

TALTEORI

Følger og den kinesiske restklassesætning.

Disse noter forudsætter et grundlæggende kendskab til talteori som man kan få i Marianne Terps og Peter Trosborgs noter om talteori.

Noterne vil primært introducere forskellige opgaveteknikker med fokus på følger, samt opgaver hvor man har brug for den kinesiske restklassesætning.

1 Følger

Mange opgaver til internationale konkurrencer handler om følger af heltal som man typisk skal vise har en bestemt egenskab, fx at de er periodiske fra et vist trin eller ikke indeholder kvadrattal. Følgerne er ofte beskrevet rekursivt, og derfor skal man ofte se på rekursionsformlen og evt. omskrive denne.

1.1 Periodiske følger

En følge $(a_n)_{n \in \mathbb{N}}$ kaldes periodisk hvis der findes et positivt helt tal m så $a_{n+m} = a_n$ for alle $n \in \mathbb{N}$. Periodens længde er det mindste positive hele tal m med denne egenskab.

Følgen $(a_n)_{n \in \mathbb{N}}$ kaldes periodisk fra et vist trin hvis der findes positive hele tal m og k så $a_{n+m} = a_n$ for alle $n \geq k$.

1.2 Eksempel

I følgen 1, 9, 7, 7, 4, 7, 5, 3, 9, 4, 1, ... er hvert ciffer fra og med det femte summen af de fire foregående modulo 10. I dette eksempel skal vi undersøge hvilken af disse talkombinationer der kan indgå i følgen: a) 1,2,3,4, b) 3,2,6,9, c) 0,1,9,7.

Da der kun findes et endeligt antal kombinationer med fire cifre, vil følgen være periodisk fra et vist trin. Men da man ud fra fire cifre i følgen også entydigt kan bestemme det foregående, kan man fortsætte den uendeligt i begge retninger med en fast periode. Derfor vil 1,9,7,7 optræde igen længere fremme i følgen, og cifferet lige inden vil være 0. Dermed optræder kombinationen 0,1,9,7 i følgen. I mange opgaver med følger kan man netop konkludere at følgen må være periodisk fra et vist trin da der kun er endeligt mange muligheder. Herefter skal man så overveje om det først er fra et vist trin at den er periodisk, eller om den som i dette eksempel er periodisk fra starten.

Vi mangler stadig at finde ud af om 1,2,3,4 og 3,2,6,9 indgår i følgen. Da den er periodisk, kan man jo i princippet blive ved til man har fundet hele perioden, og så se om de indgår. Dette er dog ikke altid en god strategi da længden af perioden kan være temmelig stor. Det kan som regel betale sig at lede efter et andet system i følgen med en kortere periode. Reducerer vi i dette eksempel følgens cifre modulo 2, får vi 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, ... Her ud fra kan vi se at følgen har 1, 1, 1, 1, 0 som periode når vi regner modulo 2, og dette udelukker a) og b).

1.3 Opgave

Fibonacci-tallene er som bekendt defineret ved $F_0 = 0$, $F_1 = 1$ og $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Vis at for ethvert helt tal k findes et positivt helt tal n så k går op i F_n .

1.4 Opgave

For et positivt helt tal n betegner a_n det sidste ciffer i $n^{(n)}$. Bevis at følgen (a_n) er periodisk, og bestem længden af perioden. (Baltic Way 2006)

1.5 Eksempel

Vi ser på følgen $a_1 = a_2 = 1$ og $a_{n+2} = a_n a_{n+1} + 1$ for $n > 2$, og vil gerne vise at der ikke findes noget n , $n > 2$, så a_n er et kvadrattal. Følgen er selvfølgelig ikke periodisk, men regner vi modulo fx 4, er følgen periodisk fra et vist trin. Her får vi 1, 1, 2, 3, 3, 2, 3, 3, 2, 3, 3, \dots , dvs. at følgen er periodisk fra $n = 3$ med perioden 2, 3, 3. Da 2 og 3 ikke er kvadratiske rester modulo 4, er a_n ikke et kvadrattal for noget $n > 2$.

