**Antwoorden les 13: De inverse**

Alle uitwerkingen van les 13 zijn terug te vinden op het bijgaande [rekenblad](http://www.e-klassen.nl/access/content/group/e-klas-project/gepubliceerd/wiskunde/Cryptografie/Html_nieuw/antwoorden/antwoorden_les_13-totaal.xls).



















**Antwoorden - Extra opgaven in Zm**

**Opgave 1**b. 485

**Opgave 2**a. 7
b. 70

**Opgave 3**
Elfstedentocht op 14februari.

**Opgave 4**a.

5727=243 ·*t*+1234)mod372281

365727+372281 ·*k*=243 ·*t*+1234

372281 ·*k*-243 ·*t*= -364493

b.

(372281 ·*k*)mod 372281 = 0

-243+372281=372038
en (-364493)mod372281=7788
zodat 372281·*k* -243·*t* =- 364493 gelijkwaardig is met
372038·*t*=7788 in **Z372281**

c.

280785 =(243 ·*t*+1234)mod372281
280785+372281·*k* =243·*t*+1234
372281·*k* - 243·*t*=-279551
Dus 372038·*t*=92730in **Z372281**

d.

cijfer=(243 · *t*+1234)mod372281

cijfer+372281·*k* = 243·*t*+1234

372281·*k* - 243·*t*=1234-cijfer

Dus 372038·*t* = 1234-cijfer in **Z372281**

Als je nu de inverse *b* van 372038in **Z372281** weet, weet je dat *b·*372038=1 in **Z372281**. Vervolgens kun je *t* berekenen: 1·*t*=*b*·(1234-cijfer).

e.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *a* | *m*  | *a*div*m*=*q*  | *a*mod*m*=r  | *b*  | *k*  |
| 372038 | 372281  | 0  | 372038  | -148606  | 148509  |
| 372281 | 372038 | 1 | 243 | 148509 | -148606 |
| 372038 | 243 | 1531 | 5 | -97 | 148509 |
| 243 | 5 | 48 | 3 | 2 | -97 |
| 5 | 3 | 1 | 2 | -1 | 2 |
| 3 | 2 | 1 | 1 | 1 | -1 |
| 2 | 1 | 2 | 0 | 0 | 1 |

De inverse van 372038 in **Z372281**is dus(-148606) mod 372281 = 223675.

f. *t* = *b* *·* (1234-*c*)= 223675 · (1234-365727)=078101
Dus *t*=078101 en de eerste twee letters van de boodschap zijn: "Ne".

g. Newton: actie=-reactie

**Opgave 5**
cijfer=(1719 ·*t* ) mod 294808, dus cijfer=1719·*t* in**Z294808.**Als je de inverse *b* van 1719 in Z294808 weet, weet je de oplossing van 1719·*b*=1 in Z294808.
Vervolgens kun je *t* berekenen: *t*=*b·*cijfer.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *a* | *m* | *a*div*m*=*q* | *a*mod*m*=*r* | *b* | *k* |
| 1719 | 294898 | 0 | 1719 | 343 | -2 |
| 294808 | 1719 | 171 | 859 | -2 | 343 |
| 1719 | 859 | 2 | 1 | 1 | -2 |
| 859 | 1 | 859 | 0 | 0 | 1 |
| 1 | 0 |   |   |   |   |

De inverse van 1719 in **Z294808** is dus 343, dus *t*=343 · cijfer.

Boodschap: Loper van B2 naar B5