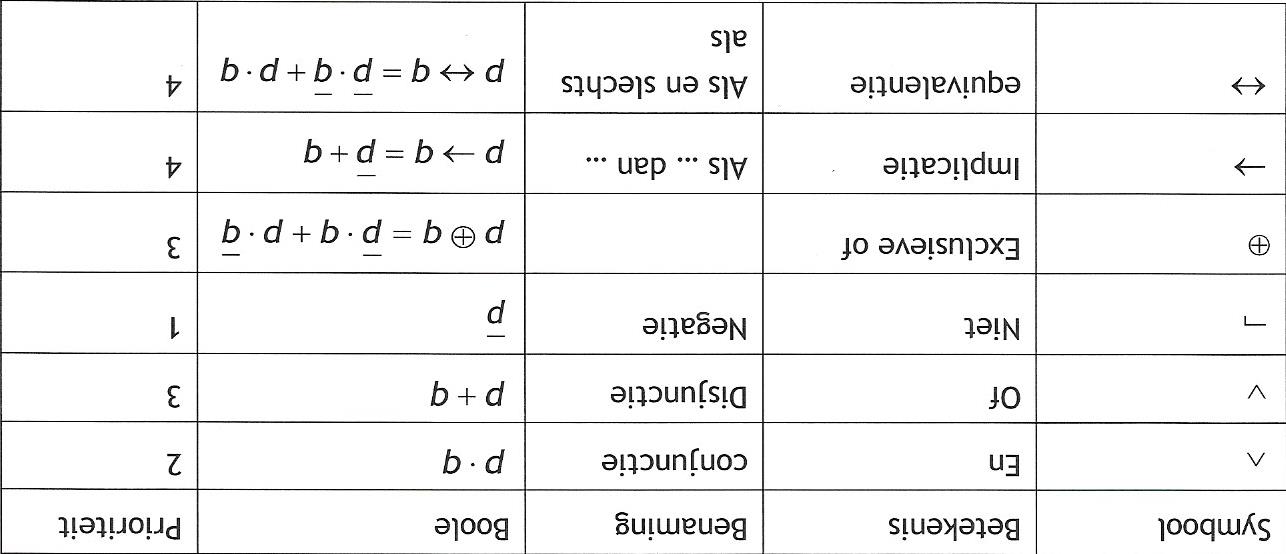
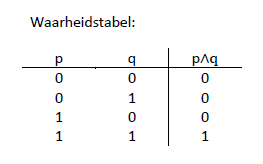


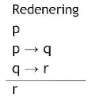
Als er gevraagd word om te kijken in welke waarde gelijk is aan 0 kan je kijken in je VK waar er geen kruisjes staan.

Als je een som van termen met een component streep boven hebt dan kan je dit ook in je VK zetten maar ipv met kruisjes met 0 en zodat je weet dit zijn het niet en dan degene zonder een 0 zijn waar je normaal gezien een kruisje zou zetten.



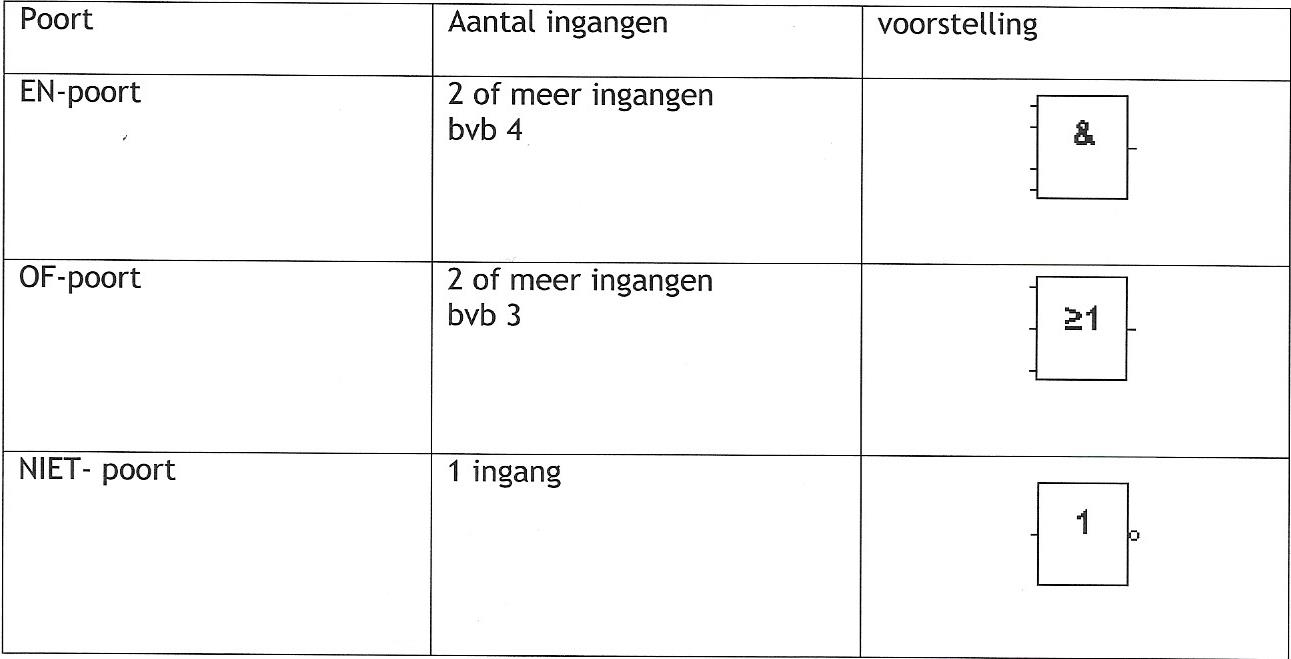
Voorbeeld van een waarheidstabel

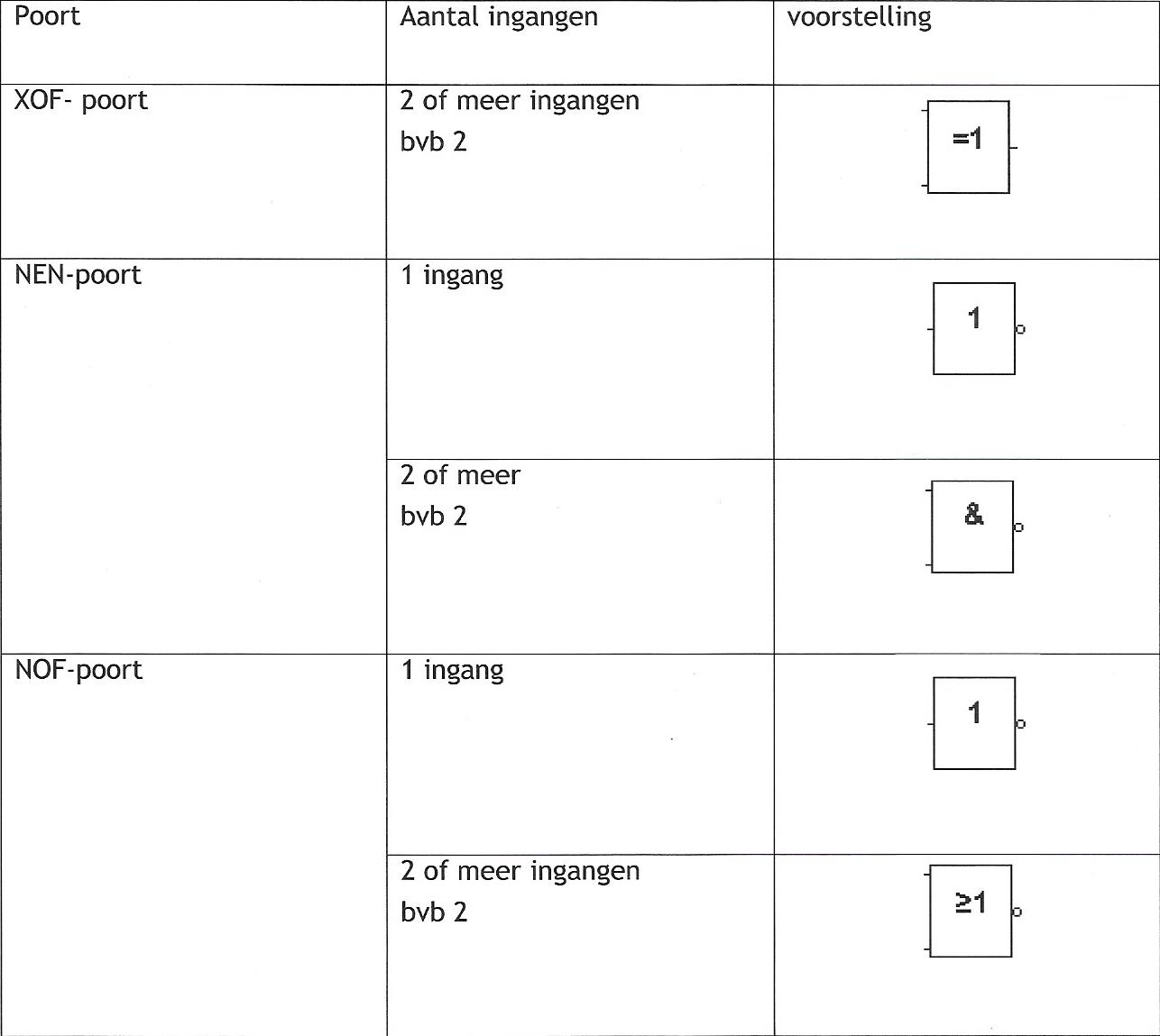


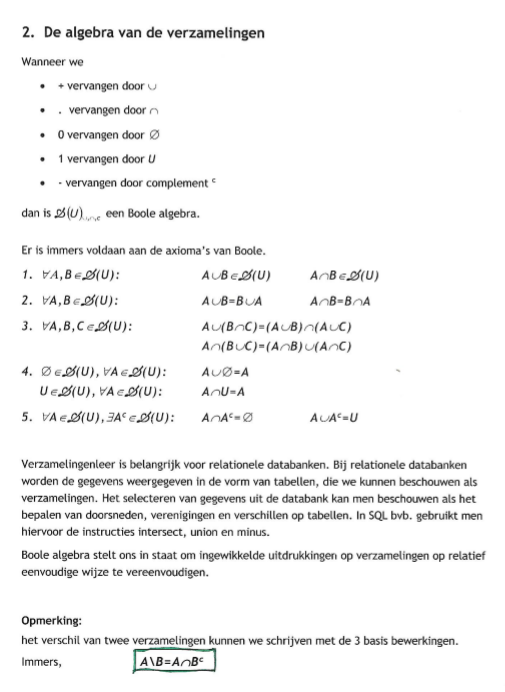


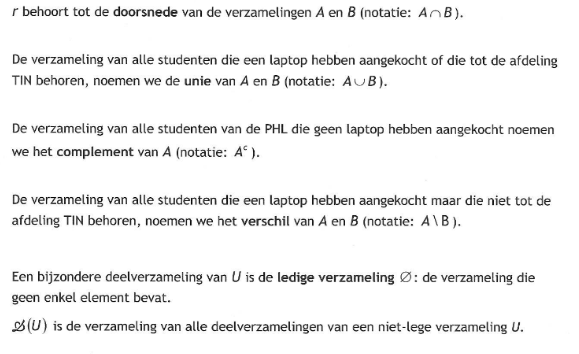
Als je dit krijgt of je dit gemaakt het dan moet je deze formule op één lijn gaan schijven. Dit doen je door gebruik te maken van en, of en dan. Dus als p en p => q en q=>r dan r .

