Talteori I - Matematisk induktion

MM1008 Utmanande matematik

Nils Jakobson Mo
Matematiska institutionen
Stockholms universitet
11 juni 2022

Innehåll

Del 1

Problem 1

Problem: Var och en av $n \geq 4$ personer känner till en hemlig upplysning som inte är identisk med någon annans. Visa att det räcker med $2n - 4$ telefonsamtal mellan dessa personer för att alla ska känna till alla hemligheter. Vi förutsätter att alla har tillgång till en telefon och att under varje samtal utbyts alla hemligheter som båda talande känner till.

Lösning: I detta bevis kommer hemligheterna numreras som $S_1,\ S_2,\ \cdots,\ S_n$ där S_i är hemligheten som bara person i vet vid initialtillståndet. Ett samtal mellan person i och person j kommer skrivas som $C(i, j)$. Antalet samtal som krävs för att sprida hemligheterna till n personer kommer betecknas som $A(n)$. Helhetstillståndet av personernas vetskap om hemligheter kommer att representeras som mängder. Exempelvis så skulle initialfallet för $n = 2$, alltså tillståndet innan något samtal har utförts, betecknas enligt följande: $T_0 = \{S_1\}\{S_2\}$. Här beskriver T_n tillståndet efter n samtal. Om en person till exempel vet hemligheter S_1 och S_5 betecknas personen som $\{S_1S_5\}$.

Induktionsbas (IB) $n = 4$: Initialtillståndet som ges i detta fall är:

$$T_0 = \{S_1\}\{S_2\}\{S_3\}\{S_4\}$$

Om vi nu utför föjlande serie av samtal kommer alla samtliga personer veta alla hemligheter:

$$\begin{aligned}
C(1,2) &\implies T_1 = \{S_1S_2\}\{S_1S_2\}\{S_3\}\{S_4\} \\
C(3,4) &\implies T_2 = \{S_1S_2\}\{S_1S_2\}\{S_3S_4\}\{S_3S_4\} \\
C(1,3) &\implies T_3 = \{S_1S_2S_3S_4\}\{S_1S_2\}\{S_1S_2S_3S_4\}\{S_3S_4\} \\
C(2,4) &\implies T_4 = \{S_1S_2S_3S_4\}\{S_1S_2S_3S_4\}\{S_1S_2S_3S_4\}\{S_1S_2S_3S_4\}
\end{aligned}$$

När alla hemligheter är spridda kan vi se att $A(4) = 4 = 2 \cdot 4 - 4$.

Induktionsantagande (IA) Antag att $A(k) = 2k - 4$ för $k \geq 4$.

Induktionssteg (IS) Visa att $A(k+1) = 2(k+1) - 4$.
Först utförs samtal $C(1, k+1)$:

$$C(1, k+1) \implies T_1 = \{S_1 S_{k+1}\}\{S_2\} \cdots \{S_k\}\{S_1 S_{k+1}\}$$

Nu kan vi enligt (IA) anta att det kommer ta $2k - 4$ samtal för personer 1 till k att sprida sina hemligheter. Eftersom samtalet $C(1, k+1)$ gjordes innan spridningen kommer alla personer även veta hemligheten som person $k+1$ bar på i initialtillståndet. Tillståndet efter spridningen, alltså efter $2k - 3$ samtal gjorts, kommer vara:

$$T_{2k-3} = \{S_1 \cdots S_{k+1}\}\{S_1 \cdots S_{k+1}\} \cdots \{S_1 S_{k+1}\}$$

Om person $k+1$ nu samtalar med vilken person som helst, till exempel person 1 för enkelhets skull, kommer tillståndet bli:

$$C(1, k+1) \implies T_{2k-2} = \{S_1 \cdots S_{k+1}\}\{S_1 \cdots S_{k+1}\} \cdots \{S_1 \cdots S_{k+1}\}$$

Eftersom ett samtal gjordes mellan person 1 och $k+1$ från början och det tog $2k-4$ samtal för att sprida hemligheterna mellan de första k personerna, utgör det slutliga samtalet mellan person 1 och $k+1$ samtal nummer $2k - 2$ vilket kan skrivas om enligt:

$$2k - 2 = 2k + 2 - 4 = 2(k+1) - 4$$

$$A(k+1) = 2(k+1) - 4$$

□

Problem 2

Problem: Låt $n \geq 1$. Visa att

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

Lösning:

