Dis1 2008-09
Ugeopgave 1

Rasmus Sylvester Bryder

13. februar 2009

1 TAL3: opgave 12

Der skal vises, at hvis a og b er primiske og positive hele tal, samt hvis ab er et kvadrattal, da er både a og b kvadrattal.

Antag derfor at a og b er primiske og positive hele tal, altså at $a, b > 0$ samt $(a, b) = 1$, og endvidere at $\exists c \in \mathbb{N} : ab = c^2$.

Hvis $a, b > 1$, vil vi ved Aritmetikkens Fundamentalsætning, TAL(3.16), kunne opskrive disse som primopløsninger (hvilket bliver praktisk i det følgende). Altså må vi behandle tilfældet for a eller b lig 1; i begge tilfælde er disse positive og primiske med alle $n \in \mathbb{N}$. Vi antager derfor $a = 1$. Da $1 = 1^2$, er a altså et kvadrattal. Da $b = 1 \cdot b = ab = c^2$ ved vores antagelse, er b altså også et kvadrattal, hvorpå det ønskede er vist. Samme begrundelse føres for $b = 1$, hvorpå a ved kvadrattallet ab også må være et kvadrattal. Specielt gælder, at hvis $ab = 1 = 1^2$ er $a = b = 1$. I følgende antager vi derfor, at $a, b > 1$.

Da så $a, b > 1$ kan begge jf. TAL(3.16) og TAL(3.17) skrives som primopløsninger på formen $a = a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r}$ og $b = b_1^{\beta_1} b_2^{\beta_2} \cdots b_s^{\beta_s}$, hvor $a_1, \ldots, a_r$ og $b_1, \ldots, b_s$ er primtal, samt de hele eksponenter $\alpha_i, \beta_j \geq 0$ for $i = 1, \ldots, r$ og $j = 1, \ldots, s$.

Hvis α_i eller β_j er lig 0 for et eller flere i eller j, er tilsvarende $a_i^{\alpha_i}$ eller $b_j^{\beta_j}$ lig 1 og kan derfor ignoreres - da dette vil gøre det tilsvarende primtal a_i eller b_j overflødigt i primopløsning, antages derfor, at a og b er på ovenstående form med $\alpha_i, \beta_j \neq 0$ og dermed $\alpha_i, \beta_j > 0$ for $i = 1, \ldots, r$ og $j = 1, \ldots, s$.

Der findes ved antagelsen $c \in \mathbb{N}$ så $c^2 = ab > 1$, dvs. $c > 1$. Dette c kan altså også skrives som en primopløsning $c = c_1^{\gamma_1} c_2^{\gamma_2} \ldots c_t^{\gamma_t}$, hvor $c_1, \ldots, c_t$ er primtal, samt hele eksponenter $\gamma_k > 0$ for $k = 1, \ldots, t$ af samme årsager som for α_i, β_j. Da har vi, at

$$c^2 = (c_1^{\gamma_1} c_2^{\gamma_2} \ldots c_t^{\gamma_t})^2 = c_1^{2\gamma_1} c_2^{2\gamma_2} \ldots c_t^{2\gamma_t},$$

men da $c^2 = ab$, har vi endvidere at

$$c_1^{2\gamma_1} c_2^{2\gamma_2} \ldots c_t^{2\gamma_t} = a_1^{\alpha_1} \cdots a_r^{\alpha_r} b_1^{\beta_1} \cdots b_s^{\beta_s}.$$

Da a og b er primiske, ved vi at $a_i \neq b_j$ for alle $i = 1, \ldots, r$ og $j = 1, \ldots, s$. Der er altså præcis $r + s$ primtal (opløftet i forskellige potenser) på højre side af lighedstegnet. Grundet entydigheden fra Aritmetikkens Fundamentalsætning,

TAL(3.16), gælder der så, at antallet af primtal på venstre side er det samme, altså at $t = r + s$. Ved samme sætning kan vi da passende omnummerere c_k'erne så $c_i = a_i$ for $i = 1, \ldots, r$ og $c_{r+j} = b_j$ for $j = 1, \ldots, s$.

