Meditation over Midterbinomialkoefficienten

– En rusrejse fra en fjern juletid

Frederik Ravn Klausen, Peter Michael Reichstein Rasmussen

Ved juletid for ikke så længe siden faldt tre russer over et åbent problem.

Formodning 1 Midterbinomialkoefficienten $\binom{2n}{n}$ er altid delelig med 4 eller 9 for $n \geq 4$ bortset fra $n = 64$ og $n = 256$.

I deres rusnaivitet så det ud til at være et sødt lille problem, som man hurtigt kunne løse. Et lille krydderi til julestemningen. Snart kunne de dog konstatere at dette ikke var tilfældet, men undervejs i arbejdet med formodningen dukkede sjov matematik frem. Dette er historien om deres rejse.

Rejsen indebærer flere hyggelige vandringer i talteoriens og kombinatorikkens snedækkede landskaber, som efter forfatternes anbefaling bør nydes foran en åben pejs.

Indledende julekagebagning

Notation 2 For $a, p \in \mathbb{N}$ og $p > 1$ skriver vi[4] $p^k \mid\mid a$, hvis k er det største heltal således at $p^k \mid a$.

Notation 3 Lad $a, b \in \mathbb{N}$ være givet med $b > 1$. Da betegner $(a)_b$ tallet a skrevet i base b, og a_b betegne at a *er* skrevet i base b.

I det følgende vil vi lege lidt med menter. Disse skal opfattes, som man lærte det, da man var en lille pebernødsgnaskende folkeskoleelev. Eksempelvis vil der komme to menter, når man lægger 1 til 99.

[4] Hvor $\mathbb{N}$ naturligvis ikke indeholder 0.

Sætning 4 (Kummers sætning) *Der gælder* $p^k \mid\mid \binom{m+n}{m}$, *hvis og kun hvis der er netop* k *menter i additionen* $(n)_p + (m)_p = (n+m)_p$.

Bevis. Beviset og matematikken bag er rigtig fin, og kan for eksempel findes i [1]. Alternativt kan den entusiastiske læser se sætningen som en opbyggelig opgave. □

Eksempel 5 Hvis vi betragter $\binom{16}{8}$, så er 8 skrevet i base 3 givet ved $22_3 = (8)_3$, og i additionen $(8)_3 + (8)_3 = 22_3 + 22_3 = 121_3 = (16)_3$ sker der 2 menter. Det vil sige at $3^2 \mid\mid \binom{16}{8}$.

Russerne så, at Kummers sætning straks indskrænker det oprindelige problem til et spørgsmål om at vise, at der ikke findes $k > 2$ så $9 \nmid \binom{2^{k+1}}{2^k}$ bortset fra $k = 6, 8$. Dette overlades ligeledes til læseren som en (noget nemmere) opgave.

På trods af reduktionen af problemet var det dog stadig for hård en julenød for de unge russer, der i stedet betragtede følgende funktion:

Definition 6 For alle $a \in \mathbb{N}$ defineres

$$\mathcal{T}_9(a) = \#\left\{0 \leq k < a \mid 9 \nmid \binom{2^{k+1}}{2^k}\right\}.$$

Denne nye funktion kunne altså tælle antallet af modeksempler til Formodning 1 mindre end 2^a. Et øvre estimat af funktionen blev derfor vore heltes mål.

Ved hjælp af Kummers sætning kan en gæv rus benytte fordelingen af cifre i $(2^k)_3$ for et generelt k til at sige noget om antallet af gange 3 deler $\binom{2^{k+1}}{2^k}$. Det vil da vise sig at de sidste t cifre af $(2^k)_3$ er periodiske med hensyn til k med periode $2 \cdot 3^{t-1}$. Da hver periode desuden kommer til at indeholde alle mulige kombinationer af t cifre i base 3, hvor det sidste ciffer enten er 1 eller 2, fås et stærkt redskab.

Dette var det første russerne satte sig ud for at vise.

Definition 7 Eulers phi-funktion $\varphi : \mathbb{N} \to \mathbb{N}$ er defineret som

$$\varphi(n) = \#\{1 \leq a < n \mid \gcd(a, n) = 1\}.$$

Sætning 8 (Euler-Fermat) *For alle indbyrdes primiske tal $a, b \in \mathbb{N}$ gælder*

$$a^{\varphi(b)} \equiv 1 \pmod{b}.$$

Bevis. Se [1, s. 133]. □

Lemma 9 *For $k \geq 0$ gælder $3^{k+1} \mid\mid 2^{2\cdot 3^k} - 1$.*

Bevis. Beviset føres ved induktion. For $k = 0$ og $k = 1$ får vi henholdsvis

$$3^1 \mid\mid 2^2 - 1 = 3 \text{ og } 3^2 \mid\mid 2^{2\cdot 3^1} - 1 = 63,$$

hvilket er sandt. Antag nu at

$$3^{k+1} \mid\mid 2^{2\cdot 3^k} - 1.$$

for et vilkårligt $k > 0$. Benyt nu følgende faktorisering:

$$2^{2\cdot 3^{k+1}} - 1 = \left(2^{2\cdot 3^k} - 1\right) \cdot \left(\left(2^{2\cdot 3^k}\right)^2 + 2^{2\cdot 3^k} + 1\right).$$