Induktionsbas (IB) $n = 1$:

$$VL = 1 \cdot 2 = 2$$

$$HL = \frac{1(1+1)(1+2)}{3} = \frac{1 \cdot 2 \cdot 3}{3} = 2$$

$$VL = 2 = HL$$

Induktionsantagande (IA) Antag för $k \geq 1$ att

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}$$

Induktionssteg (IS) Visa att

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}$$

Vi börjar med att gruppera VL enligt:

$$VL = (1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + k(k+1)) + (k+1)(k+2).$$

Enligt (IA) kan detta skrivas om till

$$VL = \frac{k(k+1)(k+2)}{3} + (k+1)(k+2)$$

$$VL = \frac{k(k+1)(k+2) + 3(k+1)(k+2)}{3}$$

Vi bryter ut faktorn $(k+1)(k+2)$ från båda termerna för att få:

$$VL = \frac{(k+1)(k+2)(k+3)}{3}$$

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}$$

□

Problem 3

Problem: Visa att för varje $n \geq 0$ är $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

Lösning:

Induktionsbas (IB) $n = 0$:

$$VL = 2 = 1$$
$$HL = 2^{0+1} - 1 = 2 - 1 = 1$$
$$VL = 1 = HL$$

Induktionsantagande (IA) Antag att $1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$ för $k \geq 0$.

Induktionssteg (IS) Visa att $1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{k+2} - 1$
Vi börjar med att gruppera VL enligt:

$$VL = (1 + 2 + 2^2 + \cdots + 2^k) + 2^{k+1}$$

Enligt (IA) kan detta skrivas om enligt:

$$(2^{k+1} - 1) + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{(k+1)+1} - 1 = 2^{k+2} - 1$$

$$1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{k+2} - 1$$

□

Problem 4

Problem: Visa att för alla $n \geq 0$ är $\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$.

Lösning: F_n är det n:te fibonaccitalet. Fibonaccitalen definieras som:

$$F_n = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ F_{n-1} + F_{n-2} & n > 1 \end{cases}$$

Induktionsbas (IB) $n = 0$:

$$VL = \sum_{i=0}^{0} F_i^2 = F_0^2 = 0^2 = 0$$

$$HL = F_0 F_{0+1} = F_0 F_1 = 0 \cdot 1 = 0$$

$$VL = 0 = HL$$

Induktionsantagande (IA) Antag att $\sum_{i=0}^{k} F_i^2 = F_k F_{k+1}$ för $k \geq 0$.

Induktionssteg (IS) Visa att $\sum_{i=0}^{k+1} F_i^2 = F_{k+1} F_{k+2}$.
Vi börjar med att dela upp summan i VL enligt:

$$\sum_{i=0}^{k+1} F_i^2 = (\sum_{i=0}^{k} F_i^2) + F_{k+1}^2$$

Enligt (IA) gäller $\sum_{i=0}^{k} F_i^2 = F_k F_{k+1}$ och vi kan därför göra följande omskrivning:

$$(\sum_{i=0}^{k} F_i^2) + F_{k+1}^2 = (F_k F_{k+1}) + F_{k+1}^2$$

Om vi nu bryter ut F_{k+1} ur båda termer får vi:

$$F_{k+1}(F_k + F_{k+1})$$

Enligt definitionen av fibonaccital från problembeskrivningen är summan av två på varandra följande fibbonacital det nästa talet i fibbonaciserien. Notera därför att $F_k + F_{k+1} = F_{k+2}$. Uttrycket kan därför skrivas om enligt:

$$F_{k+1}(F_k + F_{k+1}) = F_{k+1} F_{k+2}$$

$$\sum_{i=0}^{k+1} F_i^2 = F_{k+1} F_{k+2}$$

□

Problem 5

Problem: Talföljden $a_0,\ a_1,\ a_2,\ \ldots$ definieras rekursivt genom:
$a_0 = 7,\ a_1 = 5$ och $a_{n+1} = 2a_n + 3a_{n-1}$ för $n \geq 1$. Du misstänker att det finns två konstanter A och B sådana att $a_n = A \cdot 3^n + B \cdot (-1)^n$ för alla $n \geq 0$. Verifiera misstanken (finn möjliga A och B) och bevisa ditt påstående med induktion.

