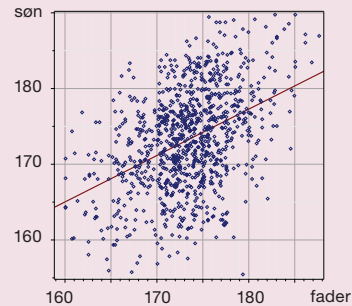


1. Regression, interpolation og secret sharing

Regression anvendes ofte som en fælles betegnelse for en række matematiske teknikker, hvor man ud fra et begrænset antal datapunkter søger at beskrive en variabelsammenhæng med et funktionsudtryk. Det fundamentale eksempel er *lineær regression*, som vi behandlede i *Hvad er matematik?* 1, kapitel 1.

Regression er en meget velegnet metode til at håndtere situationer, hvor vi har en begrundet formodning om, at de indsamlede data repræsenterer en bestemt sammenhæng, fx en lineær sammenhæng, men at data samtidig er "forurenet" af noget "støj". Dvs. at den afhængige variabel kan opfattes som en sum af to led, i det her tilfælde et *lineært led* og led, der repræsenterer *tilfældig støj*. Illustrationen viser en sky af datapunkter, hvor vi har en formodning om, at der må være en lineær sammenhæng. Dette begrundes linjen – men der er tydeligt meget støj. Dette vil vi gå dybere ned i i bog 3.



Lineær regression foretaget på Galtons datamateriale over sammenhængen mellem fædres og sønners højde. Datamaterialet er behandlet i afsnit 2.

Du kan på bogens **website** se en film om, hvordan støj indgår i kommunikationen mellem neuronerne i vores hjerner!

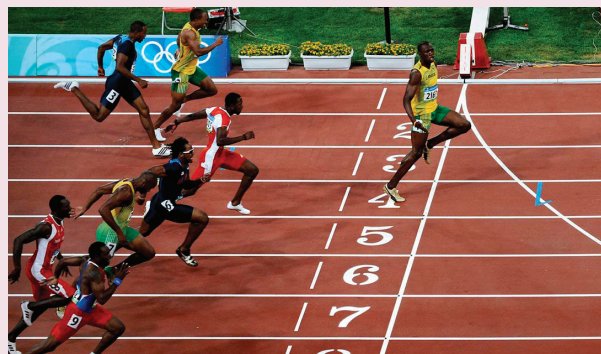


I andre situationer er vi ikke kun interesseret i at kunne foretage tilnærmede beregninger, men ønsker at få tegnet en kurve, der går *præcis* igennem de givne datapunkter. Har vi fastlagt et antal punkter i et nyt design af en skrifttype eller i tegningen af en møllevinge, så giver det ingen mening at anvende tilnærmede kurver. Den matematiske teknik, der giver sådanne kurver, kaldes for interpolation. I den indledende fortælling i kapitel 4 om logaritmefunktionerne mødte vi *lineær interpolation*.

Samtidig ønsker vi en kurve, der er pæn *glad*, så vi kan anvende differentialregning. Lad os illustrere det med følgende eksempel, der både inddrager regression og interpolation:

I 2008 gennemførte Usain Bolt et enestående løb i 100 m finalen ved OL. I en sådan situation er mange interesseret i at få gennemlyst løbet.

I tabellen er angivet en række datapunkter for hans løb, hentet fra videooptagelser. Det første man gør, er naturligvis at afbilde det tilhørende punktplot.



Usain Bolt vinder 100m finalen ved OL i 2008 i overlegen stil. Hans reaktionstid på 0,165 viser, at han var en relativt langsom starter.

Tid (s)	Distance (m)
0	0
0,165	0
1,85	10
2,87	20
3,78	30
4,65	40
5,5	50
6,32	60
7,14	70
7,96	80
8,79	90
9,69	100

De modelfunktioner, vi her leder efter, er polynomier, fordi de beregningsmæssigt er så lette at håndtere – funktionsværdier udregnes med plus, minus og gange – og de er enkle at differentiere. Men det er vigtigt at understrege, at hvis modelfunktionen er et 4. grads- eller et 11. gradspolynomium, så er det ikke udtryk for en formodning om, at variabelsammenhængen er polynomiell. Det er en ren hjælpefunktion.

