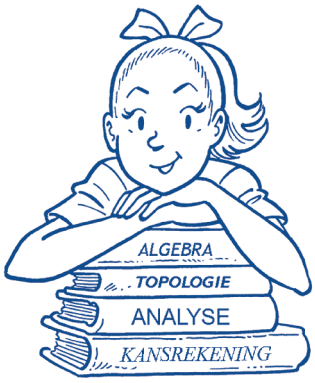
WISKUNNEND WISKE

DE STIEKEME SLEUTEL



OPGAVE 3

Wiske wil een belangrijk telegram sturen naar professor Barabas. Ze is echter bang dat Krimson het telegram kan onderscheppen. In dat geval wil ze niet dat Krimson er wijs uit kan worden. Daarom zoekt ze een manier om de boodschap te versleutelen. Dat doet ze als volgt. Ze geeft alle letters een getalwaarde: A wordt 0, B wordt 1, . . . , Z wordt 25. De symbolen spatie, komma en punt worden respectievelijk 26, 27 en 28. Nu zoekt ze een manier om de getallen van plaats te wisselen. Ze kan bijvoorbeeld bij elk getal twee optellen. Omdat de getallen dan zouden lopen tot 30 gebeurt de optelling “modulo 29”. Dat betekent dat we elk getal vervangen door zijn rest na deling door 29. 29 wordt dan 0, 30 wordt 1 enzovoort. Daarna worden de getallen weer omgezet in letters en leestekens. De versleuteling ziet er dan zo uit:

A	B	C	...	Z	spatie	komma	punt
0	1	2	...	25	26	27	28
2	3	4	...	27	28	0	1
C	D	E	...	komma	punt	A	B

Wat leuk is aan deze manier van coderen is dat de boodschap uniek te decoderen is. Dat betekent dat als je de gecodeerde boodschap krijgt, je altijd kan achterhalen wat de originele boodschap was.

Wiske stelt voor om een constante op te tellen bij de getallen. Suske stelt voor om elk getal te vermenigvuldigen met een constante, die geen veelvoud is van 29. Lambik stelt voor om elk getal te kwadrateren. Tante Sidonia stelt voor om elk getal tot de derde macht te verheffen. Al deze operaties gebeuren modulo 29.

1. Ga na en bewijs bij welke van deze 4 voorstellen de boodschap uniek te decoderen is en bij welk voorstel niet. Doe dit bij het voorstel van Suske en Wiske niet door voor elke constante afzonderlijk na te gaan of de boodschap uniek te decoderen is.
2. Besluit hieruit of een boodschap uniek te decoderen is als we elk getal x vervangen door $(7x + 10)^3 + 2$ modulo 29.
3. Wiske gebruikt deze procedure uit 2. en stuurt Barabas de boodschap “BYVG SGXQC”. Wat is de gedecodeerde boodschap?

WISKUNDIG WEETJE

De versleuteling die Wiske voorstelt is een variant van de Caesarrotatie, gebruikt door Caesar om militaire boodschappen te coderen. Naar alle waarschijnlijkheid was dit voor hem een veilige manier om informatie te beschermen, maar tegenwoordig zou deze codering snel gekraakt worden. De Duitsers versleutelden hun boodschappen in de Tweede Wereldoorlog met een machine onder de naam Enigma. Elke dag veranderde de manier van versleutelen. Omdat er voor de letters A tot Z 26! mogelijke versleutelingen zijn, was het een haast onmogelijke opdracht om elke dag de code van de Duitsers te breken. De wiskundige Alan Turing, tevens vader van de computerwetenschappen, slaagde er met zijn kompanen in Bletchley Park in een soort mechanische computer te bouwen waarmee de code gebroken kon worden. Men schat dat de oorlog hierdoor twee jaar minder lang geduurd heeft en 14 miljoen levens minder kostte!

VUB 50 JAAR