**Antwoorden les 12: Algoritme van Euclides**

**Opgave 1**
a. Ja
b. Ja
c. Ja

**Opgave 2**
a. *v*=17 en *w*=31
b. *v*+*w*= 48. *a*+*m* = 528 = 48 \*11.
c. *v*- *w*= -14. *a*- *m* = -154 = -14 \* 11.

**Opgave 3**a. een deler van *a* en *m* is een deler van *a*- *m*.
Een deler van *a*- *m* en *m* is een deler van *a*- *m*- *m*= *a*- 2*m*.b. als *e* een grotere deler is van *a* - 2*m* en *m* dan *d*, dan is *e* een deler van *a*- 2*m*+ *m*= *a* - *mI*
en dus van *a* - *m*+ *m* = *a* en *m*. Maar dan is *d* niet de ggd.

**Opgave 4**
Als*d* een deler is van *a* en een deler is van *m*, dan is *d*ook een deler van *a*+*qm* en *a*-*qm*.
Als *d* de grootste gemene deler is van *a* en *m*,
Als *e* groter is dan d en *e*is de grootste gemene deler is van *a* + *qm* en *m* dan is *e*ook een deler van *a*, want *a*+ *qm* - *qm* = *a*.
Dan is *d* niet de ggd van *a*en*m*, want *e* is een grotere deler.
**Opgave 5**
a. ggd(6466, 5429) = ggd (5429,1037) = ggd (1037, 244) = ggd (244, 61) = ggd (61, 0) = 61.
b. ggd(5346, 897) = ggd(897, 861) = ggd (861, 36) = ggd (36, 33) = ggd (33,3) = ggd (3, 0) = 3
c. ggd (47,0) = 47

**Opgave 6**
a. In opgave 4 hebben we gezien dat
ggd(2164,153) = ggd(153, 2164-14\*153), dus geldt ook
ggd(2164,153) = ggd(153, 2164(mod153)).

b. 153 (mod2164) = 153 - 0\*2164 = 153, omdat 2164>153
153(mod2164) = 153, dus dan geldt
ggd(153,2164) = ggd(2164,153(mod2164)) = ggd(2164,153) en dat dat klopt zie je meteen.

**Opgave 7**
Vergelijk met opgave 6a. *a*- *qm* = *a* (mod*m*). In opgave 4 hebben we gezien dat
ggd(*a*,*m*)= ggd(*m*, *a* - *qm*), dus geldt ook
ggd(*a*,*m*)= ggd(*m*, *a*(mod*m*)).

b. *a*(mod*m*) =*a* als *m*>*a*, dus dan geldt
ggd(*a*,*m*) = ggd(*m*, *a* - *qm*) = ggd(*m*,*a*) en dat dat klopt zie je meteen.

**Opgave 8**
a. Op de onderste rij inde kolom onder *a*, op de daarboven onder*b*en op de rij daar weer boven onder *a* mod *b*.
b. 99.

**Opgave 9**

|  |  |  |  |
| --- | --- | --- | --- |
|   | *m* | *q* | *r* |
| 96 | 22 | 4 | 8 |
| 22 | 8 | 2 | 6 |
| 8 | 6 | 1 | 2 |
| 6 | 2 | 3 | 0 |
| 2 | 0 |   |   |

a. ggd(96, 22) = 2

|  |  |  |  |
| --- | --- | --- | --- |
| *a* | *m* | *q* | *r* |
| 484 | 576 | 0 | 484 |
| 576 | 484 | 1 | 92 |
| 484 | 92 | 5 | 24 |
| 92 | 24 | 3 | 20 |
| 24 | 20 | 1 | 4 |
| 20 | 4 | 5 | 0 |
| 4 | 0 |   |   |

b. ggd(484,576) = 4

|  |  |  |  |
| --- | --- | --- | --- |
| *a* | *m* | *q* | *r* |
| 47957 | 32395 | 1 | 15562 |
| 32395 | 15562 | 2 | 1271 |
| 15562 | 1271 | 12 | 310 |
| 1271 | 310 | 4 | 31 |
| 310 | 31 | 10 | 0 |
| 31 | 0 |   |   |

c. ggd(47957,32395) = 31

**Opgave 10**
Eerst moeten we controleren of (1234,437217) een geschikt getallenpaar is. De verschuiving +192731 is daarbij niet van belang.