1.6 Opgave

En følge af positive hele tal (a_n) er givet ved

$$a_0 = m \text{ og } a_{n+1} = a_n^5 + 487, \quad n \geq 0.$$

Bestem de værdier af m for hvilke følgen indeholder flest muligt kvadrattal. (NMC 2006)

1.7 Opgave

En følge (x_n) er givet ved $x_0 = a$, $x_1 = 2$ og $x_n = 2x_{n-1}x_{n-2} - x_{n-1} - x_{n-2} + 1$ for $n > 1$. Find alle hele tal a således at $2x_{3n} - 1$ er et kvadrattal for alle $n \geq 1$.

1.8 Eksempel

Om en følge af naturlige tal a_0, a_1, a_2, \dots oplyses at $a_0 < a_1$ og $a_n = 3a_{n-1} - 2a_{n-2}$ for $n > 1$. Vi ønsker at vise at $a_m \equiv a_{m+1} \pmod{2^m}$ for alle naturlige tal m .

Følgen er ikke periodisk, og da det tal vi skal regne modulo afhænger af indekset, kan vi heller ikke betragte følgen modulo et fast tal. I stedet udnytter vi rekursionsformlen og omskriver på følgende måde. Da $a_n = 3a_{n-1} - 2a_{n-2}$, er

$$a_{m+1} - a_m = 2^1(a_m - a_{m-1}) = 2^2(a_{m-1} - a_{m-2}) = \dots = 2^m(a_1 - a_0).$$

Her af kan vi se at $a_m \equiv a_{m+1} \pmod{2^m}$ for alle naturlige tal m .

1.9 Opgave

Lad (F_n) være følgen af Fibonaccital. Vis at F_n og F_{n+1} er indbyrdes primiske.

1.10 Opgave

En følge af naturlige tal a_1, a_2, a_3, \dots opfylder at hvis $m, n \in \mathbb{N}$, $m < n$ og m går op i n , da vil a_m gå op i a_n og $a_m < a_n$.

Bestem den mindst mulige værdi af a_{2000} . (Baltic Way 2000)

1.11 Opgave

Lad a_1, a_2, \dots være en følge af heltal med uendeligt mange positive og uendeligt mange negative tal. Antag at der for ethvert naturligt tal n fås n forskellige rester når tallene a_1, a_2, \dots, a_n deles med n .

Vis at ethvert helt tal optræder netop en gang i talfølgen. (IMO 2005)

2 Den kinesiske restklassesætning

I nogle opgaver har man brug for at undersøge om der findes løsninger x til kongruenssystemer af typen

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \dots, \quad x \equiv a_m \pmod{n_m}.$$

Dette handler den kinesiske restklasse sætning om.

2.1 Den kinesiske restklassesætning

Lad n være et naturligt tal, og $n = n_1 n_2 \dots n_m$, hvor $(n_i, n_j) = 1$ når $i \neq j$.

Da findes uendeligt mange heltallige løsninger til kongruenssystemet

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_m \pmod{n_m}. \end{aligned}$$

Samtlige løsninger udgør netop en restklasse modulo n .

BEVIS: Sætningen vises ved induktion. Den er oplagt sand for $m = 1$.

Betragt nu tilfældet $m = 2$. Vi ønsker at bestemme en løsning x til

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}. \end{aligned}$$

Da $(n_1, n_2) = 1$ findes en invers n_1^{-1} til n_1 modulo n_2 . Betragt $x = a_1 + (a_2 - a_1)n_1^{-1}n_1$. Der gælder at

$$\begin{aligned} x &= a_1 + (a_2 - a_1)n_1^{-1}n_1 \equiv a_1 \pmod{n_1}, \text{ og} \\ x &= a_1 + (a_2 - a_1)n_1^{-1}n_1 \equiv a_1 - (a_2 - a_1) = a_2 \pmod{n_2}. \end{aligned}$$

Dermed har vi konstrueret en løsning til kongruenssystemet.