Dus: P ^ (P => q) ^ (P => r) = > r









Hoofdstuk 2: symmetrische cryptosystemen

* 2 standaartechnieken:
  + ~~Transpositie: het verwisselen van de letters van het bericht op een vooraf afgesproken manier~~
  + Substitutie: de letters vervangen door andere letters op een vooraf afgesproken manier

1. De ceasarrotatie
   1. Methode

Voorbeeld: de letter “m” wordt verzonden en de sleutel k=20

Coderen:

* Stap 1: m correspondeert met de waarde 12
* Stap 2: 12 + k = 12 + 30 = 32
* Stap 3: 32 >= 26 => 32(mod26) = 6 (immers 32/26 = 1 rest 6)
* Stap 4: hiermee correspondeert met de letter g.

Decoderen:

* Stap 1: g correspondeert met de waarde 6
* Stap 2: 6-20(k) = -14
* Stap 3: -14<0 => -14(mod 26) = -14 + 26 = 12
* Stap 4: hiermee correspondeert de letter m

1. Substitutiemethode mbv de bitoperator XOR

Coderen:

* Stap 1: aan elk karakter uit de boodschap een getalwaarde toekennen bv. De ascii-code
* Stap 2: XOR-operator gebruiken in combinatie met de gekozen sleutel.

Voorbeeld: we kiezen als sleutel het karakter R. de boodschap is de letter a. Wat krijgt de ontvanger?

ANSI (ASCII)

Coderen hexadecimaal Binair

Boodschap a 6 1 0110 0001  
Sleutel R 52 0101 0010

Gecodeerde  
boodschap 0011 0011

De ontvanger krijgt het getal 3 toegestuurd

Decoderen:

* Stap 1: aan elk karakter uit de boodschap een getalwaarde toekennen op dezelfde manier als gebeurd is bij het coderen.
* Stap 2: XOR-operator gebruiken in combinatie met de gekozen sleutel.

Voorbeeld: de ontvanger boodschap is het getal 3, de sleutel is het karakter R. Welk karakter is er verstuurd?

decoderen hexadecimaal Binair

Boodschap 3 3 3 0011 0011  
Sleutel R 5 2 0101 0010

Gedecodeerde  
boodschap 0011 0011

Het verzonden karakter is a.

1. Blokcijfersystemen

Voorbeeld:

**Coderen:** boodschap INFORMATICA, sleutel: TIN

I N F O R M A T I C A

T I N T I N T I N T I

Omzetten naar de bijhorende numerieke waarde

8 13 5 14 17 12 0 19 8 2 0

19 8 13 19 8 13 19 8 13 19 8

Optellen

27 21 18 33 25 25 19 27 21 21 8

Modulo 26 rekenen

1 21 18 7 25 25 19 1 21 21 8

Omzetten naar tekst geeft

B V S H Z Z T B V V I

**Decoderen**

B V S H Z Z T B V V I

T I N T I N T I N T I

Omzetten naar de bijhorden numerieke waarde

1 21 18 7 25 25 19 1 21 21 8

19 8 13 19 8 13 19 8 13 19 8

Aftrekken

-18 13 5 12 17 12 0 -7 8 2 0

Zorgen dat de uitkomst >=0 is door modulo 26 te bereken

8 13 5 14 17 12 0 19 8 2 0

Omzetten naar tekst geeft

I N F O R M A T I C A

3.2 Blokcijfersystemen op basis van XOR-methode

ANSI (ASCII)

Coderen hexadecimaal Binair

Boodschap een 6 5 6 5 6 E 0110 0101 0110 0101 0110 1110  
Sleutel Tin 5 4 6 9 6 E 0101 0100 0110 1001 0110 1110

Gecodeerde  
boodschap 0011 0001 0000 1100 0000 0000

ANSI (ASCII)

Decoderen hexadecimaal Binair

Boodschap 3 1 0 C 0 0 0011 0001 0000 1100 0000 0000  
Sleutel Tin 5 4 6 9 6 E 0101 0100 0110 1001 0110 1110

Gedecodeerde  
boodschap 0110 0101 0110 0101 0110 1110

1. Enkele nadelen symmetrische cyptrosystemen

Zender en ontvanger moeten een sleutel afspreken. Hoe kan je op een beveiligde manier deze sleutel verzenden?

In een netwerk zal je veel meer sleutels moeten creëren dan er mensen op het netwerk zijn.

Vraag: a) Hoeveel sleutels heb je nodig in een netwerk van 5 personen? 10  
 b) Hoeveel sleutels heb je nodig in een netwerk van 50 personen?

N . (N -1) /2 => 50 . (50 -1) / 2 = 1225

Hoofdstuk 4: asymetrische cyptrosystemen

Uitgewerkt voorbeeld RSA

An stuurt een boodschap naar Piet.

**Coderen**

* An zet de boodschap wiskunde is leuk in ascii-code. Dit geeft

119  105  115  107 117 110  100  101 32  105  115 32  108 101 117 107

* Hoe kan An dit bericht vercijferen? Daarvoor heeft zij de openbare sleutel van piet nodig deze bestaat uit 2 getallen e = 989 en m=1073
* An kan de boodschap vercijferen door op elk karakter de volgende bewerking uit te voeren: Me (mod m) = M989(mod1073) = 282

De eerste letter geeft 119989 (mod 1073) = 282

* Wanneer An dit op elk getal toepast, bekomt An het volgende

282 549 28 342 117 36 121 1047 311 549 28 311 826 1047 117 342

**Decoderen**

* Piet ontvangt volgende boodschap van An
* 282 549 28 342 117 36 121 1047 311 549 28 311 826 1047 117 342
* Zijn privé sleutel bestaat uit 2 getallen d=53 en m=1073.
* Piet kan de geheime boodschap ontcijferen door op elk karakter de volgende bewerking uit te voeren: S(M)d (mod m) = S(M)53(mod1073)

De eerste letter geeft 28253 (mod 1073) = 119

* Wanneer Piet dit op elk getal toepast, bekomt Piet het volgende

119  105  115  107 117 110  100  101 32  105  115 32  108 101 117 107

* Dit stellen de ASCII-codes voor van de boodschap: Wiskunde is leuk

Voorbeeld: neem P=13 en q=17 => m = p . q = 221

Wanneer nu

* M=123 dan blijkt M = M13 = M25 = … modulo 221
* M=21 dan blijkt M = M5 = M9 = … modulo 221
* M=91 dan blijkt M = M17 = M33 = … modulo 221

In het bijzonder is dus M = MK+1 = M2K+1 = … modulo m.

Het merkwaardige is nu – en dat volgt uit stellingen van Fermat(1601-1665) en Euler(1707-1783) – dat k altijd een deler is van K = (p-1) . (q-1) zodat voor elke M geldt:

M = MK+1 = M2K+1 = M 3K+1 = …. Modulo m

**Vercijferen & handteken:**

BV. Geg volgende sleutels

|  |  |  |  |
| --- | --- | --- | --- |
|  | m | e | d |
| ELIEN | 7261 | 4253 |  |
| SANDER | 3959 | 2005 |  |

Sleutels controleren (voorwaarde 1)

Eumath:

>factor(7261)

-> 53, 137

>gcdext(53,137)

-> 1 (1 gemene deler -> dan is de sleutel correct)

(voorwaarde 2)

* P= 53 / g=137

e < K (ELIEN) K = (p – 1) . (q – 1) = 52 . 136 = 7072

* 4253 < 7072

d bereken:

.{ggd,d,j}:= gcdext( e, K)

->1

>d

->2165 = d(ELIEN)

Als d < 0 dan moet je er K bij optellen.

Eumath:

Ascii-waardes opvragen:   
>Ascii(“A”) = 65  
Karakter opvragen:  
>Char(65) = A  
Priemgetallen opvragen:  
>Primes(n) = geeft alle priemgetallen tot n

Coderen en Decoderen (e, d en m zijn van de ontvanger):

& mod ( ascii-waarde vd letter ^ e , m) = codering

& mod (codering ^ d , m) = ascii-waarde

Handtekenen en Dehandtekenen(e, d, en m zijn van de verzender):

& mod ( ascii-waarde ^ d , m ) = gehandtekende boodschap

& mod ( geh. Boodschap ^ e , m) = ascii – waarde

Voorbeelden van Euler files

Bepalen openbare en prive sleutel

//Bepaal p en q

//bijvoorbeeld: getal:=10000

//v:=primes(getal)

//len:=length(v)

//1229 //len

//p:=v[intrandom(1229)], q:=v[inrandom(1229)]

//6199 //p

//1571 //q

---------------------------

//Bepaal m, K, kies een getal e dat kleiner is dan K, gcd(e,K) moet 1 zijn

//m:=p\*q //=9730860

//K:=(p-1)\*(q-1) //=9730860

//e:=997331

//gcd(e,K) //=1

---------------------------

//Bepaal d

//{ggd,d,j}:=gcdext(e,K); ggd, d, j

//1 //ggd

//-4492009 //d

//460393 //j

//Wanneer d negatief is (zoals hier het geval is)

//Dan doe je d+K om hem positief te maken

//d:=d+K //=5238851

----------------------------

//Openbare sleutel e=997331 en m=9738629

//Privésleutel d=5238851 en m=9738629

Codeer en Deconderen met RSA

//Coderen en Decoderen met RSA

//Ontvanger gebruikt privésleutel

//bijvoorbeeld e=2087 m=7597

-----------------------------

//stap 1

//Bepalen van de privésleutel

//factor(m)

//[71, 107]

-----------------------------

//stap 2

//Bepalen van K

//p:=71; q:=107; K:=(p-1)\*(q-1)

//7420

-----------------------------

//stap 3

//Bepalen van ggd, d en j

//{ggd, d, j}:=gcdext(e, K); ggd, d, j

//1 //ggd

//1863 //d

//-524 //j

-----------------------------

//Coderen

//modRek(string, e, m)

-----------------------------

//Decoderen

//modRek(string, d, m)

-----------------------------

-----------------------------

//Volledige uitwerking

//cijferTekst:=zetOmAscii("string")

//codeer:=modRek(cijferTekst, e, m)

//Bepalen van de privésleutel (zie stap1, stap 2, stap 3)

//decodeer:=modRek(codeer, d, m)

//boodschap:=zetOmTekst(decodeer)

-----------------------------

-----------------------------

//Om na te gaan of een boodschap van 'iemand' komt

//Gebruik de openbare sleutel (e) van 'iemand'

//nagaan:=modRek(boodschap, e, m)

//Als het resultaat getallen groter of gelijk aan 0 en kleiner of gelijk aan 255 zijn

//Dan is de boodschap van 'iemand', anders niet

ggd

function ggd(get1,get2)

rest:=get1;

if get1<get2

then get1:=get2; get2:=rest;

endif

repeat while (rest!=0)

rest:=mod(get1,get2);

quotient:=floor(get1/get2);

get1:=get2;

get2:=rest;

end;

return get1;

endfunction

//genereer een getal groter dan 100, kleiner dan 500 (101-499)

//get1:=intrandom(399)+100, get2:=intrandom(399)+100

Modulo rekenen

function modRek(v, exp, m)

//coderen//v = vector met asciiwaarden, exp = e, m = m

//decoderen//v = vector met gecodeerde waaren, exp = d, m = m

Mexp::exp;

Mm::m;

vuit:=[];

len:=length(v);

for i=1 to len step 1;

hulp = v[i];

