

Matematik 3000 Diskret Matematik

Tilläggsmaterial till läroboken:

◆ **Kapitel 1**

- På hur många sätt kan en blomsterbukett komponeras?
- Aktivitet 1:3* – Chokladvävlingen
- Aktivitet 1:4* – Anagram

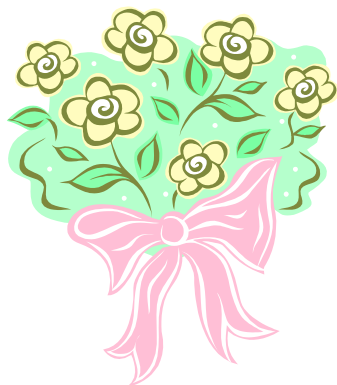
◆ **Kapitel 2**

- Hur länge levde Diofantos?
- Mera om heltalsdivision och kongruenser
- Tornet i Hanoi
- Aktivitet 2:3* – Catalans tal
- Aktivitet 2:4* – Kryptoanalys

◆ **Kapitel 3**

- Aktivitet 3:3* – Egenskaper hos relationer

På hur många sätt kan en blomsterbukett komponeras?



Idag skulle hon göra något hon aldrig gjort förut. En helt vanlig tisdag. I februari. Hon skulle köpa en bukett blommor. Bara för att de var världens bästa föräldrar. Trots allt.

Väl inne i blomsteraffären fick hon syn på en skylt med texten:

Komponera din blomsterbukett själv!

Femton snittblommor för endast 125 kronor!

Välj mellan storvuxna tulpaner, ranunkler och anemoner.

Genast vaknade matematikern inom henne till liv och viskade:

– *På hur många sätt kan du välja nu då?*

På hur många sätt? Frågan fick henne att koncentrera sig och överge rutintänkandet, väl medveten om den omedelbara risken för tankefel när frågor av den typen ska besvaras.

Hon plockade en smula förstrött ihop en bukett blommor medan hon försökte intala sig att frågeställningen var fullständigt ointressant. Vem vill veta hur många sätt det finns att komponera en blomsterbukett? Fast det är ju inte det saken egentligen gäller... Tanken ville inte släppa henne.

Frånvarande sträckte hon fram den nykomponerade blomsterbuketten till expediten som fick henne att återvända till verkligheten genom att något burdust utbrista:

”Du har bara plockat ihop 12 blommor. Ska det verkligen bara vara ranunkler i buketten? Vill du inte att jag ska hjälpa dig?”

Kanske kan du hjälpa henne? På många sätt kan man egentligen komponera ihop en blomsterbukett med 15 blommor om man kan välja mellan tre olika sorter som alla finns i tillräcklig mängd i affären?

(*Ledning:* Problemet liknar uppgift 1167 s 19 och uppgift 28 i Blandade övningar 1 s 45 i läroboken.)

Aktivitet 1:3

Choklادتävlingen

Ett chokladföretag utlyste en tävling som gick ut på att bilda så många nya ord som möjligt med hjälp av bokstäverna i ordet C-H-O-K-L-A-D. Varje bokstav i ordet fick användas högst en gång (alla bokstäverna behövde inte användas). Första pris utgjordes av två kilo blandade chokladsorter direkt från företags fabrik.

- 1 Hur många bokstavskombinationer kan man bilda utifrån bokstäverna i ordet C-H-O-K-L-A-D?
- 2 Hur många riktiga ord bland bokstavskombinationerna i föregående uppgift kan du hitta? Kan du komma på något listigt sätt att effektivisera letandet efter riktiga ord?

Aktivitet 1:4

Anagram

En omkastning av bokstäverna i ett ord eller ett uttryck så att en annan dold betydelse kommer fram kallas för ett *anagram*. Om du har läst Dan Browns bästsäljare *Da Vinci-koden* har du också stött på anagrammen

O, Draconican devil!
Oh, lame saint!

som symbolik-forskaren Robert Langdon och kryptografen Sophie Neveu efter viss möda lyckades tyda som

Leonardo da Vinci!
The Mona Lisa!