Vi viser nu at samtlige løsninger netop udgør en restklasse modulo n . Det er klart at hvis $y \equiv x \pmod{n}$, da er y også en løsning. Antag nu at x og y er løsninger. Da vil både n_1 og n_2 gå op i $x - y$, og da $(n_1, n_2) = 1$, vil også n gå op i $x - y$. Dermed udgør løsningerne netop en restklasse modulo n .

Vi skal nu til selve induktionsskridtet, men har faktisk lavet alt arbejdet i tilfældet $m = 2$. Antag nu at sætningen gælder for m . Vi ønsker nu at vise at sætningen også gælder for $m + 1$. Lad $n = n_1 n_2 \dots n_{m+1}$, hvor $(n_i, n_j) = 1$ når $i \neq j$. Betragt kongruenssystemet

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{m+1} \pmod{n_{m+1}}. \end{aligned}$$

Ifølge induktionsantagelsen udgør samtlige løsninger til de m første kongruenser netop en restklasse modulo $n' = n_1 n_2 \dots n_m$. Lad a' være en repræsentant for denne restklasse. Løsningerne til kongruenssystemet

$$\begin{aligned} x &\equiv a' \pmod{n'} \\ x &\equiv a_{m+1} \pmod{n_{m+1}} \end{aligned}$$

er identiske med løsningerne til det oprindelige kongruenssystem, og de udgør ifølge induktionsantagelsen én restklasse modulo $n'n_{m+1} = n$, da $(n', n_{m+1}) = 1$. Dermed er sætningen bevist.

2.2 Eksempel

Vi ønsker ved hjælp af den kinesiske restklassesætning at bestemme samtlige løsninger til

$$\begin{aligned}x &\equiv 3 \pmod{7} \\x &\equiv 2 \pmod{17}.\end{aligned}$$

Først bemærker vi at 5 er invers til 7 modulo 17 da $5 \cdot 7 \equiv 1 \pmod{17}$. Dermed er $x = 3 + (2 - 3)5 \cdot 7 = -32$ en løsning til kongruenssystemet, og vi ved at samtlige løsninger er $x = -32 + k7 \cdot 17$, $k \in \mathbb{Z}$.

2.3 Opgave

Bestem samtlige løsninger til kongruenssystemet

$$\begin{aligned}x &\equiv 3 \pmod{6} \\x &\equiv 6 \pmod{19}.\end{aligned}$$

2.4 Eksempel

I eksemplet før så vi hvordan man kan benytte den kinesiske restklassesætning til at bestemme samtlige løsninger til et kongruenssystem, men i nogle opgaver har man blot behov for at vide at der findes en løsning.

I dette eksempel vil vi vise at der findes 1000 (eller så mange det skal være) på hinanden følgende hele tal som alle er delelige med et kubiktal større end 1. Først vælger vi 1000 forskellige primtal $p_1, p_2, \dots, p_{1000}$. Ifølge den kinesiske restklassesætning har følgende kongruenssystem en løsning.

$$\begin{aligned}x &\equiv -1 \pmod{p_1^3} \\x &\equiv -2 \pmod{p_2^3} \\&\vdots \\x &\equiv -1000 \pmod{p_{1000}^3}.\end{aligned}$$

Hvis x er en løsning, da er $x + 1, x + 2, \dots, x + 1000$ tusind på hinanden følgende hele tal som alle er delelige med et kubiktal.

2.5 Opgave

Vis at for alle naturlige tal n findes der n på hinanden følgende hele tal således at tal nummer i er delelig en i 'te potens af et helt tal.

2.6 Opgave

Vis at for alle naturlige tal n og m findes n på hinanden naturlige tal, således at hvert af disse er deleligt med mindst m forskellige primtal.

2.7 Opgave

Vis at der eksisterer en følge af naturlige tal a_1, a_2, \dots således at summen af vilkårlige n på hinanden følgende elementer er delelig med n^2 . (Baltic Way 2006).