Under TAL(3.17) vil der nu også gælde, grundet entydigheden, at eksponenterne er de samme, altså at $2\gamma_i = \alpha_i$ for $i = 1, \ldots, r$ og $2\gamma_{r+j} = \beta_j$ for $j = 1, \ldots, s$.

Det vil sige, at vi har sørget for, at $c_1^{2\gamma_1} \ldots c_r^{2\gamma_r} = a_1^{\alpha_1} \cdots a_r^{\alpha_r}$ og $c_{r+1}^{2\gamma_{r+1}} \ldots c_{r+s}^{2\gamma_{r+s}} = b_1^{\beta_1} \cdots b_s^{\beta_s}$. Men da har vi jo, at

$$a = a_1^{\alpha_1} \cdots a_r^{\alpha_r} = c_1^{2\gamma_1} \ldots c_r^{2\gamma_r} = (c_1^{\gamma_1} \ldots c_r^{\gamma_r})^2,$$

hvorpå a altså er et kvadrattal (da alle c_k er (hele) primtal og eksponenterne er hele og positive), og ligeså har vi, at

$$b = b_1^{\beta_1} \cdots b_s^{\beta_s} = c_{r+1}^{2\gamma_{r+1}} \ldots c_{r+s}^{2\gamma_{r+s}} = (c_{r+1}^{\gamma_{r+1}} \ldots c_{r+s}^{\gamma_{r+s}})^2,$$

så også b er et kvadrattal, hvormed det ønskede er vist.

2 TAL6: opgave 9

Lad $n = n_1 \cdots n_r$ være et produkt af parvis primiske tal n_i, altså så $(n_i, n_j) = 1$ for alle $i, j \in 1, \ldots, r$ og $i \neq j$.

Lad $i \in 1, \ldots, r$. Sæt nu $n_i' = \frac{n}{n_i}$, hvor altså $n = n_i n_i'$.

Der skal vises, at der findes to hele tal x_i og y_i, således at $1 = x_i n_i + y_i n_i'$.

Sæt nu $m_1 = n_i$ og derpå m_2 op til m_r lig n_j, hvor $j \in 1, \ldots, r$ og $j \neq i$. Da er produktet af alle m_k lig produktet af alle n_k, som var lig n. Vi har endvidere at $m_2 \cdots m_r = \frac{m_1 m_2 \cdots m_r}{m_1} = \frac{n}{n_i} = n_i'$.

Nu er alle m_k parvis primiske, da vi jo praktisk talt bare har omnummereret n_k. Da n_i er primisk med alle n_j hvor $i \neq j$, er m_1 altså primisk med alle m_j for $j = 2, \ldots, r$.

Da er m_1 specielt primisk med m_2 og med m_3; derfor er m_1 jf. TAL(3.10) også primisk med produktet af disse, $m_2 m_3$. Men vi ved jo også m_1 er primisk med m_4, så m_1 er ved samme korollar også primisk med $(m_2 m_3) m_4 = m_2 m_3 m_4$. Således kan vi fortsætte med at føje m_j for $j = 5, \ldots, r$ som faktor til produktet, hvorpå m_1 også er primisk med det nyfremkomne produkt jf. TAL(3.10). Derpå er m_1 altså primisk med $m_2 \cdots m_r$.

Men da vi satte $m_1 = n_i$ og fandt, at $m_2 \cdots m_r = n_i'$, vil det altså sige, at n_i er primisk med n_i'. Ved TAL(3.9) findes der altså to hele entydigt bestemte tal x_i og y_i, således at $1 = x_i n_i + y_i n_i'$.

Sæt nu $e_i = y_i n_i'$. Følgende tre kongruenser skal påvises:

1. $e_i \equiv 1 \pmod{n_i}$
2. $e_i \equiv 0 \pmod{n_i'}$
3. $e_1 + \ldots + e_r \equiv 1 \pmod{n}$

Herpå følger.

1. Der findes tal x_i og y_i således at $1 = x_i n_i + y_i n_i'$, dvs. $-x_i n_i = y_i n_i' - 1$,

så $-x_i n_i = e_i - 1$. Da $n_i | -x_i n_i$, må der også gælde at $n_i | e_i - 1$, hvilket pr. TAL(6.6) er ensbetydende med at $e_i \equiv 1 \pmod{n_i}$.

