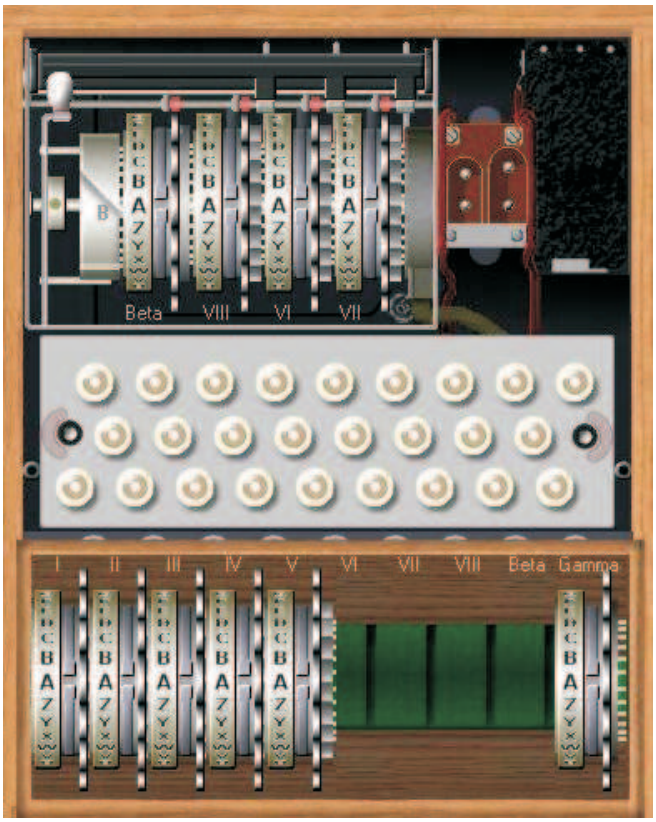
Cryptografie en getaltheorie

Een module voor Wiskunde D (vwo)

September 2009 B270809



Wiskunde D

Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven

Kerngroep vo-wo Wiskunde D i.s.m. Ernst Lambeck

TU/e Technische Universiteit Eindhoven University of Technology

Inhoudsopgave

Hoofdstuk 1

Wat is cryptografie?

1.1 Het Caesarsysteem

1 Hieronder staat een geheimzinnige tekst. Wat wordt er eigenlijk gezegd?
"FG TQOGKPUG MGKBGT LWNKWU ECGUCT JCF XGGN XKLCPFGP. FG DQQFUEJCRRGP FKG JKL CCP BKLP NGIGTU UVWWTFG OQGUVGP FCCTQO IGEQFGGTF YQTFGP. JGV UAUVGGO FCV FG MGKBGT FCCTXQQT IGDTWKMVG KU QQM DKL FGBG VGMUV IGDTWKMV. BKG LG FG UNGWVGN?"

Je hebt zojuist kennis gemaakt met een **cryptosysteem**. Wij hebben een boodschap in gewone taal (de **klare tekst**) omgezet in een soort geheimtaal (we hebben de boodschap **vercijferd**). Deze geheimzinnige boodschap (de **cijfertekst**) hebben we aan jou gegeven (naar jou **verzonden**). Vervolgens heb jij deze geheimzinnige boodschap terug vertaald (**ontcijferd**) naar klare tekst.

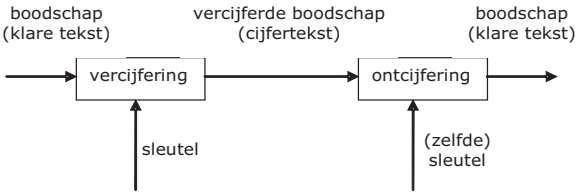
2 In de vorige opgave vond de vercijfering plaats volgens een bepaald systeem. Hierdoor wist je na het vinden van enkele letters al hoe je de rest van de tekst moest ontcijferen. Wat was dat systeem?

Het systeem waarmee wij de klare tekst hebben vercijferd heet het **Caesarsysteem**: elke letter wordt over een vast aantal plaatsen in het alfabet verschoven.

3 Hoeveel plaatsen werd elke letter verschoven?

Als je weet dat elke letter een vast aantal plaatsen in het alfabet wordt verschoven, dan kun je de volledige cijfertekst ontcijferen zodra je weet

waar bijvoorbeeld de 'A' naar toegaat. Bij het Caesarsysteem noemt men dat de **sleutel**. In het algemeen vertelt de sleutel hoe het systeem (hier dus het verschuiven van letters over een vast aantal plaatsen) precies wordt gebruikt (hier dus 'A' wordt 'C').
Schematisch werkt een cryptosysteem dus als volgt:



4 Wat is de sleutel die in de tekst hierboven is gebruikt?

5 Hoeveel sleutels zijn er mogelijk in het Caesarsysteem?

Er zijn dus 26 sleutels mogelijk in het Caesarsysteem. In de tabel hieronder zie je alle sleutels en de bijbehorende vercijfering van alle letters.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Als je de letter 'n' wilt vercijferen met de sleutel 't', dan kun je de vercijfering vinden in bovenstaande tabel door onder de 'n' en naast de 't' af te lezen. Je vindt dan als vercijfering de letter 'g'.

6 Vercijfer de volgende tekst volgens het Caesarsysteem met sleutel G: "DE HOOFDSTAD VAN NEDERLAND IS AMSTERDAM".

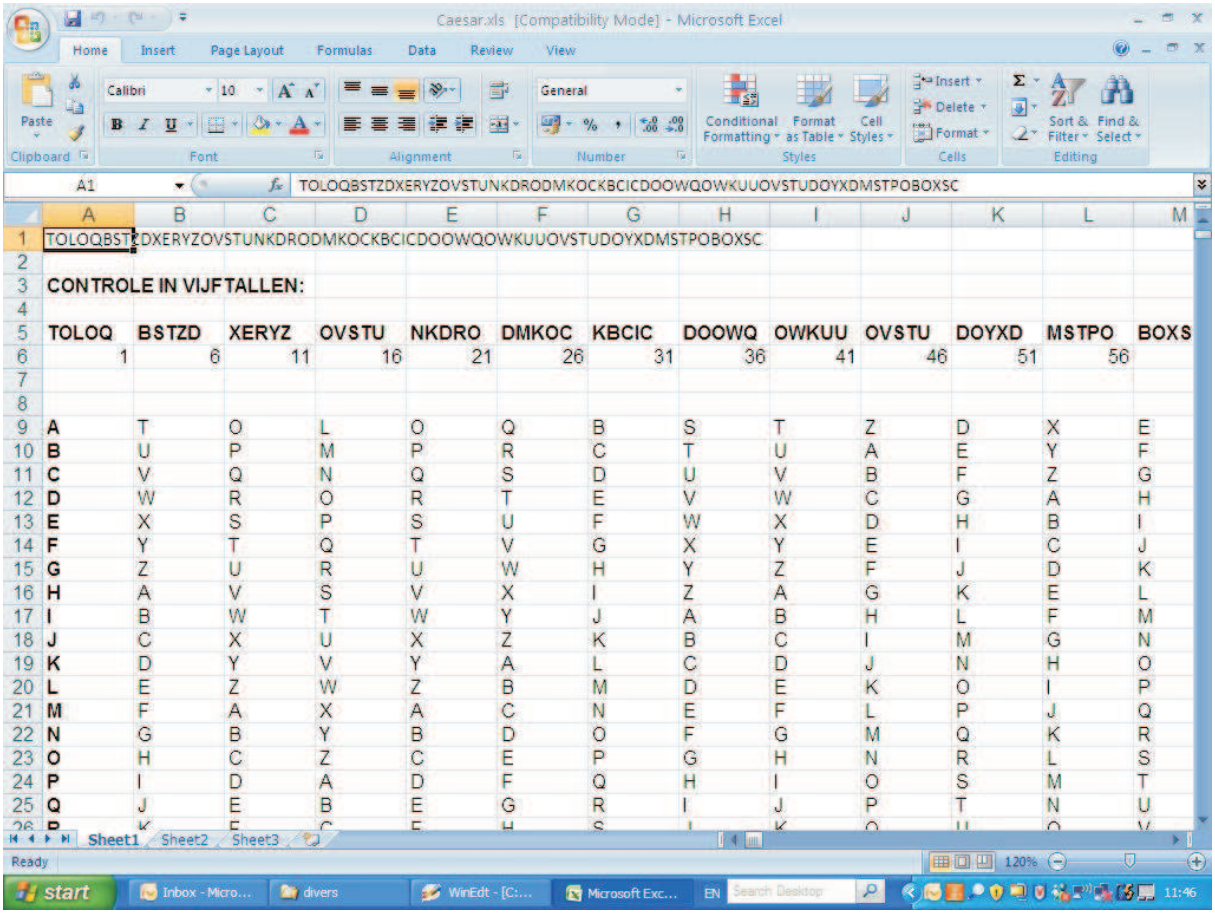
Het vercijferen van een boodschap is in het Caesarsysteem niet zo lastig. Maar zou dat ook gelden voor het decoderen?

7 Je ontvangt de volgende boodschap, die is vercijferd met behulp van het Caesarsysteem. De gebruikte sleutel weet je echter niet. Probeer desondanks de boodschap te ontcijferen. Overigens hebben we leestekens (punten, komma's, spaties, enzovoort) weggelaten, ook hebben we niet gelet op hoofdletters. Telkens worden blokken van vijf letters gegeven. Ook zorgen we er voor dat we eindigen met een blok van vijf letters, desnoods door het toevoegen van "loze" letters. Dit gebeurt regelmatig bij vercijferen van teksten (waarom zou men dat doen?).

TOLOQ	BSTZD	XERYZ	OVSTU	NKDRO
DMKOC	KBCIC	DOOWQ	OWKUU	OVSTU
DOYXD	MSTPO	BOXSC		

Boodschappen vercijferd met het Caesarsysteem zijn dus vrij gemakkelijk te ontcijferen. Zeker als je de beschikking hebt over een compu-terprogramma.
Eén van de bestanden die je kunt gebruiken is een Excel-bestand genaamd "Caesar.xls". Deze kun je, als je wilt, downloaden om te gebruiken.

Hieronder zie je de openingspagina van het bestand. Het is de enige pagina die je nodig hebt. In cel A1 voer je een met het Caesarsysteem vercijferde boodschap (maximaal 250 letters) in, alleen hoofdletters en geen leestekens en/of spaties. Op regel 5 lees je dan de ingevoerde tekst in stukken van vijf letters. In de regels daaronder zie je als uitvoer de ontcijfering volgens elke mogelijke sleutel. Je ziet dan vrij snel wat de boodschap, de klare tekst, moet zijn. In dit voorbeeld is opgave 7 daarmee ontcijferd: achter de sleutel Q zie je het begin van de klare tekst: "Je begrijpt".



8 Vercijfer volgens het Caesarsysteem een krantenbericht. Kies zelf een sleutel. Laat daarna een klasgenoot met behulp van het bestand Caesar.xls het krantenbericht ontcijferen. Ontcijfer ook zelf met behulp van dit bestand een bericht dat vercijferd is door een (andere) klasgenoot.

Cryptosystemen moeten er voor zorgen dat een boodschap alleen begrepen kan worden door de bedoelde ontvanger, ook als de boodschap wordt onderschept door anderen. Ze bieden dus een zekere bescherming tegen 'spionnen'. Maar er is meer waartegen cryptosystemen zouden kunnen beschermen.

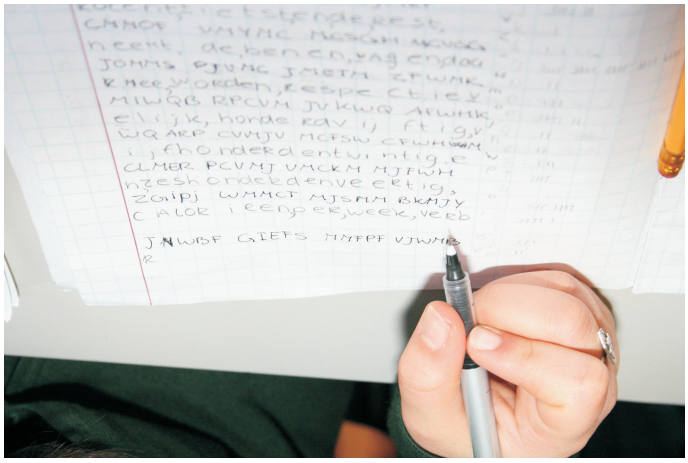
9 Stel je voor dat je een vijand van Julius Caesar bent en dat je zijn leger in een hinderlaag wilt lokken. Hoe kun je dat dan met behulp van het cryptosysteem proberen?

Cryptosystemen proberen ook authenticiteit te garanderen. Dat is belangrijk. De legeraanvoerder van het leger dat je in een hinderlaag wilt lokken zal bij een opdracht zeker willen weten dat de opdracht van Caesar zelf afkomstig is. Zo ook als je bijvoorbeeld via internet een betalingsopdracht geeft, dan moet de computer van de bank er zeker van zijn dat de opdracht van jou komt. Natuurlijk heb je ingelogd met gebruikersnaam en wachtwoord, maar ook na inloggen bestaat misschien het gevaar van 'spionnen'. Zij zouden dan zogenaamd uit jouw naam een betalingsopdracht kunnen versturen om zichzelf te verrijken met jouw geld. Misschien wil de bank ook wel een bewijs dat er met jouw boodschap (betalingsopdracht) niet is geknoeid.

Cryptosystemen zijn al zo oud als de mensheid. In het verleden werden legerorders vaak vercijferd verstuurd. Maar tegenwoordig worden cryptosystemen in tal van situaties gebruikt.

10 Waar denk je dat cryptosystemen zoal gebruikt worden? Geef een aantal voorbeelden.

In deze module maak je in hoofdstuk 1 kennis met een aantal klassieke cryptosystemen. Je ontdekt hun zwakheden, dus hoe je in principe en tamelijk eenvoudig een cijfertekst kunt ontcijferen. In hoofdstuk 3 maak je kennis met enkele moderne cryptosystemen. Deze moderne systemen zijn gebaseerd op de eigenschappen van gehele getallen. In hoofdstuk 2 bestuderen we daarom getaltheorie.



1.2 Enkelvoudige substitutie

11 Alweer een geheimzinnige boodschap. Probeer deze te ontcijferen.
"QB FBQBJCPFQWB OSEXBIZJSARBF OBDDBF FP QB RBJBCQNHNBC ZPF PVLBCSGBF UPPJ FA SSX QB EOPYGHSFW NJSGOI ZBJSZBJQ. HF QB BHFQWNJHUQ RBJQ LPWNCPFQ PJLBFNHFHB YBN 1-0 ZBJWCPLBF. YPPJNUB GPAYBF YPPXNB OBN BFHLB QSBCGAFN. THU WESSJQB PC FP NRBB YHFANBF."

12 Welk systeem is in de vorige tekst gebruikt? Wat is de sleutel?

In de voorgaande opgave heb je waarschijnlijk kunnen vertellen wat de methode is, doordat de letters niet gegroepeerd waren in groepjes van 5, de leestekens nog steeds herkenbaar waren en waarschijnlijk heeft de 1-0 je ook wel op weggeholpen.

De methode is dat elke letter van het alfabet wordt vervangen door een vaste andere letter of door een vast teken. Zo werd elke 'A' vervangen door een 'P', elke 'B' door een 'D', enzovoort. Deze methode noemt men de **methode van de enkelvoudige substitutie**.

13

a. Wat zou bij deze methode een sleutel kunnen zijn?

b. Hoeveel sleutels kun je dan bij deze methode maken?

Waarschijnlijk heb je bij het ontcijferen houvast kunnen krijgen doordat je het woordje 'DE' kon herkennen in 'QB'. Als de letters echter gegroepeerd in groepjes van 5 staan en leestekens zijn weggelaten, dan wordt het ontcijferen wel wat lastiger.

14 Met behulp van enkelvoudige substitutie is een boodschap vercijferd tot de volgende cijfertekst. Kun je de boodschap ontcijferen? Als dat niet lukt, kun je dan toch iets zeggen over de sleutel?

PGFPG	PEEPL	THAWP	EHGDH	QPEXZ
LSETP	LTHAJ	PASZZ	LPPAT	HYEPH
ASPLP	GPEEP	LNCKU		

Als je de tekst uit de voorgaande opgave hebt kunnen ontcijferen of als je een deel van de sleutel hebt kunnen vinden, dan heb je waarschijnlijk gebruik gemaakt van het feit dat de letter 'P' in deze cijfertekst wel erg vaak voorkomt. In Nederlandse teksten komt de letter 'E' wel erg vaak voor, zodat je waarschijnlijk hebt bedacht dat de 'P' een vercijferde 'E' moet zijn.