3 Løsniner

Opgave 1.3 Lad k være et fast helt tal, og lad a_n betegne resten ved division af F_n med k . Da der kun er k^2 par af restklasser modulo k , må der findes to ens par (a_i, a_{i+1}) og (a_j, a_{j+1}) , $0 \leq i < j$. Det er klart ud fra definitionen af Fibonacci-tallene at følgen af restklasserne er periodisk fra et vist trin, og da den forrige restklasse desuden kan bestemmes ud fra de to efterfølgende ($a_{n-1} \equiv a_{n+1} - a_n \pmod{k}$), er følgen periodisk fra starten. Periodelængden er divisor i $j-i$, og derfor er $a_0 \equiv a_{j-i} \pmod{k}$, dvs. at F_{j-i} er delelig med k .

Opgave 1.4 Lad b_n betegne det sidste ciffer i n .

Det er nemt at se, at hvis $b_n = 0, 1, 5, 6$, da er $a_n = 0, 1, 5, 6$.

Hvis $b_n = 4, 9$, gennemløber sidste ciffer i n^m perioden $4 - 6$ eller $9 - 1$.

Når $b_n = 4$, er n^n lige, og dermed $a_n = 6$.

Når $b_n = 9$, er n^n ulige, og dermed $a_n = 9$.

Hvis $b_n = 2, 3, 7, 8$ gennemløber sidste ciffer i n^m perioden $2-4-8-6, 3-9-7-1, 7-9-3-1$ eller $8-4-2-6$. Her er perioden af længde 4, dvs. vi skal se på n^n modulo 4.

Når $b_n = 2, 8$, er $n^n \equiv 0 \pmod{4}$, dvs. at $a_n = 6$.

Når $b_n = 3$, er $n \equiv 3 \pmod{20}$ eller $n \equiv 13 \pmod{20}$, dvs. $n^n \equiv 3 \pmod{4}$ eller $n^n \equiv 1 \pmod{4}$. Dermed er $a_n = 7$ eller $a_n = 3$.

Når $b_n = 7$, er $n \equiv 7 \pmod{20}$ eller $n \equiv 17 \pmod{20}$, dvs. $n^n \equiv 3 \pmod{4}$ eller $n^n \equiv 1 \pmod{4}$. Dermed er $a_n = 3$ eller $a_n = 7$.

Alt i alt ser vi at følgen er periodisk med længde 20.

Opgave 1.6 Svaret er $m = 9$.

Bemærk først at hvis a_n er et kvadrattal, da er $a_n \equiv 0 \vee a_n \equiv 1 \pmod{4}$.

Hvis $a_k \equiv 0 \pmod{4}$, da er $a_{k+i} \equiv 3 \pmod{4}$ når i er ulige, og $a_{k+i} \equiv 2 \pmod{4}$ når i er lige. Dermed er a_n ikke et kvadrattal for noget indeks større end k .

Hvis $a_k \equiv 1 \pmod{4}$, da er $a_{k+1} \equiv 0 \pmod{4}$. Dermed er a_n ikke et kvadrattal for noget indeks større end $k + 1$.

Dette viser at følgen højst indeholder to kvadrattal.

Antag at følgen indeholder to kvadrattal a_k og a_{k+1} . Da er $a_k = s^2$, hvor s er ulige, og $a_{k+1} = s^{10} + 487 = t^2$. Lad $t = s^5 + r$. Da er $t^2 = (s^5 + r)^2 = s^{10} + 2s^5r + r^2$, og dermed $2s^5r + r^2 = 487$.

Hvis $s = 1$, er $r(2+r) = 487$ hvilket er umuligt. Hvis $s = 3$, er $486r + r^2 = 487$, og dermed $r = 1$. Hvis $s > 3$, har ligningen ingen løsninger. Dermed er $a_k = 9$, og da $a_n > 487$ for $n > 0$, må $m = a_0 = 9$.

