måde kan vi flytte lidt rundt på ledene og konstatere at

$$a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = -a_n p^n.$$

Heraf aflæser man, at q er divisor i $a_n p^n$, og som før må dette betyde at q går op i a_n . \square

Et eksempel: Lad $f(x) = x^3 + x^2 - 13x + 3$. Det ovenstående fortæller, at de eneste mulige rationelle rødder er ± 1 og ± 3 (fordi tælleren skal være

divisor i 3 og nævneren skal være divisor i 1). Ved at indsætte disse fire kandidater finder man at 3 er en rod. Ved hjælp af polynomiers division finder man så at f kan faktoreres som $f(x) = (x-3)(x^2+4x-1)$. De øvrige rødder i f kan altså findes ved at løse andengradsligningen $x^2 + 4x - 1 = 0$, og det er en overkommelig opgave. Man finder to andre reelle rødder, nemlig $x = \frac{-4 \pm \sqrt{20}}{2} = -2 \pm \sqrt{5}$.

Som umiddelbar konsekvens har vi

Sætning 2. *Lad p være et primtal og $n \geq 2$ et heltal. Så er $\sqrt[n]{p}$ irrationel.*

Bevis. Betragt polynomiet $f(x) = x^n - p$. Ifølge Lemma 1 er de eneste mulige rationelle rødder i f tallene ± 1 og $\pm p$. Man indser let at ingen af udtrykkene

$$\begin{aligned} &1 - p \\ &(-1)^n - p \\ &p^n - p \\ &(-p)^n - p \end{aligned}$$

kan være lig 0, og derfor har f ingen rationelle rødder. Da $\sqrt[n]{p}$ er en rod må det betyde, at $\sqrt[n]{p}$ er irrationel. \square

Specielt konkluderer vi (for $n = p = 2$) at kvadratroden af 2 er et irrationelt tal. Det er heller ikke svært at vise:

Sætning 3. *Lad $m \in \mathbb{N}$ og $n \geq 2$. Hvis $\sqrt[n]{m}$ er rationel, så er det et heltal.*

Bevis. Lad $f(x) = x^n - m$. Pr. antagelse er $\sqrt[n]{m}$ et rationelt tal, så vi kan skrive det som uforkortelig brøk $\frac{p}{q}$. Men fra Lemma 1 har vi så, at $q = \pm 1$ så $\sqrt[n]{m}$ faktisk er et heltal. \square

Med andre ord kan man aldrig tage et rationelt, ikke-heltal og opløfte det til en potens n og få et heltal. Løst sagt betyder Sætning 3, at langt de fleste n 'te-rødder er irrationelle.