Mhulp::hulp;

vuit:=vuit|mxmget(&mod(Mhulp^Mexp,Mm));

end;

return vuit;

endfunction

Blok verleuteling met xor methode

function blokXorCodeer(v, sleutel)

len:=length(v);

boodschap:=[];

sl:=[0,0,0];

for i=1 to 3 step 1 sl[i]:=ascii(substring(sleutel,i,i));

end;

for i=1 to len step 1

if mod(i,3)==3 then j:=1;

elseif mod(i,3)==2 then j:=2; else j:=3; endif;

hulp:=bitxor(sl[j],v[i]);

boodschap:=boodschap|hulp;

end;

return boodschap;

endfunction

codeer substitutie methode

function codeerSub(tekst, sleutel) ...

len:=strlen(tekst);

code:=""; //lege string aanmaken. Hierin komt de gecodeerde boodschap

for i=1 to len step 1;

kar:=substring(tekst,i,i); //tekst karakter per karakter opvragen

numkar:=ascii(kar); //asciiwaarde van karakter opvragen

numcod:=numkar+sleutel;

num:=mod(numcod,256); //modulo 256 rekenen

codkar:=char(num); //asciiwaarde omzetten naar een karakter

code=code|codkar; //gecodeerde letter toevoegen aan de reeds gecodeerde tekst

end;

return code

endfunction

decodeer substitutie methode

function decodeerSub(tekst, sleutel) ...

len:=strlen(tekst); //lengte van de tekst opvragen

code:=""; //lege string aanmaken, hierin komt de gecodeerde boodschap

for i=1 to len step 1;

kar:=substring(tekst,i,i); //tekst karakter per karakter opvragen

numkar:=ascii(kar); //ascii waarde van karakter opvragen

numcod:=numkar-sleutel;

num:=mod(numcod,256); //modulo 256 rekenen

codkar:=char(num); //asciiwaarden omzetten naar een karakter

code=code|codkar; //gecodeerde letter toevoegen aan de reeds gedecodeerde tekst

end;

return code

endfunction

comment

Coderen van een boodschap met XORmethode

endcomment

function codeerXOR(tekst, sleutel)

## Coderen van een boodschap met XORmethode

len:=strlen(tekst); //lengte van de tekst opvragen

code:=""; //hierin komt gecodeerde boodschap

numsleutel:=ascii(sleutel); //sleutel omzetten naar een numerieke waarde

for i=1 to len step 1;

kar:=substring(tekst,i,i); //tekst van karakter per karakter opvragen

numkar:=ascii(kar) //asciiwaarde van karakter opvragen

numcod:=bitxor(numkar,numsleutel);

codkar:=char(numcod); //asciiwaarde omzetten naar karakter

code=code|codkar;//gecodeerde letter samenvoegen met reeds gecodeerde tekst

end;

return code

endfunction

comment

Bewerkingen op tekst

strlen(tekst) //lengte van een tekst

substring(tekst, i, j) //deel van een tekst nemen van positie i tot en met positie j (men begint te tellen vanaf 1)

ascii(letter) //asciiwaarde van een letter

char(x) //bijhorend karakter bij gegeven asciiwaarde x

tekst1|tekst2 //2 teksten aan elkaar koppelen

bitxor(x,y) //XOR-operator op 2 gehele getallen x en y

----------------------

Werken met priemgetallen

primes(n) //geeft alle priemgetallen tot aan n

isprime(n) //is 1 als n een priemgetal is, 0 als n geen priemgetal is

mod(m,n) //berekent m modulo n

gcd(x, y) //berkent grootste gemene deler van x en y

gcdext(x, y) //berekent naast de grootste gemene deler g van x en y ook de waarden a en b zodat g=a\*x+b\*y

factor(x) //schrijft een getal x als een product van priemgetallen

----------------------

Maxima

&next\_prime(n) //is het eerstvolgende priemgetal dat groter is dan n

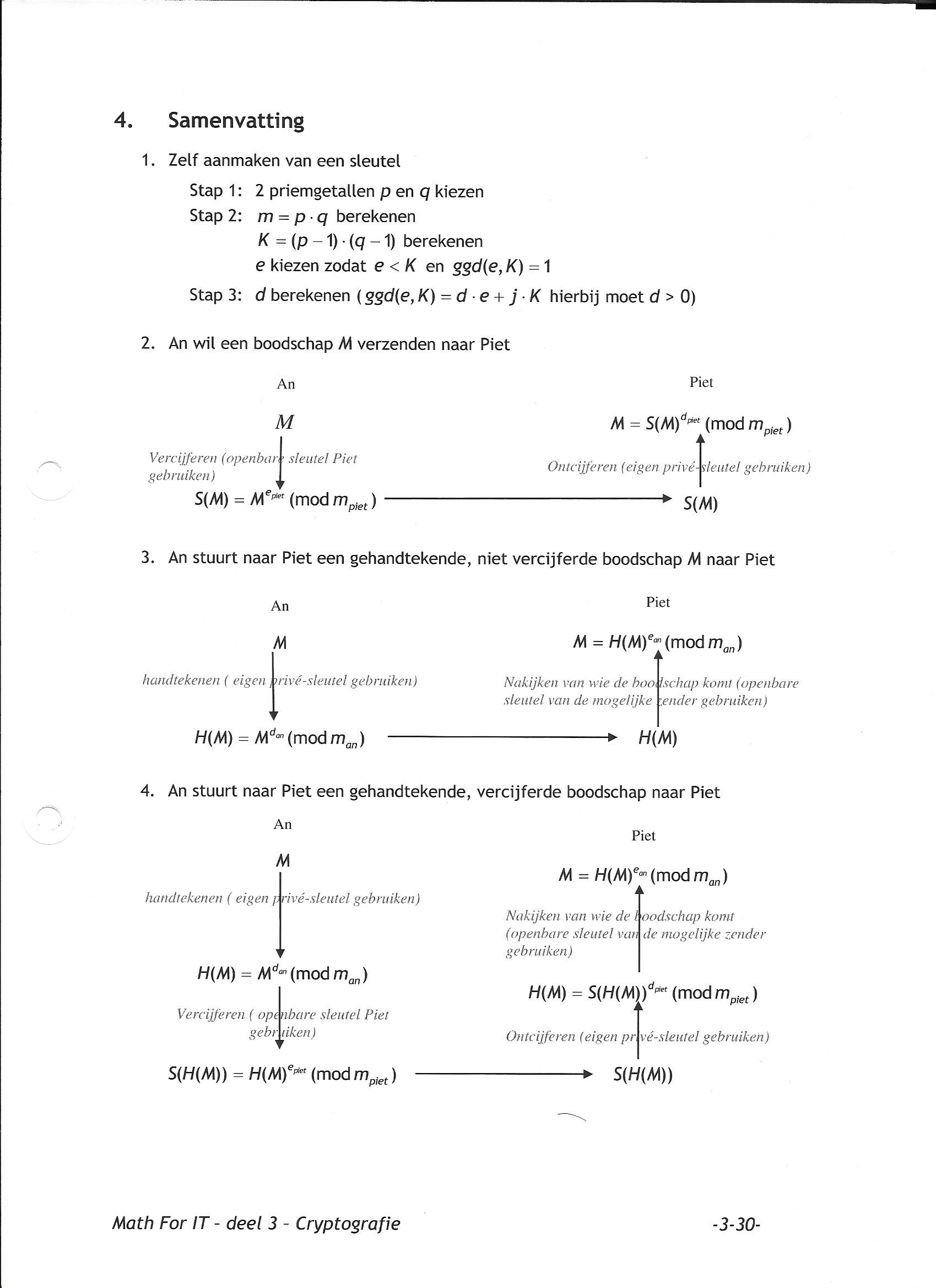
&prev\_prime(n) //het grootste priemgetal dat kleiner is dan n

&mod(m,n) //m modulo n

&gcd(a,b) //berekent de grootste gemene deler van a en b

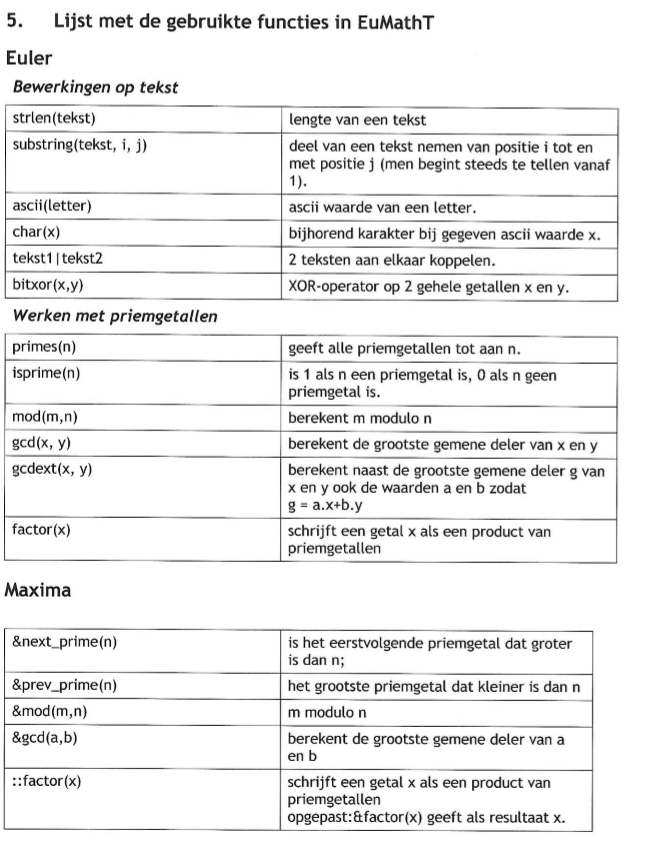
::factor(x) //schrijf een getal x als een product van priemgetallen

