Hemmeligheder og polynomier

Kasper Bjering Søby Jensen, Roskilde Katedralskole

Det er en velkendt matematisk disciplin at forsøge at skjule hemmeligheder, og at forsøge at få fat på andres hemmeligheder. Et eksempel på disciplinen er, at en gruppe mennesker skal gemme en kollektiv hemmelighed, som de kun kan afsløre, hvis et vist antal vilkårlige medlemmer af gruppen går sammen om det.

Et eksempel kan være et nationalt sikkerhedsråd på 5 medlemmer, som kan beslutte at affyre landets atomvåben. Her kunne et princip være, at 3 vilkårlige medlemmer af rådet skal kunne kende koden, mens to medlemmer ikke må kunne kende den.

Eksemplet kan udvides til større grupper. Det kan være, at en gruppe på 100 mennesker bærer på en kollektiv hemmelighed, som 20 vilkårlige medlemmer af gruppen kender, men som 19 ikke kender. Principielt set handler det altså om at konstruere 100 puslespilsbrikker, således at 20 tilfældige brikker altid kan danne hele motivet, mens 19 brikker aldrig kan give blot et indtryk af dette.

Helt generelt kan det formuleres: En hemmelighed S kendes kollektivt af en gruppe på N medlemmer, hvis en vilkårlig samling af n medlemmer af gruppen ønsker det.

Problemet virker simpelt at forstå, men kompliceret at løse. Det viser sig imidlertid at kunne gøres ganske simpelt på en måde, som der sagtens kan arbejdes lavpraktisk med i en 1.g–klasse eller med stor teoretisk dybde i en 3.g–klasse.

Teorien bag løsningen af problemet – kaldet *Secret Sharing* – blev i 1979 udviklet af den israelske kryptolog *Adi Shamir*, som normalt er kendt fra S'et i RSA–kryptering. Hans idé er uhyre simpel og bygger på grundlæggende teori om *polynomier*. Den centrale sætning er:

> *Der eksisterer netop ét polynomium af grad n, hvis graf går gennem n + 1 givne punkter*

Den simple idé er at gemme hemmeligheden S i et polynomium $p(x)$ af grad $n-1$. Det kan gøres på mange måder, men den simpleste er at gemme den i konstantledet. Hvis hvert medlem af gruppen udstyres med sit eget unikke punkt fra grafen for p, vil enhver vilkårlig delgruppe med n medlemmer kunne genskabe polynomiet ved polynomiel regression og dermed aflæse hemmeligheden. Grupper på færre end n medlemmer, vil derimod ikke kunne genskabe det.

For at danne et brugbart polynomium til at gemme hemmeligheden S vælges blot en vilkårlig serie på $n-1$ koefficienter $a_1, a_2, \ldots a_{n-1}$, og polynomiet dannes nu som:

$$p(x) = a_{n-1}\cdot x^{n-1} + a_{n-2}\cdot x^{n-2} + \ldots + a_2\cdot x^2 + a_1\cdot x + S$$

Hvert gruppemedlem udstyres nu med et vilkårligt punkt. Mest simpelt kan de N medlemmer hver tildeles netop ét af punkterne $(1, p(1)), (2, p(2)), \ldots, (N, p(N))$.

Simpelt eksempel

Metoden til *Secret Sharing* kan anvendes allerede inden for de første uger af grundforløbet, når eleverne skal øve sig i to–punktsformlen for lineære sammenhænge. Lad os sige, at eleverne får at vide, at de som kollektiv kender hemmeligheden "lærerens alder", men kun kan afsløre den i makkerpar. Hver elev er udstyret med et af nedenstående punkter og skal selv finde sig en makker.

