**Antwoorden les 11: Vermenigvuldigen met 1**

**Opgave 1**Eerst raadplegen we de tabel van de encryptiefunctie ***E*(x)=REST(x5;26)=x5(mod 26).**Opmerking: Merk op dat de notatie in het Excel-rekenblad iets afwijkt van de functie-notatie. Dit heeft te maken met de invoer in Excel.



Uit de tabel lezen we de klare tekst af:
E -> k; F -> e; X->r; E-> k; X->r; A->a; J->d; K->e

Nu is het niet moeilijk meer om de tabel van achter naar voren in te vullen:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| k | 10 | 105=10000 | -3846\*26= | 4 | E |
| e | 5 | 55=3125 | -120\*26= | 5  | F  |
| r | 17 | 175=1419857 | -54609\*26= | 23 | X |
| k | 10 | 105=100000 | -3846\*26= | 4 | E |
| r | 17 | 175=1419857 | -54609\*26 | 23 | X |
| a | 0 | 05=0 | -0\*26= | 0 | A |
| d | 3 | 35=243 | -9\*26= | 9 | J |
| e | 4 | 45=1024 | -39\*26= | 10 | K |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| E | 4  | +3846\*26= | 100000 | 100000(1/5) = | 10 | k |
| F | 5 | +120\*26= | 3125 | 3125(1/5)= | 5 | e |
| X | 23 | +54609\*26= | 1419857 | 1419857(1/5)= | 17 | r |
| E | 4 | +3846\*26= | 100000 | 100000(1/5)= | 10 | k |
| X | 23 | +54609\*26= | 1419857 | 1419857(1/5)= | 17 | r |
| A | 0 | +0\*26= | 0 | 0(1/5)= | 0 | a |
| J | 9 | +9\*26= | 243 | 243(1/5)= | 3 | d |
| K | 10 | +39\*26= | 1024 | 1024(1/5)= | 4 | e |

**Opgave 2**a. Er geldt **9**\***3=1(mod26)**. Het getal 3 is de inverse van 9 en het getal 9 is de inverse van 3 ONDER DE VERMENIGVULDIGING (mod26).
b. Dat laatste moet er wel bij, want bijvoorbeeld onder een vermenigvuldiging (mod28) geldt **9\*3=27**.

**Opgave 3**
Bij sleutelpaar (8,1) is het resultaat

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REST(*E(x)*=8*x*+1;26)  | 1  | 9  | 17  | 25  | 7  | 15  | 23  | 5  | 13  | 21  | 3  | 11  | 19  | 1  | 9  | 17  | 25  | 7  | 15  | 23  | 5  | 13  | 21  | 3  | 11 | 19 |
| versleutelde tekst | b  | j  | r  | z  | h  | p  | x  | f  | n  | v  | d  | l  | t  | b  | j  | r  | z  | h  | p  | x  | f  | n  | v  | d  | l  | t  |

De helft van de letters komt tweemaal voor.

**Opgave 4**a. Bij sleutelpaar (6,5) komt ook de helft van de letters tweemaal voor.Het is geen geschikt sleutelpaar.
b. Bij sleutelpaar (5,2) komen alle letters weer terug inhet cijferalfabet. Dit is een geschikt paar:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REST(*E(x)*=5*x*+2;26)  | 2  | 7 | 12 | 17 | 22 | 1 | 6 | 11 | 16 | 21 | 0 | 5 | 10 | 15 | 20 | 25 | 4 | 9 | 14 | 19 | 24 | 3 | 8 | 13 | 18 | 23 |
| versleutelde tekst  | c | h  | m  | r | w | b  | g  | l  | q | v  | a  | f | k | p | u | z | e | j | o | t | y | d | i | n | s | x |

c. Bij sleutelpaar (6,5) krijgen we alle zesvouden plus 1kleiner dan 26, alle zesvouden plus 3 kleiner dan 26 en alle zesvouden plus 5 kleiner dan 26:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REST(*E(x)*=6*x*+5;26)  | 5  | 11 | 17 | 23 | 3  | 9  | 15 | 21 | 1  | 7  | 13 | 19 | 25 | 5  | 11 | 17 | 23 | 3  | 9  | 15 | 21 | 1  | 7 | 13 | 19 | 25 |
| versleutelde tekst | f  | l  | r  | x  | d  | j  | p  | v  | b  | h  | n  | t  | z  | f  | l  | r  | x  | d  | j  | p  | v  | b  | h  | n  | t  | z  |

**Opgave 5**

a. Het klare alfabet bestaat nu uit 28 symbolen (0 t/m 27)

b. Kies een denkbeeldig getal uit het rijtje 0, 1, 2, 3, ..., 27.
De uitkomst na versleutelen komt voor in het volgende rijtje:
7*x* (bijvoorbeeld als x=3), of
7*x* - 28 (bijvoorbeeld als x=6) of
7*x* - 56 (bijvoorbeeld als x=9) of
7*x* - 84 of ... of ...