Opgave 1.7 Lad $y_n = 2x_n - 1$. Da er

$$\begin{aligned} y_n &= 2(2x_{n-1}x_{n-2} - x_{n-1} - x_{n-2} + 1) - 1 = 4x_{n-1}x_{n-2} - 2x_{n-1} - 2x_{n-2} + 1 = \\ &= (2x_{n-1} - 1)(2x_{n-2} - 1) = y_{n-1}y_{n-2} \text{ når } n > 1. \end{aligned}$$

Bemærk at $y_1 = 3$, $y_2 = 3y_0$ og $y_3 = y_1y_2 = 3^2y_0$. Ved induktion ses let at $y_{3n} = 3^{2s}y_0^t$ hvor s og t er naturlige tal. Dermed er y_{3n} et kvadrattal for alle $n \geq 1$ præcis når y_0 er et kvadrattal. Da $y_0 = 2a - 1$, fås det ønskede resultat netop når $a = \frac{(2m-1)^2+1}{2}$ for alle naturlige tal m .

Opgave 1.9 Da $F_{n+1} = F_n + F_{n-1}$, er

$$\gcd(F_{n+1}, F_n) = \gcd(F_{n+1} - F_n, F_n) = \gcd(F_{n-1}, F_n).$$

Induktivt giver dette $\gcd(F_{n+1}, F_n) = \gcd(F_2, F_1) = \gcd(1, 1) = 1$.

Opgave 1.10 Bemærk først at

$$a_{2000} \geq 2a_{1000} \geq 2^2 a_{500} \geq 2^3 a_{250} \geq 2^4 a_{125} \geq 2^5 a_{25} \geq 2^6 a_5 \geq 2^7 a_1 \geq 2^7 = 128.$$

Betragt følgen $a_1 = 1$ og $a_n = 2^{\alpha_1 + \alpha_2 + \dots + \alpha_k}$ for $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Denne følge opfylder den ønskede betingelse, og da $2000 = 2^4 \cdot 5^3$, er $a_{2000} = 128$.

Opgave 1.11 Lad $A_n = \{a_1, a_2, \dots, a_n\}$. Mængden A_n består af n forskellige tal da de har forskellige rester modulo n . Bemærk desuden at hvis $a_i, a_j \in A_n$, da må $k = |a_i - a_j| < n$, for ellers vil $a_i, a_j \in A_k$ og $a_i \equiv a_j \pmod{k}$.

Vi har nu at forskellen mellem det største og det mindste tal i A_n er mindre end n , og derfor må A_n indeholde n på hinanden følgende tal. Da følgen indeholder uendeligt mange både positive og negative tal, må alle hele tal forekomme mindst en gang. Samlet giver dette at alle heltal netop optræder en gang i følgen.

Et eksempel på en mulig følge: $0, -1, 1, -2, 2, \dots$

Opgave 2.3 Samtlige løsninger er $x = 63 + k114$, $k \in \mathbb{Z}$.

Opgave 2.5 Først vælger vi n forskellige primtal p_1, p_2, \dots, p_n . Ifølge den kinesiske restklassesætning har følgende kongruenssystem en løsning.

$$\begin{aligned} x &\equiv -1 \pmod{p_1^1} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -1000 \pmod{p_n^n}. \end{aligned}$$

Hvis x er en løsning, da er $x + 1, x + 2, \dots, x + n$ n på hinanden følgende hele tal således at tal nummer i er delelig med en i 'te potens af et helt tal.

Opgave 2.6 For at vise dette har vi brug for den kinesiske restklassesætning.

Vælg nm forskellige primtal $p_{11}, \dots, p_{1m}, p_{21}, \dots, p_{2m}, \dots, p_{nm}$. Sæt $q_j = p_{j1} p_{j2} \dots p_{jm}$ for $j = 1, 2, \dots, n$. Da er q_1, q_2, \dots, q_n indbyrdes primiske. Den kinesiske restklassesætning giver da at der findes et naturligt tal x som løsning til kongruenssystemet

$$x + 1 \equiv 0 \pmod{q_1}, \quad x + 2 \equiv 0 \pmod{q_2}, \quad \dots, \quad x + n \equiv 0 \pmod{q_n}.$$

De n på hinanden følgende tal $x + 1, x + 2, \dots, x + n$ er nu delelige med mindst m forskellige primtal hver.