Øvelse 8.1 Anvend polynomiell regression til at finde frem til hastighedsfunktionen

- Udfør et punktplot af dataværdierne, og bestem ved polynomiell regression det bedste fjerdegradspolynomium, der tilnærmer datapunkterne.
- Bestem hastighedsfunktionen ved at differentiere polynomiet.
- Tegn grafen af hastighedsfunktionen, og bestem, hvornår hastigheden er maksimal.
- Hvad kan begrundelsen være for at vælge et 4. gradspolynomium?

Et 4. gradspolynomium er bestemt af 5 parametre:

$$p_4(x) = a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

Har vi 5 datapunkter, (x_1, y_1) , (x_2, y_2) , (x_3, y_3) , (x_4, y_4) og (x_5, y_5) , kan vi opstille 5 ligninger:

$$p_4(x_1) = y_1, p_4(x_2) = y_2, p_4(x_3) = y_3, p_4(x_4) = y_4 \text{ og } p_4(x_5) = y_5$$

og vil normalt kunne bestemme de 5 parametre ud fra dette.

Øvelse 8.2 Bestem forskrift med ligningsløsning

Vælg selv tilfældigt 5 af de 12 datapunkter, og bestem de 5 parametre ved at anvende solve. Sammenlign dit resultat med dine kammeraters og med forskriften for regressionspolynomiet.

Da der er 12 datapunkter, må der findes et 11. gradspolynomium, hvis graf helt præcist går gennem disse punkter.

Øvelse 8.3 Regression og interpolation

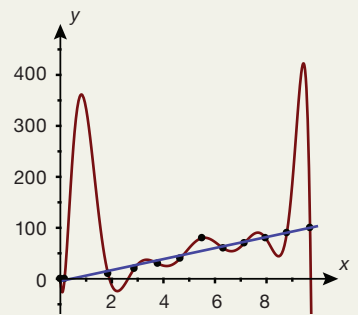
- Bestem ved regression det bedste 11. gradspolynomium, der tilnærmer datapunkterne. Indstil programmet, så der regnes med stor nøjagtighed.
- Bestem ved hjælp af solve det 11. gradspolynomium, hvis graf præcist går gennem punkterne.
- Polynomierne i a) og b) er fundet ved to helt forskellige beregningsmetoder. Tegn de to grafer i samme koordinatsystem. Kommenter hvad du ser.

Det polynomium, vi bestemte i punkt b) siger vi er bestemt ved *interpolation*. Polynomiel interpolation giver os altså et polynomium, hvis graf går præcist igennem de givne datapunkter. Skal man bestemme et polynomium, der fitter 12 datapunkter bedst muligt, vil man nok intuitivt vælge at bestemme dette ved interpolation, da det i så fald opfylder hele den information vi har. Men man skal ofte passe på med kun at anvende sin intuition.

Lad os skruer en anelse på eksemplet, idet vi erstatter (5.5,50) med (5.5,80) og lader resten være uændret. Det handler ikke om 100 m løbet nu – de løber jo ikke baglæns. Det er blot et sæt med 12 datapunkter.

Øvelse 8.4 Interpolations polynomiet er ikke altid en god tilnærmelse

- Udfør punktplottet af det ændrede datasæt. Gennemfør lineær regression på dette datasæt.
- Bestem ved hjælp af solve det 11. gradspolynomium, hvis graf præcist går gennem de nye punkter.
- Tegn de to grafer fra a) og b) i samme koordinatsystem. Du skal få et billede, der ligner illustrationen. Hvilken graf ville du vælge som den bedste tilnærmelse til punkterne.