Lösning:

Beräkning av A och B: Vi sätter in $n = 0$ och $n = 1$ i den explicita formeln för a_n och ställer upp ett ekvationssystem med hjälp av givna värden på a_0 och a_1:

$$a_0 = 7 = A \cdot 3^0 + B \cdot (-1)^0 = \ A + B$$
$$a_1 = 5 = A \cdot 3^1 + B \cdot (-1)^1 = 3A - B$$

Detta ger ekvationssystemet:

$$\begin{cases} A + B = 7 \\ 3A - B = 5 \end{cases}$$

Vi använder additionsmetoden för ekvationssystem för att beräkna variablerna:

$$A + 3A + B - B = 7 + 5$$
$$4A = 12$$
$$A = 3$$

Om vi sätter in det beräknade värdet på A i ekvationssystemet får vi:

$$A + B = 7$$
$$3 + B \ = 7$$
$$B \qquad = 4$$

Vi har nu fått fram värden på A och B. Vi kan därmed konstatera att den explicita formeln för a_n är:

$$a_n = 3 \cdot 3^n + 4 \cdot (-1)^n = 3^{n+1} + 4(-1)^n$$

Vi ska nu visa att denna formel gäller för $n \geq 0$ med induktion.

Induktionsbas (IB) $n = 0$ och $n = 1$:

$$a_0 = 3^{0+1} + 4(-1)^0 = 3 + 4 = 7$$
$$a_1 = 3^{1+1} + 4(-1)^1 = 9 - 4 = 5$$

Fallen stämmer enligt problembeskrivningen och vi går vidare.

Induktionsantagande (IA) Antag att $a_k = 3^{k+1} + 4(-1)^k$ för $k \geq 0$.

Induktionssteg (IS) Visa att $a_{k+1} = 3^{k+2} + 4(-1)^{k+1}$.
Vi använder oss av den rekursiva formeln given i problembeskrivningen och (IA) för att göra induktionssteget:

$$\begin{aligned}
a_{k+1} &= 2a_k + 3a_{k-1} \\
&= 2(3^{k+1} + 4(-1)^k) + 3(3^k + 4(-1)^{k-1}) \\
&= 2 \cdot 3^{k+1} + 3 \cdot 3^k + 8(-1)^k + 12(-1)^{k-1} \\
&= 2 \cdot 3^{k+1} + 3^{k+1} + (8 - 12)(-1)^k \\
&= 3 \cdot 3^{k+1} - 4(-1)^k = 3^{k+1} + 4(-1)(-1)^k \\
&= 3^{k+2} + 4(-1)^{k+1}
\end{aligned}$$

$$a_{k+1} = 3^{k+2} + 4(-1)^{k+1}$$

□

Del 2

Problem 6

Problem: Visa att för varje $n \geq 1$ är talet n^3+2n delbart med 3, dvs. $n^3+2n = 3q$ där $q \in \mathbb{N}$.

Lösning:

Induktionsbas (IB) $n = 1$:

$$VL = 1^3 + 2 \cdot 1 = 1 + 2 = 3$$

Induktionsantagande (IA) Antag att $k^3 + 2k = 3q$ där $q \in \mathbb{N}$ och $k \geq 1$.

Induktionssteg (IS) Visa att $(k+1)^3 + 2(k+1)$ är delbart med 3.
Vi expanderar termerna genom:

$$(k+1)^3 + 2(k+1) = (k^3 + 3k^2 + 3k + 1) + (2k + 2)$$

Från det kan vi gruppera termerna enligt följande:

$$(3k^2 + 3k + 3) + (k^3 + 2k) = 3(k^2 + k + 1) + (k^3 + 2k)$$

Enligt induktionsantagandet är $k^3 + 2k$ delbart med 3 och kan skrivas som $3q$. Uttrycket kan därför skrivas som till:

$$3(k^2 + k + 1) + 3q = 3(k^2 + k + 1 + q)$$

$$(k+1)^3 + 2(k+1) = \mathbf{3}(k^2 + k + 1 + q) \equiv 0 \pmod 3$$

□

Problem 7

Problem: En talföljd $a_0,\ a_1,\ a_2,\ \ldots$ definieras för alla heltal $n \geq 0$ genom $a_0 = 0$ och därefter $a_{n+1} = \frac{1}{2-a_n}$, för $n \geq 0$. Gissa en explicit formel för a_n och bevisa den sedan med induktion.