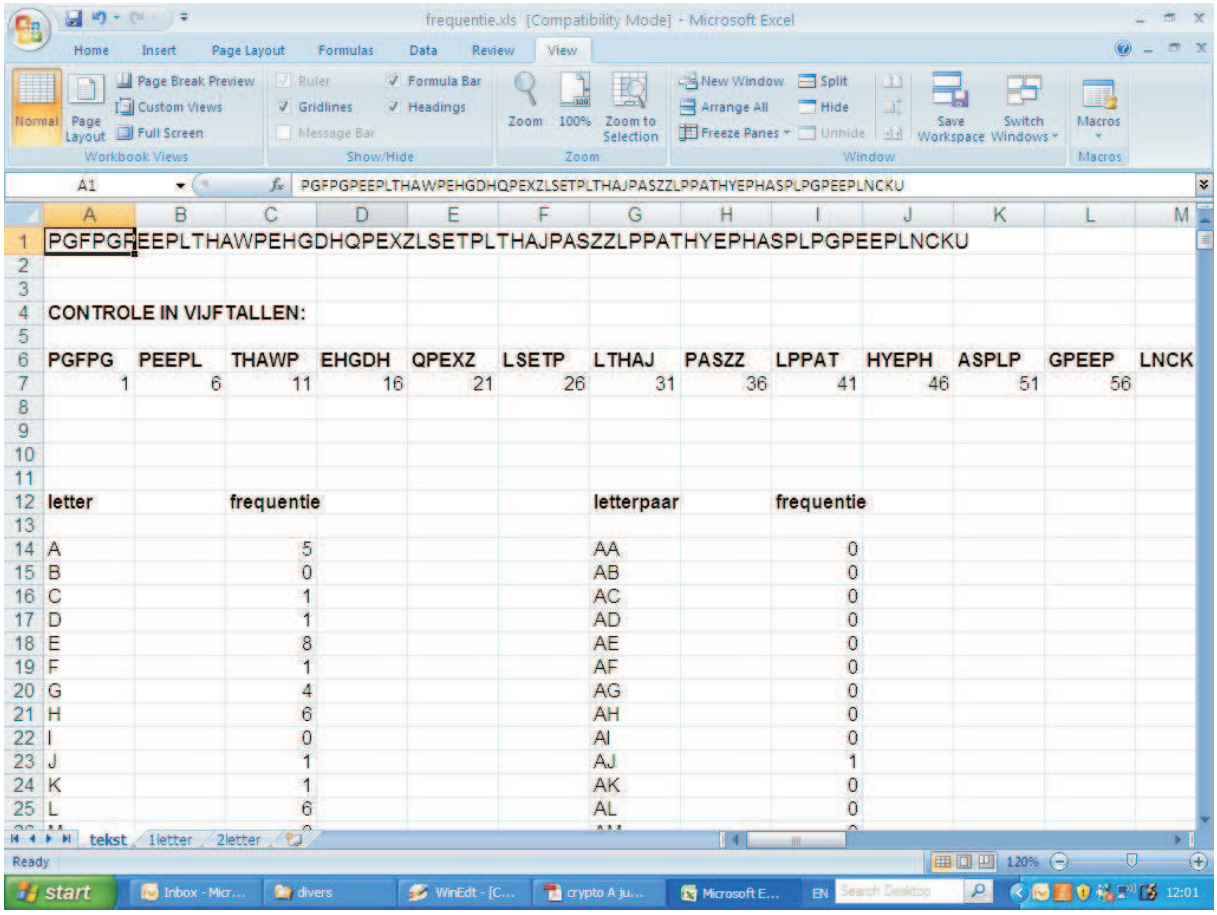
In feite is dat het idee waarmee je een met enkelvoudige substitutie vercijferde boodschap kunt ontcijferen. Je gaat gebruik maken van tabellen waarin je kunt lezen hoe vaak een letter gemiddeld voorkomt (de zogenaamde letterfrequentie). Ook zijn er tabellen met lettercombinaties die vaak voorkomen. Hieronder zie je een paar van zulke tabellen voor het Nederlands, ontleend aan *Battus, Opperlans!*, een boek dat je zeker eens in moet kijken! Soortgelijke tabellen zijn er ook te vinden voor diverse andere talen.

e	18,9%	en	15,0%	van	12,0%
n	10,2%	de	10,4%	een	9,8%
a	7,5%	er	9,4%	her	9,3%
t	6,6%	an	7,0%	ver	9,3%
r	6,5%	ge	5,5%	ing	8,8%
d	6,1%	te	5,5%	aar	7,9%
o	5,7%	in	5,3%	oor	7,7%
i	5,6%	ee	4,8%	den	7,5%
s	4,2%	aa	4,5%	gen	7,5%
l	3,7%	he	4,3%	nde	7,1%
g	3,4%	et	4,2%	der	7,0%
h	2,8%	ie	3,9%	and	6,3%
v	2,7%	el	3,9%		
m	2,2%	st	3,8%		
k	2,2%	nd	3,4%		
u	1,9%	va	3,1%		
w	1,5%	ch	3,1%		
p	1,5%	re	3,0%		
c	1,5%				
b	1,4%				
z	1,4%				
ij	1,3%				
f	0,8%				
j	0,3%				
y	0,1%				
x	0,0%				
q	0,0%				

15 Als je de boodschap in de vorige opgave niet geheel hebt kunnen ontcijferen, probeer dat dan nog eens en maak daarbij dan gebruik van bovenstaande tabellen.

Met behulp van deze tabellen heb je waarschijnlijk bepaalde letters kunnen ontcijferen. Met een beetje puzzelen, een beetje passen en meten en telkens goed lezen kun je vervolgens langzamerhand de gehele cijfertekst ontrafelen.

Voor dit werk is een Excel-bestand beschikbaar: frequentie.xls. Ook deze kun je, als je wilt, downloaden en gebruiken. Als je dit bestand opent, dan krijg je onderstaand scherm.



In cel A1 moet je de vercijferde tekst (maximaal 250 letters) invoeren, in hoofdletters en zonder leestekens of spaties. In regel 6 zie je dan de

vercijferde tekst terug, in groepjes van vijf letters. Daaronder zie je de frequenties: hoe vaak elke letter (in de eerste kolom) of elk letterpaar (in de tweede kolom) voorkomt.

16 Met behulp van enkelvoudige substitutie is een boodschap (een bericht op www.nu.nl in november 2006) vercijferd tot de volgende cijfertekst, die wordt vervolgd op de volgende pagina. Ontcijfer deze tekst. Maak, als het mogelijk is, gebruik van het bestand frequentie.xls.

LMEPT	VMFWM	CCMVM	JIGCV	MJEVP
MCRNC	YPPVE	ZRGTT	MCOMF	VMGNF
PYWQC	GKWQA	MCFSW	CFWHT	JPZMC
FAWMF	EFMCV	MJMEF	CMMOF	VMYMC
MCSGH	MCVGG	JOMMS	PJVMC	JMETM
ZFWMK	MIWQB	RPCVM	JVKWQ	AFWHK
WQARP	CVMJV	MCFSW	CFWHM	CLMER
PCVMJ	VMCKM	MJFWH	ZGIPJ	WMMCT
MJSMM	BKMJY	JNWBF	GIEFS	MMFPF
VJWMB	MMJTM	JSMMB	YPPVE	ZRGTT
MCSPJ	VMCHM	VGGCV	GFYIW	QBFVW
CEVGH	NWFPC	VMJLP	MBKGC	VMMJG
EONEN	CWKMJ	EWFMW	FJPFF	MJVGO
MCRMF	ZMCFJ	GGIYN	JMGNI	MKMCE
OWVVM	IMCRG	CVMIW	CVMEF	JWQVF
MHMCP	KMJHM	SWZRF	JPMTM	CVMPC
VMJLP	MBMJE	OMCEM	CPTPO	KGBMJ
FMIPT	MCPAA	WMFEM	CGIEL	MYPPV
EZRGT	TMCHG	GCVPM	CSMIO	PMFMC
VMENT	MJOGJ	BFMCV	GCHPM	VTMJA
WMFEY	MJMWB	YGGJL	WQCVM	PCVMJ
LPMBM	JETIM	WFMCP	CVMJO	MMJKP
PJHPM	VMAWM	FETGV	MCMCY	MFMJM
TGJBM	MJHMI	MHMCR	MWVKP	PJAWM
FEMCY	WQVMS	WCBMI		

1.3 Het Vigenèresysteem

In de vorige paragrafen heb je gezien dat cijferteksten gemaakt met het Caesarsysteem of het systeem van enkelvoudige substitutie tamelijk eenvoudig te ontcijferen zijn.

18 Zie je mogelijkheden om één van beide systemen zo aan te passen dat ontcijferen moeilijker wordt?

Misschien heb je wel bedacht om een aantal verschillende sleutels wisselend te gebruiken. Bijvoorbeeld 5 sleutels, waarbij je dan de eerste letter vercijfert met de eerste sleutel, de tweede letter met de tweede sleutel, enzovoort, waarna je na 5 letters opnieuw begint. Dit idee had ook Giovanni Batista Belaso (1505 – ?) in het midden van de 16^{e} eeuw. De Franse edelman, wetenschapper en diplomaat Blaise de Vigenère (1523 – 1596) bracht verbeteringen aan in het idee van Belaso. Door het werk van De Vigenère werd het idee van Belaso bekend, maar kreeg het ten onrechte de naam van De Vigenère. Het idee achter het Vigenèresysteem is om een aantal Caesarverschuivingen achter elkaar te gebruiken. De sleutels van deze verschuivingen samen vormen een woord, het sleutelwoord van het Vigenèresysteem.

19 De boodschap ”WISKUNDE D” is vercijferd tot ”SQKUOAGI Z”. Wat is het gebruikte sleutelwoord? (TIP: omdat het Vigeneresysteem een combinatie is van een aantal Caesarverschuivingen, is het handig om de tabel met alle Caesarverschuivingen (pagina 2) te gebruiken.)

20 Vercijfer de boodschap ”MOBILISEER DE TROEPEN. AANVAL WORDT VERWACHT IN ALLE VROEGTE MORGENOCHTEND.”met het sleutelwoord ”kogel”.

21 Het ontcijferen van een met het Vigenèresysteem vercijferde boodschap werkt niet zo gemakkelijk als het ontcijferen van een met enkelvoudige substitutie vercijferde boodschap. Waarom niet?

22 We gaan werken met het Vigenèresysteem en nemen ”WD¨ als sleutelwoord.

a. Vercijfer de tekst ”Dit valt te ontcijferen”.

b. Kijk naar de manier waarop de letters op de oneven plaatsen zijn vercijferd. Wat is het meest opvallende van deze vercijfering?

c. Kijk naar de manier waarop de letters op de even plaatsen zijn vercijferd. Wat is het meest opvallende van deze vercijfering?

Nu gaan we in gedachten een andere tekst vercijferen en gebruiken daarbij een ander sleutelwoord, weer van twee letters.

d. Kun je nu iets soortgelijks zeggen als bij vraag b.? En bij vraag c.?

e. Zou je nu de sleutel kunnen vinden bij de oneven letters (dus de eerste letter van het sleutelwoord)? En de tweede letter van het sleutelwoord?

Door alle oneven letters te tellen, weet je waarschijnlijk naar welke letter de 'E' wordt geschoven (deze letter komt immers meestal het vaakste voor in een Nederlandse tekst). Maar dan weet je ook waar de 'A' naar toe wordt geschoven, dus weet je waarschijnlijk de eerste letter van het sleutelwoord. Hetzelfde geldt natuurlijk voor de even letters en de tweede letter van het sleutelwoord.

Voorbeeld
Stel je ontvangt de boodschap "XEIMP MXBIZ WPIMJ BHMDM WTICX MPEIT OESWV LMAHM WTICX MPRWE". Je weet al dat het verstuurd is met een Vigenèresysteem met een sleutelwoord van lengte twee.
Je gaat nu de letters verdelen in twee groepen: de letters op de oneven plaatsen (XIPXIWIJHDWIXPIOSVMHWIXPW) en de letters op de even plaatsen (EMMBZPMBMMTCMETEWLAMTCMRE).
De letters op de oneven plaatsen zijn allemaal vercijferd met de eerste letter van het sleutelwoord. Aangezien onder deze letters de 'I' het meeste voorkomt, is dit waarschijnlijk een vercijferde 'E'. De sleutel is dan een 'E' geweest, dus is de eerste letter van het sleutelwoord waarschijnlijk een 'E'.
De letters op de even plaatsen zijn allemaal vercijferd met de tweede letter van het sleutelwoord. Aangezien onder deze letters de 'M' het meeste voorkomt, is dit waarschijnlijk een vercijferde 'E'. De sleutel is dan een 'I' geweest, dus is de tweede letter van het sleutelwoord waarschijnlijk een 'I', het sleutelwoord dus 'EI'.
Als je met het sleutelwoord 'EI' de boodschap gaat ontcijferen, dan krijg je 'Twee letters heeft deze sleutel. Welk woord is de sleutel.' De laatste drie letters van de boodschap staan er dus alleen ter opvulling van het vijftal.

Als je weet dat het sleutelwoord bijvoorbeeld 8 letters lang is, dan kun je eenzelfde aanpak volgen als hierboven. Je verdeelt de tekst dan in 8 delen: alle 1^e letters, alle 2^e letters, enzovoort tot en met alle 8^e letters. Vervolgens pas je het idee van letterfrequentie toe op elk der 8 delen. Daarmee kun je dan bijvoorbeeld proberen de meeste letters van het

sleutelwoord te vinden, waarna je met wat logisch denken, combineren en proberen hopelijk het gehele sleutelwoord kunt achterhalen.

Maar hoe vind je de lengte van het sleutelwoord?
In de volgende opgaven maak je kennis met een paar methoden om de lengte van het sleutelwoord min of meer te kunnen bepalen.

23

a. Laat met behulp van de letterfrequentietabel van Battus zien dat de kans dat twee willekeurige letters in een Nederlandse tekst hetzelfde zijn gelijk is aan 0,078878. (Hint: deze kans is gelijk aan de kans op twee a's of twee b's of ...).

b. In een cijfertekst gemaakt met het Vigenèresysteem met een willekeurig gekozen sleutelwoord van 7 letters bekijken we twee letters die geen 7, geen 14, geen 21, enzovoort, plaatsen uit elkaar liggen. Wat is de kans dat deze letters hetzelfde zijn?

We kijken naar de cijfertekst

WCHMW	SGKIC	NSZVZ	ODKRL	KBBEW
GCXHE	FSXAL	MVZMY	KZRIG	BCKKE
OAUVR	OBUGS	DSTHI		

We verschuiven deze tekst over één plaats. In de volgende tabel is een beginnetje gemaakt:

W	C	H	M	W	S	G	K	I	C	N	S	Z	V	Z	O	D	K	R	L	K	B	B	E	..
	W	C	H	M	W	S	G	K	I	C	N	S	Z	V	Z	O	D	K	R	L	K	B	B	..
																						*		

Je ziet een * op de plaats waar de letters van de cijfertekst en de verschoven cijfertekst gelijk zijn. Dat gebeurt in dit stukje één keer. Als je dit voor de gehele cijfertekst zou doen, dan gebeurt het twee keer: we hebben twee overeenkomsten.

24 Stel het sleutelwoord is 4 letters lang. Waarom mag je dan meer overeenkomsten verwachten bij het verschuiven over 4, over 8, enzovoort, plaatsen dan bij het verschuiven over een ander aantal plaatsen?

In de volgende tabel zie je het aantal overeenkomsten bij verschuiven over 1, over 2, enzovoort, plaatsen:

aantal plaatsen	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
aantal overeenkomsten	2	2	2	2	3	2	1	2	0	1	1	1	1	1	1	0
aantal plaatsen	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
aantal overeenkomsten	2	1	2	5	1	0	4	3	2	3	2	2	1	2	1	1
aantal plaatsen	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
aantal overeenkomsten	2	1	5	1	1	1	0	3	1	0	0	1	1	0	0	1
aantal plaatsen	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
aantal overeenkomsten	0	1	0	1	0	1	0	2	0	0	0	0	1	0	0	0

25 Uit hoeveel letters zou het sleutelwoord kunnen bestaan als je afgaat op bovenstaande tabel?

In deze tabel is het aantal overeenkomsten bij verschuivingen over 20 ($4 \cdot 5$) en over 35 ($7 \cdot 5$) plaatsen het hoogst. Op grond daarvan zou je redelijkerwijze mogen verwachten dat het sleutelwoord 5, 20 of 35 letters heeft (in feite heeft het sleutelwoord 5 letters, de cijfertekst die we hier bekijken is het antwoord op opgave 20).

26 Waarom wordt hierboven ook 5 genoemd als mogelijk aantal letters van het sleutelwoord?

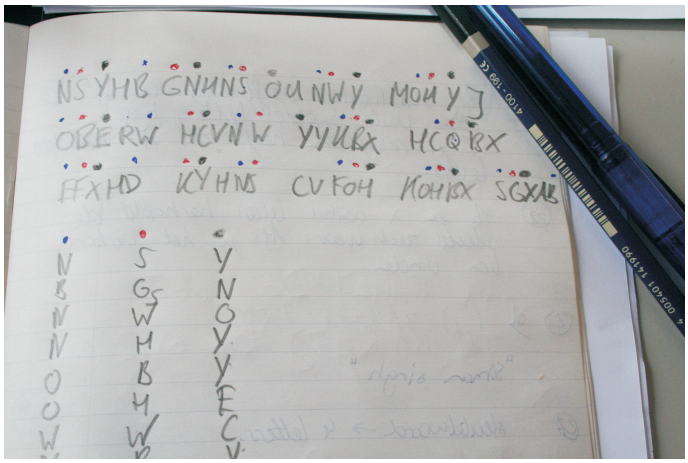
27 De volgende cijfertekst is vercijferd met het Vigenèresysteem. Vind een zo goed mogelijke schatting van het aantal letters van het sleutelwoord.

NSYHB GNHNS OUNWY MOHYJ OBERW
HCVNW YYKBX HCQBX EFXHD KYHNS
CVFOH KOHBX SGXAB

Er zijn meer hulpmiddelen om de lengte van het sleutelwoord te vinden. Nadat ongeveer 300 jaar lang de Vigenère vercijfering als praktisch onbreekbaar werd beschouwd bedacht een Pruisische majoor, Kasiski, een methode om de lengte van het sleutelwoord te vinden. Deze methode vertoont veel overeenkomst met het voorgaande, maar kijkt niet naar enkele letters die overeenkomen, maar naar de afstand tussen dezelfde letterparen op verschillende plaatsen in de tekst.

28 Bedenk hoe deze methode zou kunnen werken.

29 Stel het sleutelwoord bestaat uit 6 letters. In een stuk te vercijferen tekst staat het letterpaar OP twee keer. De eerste OP bestaat uit de 8^e en de 9^e letter van de tekst, de tweede OP uit de 26^e en de 27^e letter van de tekst. Wat gebeurt er met de beide OP's als je gaat vercijferen?