Det var i övrigt en omkastning av de första talen i Fibonaccis talföljd (se Aktivitet 2:1, uppgift 2445 på s 81 och uppgift 22 i Blandade övningar 3 på s 145 i läroboken) som fick in Robert Langdon och Sophie Neveu på rätt spår:

13 – 3 – 2 – 21 – 1 – 1 – 8 – 5

- 1 Skriv Fibonaccis tal ovan i rätt ordning. Vad utmärker talen?
- 2 Välj ett eget favorituttryck bestående av minst 3 ord. Hur många nya uttryck, inklusive ren rappakalja, går teoretiskt sett att bilda genom godtyckliga omkastningar av bokstäverna i ditt uttryck? Tänk på att de nybildade uttrycken kan ha såväl fler som färre ord än det ursprungliga uttrycket.
- 3 Hur många anagram bland omkastningarna i föregående uppgift kan du hitta?

Hur länge levde Diofantos?

Om Diofantos som person är inte mycket känt annat än att han levde och verkade i antikens Alexandria, troligen på 200-talet e. Kr. Han lämnade emellertid följande gåta efter sig som lär ha varit inristad på hans gravsten:

*Han tillbringade 1/6 av sitt liv som barn och sedan 1/12 som skäggförsedd yngling.
Efter ytterligare 1/7 av sitt liv gifte han sig och fick 5 år senare en son.
Sonen dog emellertid när han uppnått faderns halva livslängd.
Fadern levde sedan i ytterligare 4 år.*

Kan du bestämma Diofantos livslängd?

Diofantos har fått ge namn åt *diofantiska ekvationer*, dvs ekvationer som man söker heltalslösningar till. Bland mycket annat undersökte Diofantos hur heltal kan uttryckas som summor av kvadrattal. Exempelvis kan 46 skrivas som $6^2 + 3^2 + 1^2$. Hur många kvadrattal tror du vi behöver för att kunna skriva ett godtyckligt positivt heltal som en summa av kvadrattal?

Diofantos var säker på sin sak – fyra kvadrattal räcker alltid – men gav inte något bevis för sitt påstående. Beviset skulle dröja omkring 1 500 år innan Joseph Louis Lagrange på 1700-talet formulerade och bevisade det som kommit att kallas *Lagranges sats*.

Diofantos samlade såväl nya som redan kända talteoretiska problem i verket *Arithmetica* som ursprungligen omfattade 13 böcker. Under de orostider som följde under århundranden efter Diofantos levnad drabbades emellertid biblioteket i Alexandria hårt av systematiska bokbål och annan förstörelse. Därför finns bara 6 av böckerna i *Arithmetica* bevarade till eftervärlden.

Oroligheterna i Alexandria innebar också början på ett tusenårigt mörker för talteorins utveckling, åtminstone i Västerlandet. Under tiden utvecklades emellertid talteorin ytterligare bland annat i Indien, där man introducerade talet noll som representant för den tomma mängden. Indiska matematiker lade också grunden till det talsystem, decimalsystemet, som vi idag använder.

Talteorin i Västerlandet pånyttföddes så sent som på 1700-talet i Frankrike då juristen och hobbymatematikern Pierre de Fermat läste de bevarade delarna av Diofantos *Arithmetica* i en fransk översättning från 1621. Fermat antecknade flitigt i de generöst tilltagna marginalerna och formulerade bland annat det som kommit att kallas Fermats stora (eller sista) sats. Läs mer om Pierre de Fermat på s 53 i läroboken *Diskret Matematik*.

Mera om heltalsdivision och kongruenser

Heltalsdivision

Vilken rest får vi när vi dividerar 27 med 4?

