Heilig Hart Van Maria
Berlaar
6K

## Opgave 3: De stiekeme sleutel

Gegeven en gevraagd: zie opgave

Oplossing:

### Vraag 1

Om te bewijzen of een boodschap uniek te decoderen valt, beschouwen we voor de som en het product twee beginletters met elk zijn gekoppelde getalwaarde. Deze getalwaarden noemen we a en b. Na het uitvoeren van de bewerking op de getalwaarden a en b komen we 2 nieuwe getalwaarden uit, respectievelijk a' en b'. Nu komt het te bewijzen neer op aantonen dat als a $\neq$ b, dat ook a' $\neq$ b'. Met andere woorden: er bestaat een bijectie tussen de verzameling van beginletters en de verzameling van de gecodeerde letters.

Bewijs voor som:

a' en b' kunnen beschreven worden als:

$$a' = a + c - k_1 \cdot 29$$
$$b' = b + c - k_2 \cdot 29$$

Waarbij c een constante en $k_1$, $k_2$ het grootste natuurlijk getal waarvoor a' respectievelijk b' positief blijven.

Stel a' = b' dan moeten ook volgende gelijkheden gelden:

$$a + c - k_1 \cdot 29 = b + c - k_2 \cdot 29$$
$$a - b = 29(k_1 - k_2)$$

Aangezien 29 een priemgetal is, moet het linkerlid gelijk zijn aan een geheel veelvoud van 29. Aangezien a en b nooit meer dan 28 eenheden uit elkaar kunnen liggen kan deze gelijkheid nooit voldaan zijn, enkel als a = b. Hieruit volgt dat als a $\neq$ b, dat ook a' $\neq$ b'.

Bewijs voor product:

a' en b' kunnen geschreven worden als:

$$a' = a \cdot c - k_1 \cdot 29$$
$$b' = b \cdot c - k_2 \cdot 29$$

Waarbij c een constante is die geen veelvoud is van 29 en $k_1$, $k_2$ het grootste natuurlijk getal waarvoor a' respectievelijk b' positief blijven.

Stel a' = b', dan moeten ook volgende gelijkheden gelden:

$$a \cdot c - k_1 \cdot 29 = b \cdot c - k_2 \cdot 29$$
$$c(a - b) = 29(k_1 - k_2)$$

Aangezien 29 een priemgetal is, moet een van beide termen in het linkerlid een geheel veelvoud zijn van 29. Constante c voldoet hier niet aan (zie gegeven), en aangezien a en b nooit meer dan 28 eenheden uit elkaar kunnen liggen kan deze gelijkheid nooit voldaan zijn, enkel als a = b. Hieruit volgt dat als a $\neq$ b, dat ook a' $\neq$ b'.

De coderingsmethode van Lambik geeft geen unieke decodering. Als a = 14 en b = 15 dan geldt $a' = (14^2) \bmod 29 = 22$ en $b' = (15^2) \bmod 29 = 22$. Bijgevolg geldt er niet dat als a $\neq$ b, dat ook a' $\neq$ b'.

De coderingsmethode van Tante Sidonia geeft wel een unieke decodering. Dit zijn we nagegaan door voor elke waarde a de gecodeerde waarde a' te berekenen. Dit gaf een bijectie.

## Vraag 2

Om te bewijzen dat $(7x + 10)^3 + 2 \mod 29$ een unieke codering is wordt het opgedeeld in verschillende stappen. Ten eerste valt $7x$ te schrijven als $29 \cdot k + r$ waarbij $k$ het (positief) quotient en $r$ de rest is bij deling van $7x$ door 29. Uit vraag 1 weten we dat elke waarde x een unieke rest geeft. Vervolgens geldt $29 \cdot k + r + 10 = 29 \cdot k + (r + 10) = 29 \cdot k' + r'$ waarbij r' en k' de rest en het quotient zijn bij deling van $29 \cdot k + r + 10$ door 29. Door vraag 1 en omdat r een uniek getal is tussen 0 en 28 geldt dat r' ook uniek is. Om nu verder te gaan wordt de derde macht uitgewerkt, dit geeft $(29 \cdot k' + r')^3 = (29^3 k'^3 + 3 \cdot 29^2 k'^2 r' + 3 \cdot 29 k' r'^2 + r'^3)$. Omdat de eerste drie termen een veelvoud van 29 zijn en we uit vraag 1 weten dat $r'^3$ een unieke rest geeft na deling door 29 geldt $(29 \cdot k' + r')^3 = k'' \cdot 29 + r''$. Analoog volgens de optelling met 10 volgt dat de optelling $k'' \cdot 29 + r'' + 2$ een unieke rest zal geven. Na modulo houden we deze unieke rest over die perfect te coderen valt.

## Vraag 3

Om deze vraag op te lossen was het niet mogelijk direct de terugweg te maken en de letters te decoderen aangezien er met een modulo gewerkt wordt en het dus niet te achterhalen valt welk getal er eerst stond. Om deze reden moest er wel gebruik gemaakt worden van een volledige tabel waarin alle letters en de drie symbolen worden omgezet. Zoals in de vorige vraag aangetoond is de boodschap uniek gecodeerd en kan dus de terugweg ook gemaakt worden. Door de gecodeerde boodschap "BYVG SGXQC"te decoderen met de gemaakte tabel kregen we de boodschap "PRIEMGETAL".

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 7x | 0 | 7 | 14 | 21 | 28 | 35 | 42 | 49 | 56 | 63 | 70 | 77 | 84 | 91 | 98 |
| 7x+10 | 10 | 17 | 24 | 31 | 38 | 45 | 52 | 59 | 66 | 73 | 80 | 87 | 94 | 101 | 108 |
| $(7x+10)^3$ | 1000 | 4913 | 13824 | 29791 | 54872 | 91125 | 140608 | 205379 | 287496 | 389017 | 512000 | 658503 | 830584 | 1030301 | 1259712 |
| $(7x+10)^3+2$ | 1002 | 4915 | 13826 | 29793 | 54874 | 91127 | 140610 | 205381 | 287498 | 389019 | 512002 | 658505 | 830586 | 1030303 | 1259714 |
| $(7x+10)^3+3 \% 29$ | 16 | 14 | 22 | 10 | 6 | 9 | 18 | 3 | 21 | 13 | 7 | 2 | 26 | 20 | 12 |
| | Q | O | W | K | G | J | S | D | V | N | H | C | Spatie | U | M |

| | P | Q | R | S | T | U | V | W | X | Y | Z | Spatie | Komma | Punt |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 7x | 105 | 112 | 119 | 126 | 133 | 140 | 147 | 154 | 161 | 168 | 175 | 182 | 189 | 196 |
| 7x+10 | 115 | 122 | 129 | 136 | 143 | 150 | 157 | 164 | 171 | 178 | 185 | 192 | 199 | 206 |
| $(7x+10)^3$ | 1520875 | 1815848 | 2146689 | 2515456 | 2924207 | 3375000 | 3869893 | 4410944 | 5000211 | 5639752 | 6331625 | 7077888 | 7880599 | 8741816 |
| $(7x+10)^3+2$ | 1520877 | 1815850 | 2146691 | 2515458 | 2924209 | 3375002 | 3869895 | 4410946 | 5000213 | 5639754 | 6331627 | 7077890 | 7880601 | 8741818 |
| $(7x+10)^3+3 \% 29$ | 1 | 15 | 24 | 27 | 23 | 11 | 19 | 17 | 4 | 8 | 28 | 5 | 25 | 0 |
| | B | P | Y | Komma | X | L | T | R | E | I | Punt | F | Z | A |