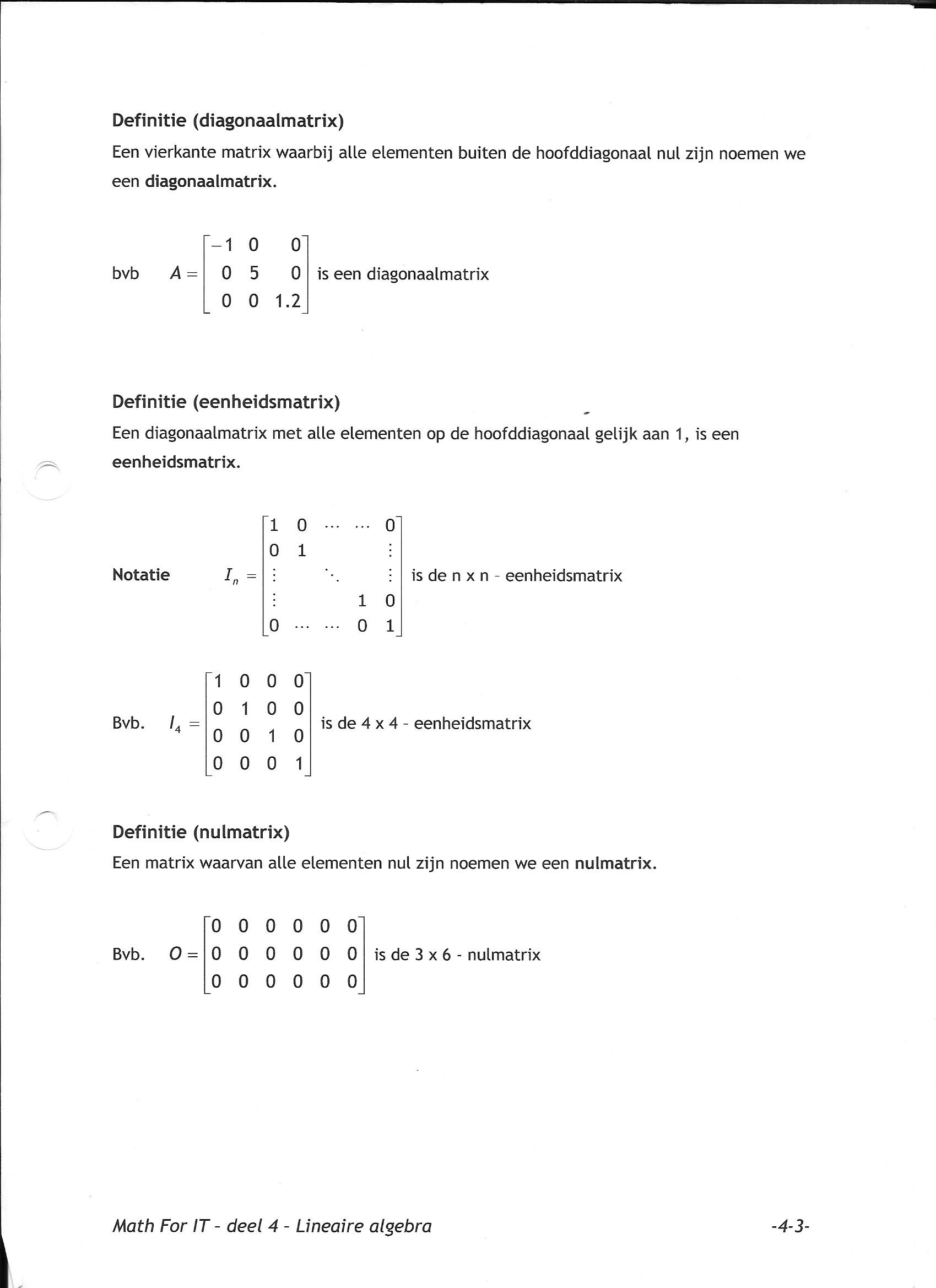
Endcomment



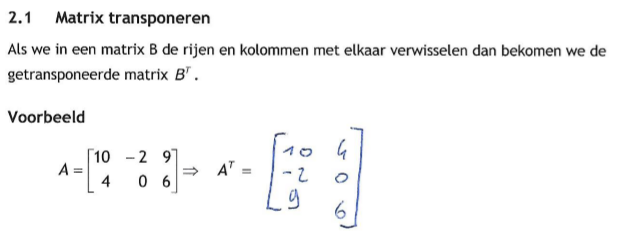
Als d kleiner is dan 0 moet je er K bij optellen

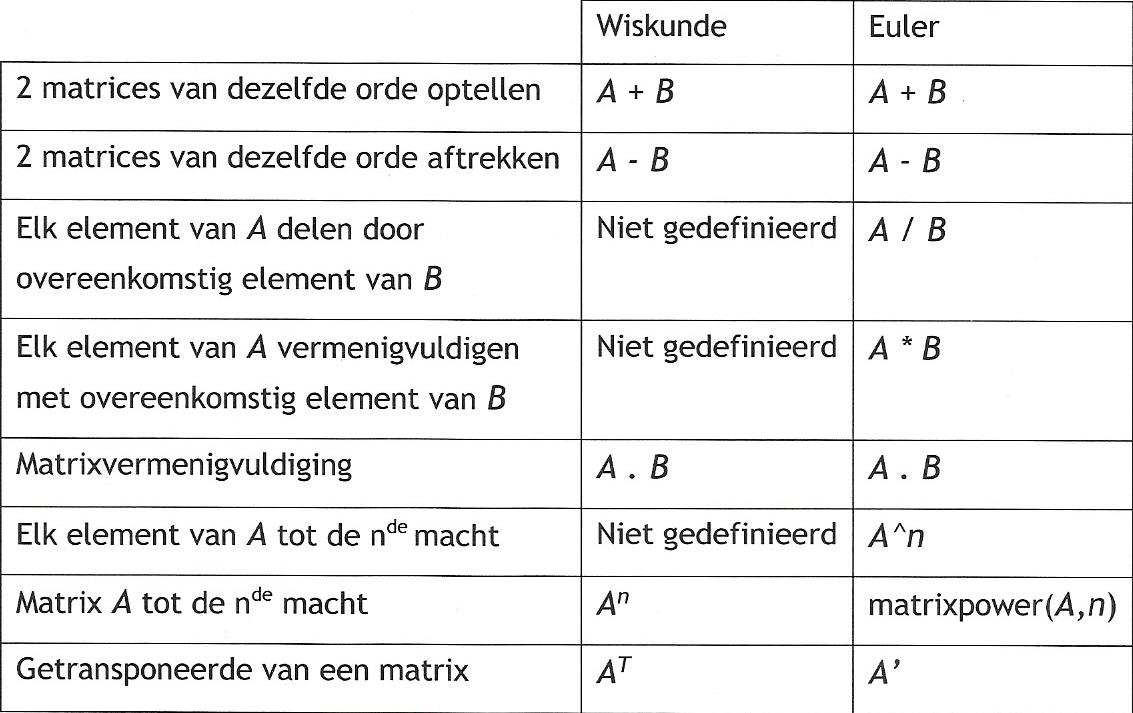
De numerieke waarde M moet kleiner zijn dan m anders werkt dit niet



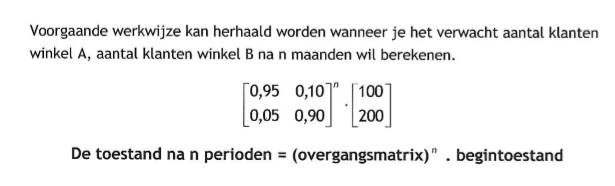


Let op : 3 X 6 matrix is dus 3 getallen naar beneden en 6 getallen naar rechts





Overgangsmatrix

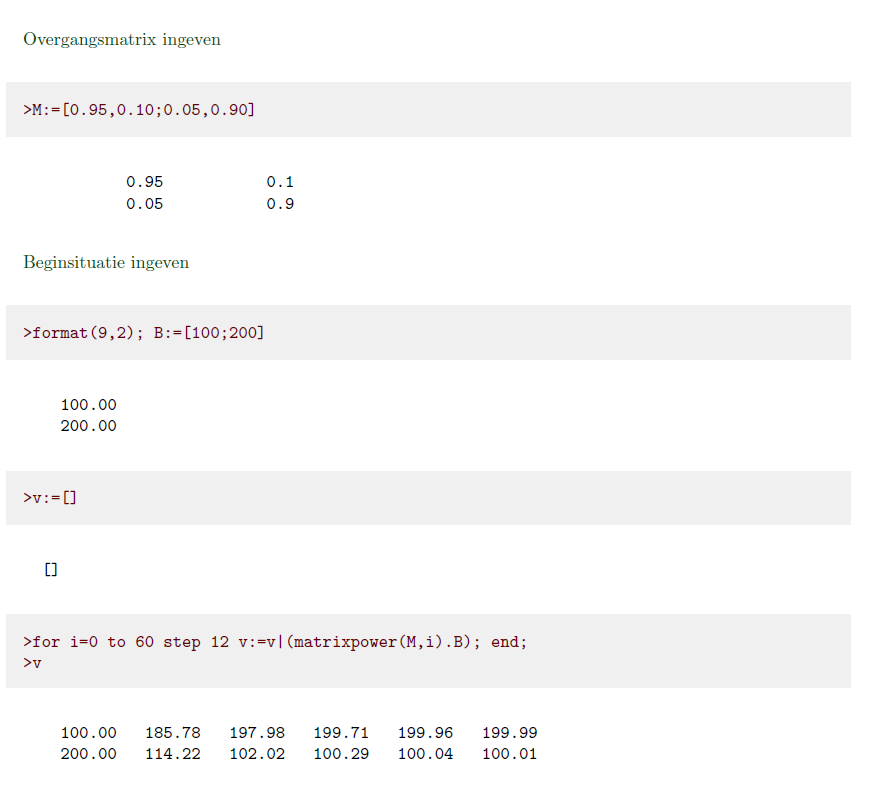


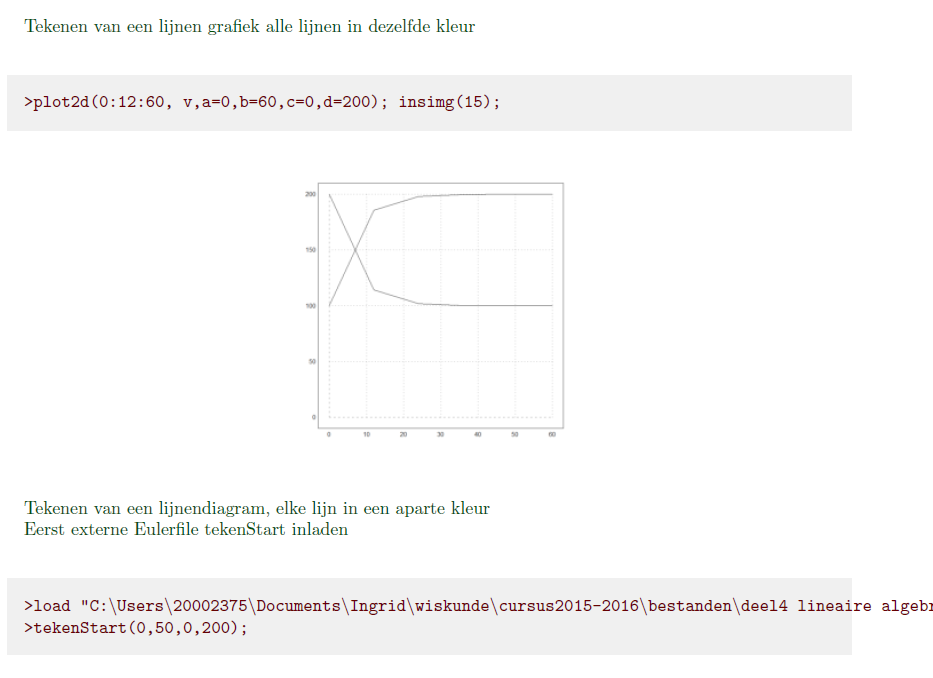
De som van de overgangsmatrix kolom moet altijd 1 zijn.

Als je dit in euler wilt doen matrixpower(M,n).B

M is hier de overgangsmatrix en B is de begintoestand

VB in euler



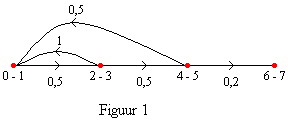




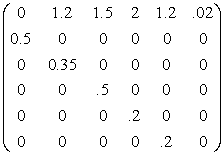
Populatie matrix of Lesiematrix

Als je het hebt over overlevings kansen of jongen of ies anders dan heb je het over een lesiematrix.

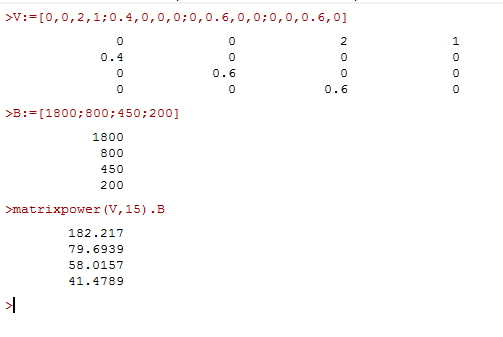
Je moet eerst een graaf maken



En daarna een matrix maken. De eerste rij zet je de jongen die een bepaalde groep maakt en daarna zet je de overlevingskansen in.(andere getallen van beide tekeningen)



Je kan dit daarna in euler bereken voor een paar jaren.



Let op dat er soms gevraagd word achter een periode die je niet kan bereken. Deze moet je dan niet invullen.