Vi bemærker nu, at

$$2^{3^k} \equiv \left(2^3\right)^{3^{k-1}} \equiv (-1)^{3^{k-1}} \equiv -1 \pmod{9},$$

hvorved vi har

$$\left(2^{2\cdot 3^k}\right)^2 + 2^{2\cdot 3^k} + 1 \equiv (-1)^4 + (-1)^2 + 1 \equiv 3 \pmod 9.$$

Dermed gælder $3 \mid\mid \left(2^{2\cdot 3^k}\right)^2 + 2^{2\cdot 3^k} + 1$, og da $3^{k+1} \mid\mid 2^{2\cdot 3^k} - 1$, så får vi

$$3^{k+2} \mid\mid \left(2^{2\cdot 3^k} - 1\right) \cdot \left(\left(2^{2\cdot 3^k}\right)^2 + 2^{2\cdot 3^k} + 1\right) = 2^{2\cdot 3^{k+1}} - 1.$$

$\square$

Definition 10 Lad $a, b \neq 1$ være indbyrdes primiske positive heltal. Da defineres ordenen $\mathrm{ord}_a(b)$ til at være det mindste positive heltal t så $b^t \equiv 1 \pmod a$.

I julelys og måneskin kan det ses, at $b^r \equiv 1 \pmod a$ hvis og kun hvis $\mathrm{ord}_a(b) \mid r$.

Lemma 11 *Lad $k \geq 0$ og $0 < s < 2 \cdot 3^k$. Da gælder*

$$2^s \not\equiv 1 \pmod{3^{k+1}}.$$

Bevis. Lad $t := \mathrm{ord}_{3^{k+1}}(2)$. Vi viser nu, at $t = 2 \cdot 3^k$. Vi har allerede $t \leq 2 \cdot 3^k$, idet $t \mid \varphi(3^{k+1}) = 2 \cdot 3^k$ jævnfør Sætning 8.

Antag nu for modstrid, at $t < 2 \cdot 3^k$. Da må der enten gælde $t \mid 3^k$ eller $t \mid 2 \cdot 3^{k-1}$. Da vi har

$$2^{3^k} \equiv 2 \pmod 3,$$

så er den første mulighed udelukket. Yderligere følger det af Lemma 9, at $3^k \mid\mid 2^{2\cdot 3^{k-1}} - 1$, og derfor må der gælde

$$2^{2\cdot 3^{k-1}} \not\equiv 1 \pmod{3^{k+1}},$$

så $t \nmid 2 \cdot 3^{k-1}$. Dette er i modstrid med antagelsen, og derfor gælder $\operatorname{ord}_{3^{k+1}}(2) = 2 \cdot 3^k$. $\square$

Denne appetitvækkende julegodte viser altså, at $2 \cdot 3^{k-1}$ er den minimale periode for de k sidste cifre af $(2^k)_3$:

Sætning 12 *Lad k, l være givet, så $0 \leq k < l < 2 \cdot 3^t$. Da gælder $2^k \not\equiv 2^l \pmod{3^{t+1}}$. Det vil sige, at de $t+1$ sidste cifre af $(2^k)_3$ og $(2^l)_3$ er forskellige.*

Bevis. Antag for modstrid at $2^k \equiv 2^l \pmod{3^{t+1}}$. Så gælder $3^{t+1} \mid 2^l - 2^k = 2^k(2^{l-k} - 1)$, men dette er i modstrid med Lemma 11, da det medfører $3^{t+1} \mid 2^{k-l} - 1$ for $0 < l - k < 2 \cdot 3^t$. $\square$

Sætning 13 *For vilkårligt $k \in \mathbb{N}_0$ får man samtlige følger af $k+1$ cifre med 1 eller 2 på den sidste plads og 0, 1 eller 2 på de andre, når man betragter de sidste $k+1$ cifre af $(2^n)_3$ for n så $0 \leq n < 2 \cdot 3^k$.*

Bevis. De mulige følger på ovenstående form kan vælges på $2 \cdot 3^k$ måder. Videre ses det, at da det sidste ciffer af $(2^n)_3$ altid vil være enten 1 eller 2, så er de sidste $k+1$ cifre altid på denne form. Til sidst følger det af Sætning 12 at alle disse sekvenser af de første $k+1$ cifre af $(2^n)_3$ er forskellige, og da der er $2 \cdot 3^k$ af disse, følger sætningen. $\square$

Densitet af trinære julegodter

Med juletræet forsvarligt pyntet med en præcis beskrivelse af opførelsen af de sidste cifre i $(2^k)_3$ og med en passende mængde småkager ved hånden, begyndte udpakningen af julegaverne; et estimat af funktionen $\mathcal{T}_9$ var indenfor rækkevidde.