Lösning:

Arbete mot gissning Vi börjar med att räkna ut de första 4 talen med hjälp av att vi vet att $a_0 = 0$:

$$a_1 = \frac{1}{2-a_0} = \frac{1}{2-0} = \frac{1}{2}$$

$$a_2 = \frac{1}{2-a_1} = \frac{1}{2-\frac{1}{2}} = \frac{1}{\frac{3}{2}} = \frac{2}{3}$$

$$a_3 = \frac{1}{2-a_2} = \frac{1}{2-\frac{2}{3}} = \frac{1}{\frac{4}{3}} = \frac{3}{4}$$

$$a_4 = \frac{1}{2-a_3} = \frac{1}{2-\frac{3}{4}} = \frac{1}{\frac{5}{4}} = \frac{4}{5}$$

Från detta kan vi notera ett mönster och göra vår gissning för den explicita formeln:

$$a_n = \frac{n}{n+1}$$

Induktionsbas (IB) $n = 0$:

$$a_0 = \frac{0}{0+1} = \frac{0}{1} = 0$$

Detta stämmer överens med faktumet att $a_0 = 0$ från problembeskrivningen.

Induktionsantagande (IA) Antag att $a_k = \frac{k}{k+1}$ för $k \geq 0$.

Induktionssteg (IS) Visa att $a_{k+1} = \frac{k+1}{k+2}$. Vi börjar med att kombinera den gissade formeln med den rekursivt definierade formeln från problembeskrivningen. Vi sätter sedan in värdet på a_k taget från (IA):

$$a_{k+1} = \frac{1}{2-a_k} = \frac{1}{2-\frac{k}{k+1}} = \frac{1}{\frac{2(k+1)-k}{k+1}} = \frac{1}{\frac{k+2}{k+1}} = \frac{k+1}{k+2}$$

$$a_{k+1} = \frac{k+1}{k+2}$$

□

Problem 8

Problem: Använd induktion för att visa att för alla $n \geq 1$ är talet $2^{2n} - 1$ delbart med 3.

Lösning:

Induktionsbas (IB) $n = 1$:

$$2^{2 \cdot 1} - 1 = 2^2 - 1 = 4 - 1 = 3$$

vilket givetvis är delbart med 3.

Induktionsantagande (IA) Antag att $2^{2k} - 1$ är delbart med 3, dvs. $2^{2k} - 1 = 3q$ där $q \in \mathbb{N}$ för $k \geq 1$.

Induktionssteg (IS) Visa att $2^{2(k+1)} - 1$ är delbart med 3.
Uttrycket kan expanderas till

$$2^{2k+2} - 1 = 2^2 \cdot 2^{2k} = 4 \cdot 2^k - 1$$

Vi kan sedan gruppera termerna enligt:

$$4 \cdot 2^{2k} - 1 = 3 \cdot 2^{2k} + 2^{2k} - 1$$

Enligt (IA) är $2^{2k} - 1$ delbart med 3 och kan skrivas om till $3q$. Därför kan uttrycket skrivas om till:

$$3 \cdot 2^{2k} + 2^{2k} - 1 = 3 \cdot 2^{2k} + 3q = 3(2^{2k} + q)$$
$$2^{2(k+1)} - 1 = \mathbf{3}(2^{2k} + q) \equiv 0 \pmod 3$$

□

Problem 9

Problem: Visa att antalet icke-tomma delmängder till en mängd med $n \geq 1$ element är $2^n - 1$.