x	1	2	3	4	5	6	7	8	9	10
$p(x)$	39	42	45	48	51	54	57	60	63	66

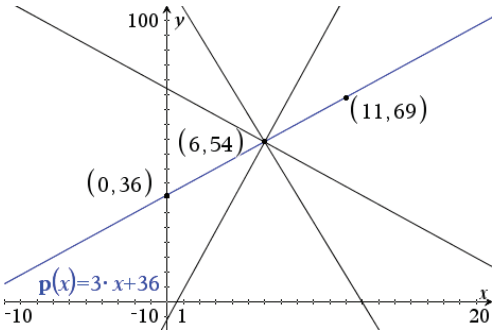
x	11	12	13	14	15	16	17	18	19	20
$p(x)$	69	72	75	78	81	84	87	90	93	96

Eleverne med punkterne (6, 54) og (13, 75) kan nu sammen bestemme det førstegradspolynomium $p(x) = a\cdot x + S$ som afslører den skjulte hemmelighed, ved anvendelse af de velkendte formler:

$$a = \frac{y_2 - y_1}{x_2 - x_1} = \frac{75-54}{13-6} = \frac{21}{7} = 3$$

$$b = y_1 - a\cdot x_1 = 54 - 3\cdot 6 = 54 - 18 = 36$$

Da $S = b$ er det vist, at $S = 36$, og hemmeligheden om, at læreren er 36 år gammel, er afsløret. Ingen elev kunne have afsløret denne hemmelighed alene – men alle elevpar kan afsløre den sammen. Opgaven kan passende bruges til at uddybe nødvendigheden af at kende to punkter, for at bestemme en forskrift, som bl.a. vist på følgende figur.



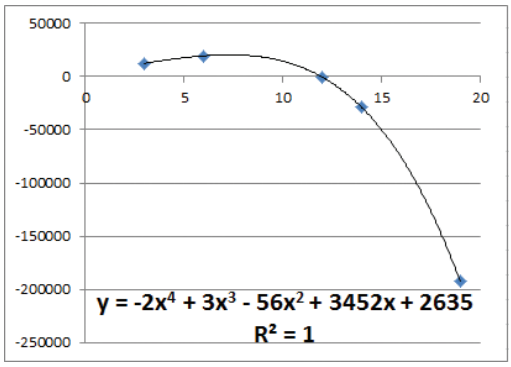
Avanceret eksempel

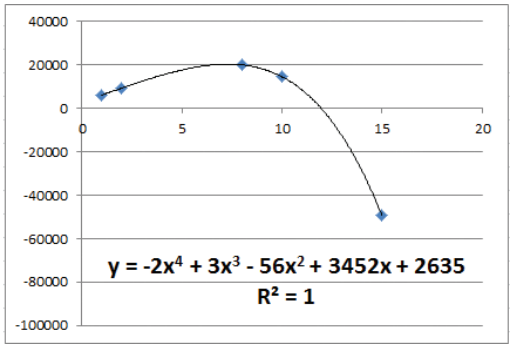
Lad os nu se på et mere avanceret eksempel, hvor kompleksiteten er større. Eleverne skal nu afsløre hemmeligheden "hvad er lærerens postnummer". Igen tildeles hver elev et punkt. Nedenstående tabel kunne være eksempler på 20 punkter.

x	1	2	3	4	5	6	7	8	9	10
$p(x)$	6032	9307	12406	15227	17620	19387	20282	20011	18232	14555

x	11	12	13	14	15	16	17	18	19	20
$p(x)$	8542	-293	-12484	-28613	-49310	-75253	-107168	-145829	-192058	-246725

Eleverne går nu sammen i selvvalgte grupper af fem personer, for at afsløre hemmeligheden. Lad os sige, at en gruppe består af elev nummer 3, 6, 12, 14 og 19 og en anden gruppe af elev nummer 1, 2, 8, 10 og 15. Ved hjælp af polynomiel regression i eksempelvis Excel, kan de to grupper nu frembringe nedenstående to figurer. Begge grupper afslører at lærerens postnummer er 2635. Efterfølgende kan eleverne danne nye grupper og se, at også denne gruppe "kender" hemmeligheden.