Het idee achter deze methode is daarom het volgende. Als de afstand tussen gelijke letterparen in de klare tekst een aantal keren het aantal letters van het sleutelwoord is, dan worden deze letterparen in andere gelijke letterparen vercijferd. De gevonden afstand is dus vaak een veelvoud van het aantal letters van het sleutelwoord.

30

a. In de tekst hierboven staat dat de gevonden afstand vaak een veelvoud van het aantal letters van het sleutelwoord is. Waarom vaak en niet altijd?

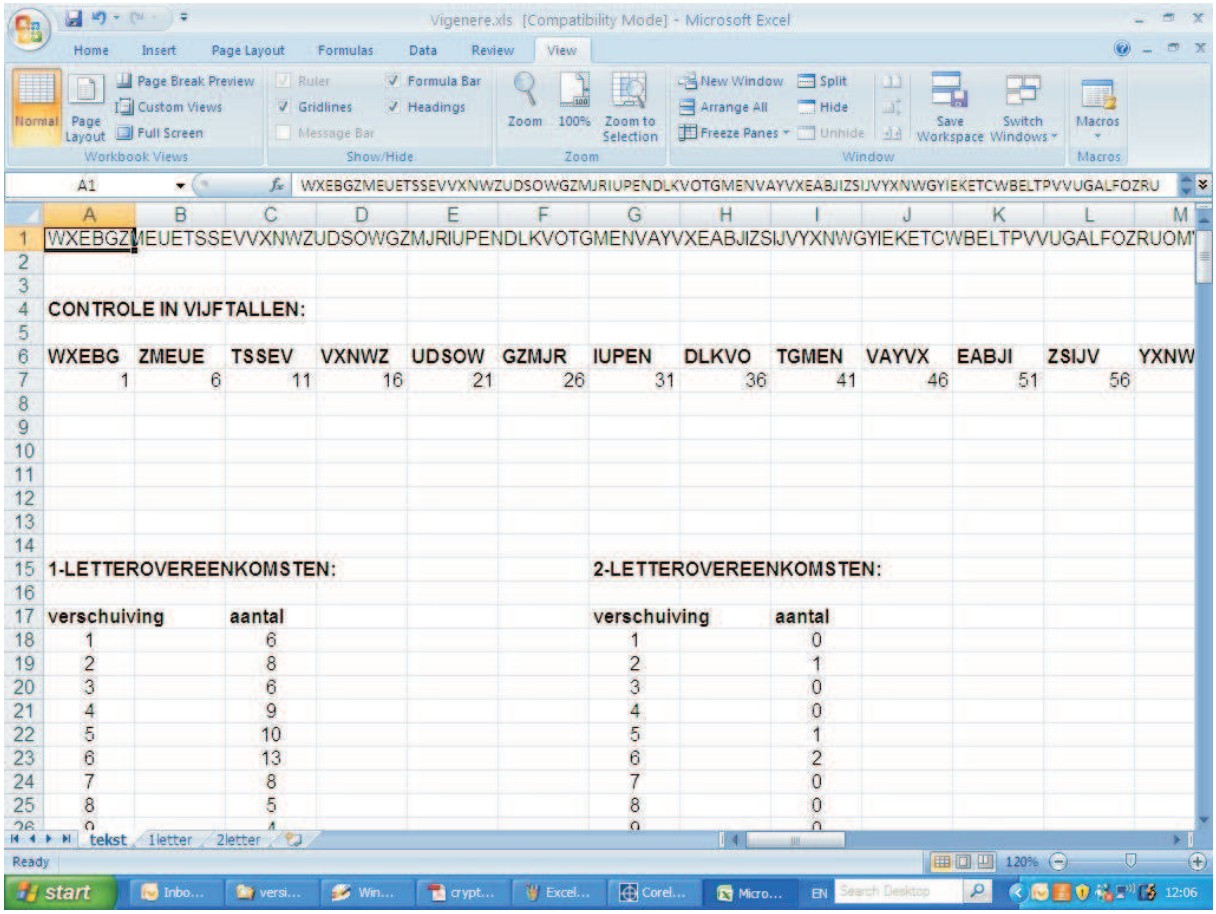
b. Werken bovenstaande methoden beter voor een korte of voor een lange tekst? Leg uit.

31 Probeer zoveel mogelijk dezelfde letterparen op te sporen in de tekst van opgave 27. Kijk naar de afstanden tussen dezelfde letterparen en probeer daarmee je schatting van het aantal letters van het sleutelwoord te verbeteren.

32 Ontcijfer de tekst van opgave 27. (Heb je het aantal letters van het sleutelwoord niet gevonden, zoek dat dan eerst op bij de antwoorden).

Ook voor het Vigenèresysteem is op http://www.win.tue.nl/wiskunded/ een Excel-bestand geplaatst: Vigenere.xls. Ook deze kun je weer, als je wilt, downloaden en gebruiken. Als je dit bestand opent, dan krijg je

onderstaand scherm.



In cel A1 moet je de vercijferde tekst (maximaal 250 letters) invoeren, in hoofdletters en zonder leestekens of spaties. In regel 6 zie je dan de vercijferde tekst terug, in groepjes van vijf letters. Daaronder zie je de overeenkomsten: in de eerste kolom hoeveel letters er gelijk zijn bij het verschuiven over 1 plaats, over 2 plaatsen, enzovoort, en in de tweede kolom hoeveel letterparen er gelijk zijn bij het verschuiven over 1 plaats, over 2 plaatsen, enzovoort.

33 Ontcijfer de volgende cijfertekst, gemaakt met het Vigenèresysteem. De klare tekst is een deel van een bericht in "de Volkskrant"van 19 december 2006. Je kunt gebruik maken van het bestand Vigenere.xls

WXEBG	ZMEUE	TSSEV	VXNWZ	UDSOW
GZMJR	IUPEN	DLKVO	TGMEN	VAYVX
EABJI	ZSIJV	YXNWG	YIEKE	TCWBE
LTPVV	UGALF	OZRUO	MVUSE	NGGUM
CZIIK	EROAV	YBSVR	ULRET	RBXMG

BINLN	DHSLU	MCNLV	LFTOW	KVOTG
WMVOR	GWKKZ	TFERU	GEDUA	VZEOQ
RHRHP	WYKLT	MIZGI	GPJAZ	MGJZV
YNIPL	BEOTG	MTOTX		

34 Laat je buurman/buurvrouw een stuk klare tekst (bijvoorbeeld een krantenbericht) vercijferen volgens het Vigenèresysteem. Aan jou de opdracht om de geproduceerde cijfertekst weer te ontcijferen. Gebruik zonodig Vigenere.xls.

In dit hoofdstuk heb je kennis gemaakt met een drietal klassieke cryptosystemen. Sommigen lagen erg voor de hand, andere wellicht niet. Bij goed kijken naar de werking van deze systemen heb je ontdekt dat ze vrij eenvoudig te ontcijferen zijn. Voor echte geheimhouding moeten we dus op zoek naar veel moeilijker te ontcijferen systemen. De sleutel om dit soort systemen te ontwikkelen is een aantal eigenschappen van gehele getallen. In het volgende hoofdstuk gaan we daarom eerst gehele getallen bestuderen. In het hoofdstuk daarna gaan we de ontdekte eigenschappen gebruiken bij het ontwikkelen van meer geavanceerde cryptosystemen.

Een samenvatting van dit eerste hoofdstuk zul je in deze module niet vinden. De volgende opgave geeft je in feite een samenvatting.

35 Cryptografie houdt zich bezig met geheimschriften.
Als je een boodschap wilt sturen die alleen voor de geadresseerde(n) leesbaar is, dan gebruik je een cryptosysteem (een systeem om de boodschap te vercijferen) en een sleutel (hoe je elke letter moet vercijferen met dit systeem) om de boodschap te vercijferen naar een cijfertekst (geheim bericht). De ontvanger heeft de sleutel ook nodig: hij kan daarmee de cijfertekst weer ontcijferen tot de oorspronkelijke boodschap (de zogenaamde klare tekst).
Het is natuurlijk de bedoeling dat iemand die de cijfertekst onderschept de boodschap niet kan vinden.
Bij de in dit hoofdstuk behandelde klassieke systemen lukt dit echter vrij eenvoudig.
Geef van elk van de drie besproken klassieke systemen duidelijk aan:

- hoe men met dit systeem boodschappen kan vercijferen;
- hoe een onderschepper toch de cijferteksten kan ontcijferen.

Vertel ook en verklaar welk systeem het meest veilig is van deze drie en welke het minst veilig.

Hoofdstuk 2

Getaltheorie

In de wiskunde onderscheidt men een aantal collectes getallen. Ongetwijfeld heb je enkele al wel eens gezien:

- De collectie **N** van de **natuurlijke getallen**, dat wil zeggen de getallen 1, 2, 3, 4, enzovoort;
- De collectie **Z** van de **gehele** getallen, dat wil zeggen de getallen 0, 1,-1, 2, -2, 3, -3 enzovoort;
- De collectie **Q** van de **rationale** getallen, dat wil zeggen alle getallen die te schrijven zijn als een breuk, zoals bijvoorbeeld $\frac{3}{5}$, $\frac{7}{9}$, $\frac{-2}{11}$ en 3 (is immers gelijk aan $\frac{3}{1}$);
- De collectie **R** van de **reële** getallen, dat wil zeggen alle getallen die je op de getallenlijn kunt vinden.

De moderne cryptografische systemen die we verderop gaan bekijken maken gebruik van allerlei eigenschappen van natuurlijke getallen. In de komende twee hoofdstukken gaan we daarom wat getaltheorie bestuderen. We beginnen met twee begrippen die je waarschijnlijk al zal kennen: delen en deelbaar zijn, maar maken eerst nog een

Afspraak: als we in dit dictaat in hoofdstuk 2 of 3 over getallen spreken, dan bedoelen we daar ***natuurlijke*** getallen mee, tenzij anders aangegeven.

2.1 Delen en priemgetallen

1 Zes jongens gaan een bedrag van 152 euro verdelen. Iedereen krijgt een geheel aantal euro's.

a. Hoeveel euro krijgt iedereen?

b. Niet het gehele bedrag van 152 euro kan worden verdeeld. Hoeveel blijft er over?

Als je een bedrag van 317 euro verdeelt onder 10 jongens, dan blijft er 7 euro over als iedereen een geheel aantal euro's moet krijgen. Iedere jongen krijgt dan 31 euro. Anders gezegd: $317 : 10 = 31$ *rest* 7. Wiskundig betekent dit dat $317 : 10 = 31\frac{7}{10}$.

2 Bereken de uitkomst van de volgende delingen. Geef ook de rest.

a. $41 : 7$

b. $73 : 11$

c. $219 : 17$

Als de getallen groter worden, dan is het delen met rest wat lastiger. Je ziet dan vaak niet direct het antwoord en de rest. Een **staartdeling** kan dan hulp bieden. Hieronder zie je stap voor stap de staartdeling horend bij $11274 : 31$.
Allereerst schrijven we de opgave iets anders op. Het getal dat je wilt delen staat tussen strepen, het getal waardoor je wilt gaan delen staat ervoor.

$$31/11274\backslash$$

We bekijken nu de veelvouden $1 \cdot 31 = 31, 2 \cdot 31 = 62, \ldots, 9 \cdot 31 = 279$ van 31. Aangezien $3 \cdot 31 = 93$ kleiner is dan 112, maar $4 \cdot 31 = 124$ niet, zetten we 93 onder 112 en berekenen $112 - 93 = 19$. De 19 komt onder de 93 en de 3 van $3 \cdot 31 = 93$ komt achter het \-teken:

$$\begin{array}{l} 31/11274\backslash 3 \\ \underline{93} \\ 19 \end{array}$$

Vervolgens zetten we achter de 19 de 7 die in de eerste regel achter de 112 staat. We krijgen dan het getal 197. Dit getal is groter dan $6 \cdot 31 = 186$, maar kleiner dan $7 \cdot 31 = 217$. Onder de 197 komt daarom 186 te staan, waarna we weer gaan aftrekken: $197 - 186 = 11$. De 11 komt nu onder de 186. Omdat $186 = 6 \cdot 31$, zetten we in de bovenste regel nu de 6 achter de 3:

```
31/11274\36
  93
  197
  186
   11
```

Tenslotte zetten we de 4 die na 1127 in de eerste regel staat nu ook naast de 11 onderaan. We krijgen dan 114. Vervolgens kijken we weer hoe vaak 31 in dat getal gaat: 3 keer. Deze 3 komt achteraan in de bovenste regel. Onder de 114 komt $93 = 3 \cdot 31$ en we trekken weer af:

```
31/11274\363
  93
  197
  186
   114
    93
    21
```

Aangezien in de eerste regel de zojuist bijgeschreven 4 het laatste cijfer tussen de deelstrepen (/ en \) is zijn we klaar. Je kunt nu hierboven het antwoord aflezen:

$$11274 : 31 = 363 \textit{ rest } 21, \text{ ofwel } 11274 : 31 = 363\tfrac{21}{31}.$$

Waarom werkt een staartdeling?

Misschien kun je je van de basisschool herinneren hoe je 11274 moest delen door 31. Je moest zo vaak mogelijk 31 aftrekken van 11274 en bijhouden hoe vaak je dat deed.
Als je het wat handiger aanpakte, dan bedacht je dat je niet iedere keer precies 31 ging aftrekken, maar misschien wel 100 maal 31 in één keer, d.w.z. je ging meteen 3100 aftrekken.
Of nog handiger: misschien wel 200 maal 31, 300 maal 31, of zelfs 400 maal 31 (als dat ging). Als je dat probeerde, dan zag je dat 300 maal 31 wel ging, maar 400 maal 31 niet.
Je trok dus direct 300 maal 31 af. Je hield dan nog $11274 - 300 \cdot 31 = 1974$ over. Eigenlijk keek je alleen naar de honderdtallen, dus naar $11200 - 300 \cdot 31 = 1900$.
Dat is ook precies wat er bij een staartdeling gebeurt, alleen noteren we alle nullen aan het einde van de getallen niet.
Vervolgens keek je naar wat je had overgehouden, 1974, en trok daar weer zo vaak mogelijk 31 van af. Je probeerde 10 maal 31, 20 maal 31, enzovoort. Hier bleek je wel 60 maal 31, maar geen 70 maal 31, te kunnen aftrekken.
Je berekende $1974 - 60 \cdot 31 = 114$. Als je nu alleen naar de tientallen kijkt, dan zie je in feite $1970 - 60 \cdot 31 = 110$, precies de tweede stap in de staartdeling, maar dan zonder de nullen aan het einde.
We doen dus eigenlijk hetzelfde, alleen anders opgeschreven.
Misschien was je de notatie zoals die hiernaast staat wel gewend: als je de getallen in de laatste kolom (300, 60 en 3) optelt, dan krijg je het resultaat van de deling: 363.
De rest staat geheel onderaan: 21.

11274	
9300	300
1974	
1860	60
114	
93	3
21	

3 Bereken met een staartdeling (geef ook de rest). Gebruik de notatie met de deelstrepen (/ en \).

a. 17265 : 14

b. 213736 : 11

c. 123456 : 321

Als de rest van $a : b$ gelijk is aan 0, dan zeggen we dat a ***deelbaar*** is door b.
Anders gezegd:

Een getal a heet deelbaar door een getal b als er een getal k is zodanig dat $a = b \cdot k$.

We zeggen dan ook wel dat b het getal a ***deelt***, dat b een ***deler*** is van a of dat a een **veelvoud** is van b.
We noteren in dat geval $b|a$.
Voorbeelden

- $5|15$, want $15 = 5 \cdot 3$.
- 11 is een deler van 99, want $99 = 11 \cdot 9$.
- 7 is geen deler van 17, want $17 = 7 \cdot \frac{17}{7}$ en $\frac{17}{7}$ is geen geheel getal.

4 Welke van de volgende beweringen is waar? $2|9$, $8|24$, $17|17$, $3|7$, $4|0$ en $100|25$.

5
a. Schrijf alle delers op van 24.

b. Schrijf alle delers op van 3.

c. Wat is het verschil tussen de antwoorden op de beide vorige vragen?

6 Hoeveel delers heeft een getal > 1 minimaal?

Er is een opmerkelijk verschil tussen de getallen 3 en 24. Het getal 24 heeft veel delers: 1, 2, 3, 4, 6, 8, 12 en 24.

Het getal 3 heeft maar twee delers: 1 en 3. In de laatste opgave heb je gezien dat elk getal > 1 minimaal twee delers heeft. 3 heeft dus het minimale aantal delers, namelijk 2. De delers 1 en 3 zijn eigenlijk "flauwe"delers: elk getal is immers deelbaar door het getal 1 en door zichzelf.
Een ***echte deler*** van een getal a is een deler van a die niet gelijk is aan 1 of aan a.

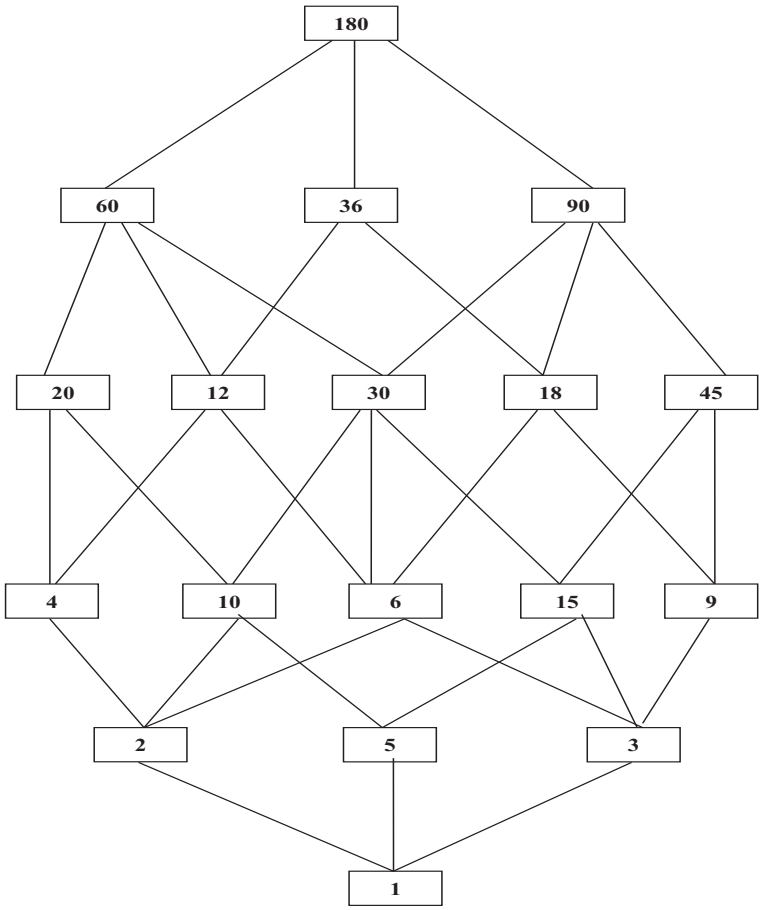
Voorbeelden

- 5 is een echte deler van 15.
- 7 is geen echte deler van 7.
- De echte delers van 24 zijn 2, 3, 4, 6, 8 en 12.
- Het getal 11 heeft geen echte delers.