1.1 Runges eksempel

Første gang man ser et resultat som det grafisk illustrerede ovenfor, tror man næppe sine egne øjne. Det strider mod vores umiddelbare opfattelse af, at polynomier giver pæne tilnærmelser til mere komplicerede funktioner. I 1885 beviste Weierstrass den approksimationssætning, vi har gengivet i den indledende fortælling i kapitel 5B: *Enhver kontinuert funktion defineret på et begrænset og lukket interval $[a;b]$ kan tilnærmes vilkårlig tæt med et polynomium.*

Givet et datasæt, kunne vi starte med at forbinde punkterne med rette linjer. Dette giver os en kontinuert funktion $f(x)$. Ifølge Weierstrass findes så en følge af polynomier, således at:

$$P_1(x), P_2(x), P_3(x), \dots \rightarrow f(x), \text{ når } n \rightarrow \infty$$

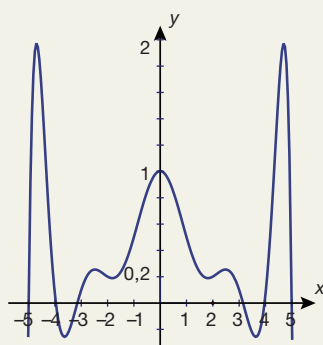
Hvis vi nu valgte flere og flere punkter på grafen for f , og for hvert af disse stadigt større datasæt ved interpolation konstruerede polynomier, der stemte overens med f i disse punkter, så var det ikke en urimelig forestilling, at de ville konvergere mod funktionen. Men det gør de stort set aldrig! Det billede, vi så ovenfor, er det normale.

Dette blev opdaget i 1901 af den tyske matematiker Carl Runge (1856-1927). Han ledte efter en formel, der kunne fortælle, hvor store fejl der opstår, når man tilnærmer en bestemt kontinuert funktion med polynomier konstrueret ved interpolation gennem en række punkter på grafen. Han fandt ud af, at en sådan formel ikke findes. Faktisk er



det sådan, at hvis de stadig flere punkter vælges, så x -værdierne fordeler sig jævnt over det givne interval, så vil interpolationsfejlen gå mod uendeligt! I artiklen, som kan findes på bogens **website**, giver han det eksempel, der i matematikhistorien simpelt hen hedder Runges eksempel.

Øvelse 8.5 Runges eksempel



Runges eksempel – dataværdier og Lagrangepolynomium af grad 10.

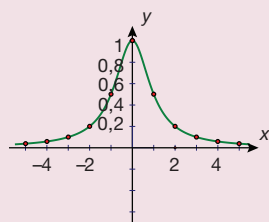
Givet datasættet:

-5	-4	-3	-2	-1	0	1	2	3	4	5
$-\frac{1}{26}$	$-\frac{1}{17}$	$-\frac{1}{10}$	$-\frac{1}{5}$	$-\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{5}$	$\frac{1}{10}$	$\frac{1}{17}$	$\frac{1}{26}$

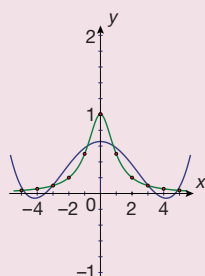
- Udfør et punktplot af de 11 datapunkter.
- Bestem ved interpolation det 10. gradspolynomium, hvis graf går gennem alle 11 punkter. I dette tilfælde får man det samme polynomium ved regression og interpolation, så anvend blot regression. På bogens **website** er demonstreret, at man får det samme. Du skal få et billede som til venstre.



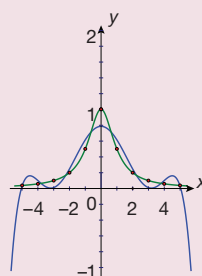
Nu kunne det jo tænkes, at punkterne kom fra en graf, der svinger vildt som denne. Men Runge havde bevidst valgt en meget simpel funktion for at illustrere det fænomen, han havde opdaget. Dataværdierne ovenfor er genereret af funktionen med forskrift: $f(x) = \frac{1}{1+x^2}$. Og de tilnærmede polynomier af grader 4, 6 og 10 ser således ud:



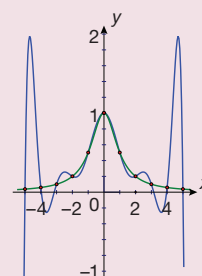
Runges funktion med 11 datapunkter.



Runges eksempel – data-værdier, graf og regressionspolynomium af grad 4.



Runges eksempel – data-værdier, graf og regressionspolynomium af grad 6.



Runges eksempel – data-værdier, graf og Lagrangepolynomium af grad 10.