|  |  |  |  |
| --- | --- | --- | --- |
| a | m | q | r |
| 1234 | 437217 | 0 | 1234 |
| 437217 | 1234 | 354 | 381 |
| 1234 | 381 | 3 | 91 |
| 381 | 91 | 4 | 17 |
| 91 | 17 | 5 | 6 |
| 17 | 6 | 2 | 5 |
| 6 | 5 | 1 | 1 |
| 5 | 1 | 5 | 0 |
| 1 | 0 |   |   |

De ggd(437217,1234)=1, dus het is een geschikt getallenpaar.
De versleuteling is nu:

We kunnen dus de cijfertekst 087 814 403 354 346 988 355 626 versturen.

**Opgave 11**De berekening is terug te vinden in [**bijgaande tabel**](http://www.e-klassen.nl/access/content/group/e-klas-project/gepubliceerd/wiskunde/Cryptografie/Html_nieuw/antwoorden/modulo468713.xls) en wordt hieronder toegelicht.
*E*(*x*) = (*x* + 398843) mod 468713
De versleutelde boodschap is 466 957 027 229 034 246 031 240.

We zetten hieronder welke berekeningen we loslaten op de eerste kolom. Door te slepen zetten we de berekening voort over de andere kolommen.
Eerst zetten we de getallen in een rekenblad .We moeten de codes voor de letters twee aan twee samenvoegen.
Dat kan in Excel door de functie 1000\* A1 + A2, met de 1e code in cel A1 en de 2ecode in cel A2.

Nu terugrekenen
*x* + 398843 = 466957 mod 468713 *is hetzelfde als*
*x* = 466957 - 398843 mod 468713 *is hetzelfde als x*= 68114
De laatste regel voert het rekenblad voor ons uit.
Nu moeten we het getal weer splitsen met de functie GEHEEL(A3/1000) in cel A4 en de functie A3 - 1000\*A4 in cel B4
Met de functie TEKEN(A4) in cel A5 vinden we de letter D.


**Antwoorden - Priemdeler**

**Opgave 1**
a) Waar
b) Niet waar
c) Waar
d) Niet waar
e) Niet waar
f) Waar
g) Waar

**Opgave 2**
a) Delers van 8: 1, 2, 4, 8. Dit zijn er 4.
Delers van 81: 1, 3, 9, 27, 81. Dit zijn er 5.
Delers van 49: 1, 7, 49 . Dit zijn er 3.
b) 8\*81\*49 heeft 4\*5\*3=60 delers.

**Opgave 3**2, namelijk 1 en zichzelf.

**Opgave 4**
2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

**Opgave 5**Hieronder laat de Zeef van Eratosthenes zien dat de priemgetallen kleiner dan 100 zijn:2, 3, 5, 7, 11, 13, 17, 19,23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 en 97.

**Opgave 6**
a) Omdat priemgetallen positief zijn en precies 2delers hebben. Het getal 1 heeft maar één deler.
b) Omdat ze niet door een ander getal dan 1 en zichzelf deelbaar zijn. Veelvouden van 1 streep je niet door (anders zou je alles doorstrepen). Dus kunnen ze niet doorgestreept worden voor ze omcirkeld worden.
c) Omdat die allemaal een deler hebben die groter is dan 1 en kleiner dan het getal zelf.