7 Schrijf alle echte delers van 36 op.

8 Welke van de volgende getallen hebben geen echte delers? 7, 8, 9, 17, 18, 19.

Een getal > 1 zonder echte delers noemen we een ***priemgetal***.



Figuur 2.1 Alle delers van 180

.

In figuur 2.1 zie je een schematisch overzicht van alle delers van 180 (1, 2, 3, 4, 5 , 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90 en 180). Twee getallen zijn rechtstreeks met elkaar verbonden als het kleinste getal het grootste deelt, maar er geen delers "tussen zitten". Zo is er geen rechtstreekse verbinding van 10 en 180. 10 deelt weliswaar 180, maar bijvoorbeeld het getal 90 zit er tussen: 10 deelt 90 en 90 deelt zelf weer 180. In de op een na onderste laag zie je de getallen 2, 3 en 5. Dit zijn de enige priemgetallen die 180 delen. De priemgetallen 2, 3 en 5 heten

de **priemfactoren** van 180.

Het getal 3 is dus een priemgetal. Priemgetallen spelen een belangrijke rol in de getaltheorie. Ze zijn, zoals je hierboven hebt kunnen zien, eigenlijk de bouwstenen van de natuurlijke getallen. Maar ook buiten de getaltheorie spelen priemgetallen een belangrijke rol, bijvoorbeeld in tal van cryptografische systemen. Maar hoe vind je nu priemgetallen?

9 Probeer alle priemgetallen onder de 15 te vinden.

Waarschijnlijk is het je wel gelukt om alle priemgetallen onder de 15 te vinden met wat proberen. Je kunt systematischer op zoek gaan naar alle priemgetallen met behulp van ***de zeef van Eratosthenes***.
Schrijf de getallen 1, 2, enzovoort op. We gaan vervolgens langzamerhand de niet-priemgetallen doorstrepen en de priemgetallen markeren met het volgende ***algoritme***:

1. Streep het getal 1 door.
2. Het kleinste getal dat nog niet is doorgestreept of gemarkeerd gaan we nu markeren (bijvoorbeeld door het te omcirkelen). Dit getal is een priemgetal, zeg p.
3. Streep vervolgens alle echte veelvouden van p door (dus $2 \cdot p$, $3 \cdot p$, $4 \cdot p$, enzovoort)
4. Als je klaar bent met stap 3, ga dan weer verder met stap 2.

Figuur 2.2 De zeef van Eratosthenes toegepast op de getallen ≤ 50

Waarom werkt de zeef van Eratosthenes?

- Stel p is een priemgetal. Dan is het niet deelbaar door de getallen $1, 2, \ldots, p-1$. Het wordt dus niet doorgestreept als veelvoud van een kleiner getal.
- Stel k is geen priemgetal. Dan is het een veelvoud van een kleiner getal en zal dus worden doorgestreept.

10 Schrijf met behulp van de zeef van Eratosthenes alle priemgetallen onder de 150 op.

Kleine priemgetallen kun je dus vrij snel vinden met de zeef van Eratosthenes, maar grote priemgetallen is een ander verhaal. Hoe kun je bijvoorbeeld snel achterhalen of 1234561 een priemgetal is? Op de website https://nl.numberempire.com/primenumbers.php kun je een "Priemtest" vinden. Als je daar 1234561 invoert, dan zie je dat dit getal geen priemgetal is.

In de volgende paragraaf zullen we bewijzen dat er oneindig veel priemgetallen zijn. Met de zeef van Eratosthenes zal het erg omslachtig zijn om echt grote priemgetallen te ontdekken of van een groot getal uit te vissen of het wel of geen priemgetal is. In de getaltheorie zijn er in het verleden tal van methoden (***priemtesten*** genoemd) ontwikkeld om te bepalen of een getal wellicht priem is. Dit gaat buiten het bestek van deze module, maar op het internet kun je ongetwijfeld priemtesten en programmaatjes voor priemtesten vinden. Ook kun je op het internet programmaatjes vinden die werken als de zeef van Eratosthenes. Kijk bijvoorbeeld eens op https://www.visnos.com/demos/sieve-of-eratosthenes

2.2 Grootste gemene deler, kleinste gemene veelvoud en priemfactorontbinding

11 Schrijf de delers op van de getallen 20 en 28. Wat zijn de gemeenschappelijke delers? Wat is de grootste gemeenschappelijke deler?

De grootste gemeenschappelijke deler van twee getallen a en b wordt ook wel de ***grootste gemene deler*** van a en b genoemd. We schrijven ***ggd(a,b)***. In de vorige opgave heb je dus gezien dat ggd(20,28)=4.
Als de twee getallen groter worden, dan is het lastig om hun ggd te vinden door alle delers van beide getallen op te schrijven. Gelukkig zijn er een paar manieren om de ggd sneller te vinden.

12 Het getal 7 deelt de getallen 21 en 49.

a. Is 7 ook een deler van 49 + 21?

b. En van 49 − 21?

13 Het getal 4 deelt de getallen 20 en 44.

a. Is 4 ook een deler van 20 + 44?

b. En van 20 − 44?

Uit bovenstaande opgave kun je het vermoeden krijgen dat uit $d|a$ en $d|b$ volgt dat $d|(a+b)$ en $d|(a-b)$. We bewijzen dat in de volgende opgave.

14 Gegeven is $d|a$ en $d|b$ met $a < b$.

a. Waarom is $a = m \cdot d$ en $b = n \cdot d$ voor zekere gehele getallen m en n?

b. Druk $b + a$ en $b - a$ uit in m, n en d.

c. Waarom geldt nu $d|(b+a)$ en $d|(b-a)$?

Uit bovenstaande opgave kun je afleiden dat ggd(a,b)=ggd(a,$b-a$).

15 Stel $d_1 = \text{ggd}(a,b)$ en $d_2 = \text{ggd}(a,b-a)$.

a. d_1=ggd(a,b), dus $d_1|a$ en $d_1|b$. Waarom geldt nu ook $d_1|(b-a)$?

b. We weten nu dat $d_1|a$ en $d_1|(b-a)$, dus d_1 is een gemeenschappelijke deler van a en $b-a$. Waarom moet nu $d_1 \leq d_2$?

c. Op eenzelfde manier kun je ook beredeneren dat $d_2 \leq d_1$. Geef die redenering.

d. Welke conclusie kun je uit b. en c. samen trekken?

Nu zijn we in staat om de ggd van een paar getallen te vinden zonder alle delers te bepalen. Telkens trek je het kleinste getal af van het grootste getal.

Voorbeeld
ggd(420,246)=ggd(174,246)=ggd(174,72)=ggd(102,72)=ggd(30,72)=ggd(30,42)=ggd(30,12)=ggd(18,12)=ggd(6,12)=ggd(6,6)=6.

16 Bepaal op dezelfde manier ggd(20,28).

17 Bepaal zo ook ggd(177,15).

Misschien heb je bij het bepalen van ggd(177,15) wel gedacht over een nog snellere manier. Die is er: in plaats van ggd(177,15)=ggd(162,15)=. . . = ggd(12,15)=. . . had je ook in één keer ggd(177,15)=ggd(12,15) mogen schrijven door in één keer zo vaak mogelijk 15 af te trekken van 177. Als je 177 deelt door 15 is de rest 12. Dit betekent dat $177 = 11 \cdot 15 + 12$, dus $177 - 11 \cdot 15 = 12$. Vervolgens trek je zo vaak mogelijk 12 af van 15, enzovoort, tot je bij 0 bent aangekomen. Op deze manier bepaal je vrij snel de ggd met het zogenaamde ***algoritme van Euclides***.
Tegelijkertijd biedt het algoritme de kans om, bij goed boekhouden, de ggd te schrijven als een lineaire combinatie van de beide getallen. In de vorige opgave vond je ggd(177,15)=3 en je kunt met het algoritme van Euclides vrij snel vinden dat $3 = 12 \cdot 15 - 1 \cdot 177$.

Met $3 = 12 \cdot 15 - 1 \cdot 177$ schrijven we 3 als ***een lineaire combinatie van 15 en 177***.

Met de volgende voorbeelden van het algoritme van Euclides kun je waarschijnlijk wel begrijpen dat zoiets altijd mogelijk is en hoe het precies werkt. De eigenschap dat je de ggd van twee getallen altijd kunt schrijven als een lineaire combinatie van die getallen komt later ook van pas als we cryptografische systemen gaan bouwen.

Voorbeeld
We zoeken ggd(177,15) en willen deze schrijven als een lineaire combinatie van 177 en 15.
$177 - 11 \cdot 15 = 12$
$15 - 1 \cdot 12 = 3$
$12 - 4 \cdot 3 = 0$
Dus ggd(177,15)=3.

Terugrekenend krijgen we nu:
$3 = 15 - 1 \cdot 12$
$= 15 - 1 \cdot (177 - 11 \cdot 15)$
$= 15 - 1 \cdot 177 + 11 \cdot 15$
$= 12 \cdot 15 - 1 \cdot 177$
Dus ggd(177,15)=3 $= 12 \cdot 15 - 1 \cdot 177$

Voorbeeld
We zoeken ggd(2400,660) en willen deze schrijven als een lineaire combinatie van 2400 en 660.
$2400 - 3 \cdot 660 = 420$
$660 - 1 \cdot 420 = 240$
$420 - 1 \cdot 240 = 180$
$240 - 1 \cdot 180 = 60$
$180 - 3 \cdot 60 = 0$
Dus ggd(2400,660)=60.

Terugrekenend krijgen we nu:
$60 = 240 - 1 \cdot 180$
$= 240 - 1 \cdot (420 - 1 \cdot 240)$
$= 2 \cdot 240 - 1 \cdot 420$
$= 2 \cdot (660 - 1 \cdot 420) - 1 \cdot 420$
$= 2 \cdot 660 - 3 \cdot 420$
$= 2 \cdot 660 - 3 \cdot (2400 - 3 \cdot 660)$
$= 11 \cdot 660 - 3 \cdot 2400$
Dus ggd(2400,660)=60 $= 11 \cdot 660 - 3 \cdot 2400$

18 Bepaal ggd(420,5148) en schrijf deze als een lineaire combinatie van 420 en 5148.

19 Bepaal ggd(4284,924) en schrijf deze als een lineaire combinatie van 4284 en 924.

Op de website https://breukenrekenmachine.nl/grootste-gemene-deler.php kun je van twee in te voeren getallen a en b de ggd berekenen.

20 Welke van de volgende beweringen is waar? $6|8 \cdot 9$, $6|8$ en $6|9$

21 Welke van de volgende beweringen is waar? $7|21 \cdot 11$, $7|21$ en $7|11$.

In de vorige twee opgaven heb je gezien dat het getal 7 een product deelde én één van de factoren van dat product, namelijk 21. Voor het getal 6 was dat niet het geval: het deelde een product, maar geen van beide factoren. Dat is niet geheel toevallig:

Stelling.
Als een priemgetal p het product $a \cdot b$ van de getallen a en b deelt, dan móet het minstens één van beide factoren a of b delen.

We gaan deze stelling in de volgende opgave proberen te bewijzen.

22 Gegeven is een priemgetal p en twee getallen a en b met de eigenschap dat $p|a \cdot b$. Te bewijzen is dat dan geldt $p|a$ of $p|b$.

a. Stel $p|a$ is niet waar. Waarom is dan $\text{ggd}(p, a) = 1$?

b. Waarom kunnen we nu schrijven $1 = ak + pl$ voor zekere getallen k en l?

c. Maar dan is ook $b = abk + bpl$. Hoe volgt hier nu uit dat $p|b$? Conclusie?

23 Schrijf de getallen 12, 18 en 45 als een product van priemgetallen.

24 Kun je deze getallen ook nog op een andere manier schrijven als een product van priemgetallen?

Na het maken van de vorige opgaven zal de volgende stelling je hopelijk niet verrassen. Het bewijs geven we in de daarop volgende opgaven.

Stelling
Elk getal > 1 is op precies één manier te schrijven als een product van priemgetallen, de zogenaamde **priemfactorontbinding**.

Hierbij spreken we overigens af dat een product ook uit één factor mag bestaan, zodat een priemgetal ook een product van priemgetallen is.

25 Waarom kunnen we elk getal > 1 schrijven als een product van priemgetallen?

We weten nu dus dat ieder getal > 1 een priemfactorontbinding $p_1^{k_1} \dots p_n^{k_n}$ heeft. Nu moeten we nog bewijzen dat het er precies één heeft.

26 Stel dat een getal $a > 1$ twee priemfactorontbindingen $p_1^{k_1} \dots p_n^{k_n} = q_1^{l_1} \dots q_m^{l_m}$ heeft.

a. Waarom moet q_1 één van de priemgetallen $p_1, \dots, p_n$ zijn?

b. Zeg $q_1 = p_i$. Waarom geldt dan voor de bijbehorende exponenten $l_1 = k_i$?

c. Herhaal a. en b. voor de overige (als die er zijn) priemgetallen $q_2, \dots, q_m$. Kan er daarna nog een extra priemgetal p_i zijn die niet gelijk is aan één van de priemgetallen $q_1, \dots, q_m$? Conclusie?

27 Bepaal in elk van de volgende gevallen de priemfactorontbinding van de genoemde getallen en van hun ggd. Valt je wat op?

a. 40 en 28

b. 60 en 192

28 Bepaal de priemfactorontbinding van de getallen 13475 en 936 en van hun ggd. Valt je ook nu wat op?

Blijkbaar kun je ook met behulp van de priemfactorontbindingen de ggd van een paar getallen vinden. Neem van alle gemeenschappelijke priemfactoren de kleinste exponent. Dat geeft je de priemfactorontbinding van de ggd.
Hebben a en b geen gemeenschappelijke priemfactoren, dan is ggd$(a,b)=1$.

In formule: als $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ en $b = p_1^{l_1} p_2^{l_2} \dots p_n^{l_n}$ de priemfactorontbindingen zijn van a en b, dan geldt ggd$(a,b) = p_1^{\min\{k_1,l_1\}} p_2^{\min\{k_2,l_2\}} \dots p_n^{\min\{k_n,l_n\}}$.
Waarschijnlijk begrijp je wel wat we met $\min\{a,b\}$ bedoelen. Maar voor alle zekerheid: daarmee bedoelen we het kleinste van de twee getallen a en b, dus bijvoorbeeld $\min\{3,7\} = 3$.

Voorbeelden

- $420 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1$ en $5148 = 2^2 \cdot 3^2 \cdot 11^1 \cdot 13^1$,
  dus ggd$(420,5148) = 2^2 \cdot 3^1 = 12$. Reken dit na met het algoritme van Euclides.

- $924 = 2^2 \cdot 3^1 \cdot 7^1 \cdot 11^1$ en $4284 = 2^2 \cdot 3^2 \cdot 7^1 \cdot 17^1$,
  dus ggd(924,4284)=$2^2 \cdot 3^1 \cdot 7^1$=84. Reken ook dit na met het algoritme van Euclides.
- $195 = 3^1 \cdot 5^1 \cdot 13^1$ en $308 = 2^2 \cdot 7^1 \cdot 11^1$,
  dus ggd(195,308)=1. Reken ook dit na met het algoritme van Euclides.

29 Bepaal met behulp van de priemfactorontbindingen de ggd van 610 en 987.

30 Bepaal met behulp van de priemfactorontbindingen de ggd van 2382 en 237.

31 Zoals we hiervoor hebben gezien kun je behulp van de priemfactorontbindingen van de getallen a en b de priemfactorontbinding van de ggd van a en b vinden. Neem van elk der gemeenschappelijke priemfactoren van a en b de kleinste exponent. Het product van deze priemfactoren en exponenten is de priemfactorontbinding van ggd(a,b). Als a en b geen gemeenschappelijke priemfactoren hebben, dan is ggd(a,b)=1. Leg uit waarom dit zo moet zijn.

Ook het nemen van de grootste exponenten van **alle** priemfactoren geeft een getal wat je misschien wel eens hebt gezien.

32 Gegeven zijn $72 = 2^3 \cdot 3^2$ en $108 = 2^2 \cdot 3^3$.

a. Waarom is $216 = 2^3 \cdot 3^3$ een veelvoud van 72?

b. Waarom is $216 = 2^3 \cdot 3^3$ een veelvoud van 108?

c. 216 is dus een gemeenschappelijk veelvoud van 72 en 108. Zijn er kleinere gemeenschappelijke veelvouden?

Het getal dat je op deze manier vindt is blijkbaar het **kleinste gemene veelvoud** (genoteerd **kgv(a,b)**) van de getallen a en b.