Opgave 2.7 Vi viser at følgen eksisterer ved at vise hvordan man konstruerer det næste element ud fra de foregående. Det er klart at a_1 kan vælges fuldstændigt frit.

Antag nu at a_1, a_2, \dots, a_m opfylder at summen af vilkårlige n på hinanden følgende elementer er delelig med n^2 for alle $n \leq m$. Vi ønsker at konstruere a_{m+1} , så

$$a_{m+1} \equiv -(a_{m-n+2} + \dots + a_m) \pmod{n^2} \quad \dagger$$

for alle $n \leq m + 1$.

Lad p_1, \dots, p_k være samtlige primtal mindre end eller lig med $m + 1$, og lad α_i være

det største hele tal så $p_i^{\alpha_i} \leq m + 1$. Lad yderligere a_{m+1} være en løsning til følgende kongruenssystem:

$$\begin{aligned} x &\equiv -(a_{m-p_1^{\alpha_1}+2} + \dots + a_m) \pmod{p_1^{2\alpha_1}} \\ &\vdots \\ x &\equiv -(a_{m-p_k^{\alpha_k}+2} + \dots + a_m) \pmod{p_k^{2\alpha_k}}. \end{aligned}$$

Vi ønsker nu at vise at a_{m+1} opfylder \dagger for alle $n \leq m + 1$ da det giver det ønskede.

Først viser vi at a_{m+1} opfylder \dagger for alle $n = p_i^{\beta_i}$, $i = 1, 2, \dots, k$ og $\beta_i = 1, \dots, \alpha_i - 1$.

Vi ved at summen af

$$a_{m-p_1^{\alpha_1}+2}, \dots, a_{m+1}$$

er delelig med $p_i^{2\alpha_i}$ og dermed også med $p_i^{2\beta_i}$. Hvis vi grupperer elementerne i $p_i^{\alpha_i - \beta_i}$ grupper med $p_i^{\beta_i}$ på hinanden følgende elementer i hver, ved vi om samtlige grupper på nær den sidste, at summen af elementerne i gruppen er delelig med $p_i^{2\beta_i}$ pga. konstruktionen af a_1, a_2, \dots, a_m . Men da summen af samtlige elementer i alle grupperne er delelig med $p_i^{2\beta_i}$, må summen af elementerne i den sidste gruppe også være det. Vi har hermed vist at \dagger er opfyldt for alle $n = p_i^{\beta_i}$, $i = 1, 2, \dots, k$ og $\beta_i = 1, \dots, \alpha_i - 1$.

Nu ønsker vi at vise at \dagger er sand for alle $n \leq m + 1$. Da n er et produkt af primtalspotenser $p_i^{\beta_i}$, $i = 1, 2, \dots, k$ og $\beta_i = 1, \dots, \alpha_i$, er det nok at vise at hvis \dagger er sand for $n = n_1$ og $n = n_2$ med $n_1 n_2 \leq m + 1$ og $(n_1, n_2) = 1$, da er \dagger også sand for $n = n_1 n_2$. Antag at \dagger er sand for $n = n_1$ og $n = n_2$ med $n_1 n_2 \leq m + 1$ og $(n_1, n_2) = 1$. Da summen af n_1 på hinanden følgende elementer er delelig med n_1^2 , må summen af $n_1 n_2$ på hinden følgende elementer også være delelig med n_1^2 . Tilsvarende gælder for n_2 . Da $(n_1, n_2) = 1$ gælder altså at summen af $n_1 n_2$ på hinanden følgende elementer er delelig med $(n_1 n_2)^2$ hvilket netop var hvad vi skulle vise.