Vi skulle kunna bilda rester på flera olika sätt, t ex skulle vi kunna få resten 11 om vi delar upp talet 27 i 4 stycken 4-mängder:

$$27 = 4 \cdot 4 + 11$$

eller resten 7 om vi istället bildar 5 stycken 4-mängder:

$$27 = 5 \cdot 4 + 7$$

Dessa rester är emellertid större än det heltal (4) som vi dividerar med. För att få en entydig (unik) rest brukar man därför inom talteorin fortsätta divisionen tills resten blir ett naturligt tal som är mindre än det heltal som man dividerar med.

Genom att fortsätta uppdelningen av 27 i 4-mängder ytterligare ett steg får vi resten 3:

$$27 = 6 \cdot 4 + 3$$

En sådan rest kallas för *principal rest*.

När man pratar om "rest" inom talteorin menar man oftast principal rest.

Vad blir den principala resten om vi dividerar 27 med -4 ?

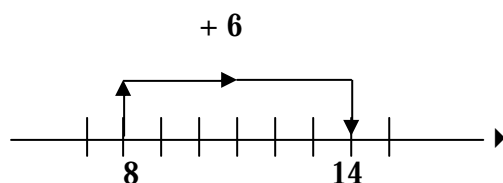
Den principala resten är alltid ett naturligt tal. Här måste vi därför kräva att den principala resten ska vara mindre än absolutbeloppet av -4 , dvs mindre än 4. Vi får därför samma principala rest som tidigare, dvs

$$27 = (-6) \cdot (-4) + 3$$

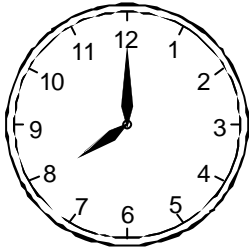
Kongruenser

Vanlig addition görs längs en *tallinje* utan början eller slut.

$$8 + 6 = 14$$



Att räkna *modulärt* eller med *kongruenser* är däremot som att räkna på en klocka eller längs en *talcirkel*.



Om klockan är 8 och det går 6 timmar så har vi kommit till klockan 2, dvs

$$8 + 6 = 14 = 2 \text{ (i 12 timmars klockaritmetik)}$$

Med talteoretiskt språk säger vi att "2 och 14 är kongruenta modulo 12" och skriver

$$14 \equiv 2 \pmod{12}$$

När vi räknar på en klocka räknar vi således i 12-mängder och noterar bara den *principalresten*:

$$58 = 4 \cdot 12 + 10$$

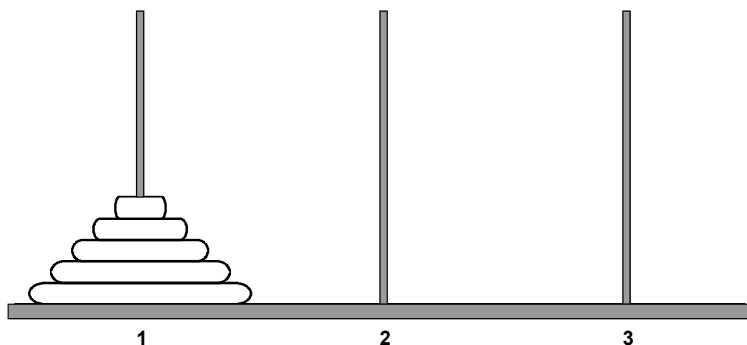
dvs

$$58 = 10 \text{ (i 12 timmars klockaritmetik),}$$

vilket skrivs

$$58 \equiv 10 \pmod{12}$$

Tornet i Hanoi



Bilden ovan, som också finns på s 81 i läroboken, visar tornet i Hanoi, ett klurigt pusselspel som lanserades av den franske matematikern Édouard Lucas (1842–1891).