Stelling
Als $a = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ en $b = p_1^{l_1} p_2^{l_2} \ldots p_n^{l_n}$ de priemfactorontbindingen zijn van a en b, dan geldt ggd(a,b)=$p_1^{\min\{k_1,l_1\}} p_2^{\min\{k_2,l_2\}} \ldots p_n^{\min\{k_n,l_n\}}$ en kgv(a,b)=$p_1^{\max\{k_1,l_1\}} p_2^{\max\{k_2,l_2\}} \ldots p_n^{\max\{k_n,l_n\}}$

33 Waarom vind je op deze manier het kleinste gemene veelvoud?

34 Bepaal kgv(420,5148), kgv(924,4284) en kgv(30,192).

35 Bereken in de volgende gevallen telkens $a \cdot b$ en ggd(a,b)·kgv(a,b).

a. a=420 en b=5148

b. a=924 en b=4284

c. a=30 en b=192

d. Wat valt je op aan de antwoorden bij a. t/m c.? Kun je dat verklaren?

Omdat altijd $\min\{a,b\} + \max\{a,b\} = a + b$ volgt uit bovenstaande stelling dat ook de volgende stelling geldt

Stelling Voor ieder paar getallen a en b geldt $a \cdot b$= ggd(a,b)·kgv(a,b).

36 Gebruik het feit dat je de ggd van twee getallen kunt schrijven als een lineaire combinatie van die twee getallen om de volgende eigenschap van de ggd te bewijzen:

Als ggd(k,n)=1 en ggd(m,n)=1, dan moet ggd(km,n)=1.

(Tip: $1 \cdot 1 = 1$)

37 Hoe kun je met het principe van de priemfactorontbinding de volgende eigenschap bewijzen?

Als ggd(m,n)=1, $m|a$ en $n|a$, dan geldt ook $m \cdot n$ is een deler van a.

Waarschijnlijk ben je (onbewust) de ggd en de kgv ook al tegengekomen op een ander gebied van de wiskunde. Bijvoorbeeld bij het rekenen met breuken. Als je breuken wilt optellen, dan moest ze je eerst gelijknamig maken. Meestal ging je dan op zoek naar de kgv van de noemers.

Voorbeeld

- $\frac{2}{15} + \frac{7}{12} = \frac{8}{60} + \frac{35}{60} = \frac{43}{60}$ (immers kgv(12,15)=60)
- We willen de son van de breuken $\frac{1}{2940}$ en $\frac{5}{280}$ uitrekenen.
  We bepalen daartoe eerst de kgv van de noemers: $2940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$ en $280 = 2^3 \cdot 5 \cdot 7$, dus kgv(2940,280)= $2^3 \cdot 3 \cdot 5 \cdot 7^2 = 5880$.
  Hiermee vinden we $\frac{1}{2940} + \frac{5}{280} = \frac{2}{5880} + \frac{105}{5880} = \frac{107}{5880}$.

38 Bereken de volgende sommen. Bepaal daartoe telkens eerst de kgv van de noemers.

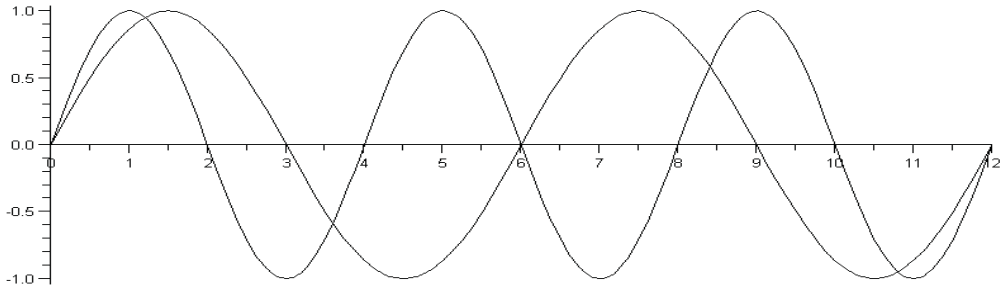
a. $\frac{5}{264} + \frac{7}{432}$

b. $\frac{3}{605} + \frac{6}{77}$

c. $\frac{13}{1155} + \frac{11}{910}$

Ook kun je de ggd en de kgv zijn tegengekomen in de goniometrie: als je twee periodieke functies met verschillende perioden optelt, dan krijg je weer een periodieke functie. De periode van deze somfunctie is de kgv van de twee perioden.

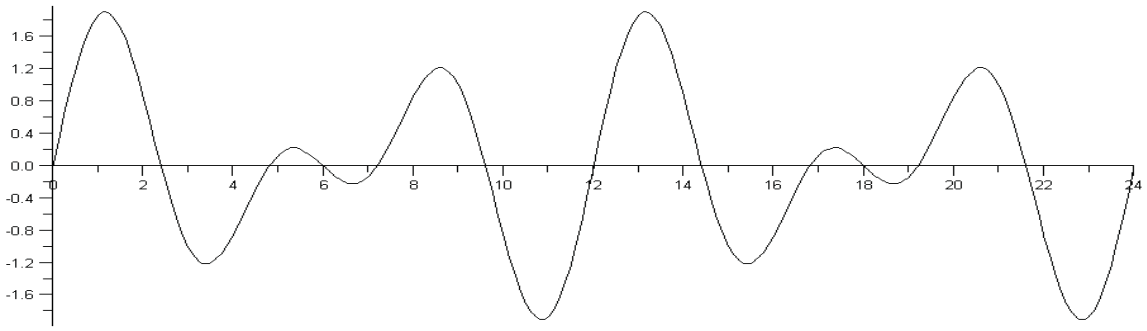
Voorbeeld
In figuur 2.3 zie je de grafieken van $f(x) = \sin \frac{1}{2}\pi x$ en $g(x) = \sin \frac{1}{3}\pi x$. f heeft periode 4, g heeft periode 6. Ook kun je zien dat kgv(4,6)=12. Figuur 2.4 toont de grafiek van $h(x) = \sin \frac{1}{2}\pi x + \sin \frac{1}{3}\pi x$. Je ziet dat deze functie periode 12 = kgv(4,6) heeft.



Figuur 2.3 De grafieken van $f(x) = \sin \frac{1}{2}\pi x$ en $g(x) = \sin \frac{1}{3}\pi x$

39 Waarom is de kgv van de twee perioden de periode van de somfunctie?

Meestal kun je de kgv van deze perioden overigens niet vinden door een priemfactorontbinding omdat de periode geen geheel getal of een geheel aantal keren π is. Je zult dan een aantal veelvouden van de perioden op moeten schrijven om de kgv te vinden. Zie de volgende voorbeelden. Je kunt natuurlijk met je GR controleren of de genoemde



Figuur 2.4 De grafiek van $h(x) = \sin\frac{1}{2}\pi x + \sin\frac{1}{3}\pi x$

periodes kloppen! Zou je bij het tweede voorbeeld in plaats van de kgv de ggd op de een of andere manier kunnen gebruiken?

Voorbeelden

- De periode van $f(x) = \sin\frac{1}{6}\pi x$ is 12,
  de periode van $g(x) = \cos\frac{1}{10}\pi x$ is 20.
  kgv(12,20) = 60, dus de periode van $h(x) = \sin\frac{1}{6}\pi x + \cos\frac{1}{10}\pi x$ is 60.
- De periode van $f(x) = \sin 8x$ is $\frac{2}{8}\pi = \frac{1}{4}\pi$,
  de periode van $g(x) = \cos 12x$ is $\frac{2}{12}\pi = \frac{1}{6}\pi$.
  De veelvouden van $\frac{1}{4}\pi$ zijn $\frac{1}{4}\pi = \frac{3}{12}\pi$, $\frac{2}{4}\pi = \frac{6}{12}\pi$, $\frac{3}{4}\pi = \frac{9}{12}\pi$, ...,
  de veelvouden van $\frac{1}{6}\pi$ zijn $\frac{1}{6}\pi = \frac{2}{12}\pi$, $\frac{2}{6}\pi = \frac{4}{12}\pi$, $\frac{3}{6}\pi = \frac{6}{12}\pi$, ...
  De kgv is dan $\frac{6}{12}\pi = \frac{1}{2}\pi$. Dus heeft $h(x) = \sin 8x + \cos 12x$ een periode $\frac{1}{2}\pi$.

40 Hoe zou je de ggd in plaats van de kgv kunnen gebruiken om de periode van $h(x)$ in het tweede voorbeeld hierboven te kunnen berekenen? (Hint: $\frac{1}{2}\pi = \frac{2\pi}{4}$) Kun je iets zeggen over wanneer je de kgv wilt gebruiken en wanneer je de ggd zou gebruiken?

41 Bepaal de periode van elk van de volgende functies.

a. $f(x) = \sin 16x + \sin 40x$

b. $g(x) = \cos\frac{1}{8}x + \cos\frac{1}{10}x$

c. $h(x) = \cos 22x + \sin 28x$

d. $j(x) = \cos\frac{2}{90}x + \sin\frac{1}{30}x$

Aan het eind van deze paragraaf gaan we nog even terug naar de priemgetallen zelf. We beweerden aan het eind van de vorige paragraaf dat er oneindig veel priemgetallen zijn. We geven in de volgende opgave het bewijs van Euclides voor deze bewering.

42 Stel er zijn maar eindig veel priemgetallen, n.l. $p_1, p_2, \ldots p_k$. We gaan dan kijken naar het getal $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

a. Waarom kan a geen priemgetal zijn?

b. Omdat a geen priemgetal is, is a deelbaar door een priemgetal, zeg p. Waarom?

c. Waarom moet nu $p|1$ en waarom kan dat niet?

d. Waarom kun je nu concluderen dat er oneindig veel priemgetallen zijn?

e. Zou deze redenering ook werken als je had gekeken naar het getal $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 5$? Zo ja, waarom wel? Zo nee, waarom niet?

Hoeveel priemgetallen zijn er dan?

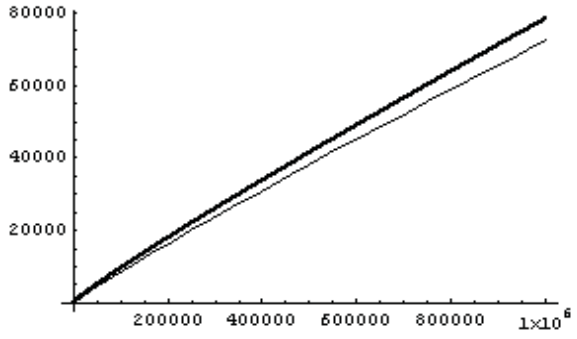
Er zijn dus oneindig veel priemgetallen. Maar zou je ze toch op de een of andere manier kunnen tellen? Hoeveel priemgetallen zijn er bijvoorbeeld kleiner dan 1 miljoen? Dan 1 miljard? Dan 10^{20}? Voor kleine getallen x zou je kunnen tellen hoeveel priemgetallen $\leq x$ er zijn. Maar voor grotere getallen is dat praktisch niet te doen.

Toch hebben Gauss (1792) en Legendre (1798) priemgetallen geteld. Hierdoor kregen zij het vermoeden dat als x steeds groter word, dan is het aantal priemgetallen $\leq x$ ongeveer gelijk aan $\frac{x}{\ln x}$.

Wiskundiger gezegd: als $\pi(x)$ het aantal priemgetallen $\leq x$ voorstelt, dan geldt $\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1$. In 1896 bleek het vermoeden juist doordat Hadamard en de la Vallée Poussin een bewijs leverden.

Hieronder zie je een tabelletje waarin $\pi(x)$ en $\frac{x}{\ln x}$ (afgrond op gehelen) voor een aantal waarden van x met elkaar worden vergeleken. Daaronder zie je de grafieken van $\pi(x)$ (de vette kromme) en $\frac{x}{\ln x}$.

x	$\pi(x)$	$\frac{x}{\ln x}$
10	4	4
100	25	22
1000	168	145
10000	1229	1086
100000	9592	8686
1000000	78498	72382
10000000	664579	620421
100000000	5761455	5428681



2.3 Modulorekenen

43 Het is nu 7 uur. Hoe laat is het over 8 uur? Hoe laat was het 10 uur geleden?

De berekeningen van opgave 40 zijn voorbeelden van **modulorekenen**, in dit geval modulo 12. Je telt gewoon op of trekt gewoon af, maar krijg je dan een antwoord onder 0 of boven 12, dan tel je er 12 bij of trek je er 12 af, zodat je weer tussen de 0 en 12 uitkomt. De berekeningen van opgave 40 schrijven we wiskundig als volgt op.

Voorbeelden

- $7 + 8 = 15 \equiv 3 \pmod{12}$ of korter: $7 + 8 \equiv 3 \pmod{12}$
- $7 - 10 = -3 \equiv 9 \pmod{12}$ of korter: $7 - 10 \equiv 9 \pmod{12}$

We zeggen dat twee gehele getallen a en b modulo 12 equivalent (gelijk) zijn als hun verschil deelbaar is door 12, notatie:

$$a \equiv b \pmod{12}.$$

Het getal 12 noemt men de **modulus**.

Aan deze afspraak zie je overigens dat het niet persé nodig is om tussen de 0 en de 12 uit te komen. Soms is het juist handiger om dat niet te doen, zie het laatste voorbeeld hieronder.

Voorbeelden

- $13 \equiv 1 \pmod{12}$
- $-2 \equiv 10 \pmod{12}$
- $13 \equiv 25 \pmod{12}$
- $11 \equiv -1 \pmod{12}$ en $11^2 \equiv (-1)^2 \equiv 1 \pmod{12}$

44 Bereken modulo 12:

a. 7+9

b. 3-11

c. 6+6

d. 3·7

e. 5·5

f. 5^2

g. 6^3

h. 5^5

45 Hoe zou je 5^3 modulo 15 berekenen?

Wat we hierboven modulo 12 en modulo 15 gezien hebben, kunnen we op dezelfde manier modulo ieder ander geheel getal doen.

Je zag het misschien al in de vorige opgave:

$$5^3 = 125 \equiv 5 \pmod{15},$$

want 125 – 5 = 120 kun je delen door 15.
Je trekt dus zo vaak mogelijk 15 van 125 af.

Door te bedenken dat 125 : 15 = 8 *rest* 5 had je het antwoord ook kunnen vinden . De rest 5 en het te delen getal 125 zijn dan equivalent modulo 15.

46 Waarom kun je het antwoord ook vinden door te delen met rest?

47 Omschrijf wat we bedoelen met $a \equiv b \pmod{k}$

48 Bereken:

a. $94 \pmod 3$

b. $94 \pmod 5$

c. $94 \pmod 7$

d. $17 + 39 \pmod{24}$

e. $3 - 41 \pmod{30}$

f. $26 + 26 \pmod{37}$

g. $3 \cdot 7 \pmod{14}$

h. $5 \cdot 19 \pmod{40}$

i. $3^2 \pmod 7$

j. $3^4 \pmod 7$

k. $2^2 \pmod 7$

In de laatste drie onderdelen van bovenstaande opgave heb je kunnen zien dat je in plaats van $3^4 \pmod 7$ direct uit te rekenen, net zo goed eerst $3^2 \equiv 2 \pmod 7$ kunt uitrekenen en daarna $2^2 \pmod 7$.

49

a. $3^2 \equiv 2 \pmod 7$ betekent dat 3^2 te schrijven valt als $3^2 = 2 + 7k$ voor een zeker geheel getal k. Gebruik dit om te laten zien dat $3^4 = (3^2)^2$ modulo 7 equivalent is met 2^2.

b. $17 \cdot 15 \equiv 7 \cdot 5 \pmod{10}$. Laat zien waarom, gebruik daarbij dat $17 \equiv 7 \pmod{10}$ en $15 \equiv 5 \pmod{10}$.

c. In het algemeen geldt iets soortgelijks. Waarom?

50 Bereken:

a. $23^4 \pmod{397}$

b. $23^8 \pmod{397}$

c. $23^{16} \pmod{397}$

d. $23^{32} \pmod{397}$

51 Bereken met behulp van je antwoorden uit de vorige opgave op een handige manier:

a. $23^{48} \pmod{397}$

b. $23^{56} \pmod{397}$

c. $23^{57} \pmod{397}$

Je kunt dus blijkbaar $23^{57} \pmod{397}$ handig en snel berekenen door te bedenken dat $23^{57} = 23^{32+16+8+1} = 23^{32} \cdot 23^{16} \cdot 23^8 \cdot 23^1$. Door telkens te kwadrateren reken je 23, 23^2, 23^4, 23^8, enzovoort snel uit. Gebruik telkens het antwoord modulo 397 om verder te gaan.

Voorbeeld
Bereken $2513^{79} \pmod{7193}$.
$2513^2 \equiv 6908 \pmod{7193}$
$2513^4 \equiv 6908^2 \equiv 2102 \pmod{7193}$
$2513^8 \equiv 2102^2 \equiv 1902 \pmod{7193}$
$2513^{16} \equiv 1902^2 \equiv 6718 \pmod{7193}$
$2513^{32} \equiv 6718^2 \equiv 2642 \pmod{7193}$
$2513^{64} \equiv 2642^2 \equiv 2954 \pmod{7193}$

$2513^{79} = 2513^{64} \cdot 2513^8 \cdot 2513^4 \cdot 2513^2 \cdot 2513$
$\equiv 2954 \cdot 1902 \cdot 2102 \cdot 6908 \cdot 2513$
$\equiv 775 \cdot 2102 \cdot 6908 \cdot 2513$
$\equiv 3432 \cdot 6908 \cdot 2513$
$\equiv 113 \cdot 2513$
$\equiv 3442 \pmod{7193}$

52 Bereken.

a. $97^{97} \pmod{1017}$

b. $891^{133} \pmod{907}$

c. $17^{117} \pmod{217}$

Ook voor modulorekenen zijn er websites, bijvoorbeeld https://planetcalc.com/8326/ Je kunt daar een getal a (al dan niet in de vorm van een uitdrukking zoals bijvoorbeeld 17^{117}) in-voeren en een modulus. De applet geeft je dan het antwoord. Je kunt dit bijvoorbeeld een paar keer proberen bij de vorige opgave.

