**Antwoorden les 14: Rivest Shamir en Adleman**

Het [rekenblad](http://www.e-klassen.nl/access/content/group/e-klas-project/gepubliceerd/wiskunde/Cryptografie/Html_nieuw/antwoorden/antwoorden_les_14.xls)met de berekeningen is onder de link toegevoegd.







**Opgave 4**  
Het is moeilijk het getal 1040257 te ontbinden.Met een rekenblad s dit echter nog steeds eenvoudig te doen. 1040257(1/2) = ongeveer 1020, dus we zoeken de eerste 1020 regels af op het rekenblad. In kolom 1 zetten we de getallen 1 t/m 1020 en in kolom 2 de berekening 1040257/getal uit kolom 1.We vinden **1040257=127\*8191**

**Opgave 5**  
a.

**Ka=(5-1)\*(13-1)=48, Kb=(7-1)\*(11-1)=60**

b. Alice kiest 19. Bereken de inverse modulo 48

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **a** | **Ka** | **q** | **r** | **x** | **y** |
| 19 | 48 | 0 | 19 | -5 | 2 |
| 48 | 19 | 2 | 10 | 2 | -5 |
| 19 | 10 | 1 | 9 | -1 | 2 |
| 10 | 9 | 1 | 1 | 1 | -1 |
| 9 | 1 | 9 | 0 |  |  |

De inverse is **-5+48=43, na=5\*13=65**, dus de publieke sleutel van Alice is **{43,65}** en de privé-sleutel van Alice is **{19,65}**

Bob kiest 17.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **b** | **Kb** | **q** | **r** | **x** | **y** |
| 17 | 60 | 0 | 17 | -7 | 2 |
| 60 | 17 | 3 | 9 | 2 | -7 |
| 17 | 9 | 1 | 8 | -1 | 2 |
| 9 | 8 | 1 | 1 | 1 | -1 |
| 8 | 1 | 8 | 0 |  |  |

De inverse is **-7+60=53, ma=7\*11=77**, dus de publieke sleutel van Bob is **{53,65}** en de privé-sleutel van Bob is **{17,65}**

c. Alice berekent **619mod65=46** en vervolgens **4653mod77=30.** **c=30**

d. Bob ontvangt het bericht **30**en berekent **3017mod77=46** en **4643mod6=6. s=6**

**Antwoorden - Machtsverheffen modulo m**

**Opgave 1**  
a. Kwadrateren is hetzelfde als een getal met zichzelf vermenigvuldigen.  
b. Tot de derde macht verheffen is het kwadraat van een getal met het getal zelf vermenigvuldigen,enz.  
c. Herhaald vermenigvuldigen.

**Opgave 2**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ^ | 0 | 1 | 2 | 3 | 4 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 4 | 3 | 1 |
| 3 | 1 | 3 | 4 | 2 | 1 |
| 4 | 1 | 4 | 1 | 4 | 1 |

**Opgave 3**

|  |  |  |
| --- | --- | --- |
| a. In **Z31:** | b. In **Z25**: | c. In **Z325:** |
| **225= (25)5= 325= 15= 1** | **3301= (33)100\*3= 27100\*3= 2100\*3= (27)14\*22\*3= 314\*4\*3= 315\*4= (33)5\*4=**  **25\*4= 7\*4=3** | **1896= (182)48= (324)48= (-1)48mod325= 1** want **(-1)mod325 = 324** |

**Opgave 4**

|  |  |  |
| --- | --- | --- |
| a. In **Z553:** | b. In **Z1000:** | c. In **Z640:** |
| **1733= (173)11= 48911= (4892)5\*489= 2255\*489= (2252)2\*225\*489= 3022\*531= 512\*531=349** | **1240= (124)10= 73610= 6965= (6962)2\*696= (416)2\*696= 56\*696=976** | **73843= (74)960\*73= (481960)\*343= 321480\*343= 1240\*343=343** |

**Opgave 5**

|  |  |
| --- | --- |
| a. In **Z47:** | b. In **Z10:** |
| **247= (26)7\*25= 177\*32= (172)3\*17\*32= 73\*544= 72\*7\*27= 49\*189= 2\*1=2** | **381= (34)20\*3= 8120\*3= 120\*3=3** |

c. Van de uitkomsten van de machten van 3 schrijf je steeds het laatste cijfer op: 3,9,7,1,3,9,7,1,3,....  
De uitkomsten van de machten van 3 die een *viervoud plus één*als macht hebben eindigen steeds op 3, dus 381 ook.