I utgångsläget av tornet i Hanoi är ett antal skivor av varierande storlek trädde på pinnen till vänster (nr 1). Spelet går ut på att flytta skivorna en i taget tills samtliga skivor ligger på pinnen längst till höger (nr 3). En större skiva får aldrig placeras ovanpå en mindre skiva. Pinnen i mitten (nr 2) används som "mellanlagringsplats". En allmän lösning på problemet med n skivor i utgångsläget kan formuleras rekursivt. *Kan du komma på hur?*

Tanken bakom en rekursiv algoritm är att ursprungsproblemet, att flytta n skivor från vänsterpinnen till högerpinnen, successivt bryts ner i mindre och mindre delproblem av samma typ tills man kommer fram till ett problem med en trivial lösning. Om $n = 1$, endast en skiva ska flyttas, är förstås lösningen på tornet i Hanoi trivial. Slutligen kombineras lösningarna på delproblemen till en lösning på det ursprungliga problemet.

Förflyttningen av tornet i Hanoi med n skivor från pinne nr x till pinne nr z , med pinne nr y som mellanlagringsplats, kan utföras rekursivt på följande sätt:

Om $n = 1$, flytta skivan från x till z .

Om $n > 1$, lös först problemet med att flytta de $n-1$ översta skivorna från x till y med z som mellanlagringsplats.

Flytta sedan den understa skivan från x till z .

Lös slutligen problemet med att flytta de resterande $n-1$ skivorna, som nu befinner sig på pinne y , till z med x som mellanlagringsplats.

Med pseudokod kan vi formulera lösningen så här:

```

Procedure hanoi(f: positivt heltal, t: positivt heltal, m: positivt heltal, n: positivt heltal)
  If n = 1 Then
    Write(Flytta skiva från pinne nr f till t)
  Else
    hanoi(f, m, t, n - 1)
    hanoi(f, t, m, 1)
    hanoi(m, t, f, n - 1)
  End If
End Procedure

```

Inparametern n talar om hur många skivor som ska flyttas. Övriga inparametrar anger hur förflyttningen ska genomföras, dvs från pinne nr f till pinne nr t med pinne nr m som mellanlagringsplats.

Vi illustrerar anropskedjan för $n = 3$ skivor som ska flyttas från pinne nr 1 i utgångsläget till pinne nr 3 med pinne nr 2 som mellanlagringsplats på följande sätt:

```

hanoi(1,3,2,3) → hanoi(1,2,3,2) → hanoi(1,3,2,1) → 1) Flytta skiva från pinne nr 1 till 3
                → hanoi(1,2,3,1) → 2) Flytta skiva från pinne nr 1 till 2
                → hanoi(3,2,1,1) → 3) Flytta skiva från pinne nr 3 till 2
                → hanoi(1,3,2,1) → 4) Flytta skiva från pinne nr 1 till 3
                → hanoi(2,3,1,2) → hanoi(2,1,3,1) → 5) Flytta skiva från pinne nr 2 till 1
                → hanoi(2,3,1,1) → 6) Flytta skiva från pinne nr 2 till 3
                → hanoi(1,3,2,1) → 7) Flytta skiva från pinne nr 1 till 3

```

Enligt legenden var det ursprungliga tornet i Hanoi byggt i renaste guld och 64 skivor högt. Munkarna vid ett närliggande kloster hade fått till uppgift att flytta tornet enligt reglerna ovan. Uppgiften var synnerligen otacksam eftersom tornet, också enligt legenden, var dömt att kollapsa innan munkarna hunnit färdigt, vilket i sin tur skulle leda till jordens undergång. Eftersom man kan visa att det krävs åtminstone $2^{64} - 1 = 18\,446\,744\,073\,709\,551\,615$ förflyttningar att lösa pusslet med 64 skivor i utgångsläget var förmodan om att något skulle hända med tornet långt innan sista förflyttningen säkert inte helt orimlig.

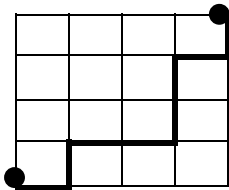
Mannen bakom tornet i Hanoi, Édouard Lucas, upptäckte också en lång rad intressanta egenskaper hos talföljden

$$f_n = f_{n-1} + f_{n-2}, f_0 = 1 \text{ och } f_1 = 1$$

som han döpte till *Fibonaccis tal* efter talföljdens italienske upphovsman (se även Aktivitet 2:1 s 92, uppgift 2445 s 81 och uppgift 22 i Blandade övningar 3 på s 145 i läroboken samt Aktivitet 1:4 på denna nätplats, www.matematik3000.nu).