53 Net als bij het "normale rekenen"kun je ook bij het modulorekenen vergelijkingen oplossen. Probeer bij elk van de volgende vergelijkingen maar eens een geheel getal x te zoeken dat aan de betreffende vergelijking voldoet.

a. $5x \equiv 3 \pmod{7}$

b. $7x + 5 \equiv 2x - 1 \pmod{9}$

c. $x^5 \equiv 10 \pmod{11}$

d. $5^x \equiv 4 \pmod{11}$

54 Zoek een geheel getal x dat voldoet aan *alle* onderstaande vergelijkingen.
$x \equiv 1 \pmod{2}$
$x \equiv 1 \pmod{3}$
$x \equiv 2 \pmod{5}$

Waarschijnlijk heb je de vergelijkingen uit de vorige opgaven kunnen oplossen door te proberen. Zo kun je bijvoorbeeld $7x + 5 \equiv 2x - 1 \pmod{9}$ oplossen door achtereenvolgens $0, 1, 2, \ldots, 8$ te proberen. Je ontdekt dan dat 6 een oplossing is. Maar zo'n lineaire vergelijking kan ook systematisch worden opgelost, zie de volgende voorbeelden.

Voorbeelden

- Los op: $5x + 2 \equiv 2x + 9 \pmod{11}$.
  We kunnen de vergelijking herschrijven tot: $3x \equiv 7 \pmod{11}$
  We zoeken nu een veelvoud van 3 equivalent met 1 mod 11
  Omdat $4 \cdot 3 = 12 \equiv 1 (\mathrm{mod} 11)$ gaan we met 4 vermenigvuldigen.
  We krijgen daardoor als oplossing: $x \equiv 28 \equiv 6 \pmod{11}$.

■ Los op: $14x + 2 \equiv 4x + 27 \pmod{35}$.

We kunnen de vergelijking herschrijven tot: $10x \equiv 25 \pmod{35}$

We kunnen nu door 5 delen en krijgen dan: $2x \equiv 5 \pmod{7}$

Daarna vermenigvuldigen we met 4, immers $4 \cdot 2 = 8 \equiv 1 (\text{mod} 7)$

Dit geeft de oplossing: $x \equiv 20 \equiv 6 \pmod{7}$.

55 a. In het tweede voorbeeld hierboven stond "We kunnen nu door 5 delen en krijgen dan: $2x \equiv 5 \pmod{7}$". Waarom kun je eigenlijk door 5 delen?

b. En hoe zit het met de vergelijking $10x \equiv 24 \pmod{35}$?

Lineaire vergelijkingen schrijf je dus eerst om naar de vorm $ax \equiv b \pmod{k}$. Als b een veelvoud is van de ggd van a en k, dan kun je alles door die ggd delen. Je krijgt dan een vergelijking $cx \equiv d \pmod{m}$. Nu is er een veelvoud van c die gelijk is aan 1 $\pmod{m}$, dus kun je via een geschikte vermenigvuldiging komen tot $x \equiv e \pmod{m}$, met andere woorden tot de oplossing.
Als b geen veelvoud is van de ggd van a en k, dan heeft de vergelijking geen oplossing.

56 a. Waarom is er een veelvoud van c dat gelijk is aan 1 $\pmod{m}$?

b. Waarom heeft de vergelijking geen oplossing als b geen veelvoud is van de ggd van a en k?

57 Los op.

a. $5x \equiv 3 \pmod{7}$

b. $7x + 5 \equiv 2x - 1 \pmod{9}$

c. $13x - 5 \equiv 3x + 7 \pmod{5}$

d. $7 + 14x \equiv 2x + 25 \pmod{30}$

Voor vergelijkingen als $x^5 \equiv 10 \pmod{11}$ en $5^x \equiv 4 \pmod{11}$ is er geen systematische aanpak, anders dan wat je waarschijnlijk al geprobeerd hebt, namelijk domweg alle mogelijkheden invullen. Maar als de getallen gigantisch groot worden, zoals bijvoorbeeld in $x^{4371} \equiv 34455 \pmod{99991}$ en $6^x \equiv 34455 \pmod{99991}$, is dat een langdurige klus. Dit soort vergelijkingen (het liefst met nog veel grotere getallen)

staan aan de basis van cryptografische systemen zoals we die in het volgende hoofdstuk zullen tegenkomen. Het feit dat deze vergelijkingen alleen zijn op te lossen door alle mogelijkheden langs te lopen maakt de cryptografische systemen praktisch niet te kraken. Alleen met extra informatie kun je de vercijferde boodschappen in dit soort systemen snel ontcijferen. Een deel van deze extra informatie wordt gevormd door de stellingen van Fermat en Euler, die we in de komende twee paragrafen zullen behandelen.

Een stelsel vergelijkingen als in opgave 50 is soms oplosbaar, bijvoorbeeld als voldaan is aan de

Chinese reststelling:
Als $m_1, m_2, \ldots, m_k$ moduli zijn waarbij elk tweetal ggd 1 heeft, dan heeft het stelsel

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

precies één oplossing modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

In de volgende opgave bewijs je dat er altijd zo'n x te vinden is. Verderop bewijzen we samen nog dat er modulo m ook maar één kan zijn.

58

a. Stel je voor dat je een x_1 kunt vinden met $x_1 \equiv a_1 \pmod{m_1}$ en $x_1 \equiv 0 \pmod{m_2}$, $x_1 \equiv 0 \pmod{m_3}$, ..., $x_1 \equiv 0 \pmod{m_k}$. Ook kun je een x_2 vinden met $x_2 \equiv a_2 \pmod{m_2}$ en $x_2 \equiv 0 \pmod{m_1}$, $x_2 \equiv 0 \pmod{m_3}$, ..., $x_2 \equiv 0 \pmod{m_k}$. En een x_3 met $x_3 \equiv a_3 \pmod{m_3}$ en $x_3 \equiv 0 \pmod{m_1}$, $x_3 \equiv 0 \pmod{m_2}$, ..., $x_3 \equiv 0 \pmod{m_k}$, enzovoort. Hoe kun je dan ook een x vinden die voldoet aan het gegeven stelsel vergelijkingen?

b. Nu gaan we proberen langzamerhand zo'n x_1 (en x_2, x_3, enzovoort) te vinden. Leg uit dat uit $x_1 \equiv 0 \pmod{m_2}$, $x_1 \equiv 0 \pmod{m_3}$, ..., $x_1 \equiv 0 \pmod{m_k}$ volgt dat x_1 een veelvoud moet zijn van $m_2 \cdot m_3 \cdot \ldots \cdot m_k$ (ofwel van $\frac{m}{m_1}$).

c. Moet nu altijd $\frac{m}{m_1} \equiv a_1 \pmod{m_1}$? Zo ja, waarom? Zo nee, geef een voorbeeld.

d. $\frac{m}{m_1}$ lijkt veel op de x_1 die we zoeken. Alleen moeten we nog zorgen dat x_1 equivalent met a_1 modulo m_1 is. Daartoe zoeken we eerst een b_1 zodat $b_1 \cdot \frac{m}{m_1} \equiv 1 \pmod{m_1}$. Waarom lukt dit altijd?

e. Waarom kunnen we nu $x_1 = a_1 \cdot b_1 \cdot \frac{m}{m_1} \pmod{m}$ nemen?

f. Hoe zou je nu $x_2, x_3, \ldots, x_k$ en x kunnen vinden?

Uit de vorige opgave volgt dat je de oplossing x van het stelsel kunt vinden door de volgende procedure.

1. Bepaal voor elke i het getal b_i zodat $b_i \cdot \frac{m}{m_i} \equiv 1 \pmod{m_i}$.
2. Bepaal vervolgens de getallen $x_i \equiv a_i \cdot b_i \cdot \frac{m}{m_i} \pmod{m}$.
3. Tenslotte bepaal je $x \equiv x_1 + x_2 + \ldots + x_k \pmod{m}$.

Voorbeeld
Los op:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

Oplossing:
Dus $a_1 = 1$, $a_2 = 2$, $a_3 = 2$, $m_1 = 2$, $m_2 = 3$ en $m_3 = 5$.

- $m = 2 \cdot 3 \cdot 5 = 30$
- Deel daarna m door elk der moduli: $\frac{m}{m_1} = \frac{30}{2} = 15$, $\frac{m}{m_2} = \frac{30}{3} = 10$ en $\frac{m}{m_3} = \frac{30}{5} = 6$
- Los nu achtereenvolgens op (bijvoorbeeld op de manier van opgave 54, telkens $\frac{m}{m_i} \cdot b_i \equiv 1 \pmod{m_i}$):

$$\begin{aligned} 15b_1 &\equiv 1 \pmod 2 \\ 10b_2 &\equiv 1 \pmod 3 \\ 6b_3 &\equiv 1 \pmod 5 \end{aligned}$$

- Dit geeft de oplossingen $b_1 \equiv 1 (\text{mod} 2)$, $b_2 \equiv 1 (\text{mod} 3)$ en $b_3 \equiv 1 (\text{mod} 5)$
- Dit geeft voor $x_1 \equiv 1 \cdot 1 \cdot 15 \equiv 15 (\text{mod} 30)$, $x_2 \equiv 2 \cdot 1 \cdot 10 \equiv 20 (\text{mod} 30)$ en $x_3 \equiv 2 \cdot 1 \cdot 6 \equiv 12 (\text{mod} 30)$
- We vinden nu $x = 15 + 20 + 12 = 47 \equiv 17 \pmod{30}$

Je kunt het stelsel uit dit voorbeeld ook op een andere manier oplossen. Misschien vind je de volgende manier wel handiger.

Uit $x \equiv 1 \pmod 2$ volgt dat $x = 1 + 2y$ voor een zeker getal y.
Substitutie van $x = 1 + 2y$ in $x \equiv 2 \pmod 3$ geeft $1 + 2y \equiv 2 \pmod 3$, ofwel $2y \equiv 1 \pmod 3$, en na vermenigvuldiging met 2, $y \equiv 4y \equiv 2 \pmod 3$.
Dit betekent dat $y = 2 + 3z$ voor een zeker getal z, ingevuld in $x = 1 + 2y$ geeft dan $x = 1 + 2(2 + 3z) = 5 + 6z$.
Substitutie van $x = 5 + 6z$ in $x \equiv 2 \pmod 5$ geeft $5 + 6z \equiv 2 \pmod 5$, ofwel $6z \equiv 2 \pmod 5$, en dus $z \equiv 6z \equiv 2 \pmod 5$.
Dit betekent dan $z = 2 + 5k$ voor een zeker getal k. Wanneer we dit invullen in $x = 5 + 6z$, dan krijgen we $x = 5 + 6(2 + 5k) = 17 + 30k$.
Ook hier vinden we dus de oplossing $x \equiv 17 \pmod{30}$

59 Los de volgende twee stelsels op, kies de manier die jij het handigst vindt.
a.

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 2 \pmod{11} \\ x &\equiv 1 \pmod{17} \\ x &\equiv 4 \pmod{19} \end{aligned}$$

b.

$$\begin{aligned} x &\equiv 2 \pmod 8 \\ x &\equiv 3 \pmod{15} \\ x &\equiv 4 \pmod 7 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

60 Grootvader heeft een zak vol toffees. Hij wil deze gelijkelijk verdelen onder een aantal kleinkinderen. Als hij de toffees verdeelt onder 3 kleinkinderen, dan houdt hij 2 toffees over. Verdeelt hij de toffees onder 7 kleinkinderen, dan houdt grootvader 1 toffee over. Worden 11 kleinkinderen getrakteerd, dan blijven er 3 toffees over. Hoeveel toffees zitten er minstens in de zak van grootvader?

61 We gaan nu bewijzen dat er modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ precies één oplossing is van het stelsel

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

als ggd(m_i, m_j)=1 voor ieder tweetal m_i en m_j.
Stel x en y zijn allebei oplossingen van het gegeven stelsel. Neem aan dat $x > y$.

a. Waarom is $x - y$ dan deelbaar door m_1?

b. Evenzo is $x - y$ dan deelbaar door $m_2, m_3, \ldots, m_k$. Waarom is $x - y$ dan ook deelbaar door m?

c. Leg nu uit waarom er precies één oplossing modulo m van bovengenoemd stelsel is.

In deze paragraaf heb je kennis gemaakt met het modulorekenen. Maar eigenlijk kende je het al, het dagelijkse rekenen met de klok is een voorbeeld. Maar ook eerder in deze module heb je eigenlijk al aan modulorekenen gedaan, namelijk bij de Caesarcode.

62 Leg uit hoe je de Caesarcode kunt zien als een voorbeeld van modulorekenen.

2.4 De kleine stelling van Fermat

Eeuwenlang heeft Pierre de Fermat (1601 – 1665) de wiskundigen bezig gehouden met het zoeken naar een bewijs voor zijn beroemde "stelling". De Fermat was jurist en deed daarnaast, als hobby, aan wiskunde. Hij bestudeerde oude Griekse wiskundige boeken. Als hij tijdens zijn studie bepaalde wiskundige zaken ontdekte, dan schreef hij deze ontdekkingen in het boek dat hij op dat moment bestudeerde. Op een gegeven moment ontdekte hij dat de vergelijking $x^n + y^n = z^n$ voor $n \geq 3$ geen flauwe oplossingen heeft: er zijn alleen gehele oplossingen met x, y en/of z gelijk aan 0. Deze bewering staat bekend als de **stelling van Fermat**. De Fermat beweerde voor deze stelling een wonderschoon bewijs te hebben, maar helaas was de kantlijn van het boek volgens hem te smal om het bewijs op te schrijven. Pas drieëneenhalve eeuw later is een bewijs gevonden. De Britse wiskundige Andrew Wiles haalde er in 1994 de voorpagina van de krant mee. Het bewijs van Wiles had echter nooit door De Fermat gegeven kunnen worden, de gebruikte wiskunde is zeer vergevorderd en is pas in de tweede helft van de 20^e eeuw ontwikkeld. Blijft natuurlijk de vraag of De Fermat echt een bewijs had en zo ja, of het correct was. In de eeuwen daarna hebben immers vele beroemde wiskundigen zich vergaloppeerd aan een bewijs: vaak dacht men dat men een bewijs had, maar bij nadere bestudering bleek altijd dat zo'n bewijs niet correct was.

In deze paragraaf gaat het niet over de beroemde stelling van Fermat, maar over de zogenaamde **kleine stelling van Fermat**. Eerst gaan we kijken naar een eigenschap van modulorekenen die bijzonder handig is als we de kleine stelling van Fermat willen gaan bewijzen.

63

a. Vermenigvuldig elk van de getallen 0, 1, 2, ..., 10 met 15 (mod 11).

b. Vermenigvuldig elk van de getallen 0, 1, 2, ..., 6 met 10 (mod 7).

c. Vermenigvuldig elk van de getallen 0, 1, 2, ..., 11 met 15 (mod 12).

d. Vermenigvuldig elk van de getallen 0, 1, 2, 3, 4 met 10 (mod 5).

e. Er is een opmerkelijk verschil tussen bovenstaande antwoorden. Welk?

64 In de vorige opgave heb je gezien dat soms alle producten verschillend zijn en soms niet.

a. Wat zou dat te maken kunnen hebben met de vermenigvuldigingsfactor en met de modulus?

b. Als je nu weet dat $15i \equiv 15j \pmod{11}$, wat weet je dan van de gehele getallen i en j ?

Het antwoord op de laatste vraag is een voorbeeld van de volgende eigenschap.

Eigenschap
Als p een priemgetal is en a een getal dat niet deelbaar is door p, dan volgt uit $ai \equiv aj \pmod{p}$ dat ook $i \equiv j \pmod{p}$.

In de volgende opgave gaan we proberen deze eigenschap te bewijzen. Daarna gaan we ons oriënteren op de kleine stelling van Fermat.

65 Gegeven zijn een priemgetal p en een getal a dat niet deelbaar is door p en voldoet aan $ai \equiv aj \pmod{p}$.

a. Waarom is p een deler van $ai - aj$?

b. Waarom is p dan een deler van $i - j$?

c. Hieruit volgt $i \equiv j \pmod{p}$. Laat zien hoe.

66 Bereken:

a. $15^{10} \pmod{11}$

b. $10^{6} \pmod{7}$

c. $15^{11} \pmod{12}$

d. $10^{4} \pmod{5}$

e. $6^{126} \pmod{127}$

67 In de vorige opgave kwam uit sommige berekeningen 1. Kun je zeggen wat er in dat geval aan de hand is met het grondtal en de modulus?

68 p is een priemgetal en a een getal dat niet deelbaar is door p.

a. We bekijken de getallen $1, 2, \ldots, p-1$. en gaan deze met a vermenigvuldigen. Wat kun je nu zeggen van de getallen $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a \pmod{p}$?

b. Waarom is nu $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot a \cdot 2 \cdot a \cdot \ldots \cdot (p-1) \cdot a \pmod{p}$?

c. Hoe volgt hieruit dat $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$?

d. Dit geeft $(1 - a^{p-1}) \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 0 \pmod{p}$. Wat betekent dit ook alweer?

e. Waarom moet nu $p \mid (1 - a^{p-1})$?

f. Wat betekent dit voor $a^{p-1} \pmod{p}$?

Met het maken van de vorige opgave heb je de kleine stelling van Fermat bewezen. Deze luidt dus als volgt.