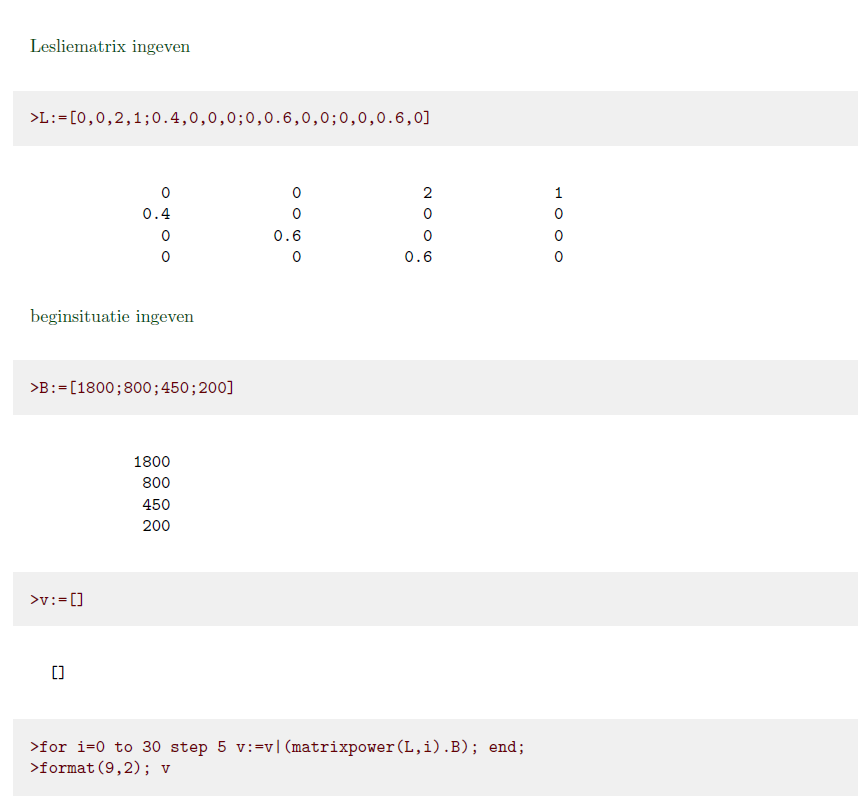
Het kan ook soms zijn dat er gevraagd word achter 3 jaar later terwijl de periode’s één maand is dus dan moet je tot de 36 ste doen ipv 3 de.

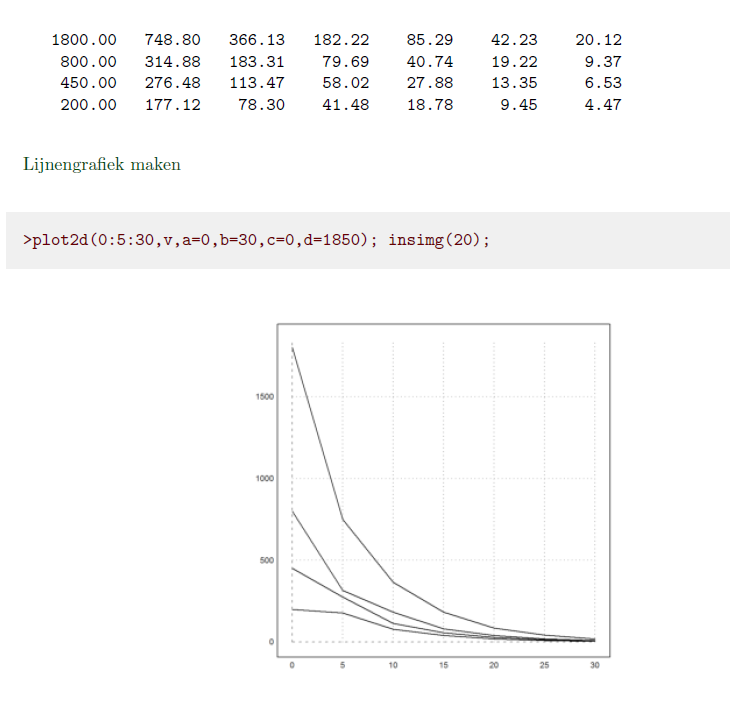
Als er gevraagd word wat betekent dit getal in de matrix kan dit zijn voor een overlevingscijfer of een aantal kinderen.

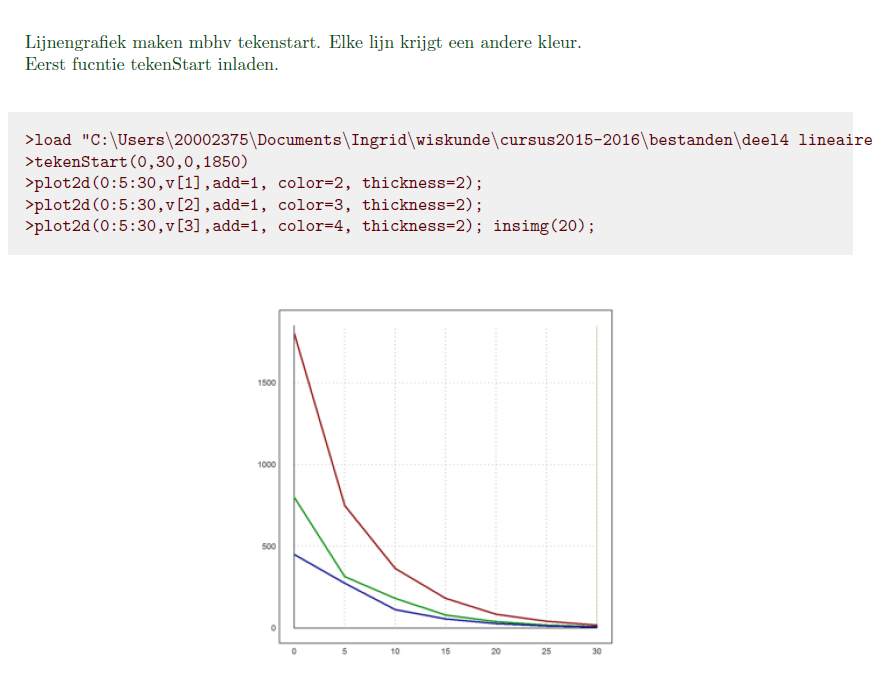
Aantal kinderen : het gemiddeld aantal jongen dat één iets voortbrengt op één periode.

Overlevingscijfer : de gemiddelde kans dat één iets nog leeft na één periode

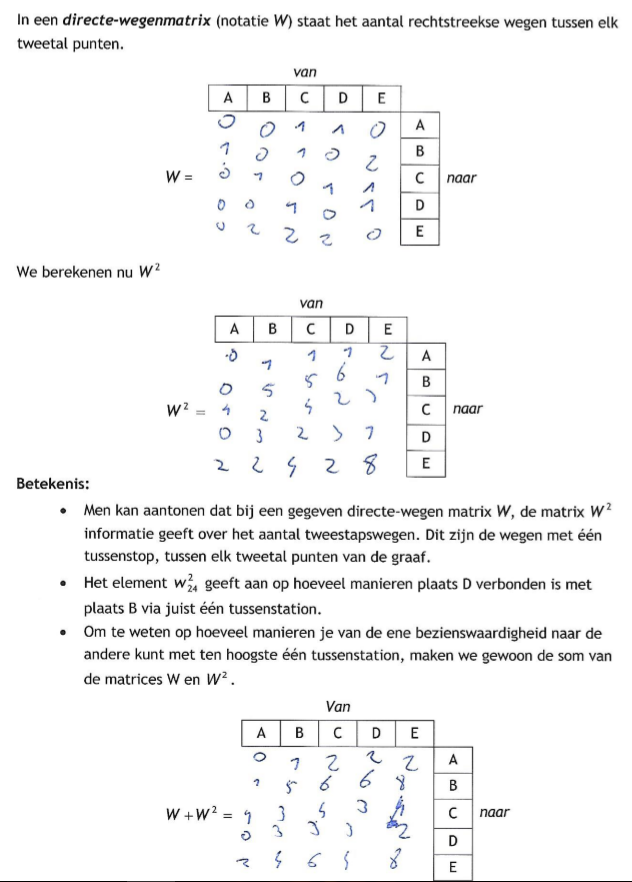
VB in euler







Verbindingen matrix



Rechtstreeks => W

Juist 1 tussenstation => W^2

Hoogstens 1 tussenstation => W+>^2

Juist 2 Tussenstations => W^3

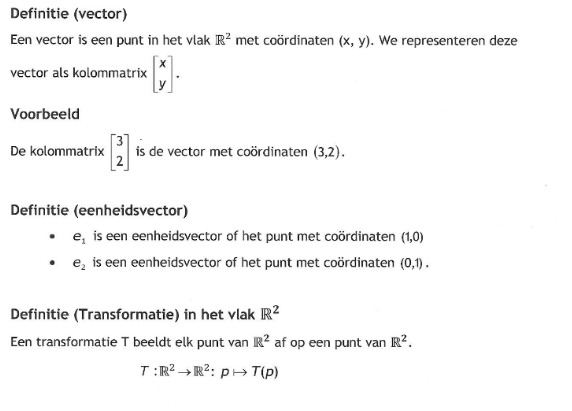
1 of twee tussenstation => W^2+W^3

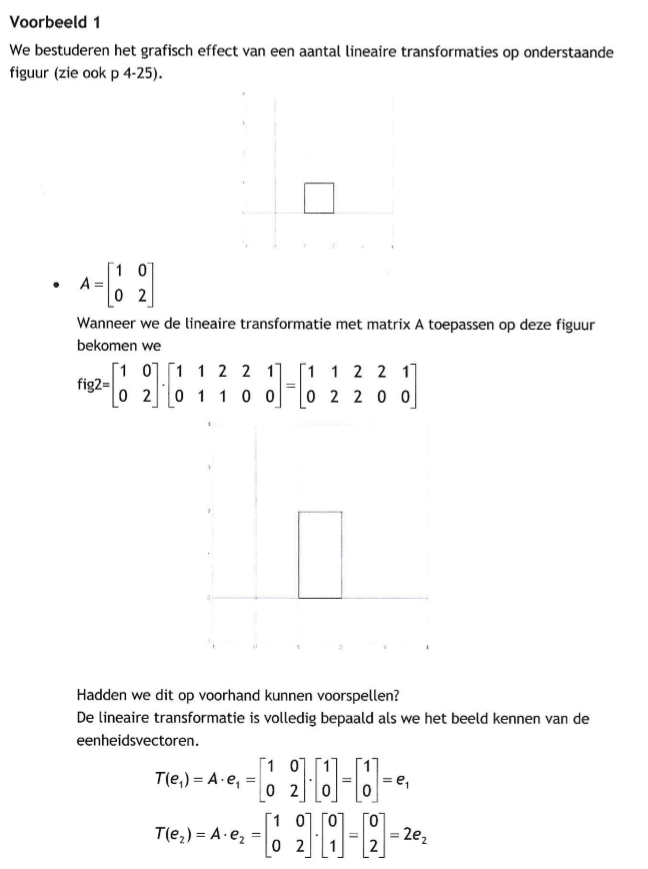
Code matrices

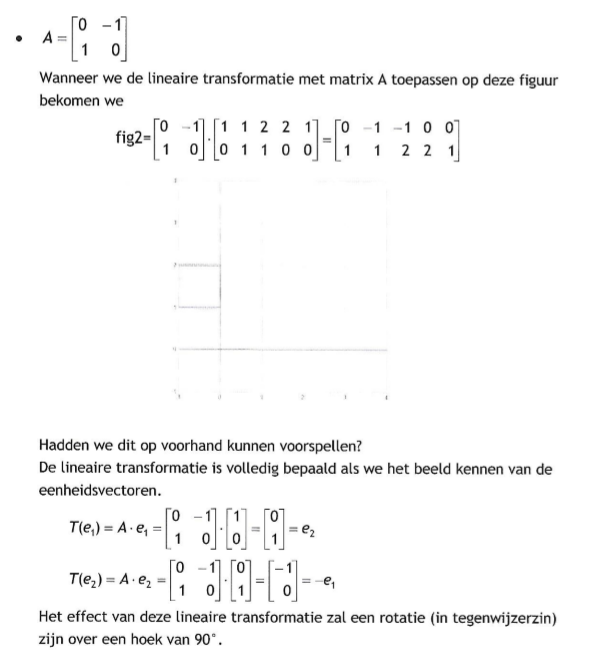
Code matrices worden vooral gebruikt voor het versleutelen van een boodschap met een sleutel dat je ook in een matrix stopt en die boodschap steek je dan ook in een matrix en deze doe je dan maal elkaar.