Lösning:

Induktionsbas (IB) $n = 0,\ n = 1$:
Låt $A = \varnothing$ och $B = b_0$. Potensmängden $\mathbb{P}(X)$ till mängden X är mängden av alla delmängder till X. Då vi inte vill inkludera den tomma mängden i kardinaliteten av potensmängden för X definierar jag en ny mängd $\lambda(X) = |\mathbb{P}(X)| - 1$. Nedan visas $\lambda(A)$ respektive $\lambda(B)$:

$$\begin{aligned} \mathbb{P}(A) = \ \mathbb{P}(\varnothing) \ &= \quad \{\varnothing\} \quad \implies \lambda(A) = 0 = 2^0 - 1 \\ \mathbb{P}(B) = \mathbb{P}(\{b_0\}) &= \{\varnothing,\ \{b_0\}\} \implies \lambda(B) = 1 = 2^1 - 1 \end{aligned}$$

Induktionsantagande (IA) Antag att $\lambda(M_k) = 2^k - 1$ för godtycklig mängd M_k där $|M_k| = k,\ k \geq 1$.

Induktionssteg (IS) Visa att $\lambda(M_{k+1}) = 2^{k+1} - 1$ för en mängd M_{k+1} med $k + 1$ element.
Ett mönster vi kan notera är att potensmängden till M innehåller alla mängder med i element, där $0 \leq i \leq k + 1$, av kombinationerna av elementen från M:

$$\begin{aligned} \mathbb{P}(M) = \ &\{\varnothing,\ \{m_0\},\ \{m_1\},\ \cdots,\ \{m_k\}, \\ &\{m_0,\ m_1\},\ \{m_0,\ m_2\},\ \cdots,\ \{m_1,\ m_2\},\ \cdots, \\ &\cdots \\ &\{m_0,\ m_1, \cdots,\ m_{k+1}\}\} \end{aligned}$$

Vi kan notera att unionen mellan $\{m_{k+1}\}$ och alla mängder förutom den tomma mängden i mängden med k element skapar lika många unika delmängder. Exempel visas nedan för mängd M med 2 element:

$$\mathbb{P}(M_k) = \{\varnothing,\ \{m_0\},\ \{m_1\},\ \{m_0,\ m_1\}\}$$

Mängden med 3 element innehåller alltså $3 = 2^2 - 1$ icke-tomma delmängder. Om vi lägger till dubletter av alla delmängder som genomgår union med element m_2 får vi:

$$\{\varnothing, \{m_0\}, \{m_1\}, \{m_0, m_1\}\} \cup \{\{m_2\}, \{m_0\} \cup \{m_2\}, \{m_1\} \cup \{m_2\}, \{m_0, m_1\} \cup \{m_2\}\}$$

$$=$$

$$\{\varnothing,\ \{m_0\},\ \{m_1\},\ \{m_2\},\ \{m_0,\ m_1\},\ \{m_0,\ m_2\},\ \{m_1,\ m_2\},\ \{m_0,\ m_1,\ m_2\}\}$$

Den nya mängden innehåller $7 = 2^3 - 1$ icke-tomma delmängder. Enligt (IA) har mängden M_k med k element $2^k - 1$ icke-tomma delmängder. Om vi nu använder oss av samma metod för M_k ser vi att antalet icke-tomma delmängder blir:

$$\lambda(M_k) = 2^k - 1$$

$$|\,\mathbb{P}(M_k) \cup \{\{x\} \cup \{m_{k+1}\} \mid x \in \mathbb{P}(M_k)\}\,| = (2^k - 1) + (2^k)$$

Det utförs alltså en union mellan potensmängden och mängden med unionen av potensmängdens med $\{m_{k+1}\}$ element. Vi får $2^k - 1$ element från potensmängden och lika många, plus 1 från den andra mängden eftersom unionen mellan $\{m_{k+1}\}$ och $\varnothing$ blir $\{m_{k+1}\}$. Vi får alltså slutligen en kardinalitet på:

$$\lambda(M_{k+1}) = (2^k - 1) + (2^k) = 2 \cdot 2^k - 1 = 2^{k+1} - 1$$

□

Problem 10

Fermattalen Fe_n definieras som $Fe_n = 2^{2^n} + 1$, för alla $n \geq 0$.

Delproblem 1: Visa att $Fe_n = Fe_0 Fe_1 \cdots Fe_{n-1} + 2$, för alla $n \geq 1$.

Lösning:

Induktionsbas (IB) $n = 1$: Från definition:

$$Fe_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$$

Från beskrivning i delproblem 1:

$$Fe_1 = Fe_0 + 2 = (2^{2^0} + 1) + 2 = 2^1 + 3 = 5$$

Induktionsantagande (IA) Antag att $Fe_k = Fe_0 Fe_1 \cdots Fe_{k-1} = 2^{2^k} + 1$ för $k \geq 1$.