Kleine stelling van Fermat.
Als p een priemgetal is en a een getal dat niet deelbaar is door p, dan geldt

$$a^{p-1} \equiv 1 \pmod{p}.$$

69 Bereken zo handig mogelijk (gebruik bijvoorbeeld de kleine stelling van Fermat):

a. $33^{96} \pmod{97}$

b. $57^{100} \pmod{101}$

c. $57^{101} \pmod{101}$

d. $57^{104} \pmod{101}$

e. $991^{1017} \pmod{1009}$

f. $871^{10000} \pmod{9973}$

g. $72^{443} \pmod{439}$

h. $991^{562} \pmod{563}$

2.5 De stelling van Euler

Het oplossen van een sudoku is een populaire bezigheid tegenwoordig. Een correct ingevulde sudoku is een voorbeeld van een Latijns vierkant. Latijnse vierkanten zijn ontwikkeld door de Zwitserse wiskundige Leonhard Euler (1707 – 1783). Euler werkte een groot deel van zijn leven in Rusland. Hij heeft in bijna alle takken van de wiskunde zijn sporen achtergelaten. Zelf ben je ongetwijfeld een aantal van deze sporen tegengekomen, bijvoorbeeld de notaties e en π voor de overbekende getallen (ongeveer 2.71828182845904... en 3.14159265358979...), de notatie $f(x)$ voor een functie en het Σ-teken als notatie voor een som. Hij hield zich onder meer bezig met analyse, meetkunde, mechanica en getaltheorie. Enorm veel wiskunde heeft Euler geproduceerd, indrukwekkend veel, zeker als je bedenkt dat hij lange tijd blind is geweest. In deze paragraaf staat één van zijn stellingen uit de getaltheorie centraal. Het is in feite een uitbreiding van de kleine stelling van Fermat uit de vorige paragraaf.

We beginnen met de zogenaamde **functie van Euler**. Voor een natuurlijk getal m is de functie $\phi(m)$ het aantal getallen uit $1, 2, \ldots, m$ die geen echte delers met m gemeen hebben, anders gezegd:

$$\phi(m) = \text{aantal getallen } i \text{ met de eigenschap } i \leq m \text{ én } \text{ggd}(i, m) = 1.$$

70 Bepaal in elk van de volgende gevallen $\phi(m)$ door te kijken hoeveel getallen i er zijn met $i \leq m$ én $\text{ggd}(i, m) = 1$:

a. $m = 7$

b. $m = 9$

c. $m = 10$

d. $m = 11$

e. $m = 21$

f. $m = 25$

71 a. In de vorige opgave waren twee van de getallen m priem. Wat valt je op aan hun $\phi(m)$? Zou dat toeval zijn? Zo nee, kun je de uitkomst verklaren?

b. Ook waren twee van de getallen m een kwadraat. Valt je ook iets op aan hun $\phi(m)$? Zo ja, kun je dat verklaren?

c. Tenslotte waren de andere twee getallen m het product van twee verschillende priemgetallen. Kun je ook iets zeggen (en misschien ook verklaren) over hun $\phi(m)$?

72 Als p een priemgetal is, welke van de getallen $1, 2, \ldots, p$ hebben dan een ggd gelijk aan 1 met p? Waarom geldt nu $\phi(p) = p - 1$?

73 We gaan uitzoeken hoe we handig $\phi(m)$ kunnen uitrekenen als m het product is van twee verschillende priemgetallen.

a. Wat is de priemfactorontbinding van het getal 10?

b. Hoeveel van de getallen $1, 2, \ldots, 10$ zijn deelbaar door 2? Hoeveel deelbaar door 5?

c. Hoeveel van de getallen $1, 2, \ldots, 10$ hebben dus ggd gelijk aan 1 met 10? Wat is dus $\phi(10)$?

d. Wat is de priemfactorontbinding van het getal 21?

e. Hoeveel van de getallen $1, 2, \ldots, 21$ zijn deelbaar door 3? Hoeveel deelbaar door 7?

f. Hoeveel van de getallen $1, 2, \ldots, 21$ hebben dus ggd gelijk aan 1 met 21? Wat is dus $\phi(21)$?

g. Stel $m = p \cdot q$ is het product van twee verschillende priemgetallen p en q. Hoeveel van de getallen $1, 2, \ldots, p \cdot q$ zijn er deelbaar door p? Hoeveel door q?

h. Hoeveel van de getallen $1, 2, \ldots, p \cdot q$ hebben dus ggd gelijk aan 1 met $p \cdot q$? Wat is dus $\phi(p \cdot q)$? Kun je dat herleiden tot $(p-1)(q-1)$?

74 We zoeken nu ook uit hoe we handig $\phi(m)$ kunnen uitrekenen als m het kwadraat of een hogere macht van een priemgetal is.

a. Wat is de priemfactorontbinding van het getal 9?

b. Hoeveel van de getallen $1, 2, \ldots, 9$ zijn deelbaar door 3?

c. Hoeveel van de getallen $1, 2, \ldots, 9$ hebben dus ggd gelijk aan 1 met 9? Wat is dus $\phi(9)$?

d. Wat is de priemfactorontbinding van het getal 25?

e. Hoeveel van de getallen $1, 2, \ldots, 25$ zijn deelbaar door 5?

f. Hoeveel van de getallen $1, 2, \ldots, 25$ hebben dus ggd gelijk aan 1 met 25? Wat is dus $\phi(25)$?

g. Stel $m = p^2$ is het kwadraat van een priemgetal p. Hoeveel van de getallen $1, 2, \ldots, p^2$ zijn er deelbaar door p?

h. Hoeveel van de getallen $1, 2, \ldots, p^2$ hebben dus ggd gelijk aan 1 met p? Wat is dus $\phi(p^2)$? Kun je dat herleiden tot $p(p-1)$?

i. Stel $m = p^k$ is een macht van een priemgetal p. Hoeveel van de getallen $1, 2, \ldots, p^k$ zijn er deelbaar door p?

j. Hoeveel van de getallen $1, 2, \ldots, p^k$ hebben dus ggd gelijk aan 1 met p? Wat is dus $\phi(p^k)$? Kun je dat herleiden tot $p^{k-1}(p-1)$?

We hebben nog één stap nodig om $\phi(m)$ voor elk getal m tamelijk eenvoudig te kunnen uitrekenen. Deze laatste stap zetten we in de volgende opgave.

75 Gegeven zijn twee getallen m en n met ggd(m,n)=1.

a. Hoeveel getallen a zijn er kleiner dan m die geen echte deler met m gemeen hebben? En hoeveel getallen b zijn er kleiner dan n die geen echte deler met n gemeen hebben?

b. Hoeveel verschillende stelsels

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

met $a < m$, ggd(a,m)= 1, $b < n$ en ggd(b,n)= 1 zijn er dus mogelijk?

c. Voor elk dergelijk stelsel is er precies één oplossing x die kleiner is dan mn en geen echte deler met mn gemeen heeft. Waarom?

d. Voor elke x kleiner dan mn die geen echte deler met mn gemeen heeft, hoort precies één stelsel als in vraag b. Waarom?

e. Hoe volgt nu uit het bovenstaande dat $\phi(mn) = \phi(m)\phi(n)$?

76 Gegeven is de priemfactorontbinding van het getal $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$. Dan volgt uit de vorige opgaven dat

$$\phi(n) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1) \cdot \ldots \cdot p_k^{a_k-1}(p_k-1).$$

Leg uit hoe.

77 Bereken:

a. $\phi(32)$

b. $\phi(72)$

c. $\phi(1976)$

d. $\phi(96)$

e. $\phi(3232)$

f. $\phi(3600)$

g. $\phi(12345)$

h. $\phi(543210)$

78 Bereken:

a. $11^{\phi(32)} \pmod{32}$

b. $11^{\phi(72)} \pmod{72}$

c. $6^{\phi(72)} \pmod{72}$

d. $6^{\phi(96)} \pmod{96}$

e. $13^{\phi(32)} \pmod{32}$

f. $7^{\phi(48)} \pmod{48}$

g. $7^{\phi(56)} \pmod{56}$

h. $11^{\phi(100)} \pmod{100}$

79 Kun je aangeven wanneer het antwoord in de vorige opgave 1 was en wanneer niet?

In de vorige opgaven hebben we je op het spoor gezet van de

Stelling van Euler
Als ggd(a,m)=1, dan geldt dat $a^{\phi(m)} \equiv 1 \pmod{m}$.

Het bewijs van de stelling van Euler gaat op dezelfde wijze als het bewijs van de kleine stelling van Fermat. We geven dat bewijs in de volgende opgave.

80 Gegeven zijn de getallen a en m met ggd(a,m)=1.

a. We bekijken de collectie G van die $\phi(m)$ getallen uit $1, 2, \ldots, m-1$ die geen echte deler met m gemeen hebben. Elk getal uit deze collectie G wordt vermenigvuldigd met a, zo ontstaat een nieuwe collectie P. Waarom zijn deze twee collecties modulo m dezelfde?

b. We nemen het product g van alle getallen uit de collectie G en het product p van alle getallen uit de collectie P. Waarom is modulo m p gelijk aan g?

c. Hoe volgt hieruit dat $a^{\phi(m)} \cdot g \equiv g \pmod{m}$?

d. Dit geeft $(1 - a^{\phi(m)}) \cdot g \equiv 0 \pmod{m}$. Wat betekent dit ook alweer?

e. Waarom moet nu $a^{\phi(m)} \equiv 1 \pmod{m}$?

81 Bereken zo handig mogelijk door de stelling van Euler te gebruiken:

a. $5^{1008} \pmod{3528}$

b. $5^{1010} \pmod{3528}$

c. $5^{1017} \pmod{3528}$

d. $7^{320} \pmod{880}$

e. $7^{322} \pmod{880}$

f. $2^{3961} \pmod{7623}$

g. $3^{20000} \pmod{26299}$

82 Bereken zo handig mogelijk door de stelling van Euler of de kleine stelling van Fermat te gebruiken:

a. $25^{507} \pmod{637}$

b. $90^{513} \pmod{637}$

c. $7^{1573} \pmod{1573}$

d. $9^{1573} \pmod{1571}$

e. $10^{1575} \pmod{1571}$

f. $28^{25000} \pmod{49005}$

g. $28^{50000} \pmod{49005}$

h. $28^{47600} \pmod{49005}$

i. $5^{3200} \pmod{3528}$

j. $5^{4032} \pmod{3528}$

83 Geef de laatste 3 cijfers van:

a. 3^{400}

b. 27^{513}

c. 19^{1002}

d. 33^{1513}

2.6 Samenvatting getaltheorie

1 Afspraak: als we in dit dictaat in hoofdstuk 2 of 3 over getallen spreken, dan bedoelen we daar natuurlijke getallen mee, tenzij anders aangegeven.

Getallen kun je delen met rest ($11 : 4 = 2$ met rest 3). Je kunt zo'n deling handig uitvoeren met een staartdeling.

Een getal a heet deelbaar door een getal b als er een getal k is met de eigenschap dat $a = b \cdot k$.

Notatie: $b|a$.

We zeggen ook wel dat b a deelt, dat b een deler is van a, of dat a een veelvoud is van b.

Een echte deler van een getal a is een deler van a die niet gelijk is aan 1 of aan a.

Een priemgetal is een getal zonder echte delers.

Met de zeef van Eratosthenes kun je priemgetallen vinden.

2 De grootste gemene deler van twee getallen a en b is hun grootste gemeenschappelijke deler. Notatie: ggd(a,b).

Het kleinste gemene veelvoud van twee getallen a en b is hun kleinste positieve gemeenschappelijke veelvoud. Notatie: kgv(a,b).

De ggd van de getallen a en b kun je vinden met behulp van het algoritme van Euclides. Dit algoritme biedt tegelijkertijd de kans om de ggd te schrijven als een lineaire combinatie van de getallen a en b.

Als een priemgetal p een product $a \cdot b$ van getallen a en b deelt, dan móet het minstens één van beide factoren a of b delen.

Elk getal is op precies één manier te schrijven als een product van priemgetallen, de zogenaamde priemfactorontbinding.

Met behulp van de priemfactorontbinding van de getallen a en b kun je vrij snel de ggd en de kgv van deze getallen bepalen:
Als $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ en $b = p_1^{l_1} p_2^{l_2} \dots p_n^{l_n}$ de priemfactorontbindingen zijn van a en b, dan geldt $\text{ggd}(a,b) = p_1^{\min\{k_1,l_1\}} p_2^{\min\{k_2,l_2\}} \dots p_n^{\min\{k_n,l_n\}}$ en $\text{kgv}(a,b) = p_1^{\max\{k_1,l_1\}} p_2^{\max\{k_2,l_2\}} \dots p_n^{\max\{k_n,l_n\}}$

Voor ieder paar getallen a en b geldt $a \cdot b = \text{ggd}(a,b) \cdot \text{kgv}(a,b)$.

Er zijn oneindig veel priemgetallen.

3 Twee gehele getallen a en b heten modulo een geheel getal k equivalent (gelijk) als hun verschil $a - b$ deelbaar is door k. Notatie: $a \equiv b \pmod{k}$.

Als je het gehele getal a door het gehele getal k deelt en de rest is b, dan is $a \equiv b \pmod{k}$

Modulo k zijn grote machten van een getal a gemakkelijk uit te rekenen door achtereenvolgens $a^2, a^4 = (a^2)^2, a^8 = (a^4)^2$, enzovoort direct modulo k te berekenen en daarna gebruik te maken van $a^p \cdot a^q = a^{p+q}$.

Lineaire vergelijkingen van de vorm $ax \equiv b \pmod{k}$ zijn oplosbaar als b een veelvoud is van $\text{ggd}(a,k)$. Je kunt dan alles door die ggd delen. Je krijgt dan een vergelijking $cx \equiv d \pmod{m}$. Nu is er een veelvoud van c die gelijk is aan 1 (mod m), dus kun je via een geschikte vermenigvuldiging komen tot $x \equiv e \pmod{m}$, met andere woorden tot de oplossing. Als b geen veelvoud is van $\text{ggd}(a,k)$, dan is de vergelijking niet oplosbaar.

Chinese reststelling: Als $m_1, m_2, \ldots, m_k$ moduli zijn waarbij elk tweetal ggd 1 heeft, dan heeft het stelsel

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

precies één oplossing modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

4 Als p een priemgetal is en a een getal dat niet deelbaar is door p, dan volgt uit $ai \equiv aj \pmod{p}$ dat ook $i \equiv j \pmod{p}$.

Kleine stelling van Fermat: Als p een priemgetal is en a een getal dat niet deelbaar is door p, dan geldt

$$a^{p-1} \equiv 1 \pmod{p}$$

5 Voor een getal m is de functie van Euler

$$\phi(m) = \text{aantal getallen } i \text{ met de eigenschap } i \leq m \text{ én } \text{ggd}(i, m) = 1.$$

Als van het getal n de priemfactorontbinding gelijk is aan $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, dan geldt voor $\phi(n)$:

$$\phi(n) = p_1^{a_1-1}(p_1 - 1)p_2^{a_2-1}(p_2 - 1)\ldots p_k^{a_k-1}(p_k - 1).$$

Stelling van Euler: Als ggd(a,m)=1, dan geldt dat $a^{\phi(m)} \equiv 1 \pmod{m}$.

2.7 Gemengde opgaven getaltheorie

84 Bereken met een staartdeling en geef ook de rest:

a. 7890 : 313

b. 212565 : 47

c. 18394503 : 3949

d. 29102834 : 701

85 Bepaal van de volgende paren getallen telkens de ggd en schrijf deze als een lineaire combinatie van die twee getallen.

a. 2714 en 2942

b. 3213 en 9972

c. 2445 en 4035

d. 2761 en 3311

e. 1414 en 4228

f. 12345 en 54321

g. 10101 en 456

h. 9172 en 5364

86 Bepaal voor elk van de volgende paren getallen de priemfactorontbinding van beide getallen en met behulp daarvan de ggd en de kgv van het paar.

a. 35640 en 1907400

b. 166320 en 2608515

c. 1524 en 254

87 Bereken:

a. $47^{19} \pmod{45}$

b. $231^{29} \pmod{2001}$

c. $764^{121} \pmod{3101}$

d. $291^{322} \pmod{100}$

e. $95^{99} \pmod{97}$

f. $39^{85} \pmod{200}$

g. $74^{51} \pmod{105}$

h. $19^{919} \pmod{91}$

88 Los de volgende vergelijkingen op.

a. $17x - 8 \equiv 10x + 10 \pmod{45}$

b. $6x + 14 \equiv 2x + 23 \pmod{31}$

c. $-2x + 8 \equiv 18x - 21 \pmod{51}$

d. $11x - 34 \equiv 4x + 22 \pmod{5}$

e. $79x + 53 \equiv 32x + 1 \pmod{95}$

f. $7x + 8 \equiv 10x - 34 \pmod{117}$

89 Los de volgende stelsels op.

a. $4x \equiv 2 \pmod{5}$
$5x \equiv 1 \pmod{7}$
$6x \equiv 7 \pmod{11}$

b. $7x \equiv 0 \pmod{2}$
$2x \equiv 1 \pmod{11}$
$3x \equiv -1 \pmod{19}$

c. $4x \equiv 2 \pmod{6}$
$21x \equiv 0 \pmod{35}$
$8x \equiv 6 \pmod{17}$

90 Bepaal de rest als je 20^{2003} deelt door 7.

91 a. Wat is het laatste cijfer van het getal $1! + 2! + \ldots + 100!$?

b. Wat zijn de laatste twee cijfers van het getal $1! + 2! + \ldots + 100!$?

c. Wat zijn de laatste drie cijfers van het getal $1! + 2! + \ldots + 100!$?

92 a. Toon aan dat je het getal $53^{103} + 103^{53}$ kunt delen door 13.

b. Toon aan dat je het getal $143^{32} + 143^{23}$ kunt delen door 7.

c. Is $9^{244} - 4^{124}$ deelbaar door 13?

93 Er is een mooie en snelle manier om te zien of een getal deelbaar is door 3: een getal is deelbaar door 3 precies dan als de som van zijn cijfers deelbaar is door 3. Zo is 12345 deelbaar door 3, want $1+2+3+4+5 = 15$ is deelbaar door 3. Maar 23456 is niet deelbaar door 3, want $2+3+4+5+6 = 20$ is het ook niet. In deze opgave zul je moeten uitleggen waarom deze methode werkt.

a. Bereken $10 \pmod 3$, $10^2 \pmod 3$, $10^3 \pmod 3$.

b. Wat kun je zeggen van $10^k \pmod 3$ als k positief en geheel is?

c. Waarom is nu $34567 \equiv 3 + 4 + 5 + 6 + 7 \pmod 3$? Waarom zijn nu 34567 en $3 + 4 + 5 + 6 + 7$ allebei deelbaar door 3 of allebei niet deelbaar door 3?

d. Waarom werkt de bovengenoemde methode nu altijd?

e. Gebruik bovenstaand idee om een snelle manier te vinden waarmee je kunt bepalen of een getal deelbaar is door 9 of niet.

f. Doe hetzelfde voor deelbaarheid door 11.