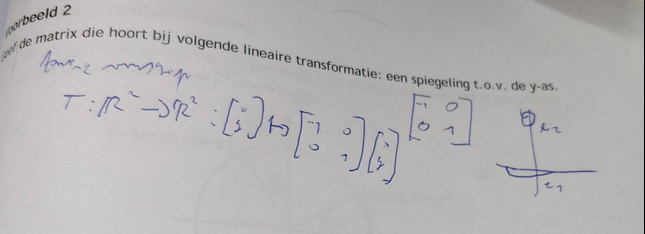
Dit is eigenlijk het zelfde als elke andere matrix berekening alleen hier staat de uitkomst van je matrix voor ascci waardes ipv andere getallen of posities.

2D computergrafieken

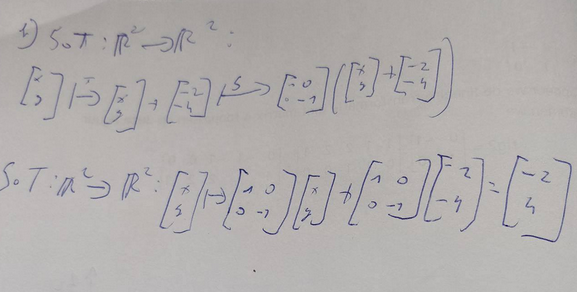


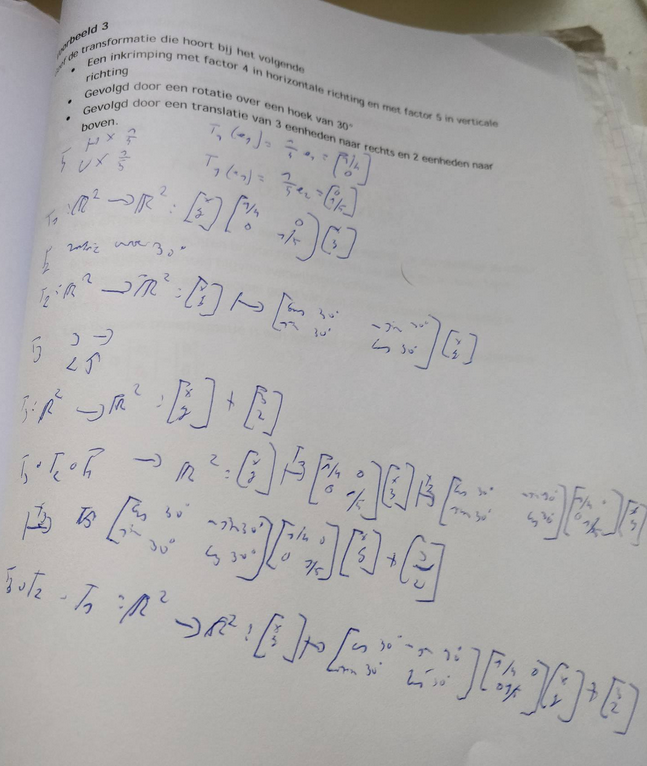


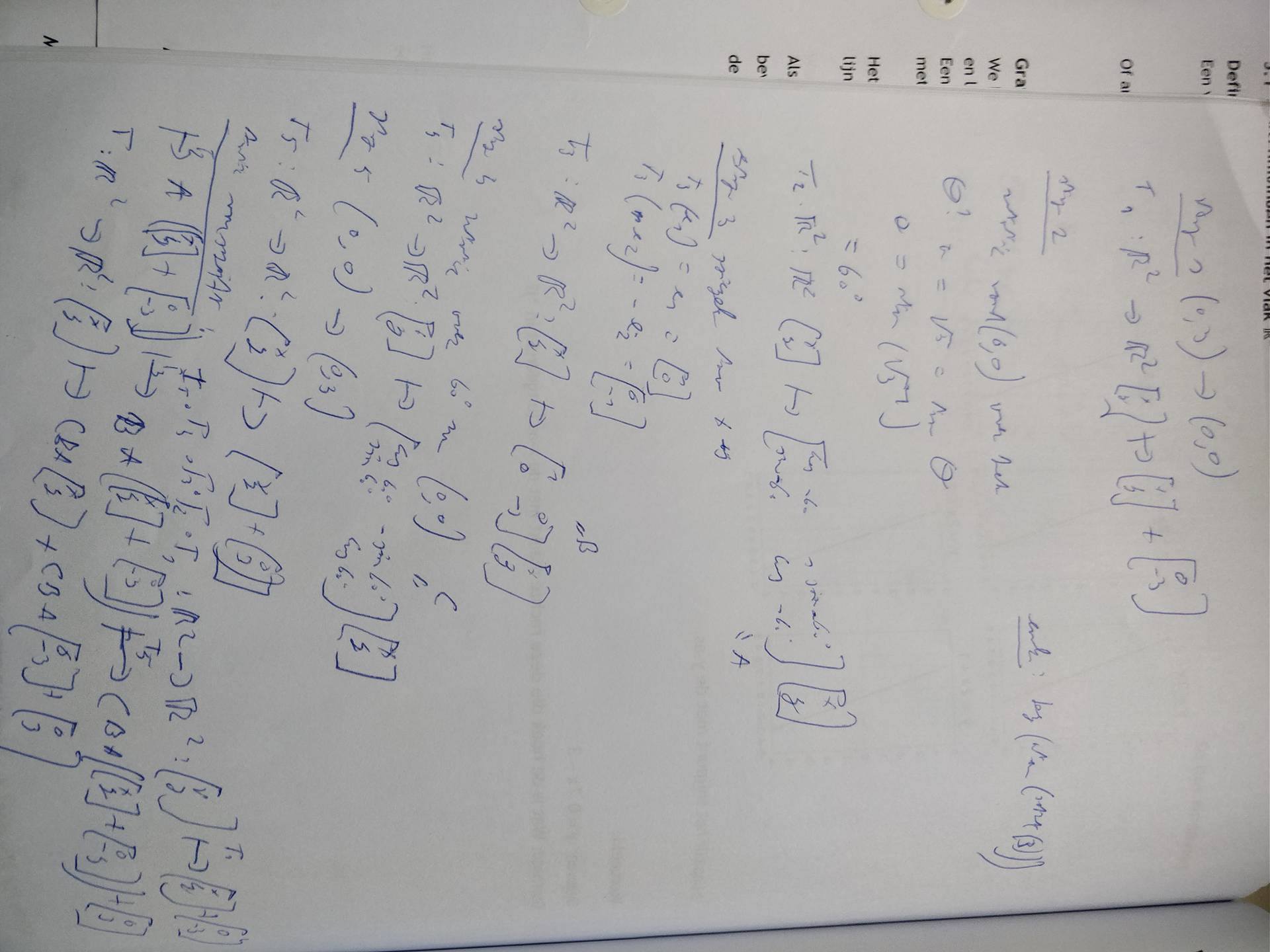


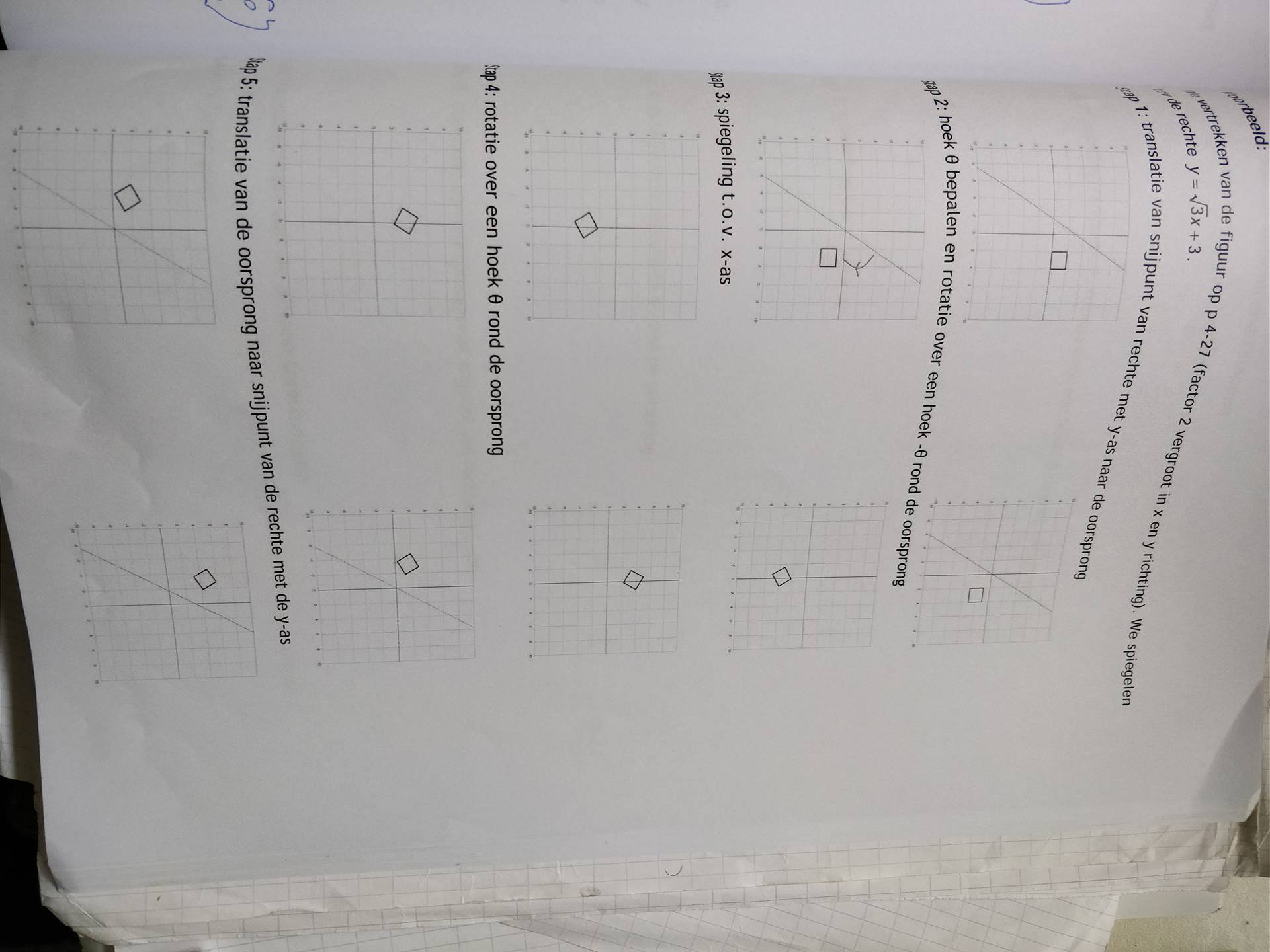






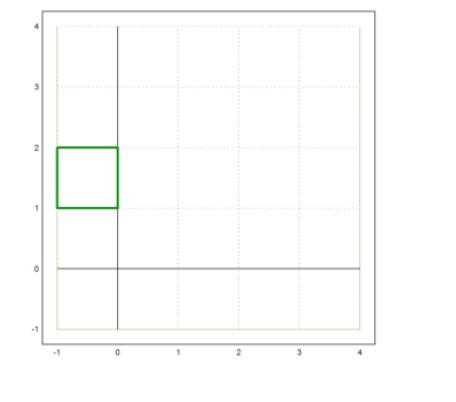




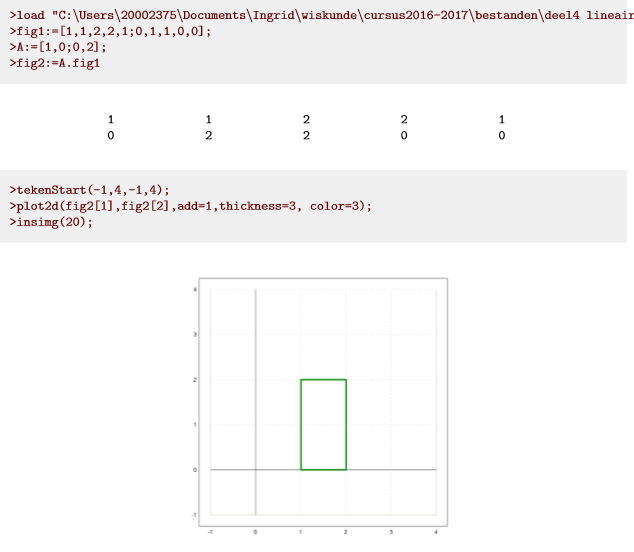


In euler











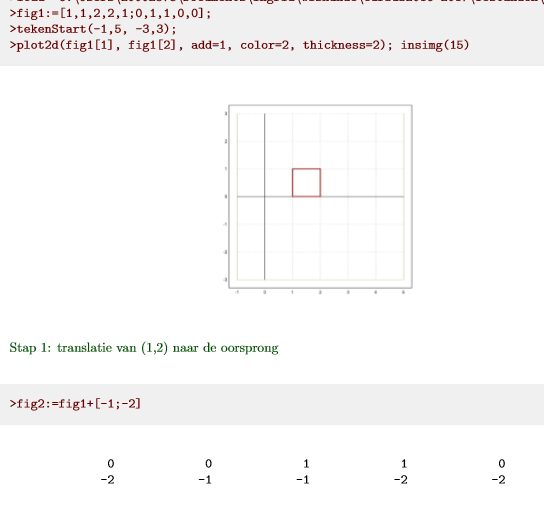
Een rotatie rond de oorsprong

Als je een draaing wilt uitvoeren moet je maal die matrix doen en gewoon de hoek die je wilt draaien ingeven voor elka apha

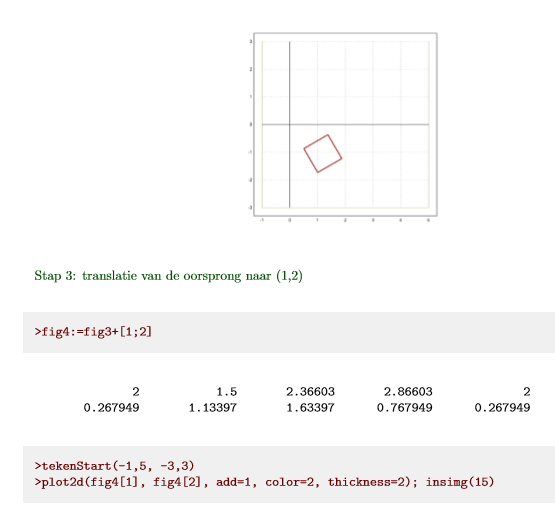


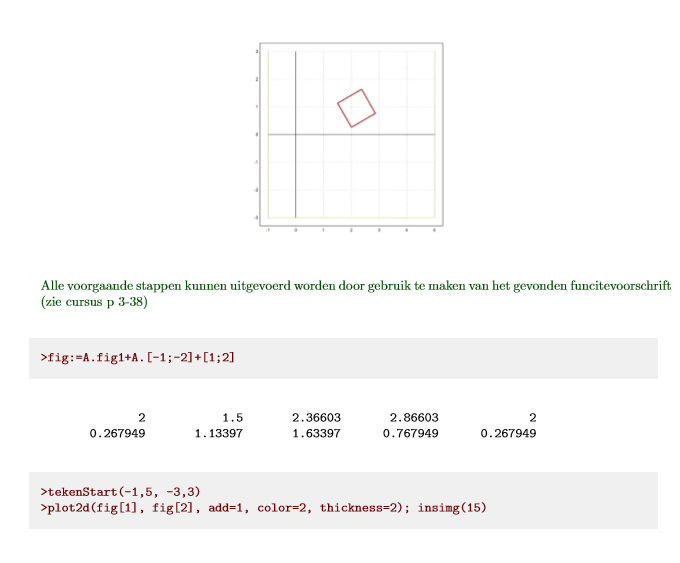
Geen idee hoe ik dit allemaal moet schijven

