Wiskunnend Wiske opdracht 3

Heilig Graf
Patersstraat 26
2300 Turnhout
Klas 602 wetenschappen-wiskunde

Doel: een geheime code S verdelen in n delen zodat we bij :

- elke m delen S steeds kunnen vinden
- elke m-1 delen S niet kunnen vinden.

Basisredenering:

- 2 punten met verschillende x-coördinaten (koppels) bepalen éénduidig een rechte, dus een eerstegraadsfunctie, maar 1 punt volstaat niet.
- Analoog bepalen 3 verschillende punten een parabool, dus een tweedegraadsfunctie, maar 2 punten volstaan niet want er zijn oneindig veel parabolen door 2 punten.
- In 't algemeen kan men aantonen (zie Lagrange-polynomen) dat m punten **precies één** (m-1) – de graadsfunctie bepalen, terwijl m-1 punten daarvoor niet volstaan. We noemen dit verder ***stelling p***.

Werkwijze voor 10 bewakers:

Stel dat de geheime code (bvb 1500) moet verdeeld worden over 10 schatbewakers en elk trio bewakers moet in staat zijn de kluis te kunnen openen, maar geen enkel tweetal mag hiertoe in staat zijn.

Barabas neemt 1500 als constante term van $f(x) = a + bx + cx^2$.

Om de code te kunnen verdelen over de 10 bewakers, neemt hij voor b en c twee willekeurige getallen: bvb. 326 en 25.

Dan is in dit voorbeeld: $f(x) = 1500 + 326x + 25x^2$

Hij berekent 10 punten die tot die functie behoren: bvb. (-4, 596), (-3, 747), (-2, 948), (-1, 1199), (0,1500),(1,1851), (2,2252), (3,2703), (4,3204) en (5,3755).

Elke schatbewaker krijgt één koppel.

Om de code te KUNNEN vinden heeft men nu zeker 3 punten nodig, bvb.

(1, 1851), (2, 2252) en (3, 2703).

Als we deze drie punten invullen in het functievoorschrift krijgen we namelijk het volgende stelsel:

$$\begin{cases} f(1) = a+b.1+c.1^2 = 1851 \\ f(2) = a+b.2+c.2^2 = 2252 \\ f(3) = a+b.3+c.3^2 = 2703 \end{cases}$$

Dat is een stelsel van drie vergelijkingen met drie onbekenden met precies één oplossing (zie ***stelling p*** hierboven) namelijk (a, b, c) = (1500, 326, 25).

Als Barabas nu stelt dat de constante term van deze functie de code is, kan de code gevonden worden aan de hand van om het even welke drie koppels.

Kanttekeningen:

- Worden er maar twee koppels geleverd (door twee bewakers) dan komt men steeds één koppel tekort om een stelsel te bekomen dat precies één oplossing heeft, aangezien de rang van de coëfficiëntenmatrix dan maximum 2 is en het aantal onbekenden 3, dus heeft dat stelsel steeds oneindig veel oplossingen, waardoor je de code nooit kan bepalen via die gegevens.
- Als Barabas slim is (en we gaan daar van uit, aangezien hij professor is) neemt hij in praktijk best geen negatieve x-coördinaten (dat insinueert direct dat je met functies werkt) en evenmin het snijpunt met de y-as (want iemand die dan wat op internet gaat surfen, komt op de idee 1500 als code te proberen, aldus Shamir's secret sharing-principe) en dan is deze oplossing van Barabas weinig verdienstelijk.
- Varianten: In plaats van de constante term kan eveneens de coëfficiënt van de hoogstegraadsterm genomen worden als geheime code, of de som van alle coëfficiënten, …

Werkwijze voor n bewakers:

Stel van de n bewakers moet elk m-tal de code kunnen vinden, maar geen enkel

(m-1)-tal mag hiertoe in staat zijn.

Stel $f(x)= a_0 + a_1x + a_2x^2 +\ldots+ a_{m-1}x^{m-1}$

Zet een geheime code in de plaats van a_0 en vervang a_1, a_2, …, a_{m-1} door m – 1 willekeurige getallen.

Bereken n verschillende koppels van f en bezorg elke bewaker één koppel.

Elk m-tal bewakers zal m koppels leveren: zo bekom je door invullen (analoog als hierboven) een stelsel van m vergelijkingen met m onbekenden a_0, a_1, a_2, …, a_{m-1} dat volgens ***stelling p*** precies één oplossing zal hebben.

Als Barabas stelt dat de constante term de geheime code is, kan die met de hulp van elk m-tal bewakers dus ontcijferd worden.

Elk (m-1)-tal bewakers zal slechts m-1 koppels leveren, dus is er telkens één vergelijking te weinig om een bepaald stelsel te bekomen; er zullen oneindig veel oplossingen zijn, dus de code kan niet gevonden worden.