**Opgave 7**a) Samengesteld:91, 121, 231, priemgetallen: 41, 101, niet samengesteld en niet priem: 1.
b) 91**=**7\*13,121=112, 231=3\*7\*11

**Antwoorden - Grootste Gemene Deler**

**Opgave 1**
a. 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 60, 120.
b. 1, 2, 4, 7, 8, 14, 16, 28, 56, 112.
c. 1, 2, 4, 8.
d. 8.

**Opgave 2**
a. 18
b. 61
c. 47
d. a
e. Elk getal is een deler van 0, dus is er geen ggd(0,0).

**Antwoorden - (a div m) en (a mod m)**

**Opgave 1**
a. 3
b. 72
c. 13
d. -4

**Opgave 2**
a. 2
b. 8
c. 0
d. 6

**Opgave 3**a. 17 = 5\*(17div 5 +(17 mod 5) = 5\*3+2, klopt.
b. - 22 = 7\*(- 22 div 7)+ (- 22mod 7) = 7\*- 4 + 6, klopt ook.
c. *a*= *m*\**a* div *m* + *a* mod*m* = *m*\**a*div *m* + (*a* - *m*\*(*a* div *m*)) = *a*.

**Opgave 4**a) 15 cm
b) Omdat ze dezelfde rest na deling door 25 hebben.

**Opgave 5**a) 17mod5 =2= 32mod5, (32-17)mod5 =15mod5 = 0.
b) 22mod11 =0, 35mod11 = 3, (35-22)mod11 = 13mod11 ≠ 0.
c) *m* =13.

**Opgave 6**a) 20 cm.
b) 20 cm.
c) (240-190)mod25 = 0,(105-155)mod25 = 0.

**Opgave 7**a) 5 cm.
b) (240-190)mod25 = 0,dus weer 5 cm.
c) Van 25 keer 240 houd je niks over want 25\*240 is een 25-voud, dus houd je 7 keer 240 over en daarvan houd je 5 cm over.
d) Zie c).

**Opgave 8**a) 9 (som)
b) 6(product)
c) 17\*(335+773)mod7= 3\*(6+3)mod7 = 27mod7 = 6 (som en product)

**Opgave 9**Omdat 35 niet bestaat in **Z12**.

**Opgave 10**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| +  |  0 | 1 | 2 | 3 | 4 |  | \* | 0 | 1 | 2 | 3 | 4 |  |
| 0 | 0 | 1 | 2 | 3 | 4 |  | 0 | 0 | 0 | 0 | 0 | 0 |  |
| 1 | 1 | 2 | 3 | 4 | 0 |  | 1 | 0 | 1 | 2 | 3 | 4 |  |
| 2 | 2 | 3 | 4 | 0 | 1 |  | 2 | 0 | 2 | 4 | 1 | 3 |  |
| 3 | 3 | 4 | 0 | 1 | 2 |  | 3 | 0 | 3 | 1 | 4 | 2 |  |
| 4 | 4 | 0 | 1 | 2 | 3 |   | 4 | 0 | 4 | 3 | 2 | 1 |   |

**Opgave 11**a) 3
b) 6
c) 10
d) 8

**Opgave 12**a)
16+*x* = 7 in **Z23**(16+*x*)mod23 = 7
16+*x* - 23\**k* = 7
16+x - 23\*k = 7
9+*x* = 23*k*, dus *x* = 14 en *k* = 1

b)
756+*x* = 341 in **Z1278**
(756+*x*)mod1278= 341
756+*x* - 1278\**k* = 341
415+*x* = 1278*k*, dus *x* = 863 en *k* = 1

**Opgave 13**a) (12\*6)mod10**= 72mod10 = 2,**(7\*6)mod10**=** 42mod10 = 2 maar 12mod10 ≠7mod10
b) Het verschil tussen 12 en 7 is 5. Wanneer je deze getallen met een even getal vermenigvuldigd wordt het verschil een veelvoud van 10.
c) Als *m* geen gemeenschappelijke deler heeft met *a*, *b* of *c* geldt wel
dat *a* = *b* als *a\*c* = *b\*c*.