In euler rotatie rond een punt verschillend van de oorsprong



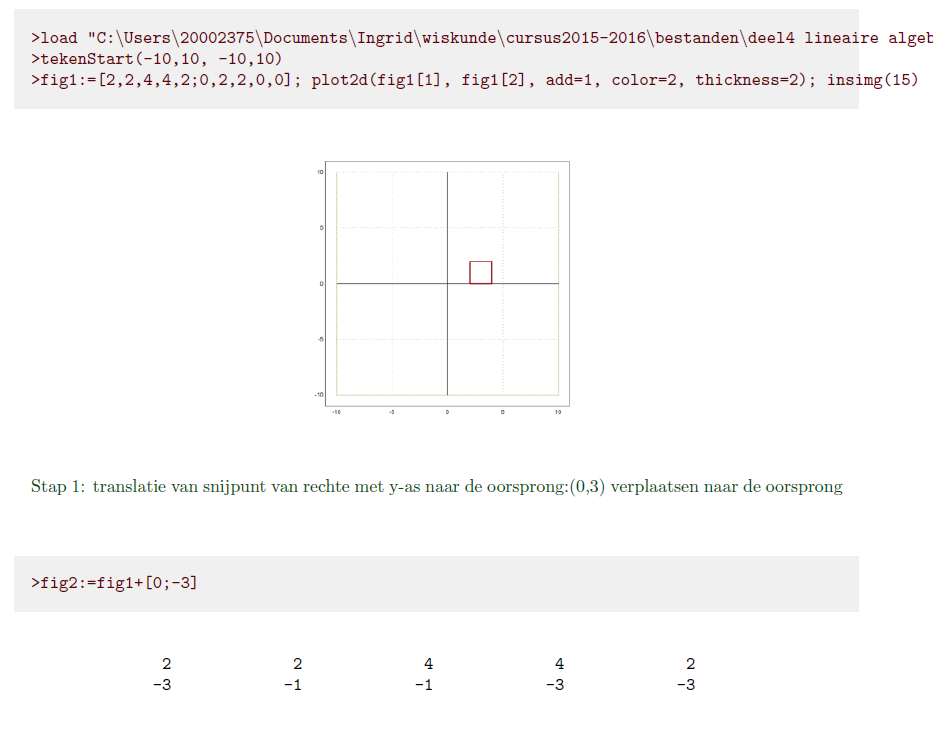


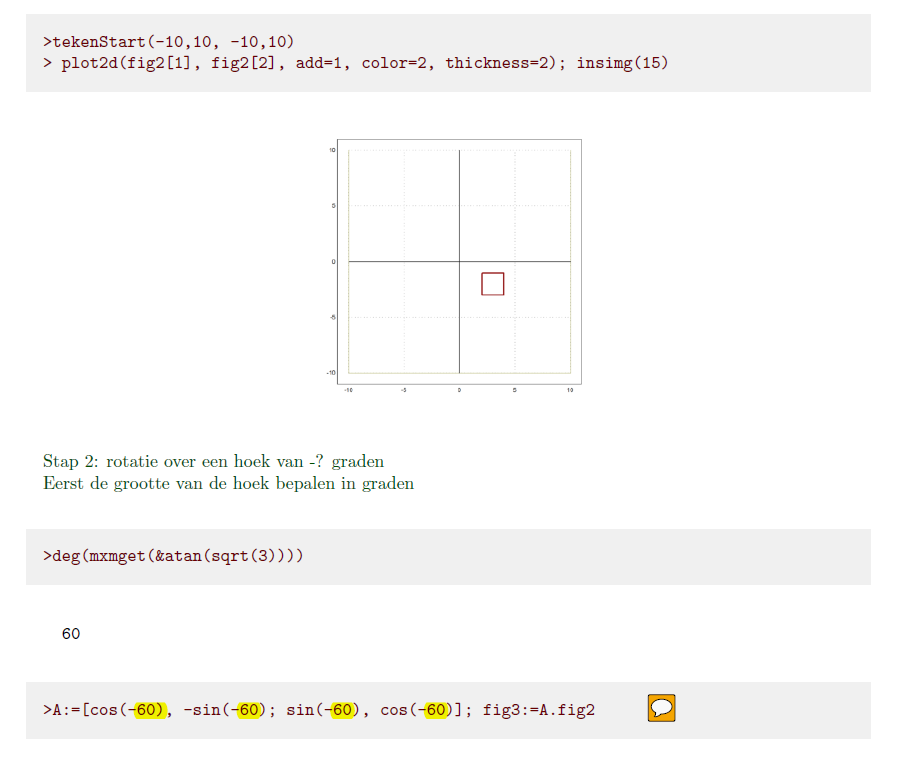


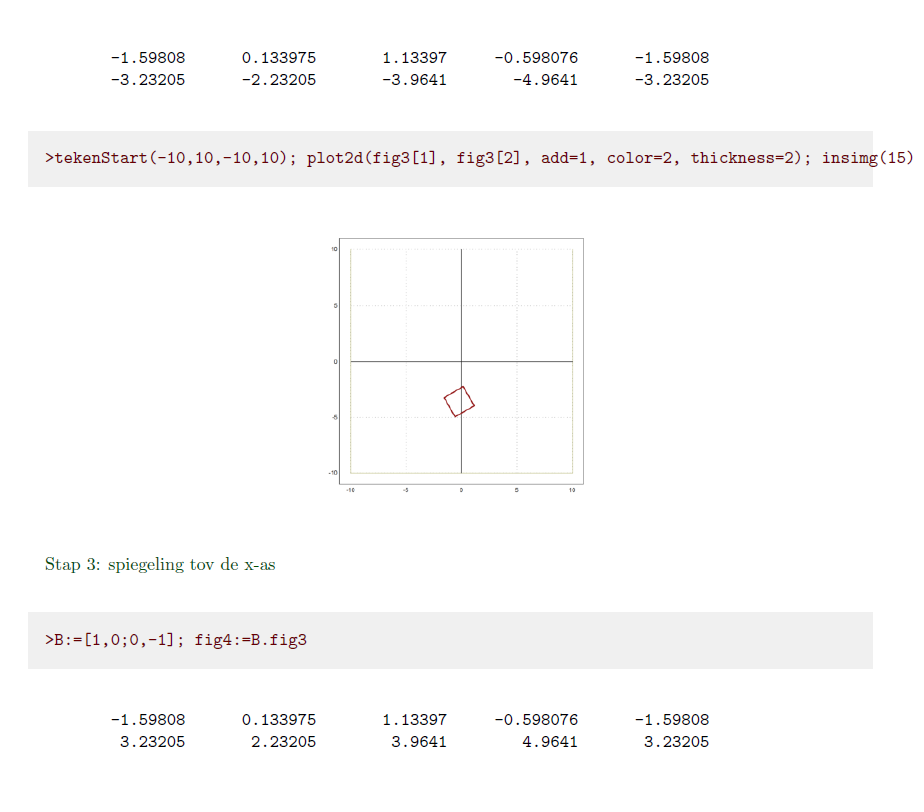


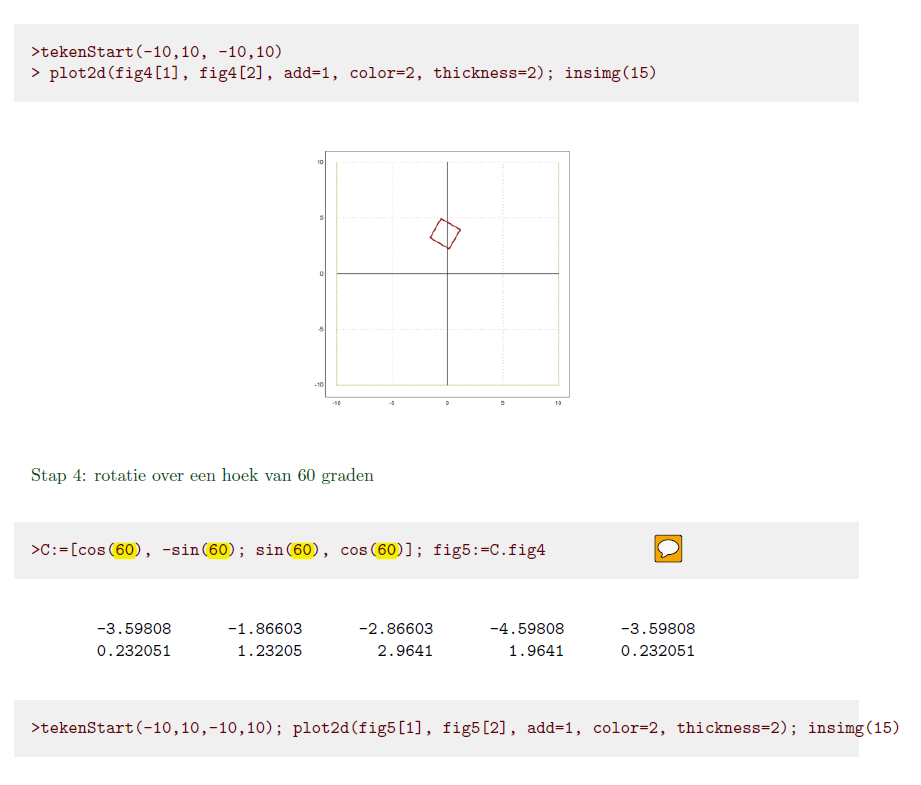


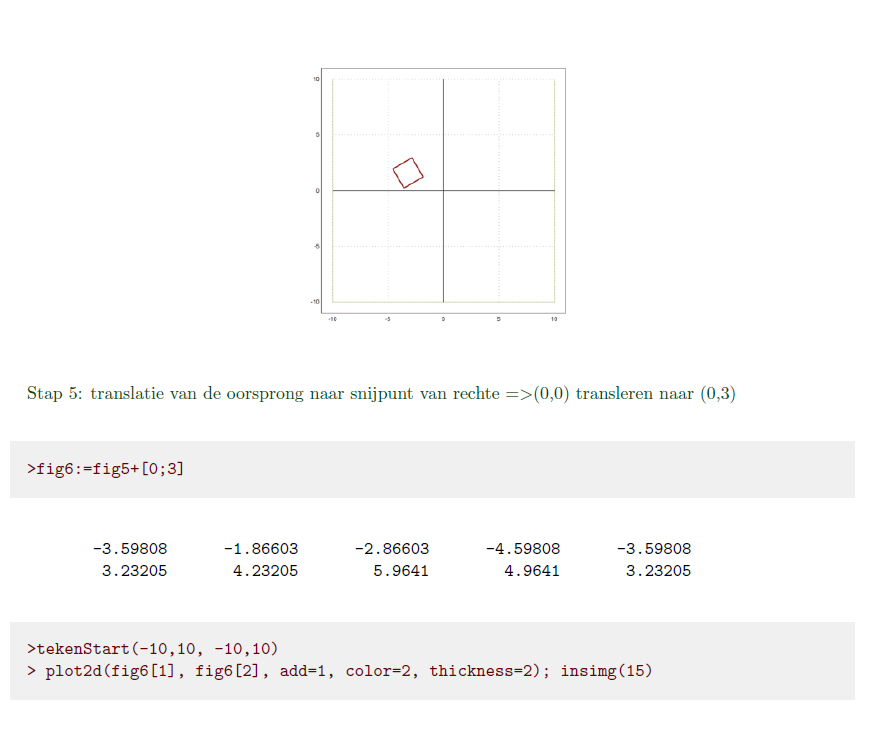
Spiegeling tov een willekeurige rechte y = ax +b

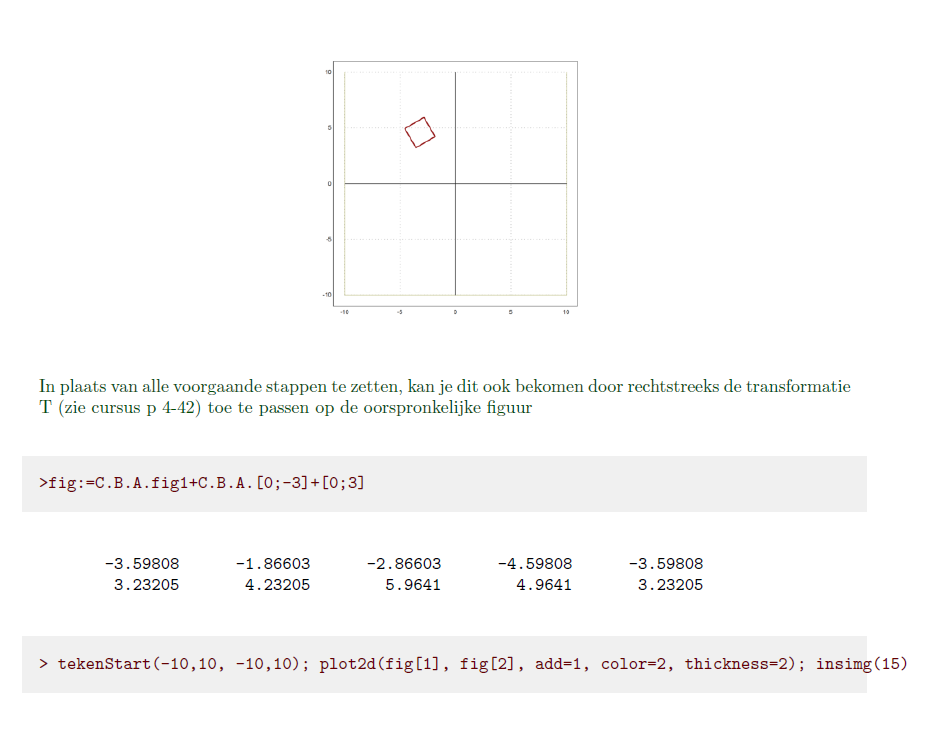