Sætning 14 *Lad $t \geq 0$. Da gælder*

$$\mathcal{T}_9(2 \cdot 3^t) \leq 2^{t-1} \cdot (t+4)$$

Bevis. Det følger af Kummers sætning, at 9 ikke deler $\binom{2^{k+1}}{2^k}$ hvis og kun hvis additionen $(2^k)_3 + (2^k)_3 = (2^{k+1})_3$ indebærer færre end to menter. For hvert eneste 2-tal i $(2^k)_3$ forekommer der en mente i additionen, og altså vil 9 dele $\binom{2^{k+1}}{2^k}$ hvis der er to eller flere 2-taller i $(2^k)_3$. [5]

Ved Sætning 13 vil de sidste $t+1$ cifre af $(2^k)_3$ antage alle kombinationer, hvor det sidste ciffer er 1 eller 2 og de andre er 0, 1 eller 2, når $0 \leq k < 2 \cdot 3^t$. Vi vil tælle, hvor mange af disse kombinationer som indeholder færre end to 2-taller. Der er to tilfælde:

Ingen 2-taller: Der er 2^t kombinationer af de sidste $t+1$ cifre, så de ikke indeholder nogen 2-taller, da det sidste ciffer må være 1 og de andre enten er 0 eller 1.

Netop ét 2-tal: Antallet af måder, hvorpå de sidste $t+1$ cifre kan indeholde præcis ét 2-tal kan findes på følgende måde. Hvis det sidste ciffer er et 2-tal, så er der 2^t forskellige måder de resterende cifre kan fordeles. Hvis det sidste ciffer er 1, så må et af de t cifre være et 2-tal, og de resterende kan antage værdierne 0 eller 1 på 2^{t-1} måder. Dermed er der $2^t + t2^{t-1}$ kombinationer, som opfylder dette.

[5] Læseren, der endnu ikke er påvirket af juleøl, vil her bemærke, at man kan opnå bedre resultater ved også at kigge på menter fra et-taller. Det vil vi i denne fremstilling afholde os fra.

Det vil sige, at der ialt maksimalt er $2^t + 2^t + t2^{t-1} = 2^{t-1}(t+4)$ tal $0 \leq k < 2 \cdot 3^t$ således at $(2^k)_3$ giver mindre end to menter, når den lægges til sig selv i base 3. Dermed fås det ønskede estimat. $\square$

Med denne gave godt udpakket kan vi nu få et generelt estimat:

Sætning 15 *For et vilkårligt $a \in \mathbb{N}$ gælder*

$$\mathcal{T}_9(a) \leq a^{\log_3(2)} \left(\log_3(a) + 5\right).$$

Bevis. Lad t være givet, så $2 \cdot 3^t \leq a < 2 \cdot 3^{t+1}$. Da har vi

$$t \leq \log_3(a) - \log_3(2).$$

Da $\mathcal{T}_9$ oplagt er en voksende funktion, så kan vi vurdere[6] $\mathcal{T}_9(a)$ ved Sætning 14:

$$\begin{aligned}
\mathcal{T}_9(a) &\leq \mathcal{T}_9\left(2 \cdot 3^{t+1}\right) \\
&\leq 2^t \cdot (t+5) \\
&\leq 2^{\log_3(a) - \log_3(2)} \left(\log_3(a) - \log_3(2) + 5\right) \\
&\leq 2^{\log_3(a)} \left(\log_3(a) + 5\right) \\
&= a^{\log_3(2)} \left(\log_3(a) + 5\right).
\end{aligned}$$

$\square$

Russerne kunne nu bruge dette estimat til at sige noget om, hvor ofte Formodning 1 fejler. Eller med andre ord: densiteten af de bløde pakker blandt midterbinomialkoefficienterne.

[6] Igen vil den opmærksomme læser bemærke, at vi for overskuelighedens skyld smider mere væk end julemanden i Bamses Julerejse.