2. Endvidere gælder da $n_i' | y_i n_i'$, at $n_i' | e_i$ eller $n_i' | e_i - 0$, hvorpå pr. TAL(6.6) at $e_i \equiv 0 \pmod{n_i'}$.

3. Vi kigger på produktet $(1 - e_1) \cdots (1 - e_r)$ (fremover henvist til som *produktet*). Da $1 - e_i = 1 - y_i n_i' = x_i n_i$, er

$$\begin{aligned}(1 - e_1) \cdots (1 - e_r) &= (x_1 n_1) \cdots (x_r n_r) \\ &= (x_1 \cdots x_r)(n_1 \cdots n_r) = (x_1 \cdots x_r) n,\end{aligned}$$

så vi har at $n | (1 - e_1) \cdots (1 - e_r)$. Vi ved nu, at $e_i e_j$ for $i, j \in 1, \ldots, r$ og $i \neq j$ kan omskrives til

$$e_i e_j = (y_i n_i')(y_j n_j') = \left(y_i \frac{n}{n_i} \right) \left(y_j \frac{n}{n_j} \right) = n \left(y_i y_j \frac{n}{n_i n_j} \right),$$

hvor brøken er et helt tal, da både n_i og n_j er at finde i $n_1 \cdots n_r$, hvorpå kvotienten er produktet af alle n_k for $k \in \{1, \ldots, r\}$ fraregnet i og j[1]. Altså har vi også at $n | e_i e_j$ for $i \neq j$.

Vi vil nu kigge igen på $(1 - e_1) \cdots (1 - e_r)$. Da vi ved, at $n | e_i e_j$ for $i \neq j$, vil der altså gælde, at lige så snart et af leddene i den endelige sum vil have mindst to faktorer $e_i e_j$ hvor $i \neq j$, vil n gå op i dette led. Vi ved også at der er ingen led indeholdende faktoren e_k to gange eller mere, da ingen e_k optræder to gange i produktet som opskrevet.

Altså; alle faktorer e_k i hvert led har forskellige indices k, så n går op i alle led med mindst to faktorer $e_i e_j$ hvor $i \neq j$, og dermed også op i summen af disse.

Da n som fundet også går op i hele produktet, må n altså også gå op i summen af alle de led hvor der er højst én faktor e_k (ellers ville n ikke gå op i produktet).

Da har vi, at de første led i hver parantes alle ganget sammen giver $1^r = 1$, og yderligere hvis vi ganger det andet led $-e_k$ ud i hver parantes med ettallerne i de $(r - 1)$ andre, har vi da alle leddene med højst én faktor e_k.

Vi får så med vores viden fra før, at n altså går op i summen af disse, $1 - e_1 - \ldots - e_r$. Men da har vi, at $n | 1 - (e_1 + \ldots + e_r)$, og pr. TAL(6.6) er $e_1 + \ldots + e_r \equiv 1 \pmod{n}$.

Vi har nu givet et system af kongruenser, $x \equiv a_i \pmod{n_i}$, hvor $i \in \{1, \ldots, r\}$. Vi vil vise, at dette system har en løsning i $\mathbb{Z}$ og modulo n kun én løsning.

Vi benytter nu den Kinesiske Restklassesætning, TAL(6.14), og får ved denne at systemet har løsninger $x \in \mathbb{Z}$, da $n_1, \ldots, n_r$ var parvis primiske. Endvidere vil alle disse løsninger udgøre én restklasse modulo n. Sætningen siger dog ikke noget om formen på disse løsninger.

Vi vil her vise, at $x_0 = e_1 a_1 + \ldots + e_r a_r$ er en løsning til systemet.

Thi lad $i, j \in \{1, \ldots, r\}$ og $i \neq j$, samt være givet et talsæt $(a_1, \ldots, a_r)$. Vi har da, at $n_i | n_j'$, hvilket er meget rimeligt, da n_j' jo er produktet af alle parvis primiske faktorer i n undtagen n_j, hvoriblandt n_i må ligge, da $n_i \neq n_j$.