De uitkomst is nu altijd deelbaar door 7 omdat zowel 7*x* als de getallen 28,56, 84, enz. deelbaar zijn door 7. Dit zijn immers veelvouden van de deler 28 en deze is deelbaar door 7.

Doen we hetzelfde met 26 als deler dan gaat dit niet op omdat 26 niet deelbaar is door 7.



**Opgave 6**

a. a=7 en b=0

b en c. We hebben de tabel voor affiene versleuteling uitgebreid met twee symbolen. Deze geven de code 26 en 27.
Bij de restfunctie ***E*(*x*)=REST(5*x*+2;28)** komen alle 28 letters terug in het cijferalfabet.
Bij de restfunctie ***E*(*x*)=REST(7*x*;28)** en ***E*(*x*)=REST(7*x* - 3;28)** krijgen we maar 4 letters terug:


Het is duidelijk dat het getal a=7 geen geschikte waarde is bij de deler 28.

**Opgave 7**

De encryptiefunctie *E*(*x*)=REST( **a***x* ;**26**) werkt correct
als **a**een van de getallen**3, 5, 7, 9, 11, 15, 17, 19, 21, 23 of 25**is.
Het gaat mis als **a** en **26** niet relatief priem zijn, zoals bij de even getallen en als **a**=13

**Opgave 8**De inverse van **436** is **1771** onder de vermenigvuldiging (mod **17159**) want **436\*1771-45\*17159=1**
Zonder rekenblad is het nauwelijks te doen om de inverse te berekenen.

**Antwoorden - Delen in Zm**

**Opgave 1**a. *x*= 26, want 10\*26 = 260 en 260 - 7\*37 = 260 - 259 = 1
b. *x* = 19, want 10\*19 = 190 en 190 - 5\*37 = 190 - 185 = 5

**Opgave 2**a. 10\*6 mod 59 = 60 mod 59 = 1.
b.

|  |  |
| --- | --- |
| 10\**x* mod 59 = | 4  |
| 6\*10\**x* mod 59 = | 6\*4 |
| 60\**x* mod 59 = | 24 |
| *x*mod 59 = | 24 |

*x*= 24 (of*x* = 83 of *x* = 142 of ... of ...)

c.

|  |  |
| --- | --- |
| 10\**x* mod 59 = | 5  |
| 6\*10\**x* mod 59 = | 6\*5  |
| *x* mod 59 = | 30 |

*x* = 30 (of *x* = 89 of *x* = 148 of ... of ...)

**Opgave 3**a. 0
b. 1

**Opgave 4**a. In **Z5**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 |
| Inverse | - | 1 | 3 | 2 | 4 |

b. In **Z6**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 | 5 |
| Inverse | - | 1 | - | - | - | 5 |

c. In **Z7**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| Inverse | - | 1 | 4 | 5 | 2 | 3 | 6 |

d. In **Z8**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Inverse | - | 1 | - | 3 | - | 5 | - | 7 |

e. In **Z9**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Inverse | - | 1 | 5 | - | 7 | 2 | - | 4 | 8 |

f. In **Z10**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Inverse | - | 1 | - | 7 | - | - | - | 3 | - | 9 |

g. In **Z11**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Getal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Inverse | - | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |

h. Ja, *a* heeft een inverse modulo *m* als *a*en *m* geen gemeenschappelijke delers hebben.

**Opgave 5**
(*m* - 1)2= *m*2 - 2*m* + 1 = 1 want *m*2 en 2*m* zijn veelvouden van *m*.

**Opgave 6**a. 24 = 2\*2\*2\*3. Dus 5 is bijvoorbeeld relatief priem met 24, maar ook 7, 11, 13, 17, 19, 23, 25, 29, 31,33, 35, ...
b. Nee, die zijn allebei deelbaar door 2. Dat geldt verder voor elk even getal.
c. Nee, alle 3-vouden zijn niet relatief priem met 24 want die is ook deelbaar door 3.