Definition 16 Densiteten af en mængde $\mathcal{A} \subset \mathbb{N}$ defineres som grænsen

$$\rho(\mathcal{A}) = \lim_{a \to \infty} \frac{\#(\mathcal{A} \cap \{1, 2, \cdots, a\})}{a}.$$

Korollar 17 *Lad $\mathcal{R} \subset \mathbb{N}$ være mængden af naturlige tal k, som opfylder $9 \nmid \binom{2^{k+1}}{2^k}$. Da er $\rho(\mathcal{R}) = 0$.*

Bevis. Vi ser at $\frac{\mathcal{T}_9(a)}{a} \leq \frac{\log_3(a)+5}{a^{1-\log_3(2)}}$, og da

$$\lim_{a \to \infty} \frac{\log_3(a) + 5}{a^{1-\log_3(2)}} = 0,$$

er $\rho(\mathcal{R}) \stackrel{\text{def}}{=} \lim_{a \to \infty} \frac{\mathcal{T}_9(a)}{a} = 0$. $\square$

Juletræets grønne top

Nu kunne den pejsedøsige læser fristes til at tro at juleeventyret slutter her, men russerne fortsatte ufortrødent.

Definition 18 For ulige $m \in \mathbb{N}$ lader vi:

$$\mathcal{T}_m(a) = \# \left\{ 0 \leq s < a \mid m \nmid \binom{2^{s+1}}{2^s} \right\}$$

Denne funktion var lidt sværere at knække, men efter lang tids terningekasten skaffede russerne sig følgende julegave i matematikkens store pakkeleg:

Sætning 19 *Lad $m > 1$ være ulige og lad p være det største primtal, der deler m. Da gælder $\mathcal{T}_m(a) = o\left(a^{\log_p\left(\frac{p+1}{2}\right)+\epsilon}\right)$ for ethvert $\epsilon > 0$.*

Denne sætning blev vist, da juletiden var ved at gå på hæld og russerne lå og lavede sneengle på de salige idrætsstuderendes tilsneede spydkastmark. Her åbenbarede Herrens (eller Erdős' eller læserens yndlingsmatematikers) engle sig for dem, og de så, at man for vilkårligt $\alpha \in \mathbb{N}$ og primtal p kunne udvælge indekser i cifrene af $(\alpha^k)_p$ så samtlige "mulige" følger af cifre fremkommer ved disse indekser.[7]

Dette kunne russerne bruge. De styrtede ind til den nærmeste tavle og med samme teknik som i tilfældet $\alpha = 2$ lykkedes det dem at sikre resultatet. Glade og tilfredse løb de ned til kagesøster og varm kakao.

Det var nu blevet en rigtig jul.

Litteratur

[1] R. L. Graham, D. Knuth, O. Patashnik. *Concrete Mathematics*. Addison-Wesley, 2011.

[7] Interesserede læsere er meget velkomne til at kontakte forfatterne.

Hvad viser klokken?
– præmieopgave, 24. årgang nr. 2

Så er præmieopgaven tilbage igen! Som sædvanlig lyder præmien på et gavekort på 100 kr til GAMES.

Betragt et ur, hvor vi ser bort fra mekanikken og antager, at time og minutviser går på kontinuert vis. Hvor mange forskellige klokkeslæt findes der, hvor man kan ombytte time og minutviser og stadig vise noget gyldigt?
For eksempel får vi ikke et gyldigt klokkeslæt, når vi ombytter time- og minutviser kl. $05:00$*, da timeviseren ikke kan stå på præcist* 12*, når klokken er* 25 *over.*

Vinderen udtrækkes fra mængden af de besvarelser, som er mere eller mindre overbevisningsdygtige.

Farvel til ekstraopgaven

Mange tak til de flittige korrespondenter (særligt shoutout til Sune og Thor), der var med til at besvare *Blokkens Ekstraopgave.* Takket være jeres færdigtexede besvarelser havde vi en artikel at se frem til i hver blok. Dog er vores portrættegner optaget, og ingen af de resterende redaktionsmedlemmer har mod på at tegne Sune – de første to potrætter var så flotte, at tredje gang kun kan blive en skuffelse. Vi siger derfor farvel til ekstraopgaven for denne gang...

FAMØS

Famøs Dec 2014
Fagblad for Aktuar, Matematik,
-Økonomi og Statistik ved Københavns Universitet

Illustrationer:
Jing (Question Marc)
Deadline for næste nummer:
1. marts 2015

Indlæg modtages gerne og bedes sendt
til redaktion@famosweb.org – gerne i LaTeX
og gerne baseret på skabelonen
som kan hentes på hjemmesiden.

Fagbladet Famøs
c/o Institut for Matematiske Fag
Matematisk Afdeling
Universitetsparken 5
2100 København Ø
http://www.famosweb.org

Oplag: 300 stk.
Tryk: Frydenberg A/S ISSN: 1395-2145

24. årgang, nr. 1, Dec 2014