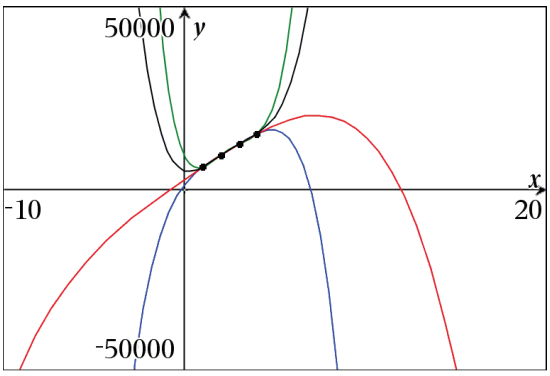




Øvelsen kan efterfølgende udvides til, at eleverne selv skal gemme på hemmeligheder. I første omgang ved at lade dem konstruere punkter, som andre grupper af elever kan afsløre hemmeligheder på baggrund af, men også mere innovative opgaver som at udvide metoden til fx at gemme på tekststrenge.

Sidstnævnte kan fx gøres ved at give hvert bogstav et unikt tal – simplest muligt A:1, B:2, C:3, osv. Herefter kan der konstrueres en bunke punkter for hvert tegn i tekststrengen, som kan afsløre den værdi der fortæller tegnet. Er der fx seks tegn i tekststrengen, kan hver elev vælge et tilfældigt punkt fra hver af seks bunker og herefter afsløre ordet i passende grupper.

Det kan også diskuteres med eleverne, hvorfor det er umuligt at bryde hemmeligheden med for få punkter. I ovenstående eksempel kan man fx undersøge hvad der sker hvis de fire første elever forsøger at afsløre hemmeligheden alene. Grafen viser hvordan de kan komme frem til så forskellige postnumre som 1240, 2635, 5000 og 9000.



Et kig på koefficienterne for de fire polynomier vil dog hurtigt afsløre, at for det rigtige postnummer er disse endog meget pæne, sammenlignet med de øvrige. Dette kan være en tilgang til at angribe metoden. Det kan således være nødvendigt at øge sikkerheden på forskellig vis. Også her kan eleverne arbejde innovativt inden for en rent matematisk problemstilling.

Didaktiske overvejelser

Ovenstående eksempel er på mange måder interessant. For det første er det relevant, fordi det i skrivende stund ser ud til, at polynomiel regression bliver obligatorisk kernestof på både A– og B–niveau. Der er altså brug for at skabe relevante didaktiske situationer, hvor der kan arbejdes med emnet.

For det andet betyder det, at man kan bevæge sig ud over det forhold, at polynomier mest er noget vi interesserer os for af rent matematisk interesse. Teorien viser sig i dette eksempel at have en meget høj grad af anvendelighed, som rækker langt ud over mere eller mindre autentiske modeller over kalkuners vækst, skildpadders æglægning, temperaturvariationer, mv.

For det tredje rummer eksemplet mulighed for at arbejde mere teoretisk med emnet, herunder at bevise entydighed og eksistens af det polynomium af grad $n - 1$, hvis graf netop går igennem n givne punkter. Dette kan bl.a. indeholde arbejde med Lagrange basispolynomium og Lagrange interpolationspolynomium. Dette er svær, men overkommelig, matematisk teori, som kan give dygtige elever et indblik i matematik, som det tager sig ud i starten af et matematikstudium. Emnet er også oplagt til SRP. Jeg vil dog overlade det til andre at didaktificere arbejdet med denne teori.

Jeg skal her sige tak til lektor ved Aarhus Universitet, *Johan Peder Hansen*, for i forbindelse med Institut for Matematiske Fags Matematiklærerdag at have åbnet mine øjne for ovenstående eksempel. Og jeg vil anbefale enhver, der ønsker et dybere indblik i teorien omkring dette emne, til at se på hans præsentation fra dagen:
math.au.dk/fileadmin/Files/matlaererdag/2017/JPH_slide_ShamirSecretSharing.pdf