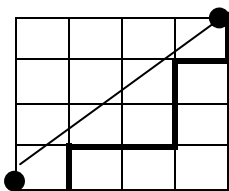
Aktivitet 2:3

Catalans tal

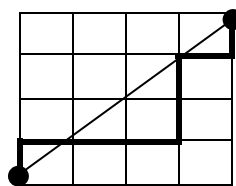


Exempel på färd

- 1 På hur många olika sätt kan man förflytta sig från nedre vänstra hörnet till övre högra hörnet i figuren ovan, om man bara får förflytta sig uppåt eller åt höger längs linjerna i rutnätet? (Se även uppgift 1164 s 19 i läroboken.)
- 2 Ge ett allmänt uttryck för antalet olika sätt som man kan förflytta sig från nedre vänstra hörnet till övre högra hörnet enligt reglerna ovan i ett rutnät med $n \cdot n$ rutor.
- 3 Anta att man får beröra men ej gå över diagonalen som går från nedre vänstra hörnet till övre högra hörnet. Nedan visas exempel på en tillåten färd (A) och en otillåten färd (B):



A Exempel på tillåten färd



B Exempel på otillåten färd

Försök visa att antalet olika tillåtna färder från nedre vänstra hörnet till övre högra hörnet enligt reglerna ovan i ett rutnät med $n \cdot n$ rutor är

$$C(2n, n) - C(2n, n - 1),$$

där $C(2n, n)$ betecknar antalet kombinationer av storlek n bland $2n$.

- 4 Visa att $C(2n, n) - C(2n, n - 1) = C(2n, n) / (n + 1)$ och bestäm de fem första talen ($n = 0, 1, 2, 3, 4$) i denna talföljd.
- 5 Den erhållna talföljden $b_n = C(2n, n) / (n + 1)$, $n \geq 0$, kallas för *Catalans tal* efter den belgiske matematikern Eugène Charles Catalan (1814–1894).

Visa att $b_n \geq 4^{n-1} / n^2$ för alla $n \geq 1$ (se även uppgift 31 i Blandade övningar 3 s 146 i läroboken).

Aktivitet 2:4

Kryptoanalys

Ett *krypto* är en algoritm som används vid kommunikation för att dölja information för obehöriga. Ett *substitutionskrypto* är en enkel form för krypto som innebär att varje bokstav ersätts med en annan enligt en hemlig regel.

Julius Caesar (100– 44 f. Kr.) använde följande substitutionskrypto för att översätta *klartextalfabetet* till ett *kryptoalfabet*:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö	a	b	c

dvs *a* ersätts med *d*, *b* med *e*, *c* med *f* osv.

- 1** Vilken enkel regel använde Caesar för att skapa sitt kryptoalfabet utifrån klartextalfabetet?
- 2** Skapa ett eget substitutionskrypto som du inte visar för någon och använd detta för att skapa en *kryptotext*, dvs för att kryptera ett meddelande på svenska som innehåller 50–75 ord.
- 3** Byt kryptotext med en kamrat utan att ta del av dennes algoritm. Försök få fram meddelandet i klartext. Hur går du till väga? Sammanfatta din metod i några viktiga punkter.

Aktivitet 3:3

Egenskaper hos relationer

En relation kan bl a beskrivas utifrån följande egenskaper: reflexivitet, symmetri, asymmetri, transitivitet.

- 1 Ta reda på vad dessa egenskaper innebär.
- 2 Låt A vara mängden $\{1, 2, 3, 4, 5\}$.
Ge exempel på en relation R från A till A , dvs en delmängd till den cartesiska produkten $A \times A$, som är
 - a) reflexiv och symmetrisk men inte transitiv
 - b) transitiv och symmetrisk men inte reflexiv
 - c) transitiv men varken symmetrisk eller asymmetrisk.