[1] Dette kunne ikke lade sig gøre, hvis i kunne være lig j; da alle n_k er parvis primiske, så kan $n_i n_j = n_i^2$ ikke gå op i n.

Da $e_j = y_j n'_j$, må $n_i | e_j$ for $i \neq j$, og endvidere $n_i | e_j a_j$. Da dette gælder for alle $i \neq j$, må n_i altså også gå op i summen af alle $e_j a_j$, hvor $i \neq j$.

Det vil sige at n_i går op i $e_1 a_1 + \ldots + e_r a_r - e_i a_i = x_0 - e_i a_i$.

Da vi har kongruensen $e_i \equiv 1 \pmod{n_i}$, må der altså gælde $n_i | e_i - 1$, og at der findes et $q_i \in \mathbb{Z}$, så $e_i - 1 = q_i n_i$, dvs. $e_i = q_i n_i + 1$.

Men nu vil vi så have, at

$$x_0 - e_i a_i = x_0 - (q_i n_i + 1) a_i = x_0 - q_i n_i a_i - a_i,$$

og da vi ved at $n_i | x_0 - e_i a_i$, må der altså også gælde at $n_i | x_0 - q_i n_i a_i - a_i$.

Men da vi ved med sikkerhed, at $n_i | -q_i n_i a_i$, må vi også have, at $n_i | x_0 - a_i$; hvis ikke, ville n_i ikke gå op i $x_0 - e_i a_i$, hvilket vi jo har fundet at den gør.

Pr. TAL(6.6) har vi så ved $n_i | x_0 - a_i$, at $x_0 \equiv a_i \pmod{n_i}$ for ethvert $i \in \{1, \ldots, r\}$, altså er x_0 en løsning til kongruenssystemet, og vi har dermed fundet en løsning.

Ved den Kinesiske Restklassesætning vil alle løsninger være da elementer i restklassen $[x_0]_n$, og kun i denne.

Det er her opgaveformuleringen i bogen klunter lidt; der er ikke én løsning $x = x_0$ for systemet modulo n, men uendeligt mange løsninger på formen $x = x_0 + qn = x_0 + qn_1 \cdots n_r$, hvor $q \in \mathbb{Z}$.

Op til kongruens modulo n er der imidlertid kun én løsning, nemlig restklassen $[x_0]_n$, og det er sådan formuleringen – forhåbentlig – skal læses.

Det kan selvfølgelig være, at $x_0 < 0$ eller $x_0 \geq n$, hvorpå der kan vælges et passende $p \in \mathbb{Z}$ så $0 \leq x_0 + pn < n$, hvorpå $[x_0 + pn]_n$ ville være en eventuelt mere præsentabel restklasserepræsentant.

I alle tilfælde kan systemet løses ved at sætte $x = e_1 a_1 + \ldots + e_r a_r$, hvormed $x \equiv a_i \pmod{n_i}$, hvor $i \in \{1, \ldots, r\}$.

Opgaven beder om specifikt at overveje tilfældet $r = 2$, hvor vi altså har et produkt $n = n_1 n_2$, da n_1 og n_2 er primiske.

Der findes da hele tal x og y, så $1 = x n_1 + y n_2$ (eller $1 = y n_2 + x n_1$), da $(n_1, n_2) = 1$ – vi har brugt TAL(3.9), men kunne lige så godt sætte $n'_1 = n_2$ og $n'_2 = n_1$ ud fra ovenstående definition på n'_i.

Derpå sættes $e_1 = y n_2$ og $e_2 = x n_1$. Så er $e_1 \equiv 1 \pmod{n_1}$ og $e_1 \equiv 0 \pmod{n_2}$, og tilsvarende for e_2. Endelig har vi, at $e_1 + e_2 = y n_2 + x n_1 = 1 \equiv 1 \pmod{n}$, altså ingen overraskelse.

Vi vil da endelig få, at ethvert kongruenssystem $x \equiv a_1 \pmod{n_1}$ og $x \equiv a_2 \pmod{n_2}$ har en løsning

$$x_0 = e_1 a_1 + e_2 a_2 = y n_2 a_1 + x n_1 a_2,$$

hvoraf vi altså har en nem løsningsformel til et sådant tilfælde.