**Antwoorden - Euler en Fermat**

**Opgave 1**a. 4 (1,5,7,11)  
b. 4 (1,2,3,4)  
c. 6 (1,2,3,4,5,6)  
d. *p*-1.  
e. 24(1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34)  
f. 4\*6=24, oftewel ***φ*(5*\*7*)=*φ*(35)**

**Opgave 2**  
a. ***φ*(7*7*)=*φ*(7)\**φ*(11)=6\*10=60**b. ***φ*(82)=*φ*(2)\**φ*(41)=1\*40=40**  
c. ***φ*(1055)=*φ*(5)\**φ*(211)=4\*210=840**  
d. ***φ*(8)=4**(1,3,5,7). De regel geldt nu niet omdat 8=2\*2\*2 en de factoren dus gelijk zijn.

**Opgave 3**  
a. *p*\**q* - 1 - (*p* - 1) - (*q*- 1) want er zijn *p -*1 veelvouden van *q* kleiner dan *pq* die niet ggd 1 hebben met *pq* en net zo *q -*1 veelvouden van *p*die wegvallen. Het getal *pq* zelf zorgt voor de -1 want dat telt zelf natuurlijk ook niet mee.

b. ***φ*(*p\*q*)=*p*\**q*-1-(*p*-1)-(*q*-1)=*p*\**q*-*p*-*q*+1)=(*p*-1)\*(*q*-1)=*φ*(*p*)\**φ*(*p*)**

**Opgave 4**a. 20 (getallen 1 t/m 25behalve de 5 vijfvouden.)  
b. 100 (getallen 1 t/m125 behalve de 25 vijfvouden.)  
c. 500 (getallen 1 t/m625 behalve de 125 vijfvouden.)  
d.Merk opdat ***pr/p* met *p* priem** gelijk is aan het aantal veelvouden van *p* kleiner dan ***pr***.  
Zo is het aantal veelvouden van 5 kleiner dan 53 de verzameling 0\*5,1\*5, ... 24\*5. De laatste, 25\*5 = 53. Er zijn dus 125 - 25 priemdelers omdat geen enkel ander getal een factor 5 bevat.   
Dus: ***φ*(*pr*)=*pr*-*pr/p= pr*-*pr-*1= (*p-*1)\**pr-*1**.

**Opgave 5**  
a. ***φ*(640)=*φ*(27)\**φ*(5)=(1\*26)\*4=64\*4=256**  
b. ***φ*(49000)=*φ*(23)\**φ*(53)\*(72)=(1\*22)\*(4\*52)\*(6\*71)=4\*100\*42=16800**  
c. ***φ*(245025)=*φ*(34)\**φ*(52)\**φ*(112)=(2\*33)\*(4\*51)\*(10\*111)=18\*20\*110=39600**  
  
**Opgave 6**  
a. ggd(7,640)=1, *φ*(640)= 256 (zie5a), dus mbv Euler: 73843=(7256)15\*73=115\*73=1\*343=343  
b. ggd(16,81)=1, *φ*(81)= 54, dus mbv Euler: 161033=(1654)19\*167=119\*167=1\*(162)3\*16=(13)3\*16=10\*16=79   
c. ggd(25,99)=1, *φ*(99)= 60, dus mbv Euler: 253000=(2660)50=1, dus geldt 25\*252999=1, dus is 252999 de inverse van 25 in **Z99** en we kunnen met Euclides of door gewoon even te rekenen vinden dat deze 4 is.

**Opgave 7**  
Als *p* een priemgetal is geldt ***φ*(*p*)=*p*-1** en **ggd(*a*,*p*)=1**. De stelling van Euler zegt dat voor alle gehele *a* met **ggd(*a*,*m*)=1** geldt, dat *a****φ*(*m*)=1** in **Z*m*.** In dit geval kun je *m*vervangen door *p* en volgt dan ***φ*(*m*)=*φ*(*p*)=*p*-1**. Dit invullen in de stelling van Euler levert de kleine stelling van Fermat.