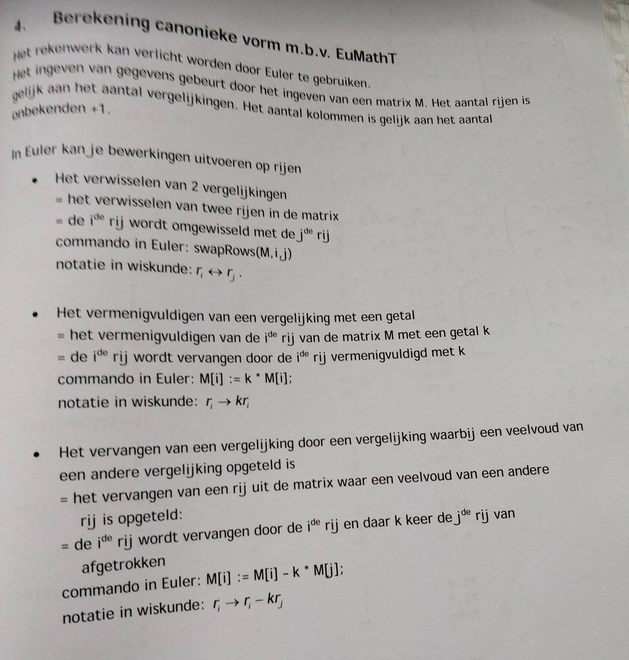
Stelsels



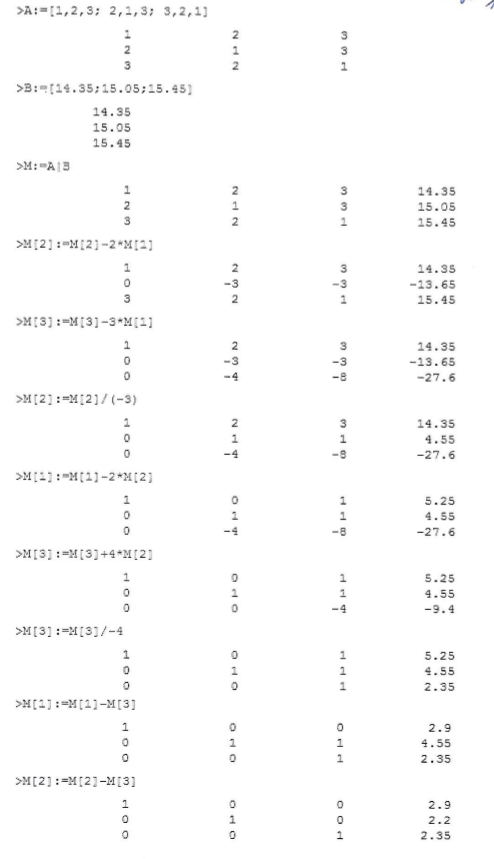
Correcte manier van samenvatten met twee keer haakjes eerst met een bekje en dan gewone

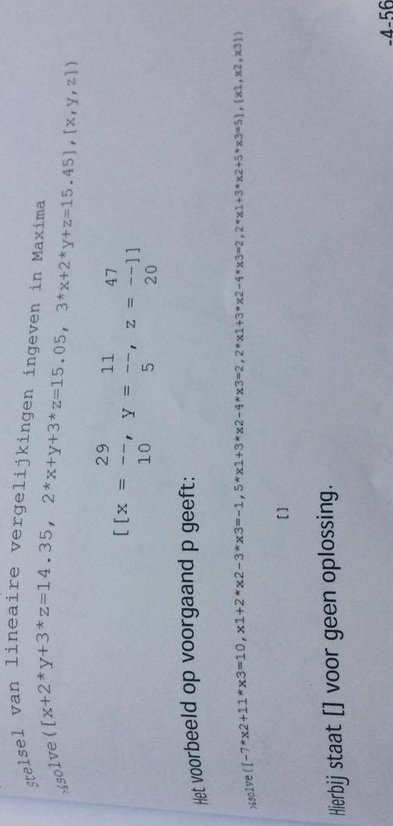
Oplossing verzameling V= { ( 2.9,2.2,2.35) } | e R

Notatie van een vals stelsel = V = {}



In euler





Inverse matrix