Det Runge havde opdaget, og som siden blev udbygget med en omfattende teori, var, at man ikke får en generelt bedre tilnærmelse af en given funktion ved at gå op i grad. Det er en dårlig strategi. Men vi ser også, at problemerne tilsyneladende opstår ude i enderne af intervallet. Man kan vise, at ved at vælge x -værdierne, så de ikke er jævnt fordelt, men fordelt efter et ganske bestemt mønster, så kan man mindske forskellen på interpolationspolynomierne og den oprindelige funktion, mens graden vokser.

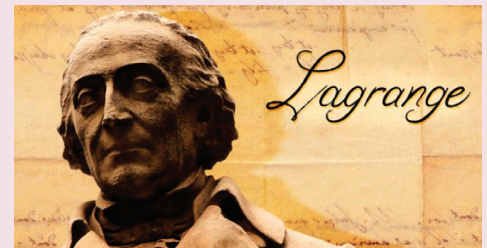
Men hvordan løses så opgaver, hvor vi skal konstruere en modelfunktion, hvis graf går gennem bestemte punkter. Det sker i praksis ved at anvende *splines*: Dette er funktioner, der er defineret stykkevis, således at grafen forbinder to nabopunkter med en polynomiell kurve, og hvor det yderligere er sikret, at to sådanne dele af den samlede kurve er stykket glat sammen. Moderne værktøjsprogrammer har indbygget faciliteter til at konstruere splines ud fra givne datapunkter. Du kan læse mere om splines på bogens **website**.



Alt dette betyder imidlertid ikke, at polynomiell interpolation er sat ud på et sidespor og kun har historisk interesse. Der er i vor tid dukket meget spændende anvendelser op i helt andre områder, nemlig inden for kodning og kryptologi. Og det bygger på en meget elegant metode til at gennemføre polynomiell interpolation, som blev opdaget for omkring 200 år siden.

1.2 Lagrangeinterpolation

I 1795 publicerer den store franske matematiker Joseph Louis Lagrange (1736-1813) et værk, hvori han præsenterer den metode, der siden er blevet kaldt *Lagrangeinterpolation*. Givet eksempelvis 11 datapunkter, så viser Lagrange, hvordan man umiddelbart kan opskrive forskriften for et polynomium af 10. grad, hvis graf går gennem de 11 datapunkter.



Dette resultat har naturligvis ikke noget med tallene 10 og 11 at gøre. Det polynomium, man således opskriver, er samtidig *entydigt* bestemt og er dermed interpolationspolynomiet. Det beviser vi nedenfor, men lad os først demonstrere Lagranges teknik ved i et praktisk eksempel at bestemme det 3. gradspolynomium, hvis graf går gennem 4 datapunkter. (*Bemærk*: De 4 x -værdier skal være forskellige).

Vi har givet 4 datapunkter:

	Generelt	Konkret eksempel
Dataværdier	$(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$	$(-1, 3), (0, -4), (1, 5), (2, -6)$

1. trin:

Konstruer 4 polynomier, hver af grad 3, og som hver har nulpunkter i 3 af de 4 punkters x -værdier:

	Generelt	Konkret eksempel
Basis polynomier	$p_1(x) = (x - x_2) \cdot (x - x_3) \cdot (x - x_4)$	$p_1(x) = (x - 0) \cdot (x - 1) \cdot (x - 2)$
	$p_2(x) = (x - x_1) \cdot (x - x_3) \cdot (x - x_4)$	$p_2(x) = (x + 1) \cdot (x - 1) \cdot (x - 2)$
	$p_3(x) = (x - x_1) \cdot (x - x_2) \cdot (x - x_4)$	$p_3(x) = (x + 1) \cdot (x - 0) \cdot (x - 2)$
	$p_4(x) = (x - x_1) \cdot (x - x_2) \cdot (x - x_3)$	$p_4(x) = (x + 1) \cdot (x - 0) \cdot (x - 1)$

2. trin:

"Normér" basispolynomierne, så vi får 4 tredjegradspolynomier, der stadig har de samme 3 nulpunkter, men som har værdien 1 i den 4. x -værdi. Det gør vi ved at dividere det i 'te polynomium, $p_i(x)$ med tallet $p_i(x_i)$:

	Generelt	Konkret eksempel
Normerede polynomier	$f_1(x) = \frac{p_1(x)}{p_1(x_1)} = \frac{(x-x_2) \cdot (x-x_3) \cdot (x-x_4)}{(x_1-x_2) \cdot (x_1-x_3) \cdot (x_1-x_4)}$	$f_1(x) = \frac{p_1(x)}{p_1(-1)} = \frac{(x-0) \cdot (x-1) \cdot (x-2)}{(-1-0) \cdot (-1-1) \cdot (-1-2)}$
	$f_2(x) =$	$f_2(x) =$
	$f_3(x) =$	$f_3(x) =$
	$f_4(x) =$	$f_4(x) =$

Øvelse 8.6 Opstil de normerede polynomier

- Opskriv selv formlerne for de resterende polynomier i det generelle tilfælde.
- Kontroller, at $f_1(x_1) = 1$, $f_1(x_2) = 0$, $f_1(x_3) = 0$, $f_1(x_4) = 0$.
- Opskriv og kontroller de tilsvarende ligninger med de andre tre normerede polynomier.
- Opskriv formlerne for de resterende polynomier i det konkrete eksempel, og reducer. Du skal eksempelvis få, at $f_3(x) = -\frac{1}{2} \cdot (x^3 - x^2 - 2x)$.

3. trin:

Det, vi er interesseret i, er at konstruere et polynomium af grad 3, hvis graf går gennem de oprindelige datapunkter. Men vi ser nu, at ganges y -værdierne på f -polynomierne, fx $l_1(x) = y_1 \cdot f_1(x)$, så vil disse "koordinat" polynomier opfylde:

$$l_1(x_1) = y_1, \quad l_1(x_2) = 0, \quad l_1(x_3) = 0, \quad l_1(x_4) = 0:$$

	Generelt	Konkret eksempel
Koordinat polynomier	$l_1(x) = y_1 \cdot f_1(x) = y_1 \cdot \frac{(x-x_2) \cdot (x-x_3) \cdot (x-x_4)}{(x_1-x_2) \cdot (x_1-x_3) \cdot (x_1-x_4)}$	$l_1(x) = 3 \cdot f_1(x) = 3 \cdot \frac{(x-0) \cdot (x-1) \cdot (x-2)}{(-1-0) \cdot (-1-1) \cdot (-1-2)}$
	$l_2(x) =$	$l_2(x) =$
	$l_3(x) =$	$l_3(x) =$
	$l_4(x) =$	$l_4(x) =$

Øvelse 8.7 Opstil koordinatpolynomierne

- Opskriv selv formlerne for de resterende polynomier i det generelle tilfælde.
- Kontroller, at $l_2(x_1) = 0$, $l_2(x_2) = y_2$, $l_2(x_3) = 0$, $l_2(x_4) = 0$, og tilsvarende med $l_3(x)$ og $l_4(x)$.
- Opskriv formlerne for de resterende polynomier i det konkrete eksempel.

Nu kan vi opskrive *Lagrange interpolationspolynomium*:

$$L_3(x) = l_1(x) + l_2(x) + l_3(x) + l_4(x) = y_1 \cdot f_1(x) + y_2 \cdot f_2(x) + y_3 \cdot f_3(x) + y_4 \cdot f_4(x)$$

Øvelse 8.8 Lagrange interpolationen giver det søgte polynomium

- Udregn $L_3(x)$ i det konkrete tilfælde. Du skal få: $L_3(x) = -6x^3 + 8x^2 + 7x - 4$.
- Tegn grafen for $L_3(x)$ sammen med datapunkterne, og kontroller, at grafen går gennem de ønskede punkter.
- Kontroller ved beregning, at polynomiet opfylder det ønskede.

Det er indlysende ud fra metoden som beskrevet ovenfor, at dette kan generaliseres. Har vi eksempelvis 11 datapunkter, som i Runges eksempel, kan vi opskrive interpolationspolynomiet af grad 10 gennem disse punkter. Når vi udtrykker os i bestemt form, er det, fordi vi er sikre på, at det polynomium, vi har fundet ved at følge Lagrange's interpolationsmetode, er det eneste af grad 10, hvis graf går gennem de givne punkter.