Induktionssteg (IS) Visa att $Fe_{k+1} = Fe_0 Fe_1 \cdots Fe_{k-1} Fe_k + 2 = 2^{2^{k+1}} + 1$.
Vi börjar med att gruppera faktorerna i produkten enligt:

$$Fe_k = (Fe_0 Fe_1 \cdots Fe_{k-1}) \cdot Fe_k + 2$$

Enligt (IA) kan vi skriva om detta som:

$$(Fe_0 Fe_1 \cdots Fe_{k-1}) \cdot Fe_k + 2 = (Fe_k - 2) \cdot Fe_k + 2$$

Vi använder nu (IA) för att skriva om likheten enligt:

$$\begin{aligned}
(Fe_k - 2) \cdot Fe_k + 2 &= Fe_k^2 - 2Fe_k + 2 \\
&= (2^{2^k} + 1)^2 - 2(2^{2^k} + 1) + 2 \\
&= ((2^{2^k})^2 + 2 \cdot 2^{2^k} + 1) - 2 \cdot 2^{2^k} - 2 + 2 \\
&= (2^{2^k})^2 \ + 1 \\
&= 2^{2 \cdot 2^k} \quad + 1 \\
&= 2^{2^{k+1}} \quad + 1
\end{aligned}$$

$$Fe_{k+1} = Fe_0 Fe_1 \cdots Fe_{k-1} Fe_k + 2 = 2^{2^{k+1}} + 1$$

□

Delproblem 2: Använd delproblem 1 för att visa att för $i \neq j$ är $SGD(Fe_i,\ Fe_j) = 1$, dvs. att två olika Fermattal inte har några gemensamma delare större än 1.

Lösning:

Test av basfall: $i = 1,\ j = 2$:

$$Fe_i = Fe_1 = F_0 + 2 = 5$$

$$Fe_j = Fe_2 = F_1 + 2 = 7$$

$$SGD(Fe_i,\ Fe_j) = SGD(5,\ 7) = 1$$

Om vi ställer upp och jämför Fe_i och Fe_j får vi:

$$Fe_i = Fe_0 Fe_1 \cdots Fe_{i-1} + 2$$

$$Fe_j = Fe_0 Fe_1 \cdots Fe_{j-1} + 2$$

Låt $d = SGD(Fe_i,\ Fe_j)$. Vi antar att $i < j$. Från det kan vi konstatera att:

$$d \mid Fe_i \implies d \mid Fe_0 Fe_1 \cdots \boldsymbol{Fe_i} \cdots Fe_{j-1} \iff \frac{Fe_j - 2}{d} \in \mathbb{N}$$

Från definitionen av delbarhet:

$$(d \mid a) \wedge (d \mid b) \implies d \mid (ax + by)$$

för $a, b, d, x, y \in \mathbb{N}$. Eftersom $d \mid Fe_j$ kan vi låta:

$$\begin{cases} a = Fe_j \\ x = 1 \\ b = Fe_j - 2 \\ y = -1 \end{cases}$$

Vilket leder till:

$$d \mid Fe_j - Fe_0 Fe_1 \cdots Fe_i \cdots Fe_{j-1} \iff d \mid Fe_j - (Fe_j - 2) \iff d \mid 2$$

Då vi vet att definitionen av det n:te Fermattalet är $2^{2^n} + 1$, för $n \geq 0$, är det 1 mer än en multipel av 2. Alla Fermattal är alltså **udda**. Detta resulterar i att d inte kan vara 2. Då de enda talen som delar 2 är 2 och 1, och $d \neq 2$, kan vi konstatera att:

$$d = SGD(Fe_i,\ Fe_j) = 1$$

. □

Delproblem 3: Dra slutsatsen att det finns oändligt många primtal.

Lösning: I delproblem 2 visade vi att alla Fermattal är parvis relativt prima. Det innebär att $p_n \mid Fe_n$ för $n \geq 1$ där p_n inte delar något annat Fermattal än Fe_n. Eftersom Fermattalen är en oändlig talföljd måste det finnas oändligt många distinkta primtal p_n som delar Fermattalen, vilket innebär att det måste finnas oändligt många primtal i allmänhet.

□