Sætning 1: Interpolationspolynomiet er entydigt bestemt

Antag, at vi har givet $n + 1$ datapunkter, hvor alle x -værdierne er forskellige. Det polynomium af grad n , vi finder ved Lagrange metode, er entydigt bestemt, dvs. det er det eneste polynomium af grad n , hvis graf går gennem de givne datapunkter.

Bevis

Vi antager uden tab af generalitet, at der er givet 11 datapunkter, og at vi har fundet et 10. gradspolynomium $p(x)$, hvis graf går gennem de 11 punkter. Påstanden er, at dette er det eneste 10. gradspolynomium med den egenskab.

Antag nemlig, at vi havde et andet 10. gradspolynomium, $q(x)$, hvis graf også gik gennem de 10 punkter, og antag $p(x) \neq q(x)$. Hvis vi nu udregner differensen:

$$r(x) = p(x) - q(x)$$

så må $r(x)$ være et polynomium af grad højst 10. Overvej selv dette!

Men da både graferne for $p(x)$ og $q(x)$ går gennem de 11 datapunkter, så har de to polynomier samme funktionsværdi i de 11 x -værdier:

$$p(x_1) = q(x_1), p(x_2) = q(x_2), \dots, p(x_{11}) = q(x_{11})$$

og derfor er (overvej selv dette):

$$r(x_1) = 0, r(x_2) = 0, \dots, r(x_{11}) = 0,$$

Men vi ved fra afsnit 3.1 i kapitel 3, at et egentligt polynomium af grad n højst har n rødder. Dette er også indholdet i sætning 32 i kapitel 5B, hvor sætningen blev bevist.

Hvis $r(x)$ har 11 rødder, kan det derfor ikke være et egentligt polynomium af grad 10 eller mindre. Men så må det være 0-polynomiet:

$$r(x) = 0 \Leftrightarrow p(x) - q(x) \Leftrightarrow p(x) = q(x)$$

Det var altså samme polynomium. ✓

Det ser ud, som om man skal starte forfra, hvis man ønsker at tilføje yderligere punkter, fx punkter med x -værdier midt mellem de allerede givne. Men der findes *algoritmer*, der giver en simpel opskrift på skridt for skridt at beregne Lagrange interpolationerne for stadigt flere punkter. Se nærmere på bogens **website**.



1.3 Secret Sharing – om at gemme og dele hemmeligheder

Hvor og hvordan gemmer man password til staters og virksomheders hemmeligste dokumenter? Hvordan opbevarer man de centrale koder til en evt. missilaffyring? I den moderne digitale verden er der brug for at kunne kryptere information, også i mere fredelige tilfælde. Krypteringen sker med bestemte *nøgler*, der ofte er snedigt konstrueret ved hjælp af talteori. Men hvor gemmer man den hemmelig del af nøglerne? Nøglerne består af meget lange strenge af tal og bogstaver, så det er urealistisk at håndtere dem manuelt.

De to centrale begreber her er *sikkerhed* og *pålidelighed*, på engelsk: *confidentiality* og *reliability*. Hvis adgangskoder til bankkonti ligger ét sted, uden back-up, risikerer man at miste dem, men ligger de spredt flere steder, er risikoen for, at de falder i andres hænder, større. Hvis resultaterne af en digital afstemning sendes afsted i én pakke, risikerer man der opstår fejl, men sendes der flere kopier, er risikoen for angreb større. Løsningen på dette dobbelte problem kan findes inden for den matematiske disciplin, der hedder *Secret Sharing*. Ideen er følgende:

En hemmelighed deles op i fx 10 dele (shares), og hver af de 10 dele gives til 10 personer eller computere. Opdelingen sker på en sådan måde, at hvis man fx har kendskab til 7 eller færre af disse, så kan man ikke opnå nogen som helst viden om hemmeligheden. Men hvis man har kendskab til 8 eller flere, så kan man genskabe hemmeligheden 100 %. Tallene 10 og 7 fastlægges af den "dealer", der opdeler hemmeligheden og fordeler de forskellige shares. Og den centrale metode, der anvendes i et af de mest benyttede af disse systemer, *Shamirs Secret Sharing Scheme*, er ret overraskende Lagrange interpolation! Via bogens **website** kan du finde et link til en film, hvor metoden præsenteres, og hvor et lidt større eksempel gennemregnes. Vi vil her illustrere med et simpelt eksempel.



Lad os sige, at hemmeligheden er tallet 1234. Hemmeligheden ønskes opdelt i 6 shares, der gives til 6 forskellige personer, der tildeles numrene 1 til 6. Opdelingen skal ske på en sådan måde, at hvis 3 (eller flere) af de 6 er tilstede og lægger deres del af hemmeligheden på bordet, så kan de rekonstruere det oprindelige tal. Men hvis kun to er tilstede, kan de ikke finde ud af noget som helst om dette tal.

Tallet 3 fortæller dealeren, at der skal konstrueres et 2. gradspolynomium. I eksemplet ovenfor skal der konstrueres et 7. gradspolynomium. Det hemmelige tal skal være konstantleddet i polynomiet, mens de andre to koefficienter vælges tilfældigt med en random-funktion, fx:

$$a_0 = 1234, a_1 = 166, a_2 = 94$$

Dealerens polynomium er altså: $p(x) = 94x^2 + 166x + 1234$.

De 6 shares udregnes som 6 forskellige funktionsværdier. Der er frit valg, så vi vælger det enkleste:

x	1	2	3	4	5	6
$p(x)$	1494	1942	2578	3402	4414	5614

De 6 personer ved, at mindst 3 af dem skal mødes for at finde hemmeligheden, og derfor ved de også, at det polynomium, der er anvendt, er et 2. gradspolynomium. For gennem tre punkter går der præcis én graf for et andengradspolynomium, mens der gennem to punkter går uendeligt mange. Lad os sige, at personerne 2, 4 og 5 mødes. De lægger deres tal på bordet, og konstruerer nu ved Lagrange interpolation polynomiet:

$$L_2(x) = 1942 \cdot \frac{(x-4) \cdot (x-5)}{(2-4) \cdot (2-5)} + 3402 \cdot \frac{(x-2) \cdot (x-5)}{(4-2) \cdot (4-5)} + 4414 \cdot \frac{(x-2) \cdot (x-4)}{(5-2) \cdot (5-4)} = 94x^2 + 166x + 1234$$

De tre fremmødte kan nu udregne eller blot aflæse, at hemmeligheden er $L_2(0) = 1234$.

Teknikken virker for alle polynomier, og den bygger på den simple iagttagelse, at der skal mindst $n + 1$ punkter til for at bestemme et n -te grads polynomium. Og der kan anvendes vilkårligt store tal, netop fordi Lagrangeinterpolationen giver mulighed for at regne eksakt og ikke tilnærmet. Du kan via bogens **website** finde et link til en demonstration af, hvordan secret sharing virker i praksis og her se, hvor enorme tal de enkelte shares er.



Øvelse 8.9

Del klassen op i tre grupper. Gruppe A vælger et hemmeligt 5-cifret tal og deler denne hemmelighed op i lige så mange dele, som der er medlemmer af gruppe B. Gruppe B giver tilsvarende shares til medlemmerne i gruppe C, og gruppe C giver til gruppe A. Opdelingen skal ske således, at er 4 tilstede, kan de finde hemmeligheden, men 3 eller færre kan ikke. Koefficienterne vælges som tilfældige 5-cifrede tal. Når en gruppe har modtaget sine shares, kan man evt. dele sig op i to grupper, der hver prøver at finde hemmeligheden – og se om man finder det samme.

Vi har ovenfor brugt de almindelige regneregler for hele tal. Når man anvender metoden i praksis, så anvendes det, der hedder "modulo-regning". Man kender det godt i det daglige – når klokken er 24, tæller man ikke videre, men starter forfra, så 27 svarer til 3, 30 svarer til 6 osv. Det kan man også gøre for ethvert andet tal end 24. Man anvender denne modulo-regning, fordi det gør koderne endnu mere sikre. Det er forklaret nærmere i eksemplet på bogens **website**.