94 Zijn de volgende getallen deelbaar door 3, 9 en/of 11?

a. 908318861

b. 146687830

c. 514701951

d. 405809642

e. 733812312

f. 43991981

g. 339362586

h. 995466340

95 Soms kun je met modulorekenen laten zien dat een vergelijking geen gehele oplossingen heeft. In deze opgave zie je hoe dat gaat.

a. Wat zijn de mogelijke uitkomsten van $x^2 \pmod{12}$ voor $x = 0, 1, 2, \ldots, 11$?

b. Wat zijn de mogelijke uitkomsten van $5x^2 \pmod{12}$?

c. Wat zijn de mogelijke uitkomsten van $8x \pmod{12}$?

d. Wat zijn dan de mogelijke uitkomsten van $5x^2 + 8x \pmod{12}$?

e. Waarom kunnen er nu geen gehele oplossingen zijn van $5x^2 + 8x = 23$?

96 Probeer op een soortgelijke wijze te laten zien dat de volgende vergelijkingen geen gehele oplossingen hebben.

a. $3x^2 + 14 = y^2$. (Tip: werk modulo 3)

b. $7x^3 + 5 = y^3$. (Tip: werk modulo 7)

c. $x^2 + y^2 = n$ als $n \equiv 3 \pmod{4}$.

97 Laat zien dat $x^2 + y^2 = z^2$ geen gehele oplossingen heeft met z even en ggd(x,y,z)=1. Werk modulo 4.

Hoofdstuk 3

Moderne cryptografische systemen

3.1 Openbare en geheime sleutels

1 Alice en Bob spelen een merkwaardig spel. Alice heeft een functie, vult een voor Bob geheim getal in en vertelt daarna de functie en de uitkomst aan Bob. Bob moet achterhalen welk getal Alice heeft ingevuld. Wat is in elk der volgende gevallen het getal dat Bob moet noemen? Hoe pakt Bob het slim aan?

a. $f(x) = 5x$, uitkomst is 20.

b. $f(x) = x^2$ voor $x \geq 0$, uitkomst is 119.

c. $f(x) = \mathrm{e}^x$, uitkomst is 7.

Als Bob het slim aanpakt, dan gebruikt hij de inverse functie. De inverse functie f^{inv} van een functie heft namelijk de werking van de functie f op. Zo is

- $f^{\text{inv}}(x) = \frac{x}{5}$ voor $f(x) = 5x$ en $f^{\text{inv}}(f(x)) = \frac{5x}{5} = x$;
- $f^{\text{inv}}(x) = \sqrt{x}$ (mits $x \geq 0$) voor $f(x) = x^2$ en $f^{\text{inv}}(f(x)) = \sqrt{x^2} = x$;
- $f^{\text{inv}}(x) = \ln x$ voor $f(x) = \mathrm{e}^x$ en $f^{\text{inv}}(f(x)) = \ln \mathrm{e}^x = x$.

Inverse functies kunnen bijzonder interessant zijn voor cryptografische systemen.

2 Waarom zouden inverse functies interessant kunnen zijn voor cryptografische systemen?

3 Alice zit samen met haar vriend Bob en haar kleine zusje Eva in de kamer. Alice wil Bob haar onvoldoende cijfer voor een proefwerk Frans vertellen, maar wil niet dat Eva het cijfer te weten komt. Eva zit in 2 vwo en kent dus het getal e nog niet. Hoe zou Alice dat feit kunnen gebruiken om Bob haar cijfer te vertellen? Wat moet Bob daarna doen om het cijfer echt te weten?

In feite is de situatie van opgave 3 redelijk kenmerkend voor het zogenaamde ***Public key systeem***, bedacht door de Amerikanen Diffie en Hellman. Alice vertelt Bob dat ze $f(x) = e^x$ heeft gebruikt en het resultaat, bijvoorbeeld $e^{4,3} \approx 73,7$. Ze vertelt dus haar sleutel en de cijfertekst, Bob gebruikt de inverse functie $f^{\text{inv}}(x) = \ln x$ en berekent $\ln 73,7 \approx 4,300003$ en weet dat Alice dus een 4,3 heeft gehaald. Eva weet nog niet (ze zit immers pas in 2 vwo) dat ze $f^{\text{inv}}(x) = \ln x$ moet gebruiken om het cijfer uit te rekenen. En toch weet Eva best veel: de cijfertekst en de sleutel waarmee de boodschap is vercijferd!
In het public key systeem heeft iedere deelnemer twee sleutels: een ***openbare*** sleutel die iedereen kan opzoeken in een lijst en een ***geheime*** sleutel, die alleen de eigenaar kent. De twee sleutels van een eigenaar zijn elkaars inverse: ze heffen elkaars werking op.

4 Alice en Bob doen beiden mee aan een public key systeem. De openbare sleutel van Alice noemen we O_A, haar geheime sleutel noemen we G_A. Op dezelfde manier noemen we de sleutels van Bob O_B en G_B.

a. Alice wil Bob een boodschap (die we voor het gemak maar even x noemen) sturen. Alleen Bob moet die kunnen lezen. Welke sleutel(s) gebruikt ze en hoe?

b. Alice wil Bob een boodschap (y) sturen en garanderen dat de boodschap van haar afkomstig is en niet van iemand anders. Welke sleutel(s) gebruikt ze en hoe?

c. Alice wil Bob een boodschap (z) sturen. Alleen Bob moet het kunnen lezen en er tegelijkertijd van overtuigd zijn dat de boodschap alleen van Alice afkomstig kan zijn. Welke sleutel(s) gebruikt ze en hoe?

5 Hoe kan Eva bij elk van de situaties in opgave 4 Alice en Bob dwars zitten, dus een geheime boodschap lezen of een boodschap sturen die zogenaamd van Alice afkomstig is?

Bij het Public key systeem heeft iedere deelnemer dus twee sleutels, een openbare en een geheime. Deze twee sleutels zijn elkaar inverse. Als de geheime sleutel van een deelnemer bekend wordt, dan lopen boodschappen van en naar deze deelnemer gevaar. Bij het Public key systeem moeten we er dus voor zorgen dat uit de kennis van een openbare sleutel (want die kent men immers!) niet of (als het echt niet anders kan) op een zéér, zéér moeilijke en tijdrovende manier de inverse, de geheime sleutel, is te achterhalen. Het RSA-systeem waar we in de volgende paragraaf naar gaan kijken is een Public key systeem. De sleutels worden daar gemaakt met behulp van de in het vorig hoofdstuk ontwikkelde getaltheorie.
Overigens zijn ook de namen van de personen in deze paragraaf niet geheel toevallig zo gekozen. Meestal worden de personen die met elkaar communiceren in een cryptografisch systeem Bob en Alice genoemd. De persoon die wil afluisteren (maar dat uiteraard niet moet kunnen) wordt doorgaans Eva (of Eve) genoemd.

3.2 RSA

In 1978 ontwikkelden R.L. Rivest, A. Shamir en L. Adleman een cryptografisch systeem gebaseerd op de ideeën van het Public key systeem. Het systeem is genoemd naar zijn ontwikkelaars: het RSA-systeem. Het maakt gebruik van de getaltheorie die ontwikkeld is in het vorige hoofdstuk en dan met name van de stelling van Euler.

6 Stel je voor dat Bob Alice een boodschap x wil sturen. Hij mailt haar een berichtje dat hij een boodschap zal gaan sturen. Alice zendt hem twee getallen e en n met de opdracht om $y = x^e \bmod n$ terug te sturen. Als Bob dit gedaan heeft, dan weet zij natuurlijk e en n, maar ook hoe y is berekend. Zij kan dan x terugvinden door gebruik te maken van de stelling van Euler. Zou je kunnen vertellen hoe? En kan dat voor alle e?

De getallen e en n zullen straks samen de openbare sleutel van Alice in het RSA-systeem vormen.
De stelling van Euler zegt dat als ggd(a,m)=1, dan geldt dat $a^{\phi(m)} \equiv 1 \pmod{m}$. Dus voor onze x, e en n krijgen we dan $x^{\phi(n)} \equiv 1 \bmod n$, mits de ggd($x$,$n$)=1.
Als we nu een d kunnen vinden zodanig dat $de \equiv 1 \bmod \phi(n)$, dan krijgen we voor een zeker getal k dat $de = k \cdot \phi(n) + 1$.

7 Bereken voor deze d de uitkomst van $(x^e)^d \bmod n$ en vereenvoudig dit zover mogelijk. Conclusie?

De boodschap x, die Bob wil versturen aan Alice, verstuurt hij als $y = x^e (\bmod n)$. Alice berekent dan $y^d (\bmod n)$, wat x op zal leveren als $de = k \cdot \phi(n) + 1$. Daarom moet ggd(e,$\phi(n)$)=1 zijn.

8

a. Waarom moet ggd(e,$\phi(n)$)=1 zijn?

b. Hoe kun je dat gebruiken om d te vinden, als je $\phi(n)$ en e kent?

c. Je kunt d ook vinden met de stelling van Euler. Hoe?

Als $\phi(n)$ bekend is, dan kun je dus tamelijk eenvoudig d vinden, bijvoorbeeld door het algoritme van Euclides toe te passen op e en $\phi(n)$.
Je kunt ook de stelling van Euler gebruiken.
We weten dat $de = k\phi(n) + 1$, ofwel $de \equiv 1 \pmod{\phi(n)}$
Omdat ggd(e,$\phi(n)$)=1 geldt $e^{\phi(\phi(n))} \equiv 1 \bmod \phi(n)$ (neem $a = e$ en $m = \phi(n)$), zodat $e \cdot e^{\phi(\phi(n))-1} = e^{\phi(\phi(n))} \equiv 1 \bmod \phi(n)$, en we $d \equiv e^{\phi(\phi(n))-1} \pmod{\phi(n)}$ kunnen nemen.

De d gebruik je om te ontcijferen (zie opgave 7) en moet dus geheim blijven. Maar dan moet natuurlijk ook $\phi(n)$ geheim blijven! De d en $\phi(n)$ samen vormen je geheime sleutel. De kunst is nu nog om er voor te zorgen dat je uit het getal n het getal $\phi(n)$ niet kunt halen.

9 Hoe bereken je ook alweer $\phi(n)$?

Als we de priemfactorontbinding van n kennen, dan weten we dus ook wat $\phi(n)$ is. We moeten dus op zoek naar getallen waarvoor de priemfactorontbinding van n lastig is te bepalen. Nu is het ontbinden in factoren n een lastig karwei als n het product is van twee grote priemgetallen (elk meer dan 100 cijfers groot), ook voor een computer. (Die kan het vaak wel, maar het kost dan gigantisch veel rekentijd, zodat een ontcijfering pas lukt op het moment dat ontcijfering geen zin meer heeft (de aanval heeft al plaatsgevonden, de bankpasjes zijn al geblokkeerd, enzovoort)). Daarom nemen we voor n het product van twee grote zeer grote priemgetallen p en q.

10 Eva onderschept een bericht van Bob aan Alice, maar slaagt er niet in om n te ontbinden. Hoe zou ze dan toch het bericht kunnen ontcijferen? Zou je dit Eva aanraden? Waarom wel, waarom niet? Neem aan dat n inderdaad 200 cijfers lang is.

11 Stel je voor dat een computer op een zeker moment tamelijk snel een product van twee priemgetallen van elk ongeveer 100 cijfers kan ontbinden, dan is een vercijfering met een n van tweehonderd cijfers niet echt veilig meer.

a. Waarom is zo'n vercijfering dan niet echt veilig meer?

b. Is dan direct het RSA-systeem onveilig? Zo ja, waarom, zo nee, wat moet je dan doen om het veilig te houden?

Samengevat: De procedure voor het maken van een setje sleutels voor het RSA-systeem en het vercijferen en ontcijferen binnen dat systeem gaat als volgt. Tegelijkertijd geven we een voorbeeld met kleine priemgetallen.

- Alice kiest twee grote priemgetallen p en q.
  Voorbeeld: $p = 17$ en $q = 29$
- Zij berekent vervolgens $n = pq$ en $\phi(n) = (p-1)(q-1)$.
  Voorbeeld: $n = 17 \cdot 29 = 493$ en $\phi(n) = 16 \cdot 28 = 448$

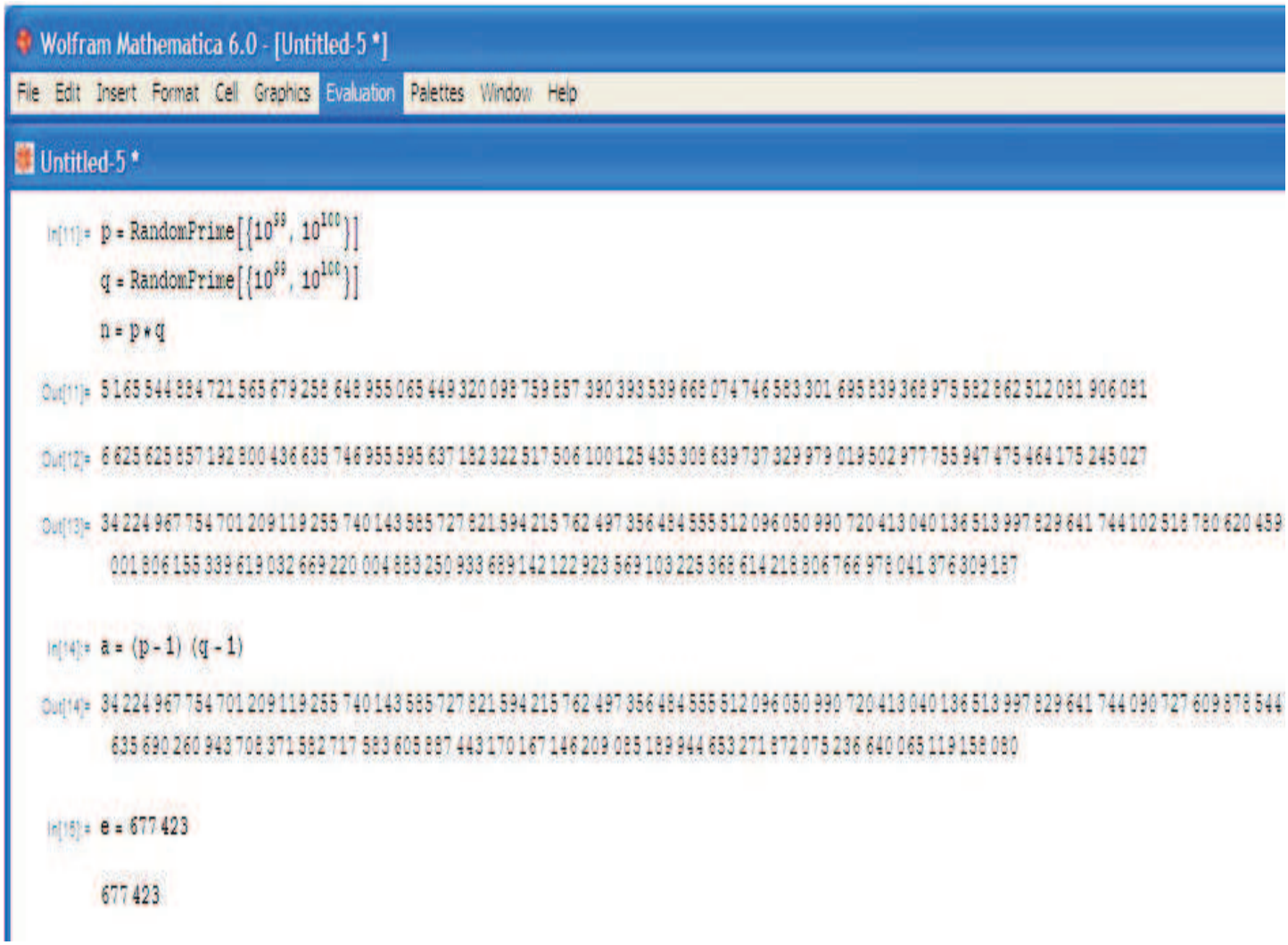
- Daarna kiest Alice een ***vercijferingsexponent*** e met de eigenschap dat ggd(e,$\phi(n)$)=1.
  Voorbeeld: $e = 55$

- Alice bepaalt d met de eigenschap dat $de \equiv 1 \bmod \phi(n)$ met behulp van het algoritme van Euclides of met behulp van $d \equiv e^{\phi(\phi(n))-1} \pmod{\phi(n)}$.
  Voorbeeld: Het algoritme van Euclides toegepast op 448 en 55 geeft het volgende.
  $448 - 8 \cdot 55 = 8$
  $55 - 6 \cdot 8 = 7$
  $8 - 1 \cdot 7 = 1$ en
  $7 - 1 \cdot 7 = 0$, dus ggd(448,55)=1.
  Terugrekenend: $1 = 8 - 1 \cdot 7 = 8 - (55 - 6 \cdot 8) = 7 \cdot 8 - 55 = 7(448 - 8 \cdot 55) - 55 = 7 \cdot 448 - 57 \cdot 55$.
  Hieruit volgt $-57 \cdot 55 \equiv 1 \pmod{448}$,
  ofwel $d = -57 \equiv 391 \pmod{448}$.
  Ook $\phi(448) = \phi(2^6 \cdot 7) = 1 \cdot 2^5 \cdot = 192$ en $55^{192} \equiv 391 \pmod{448}$ geeft $d \equiv 391 \pmod{448}$.

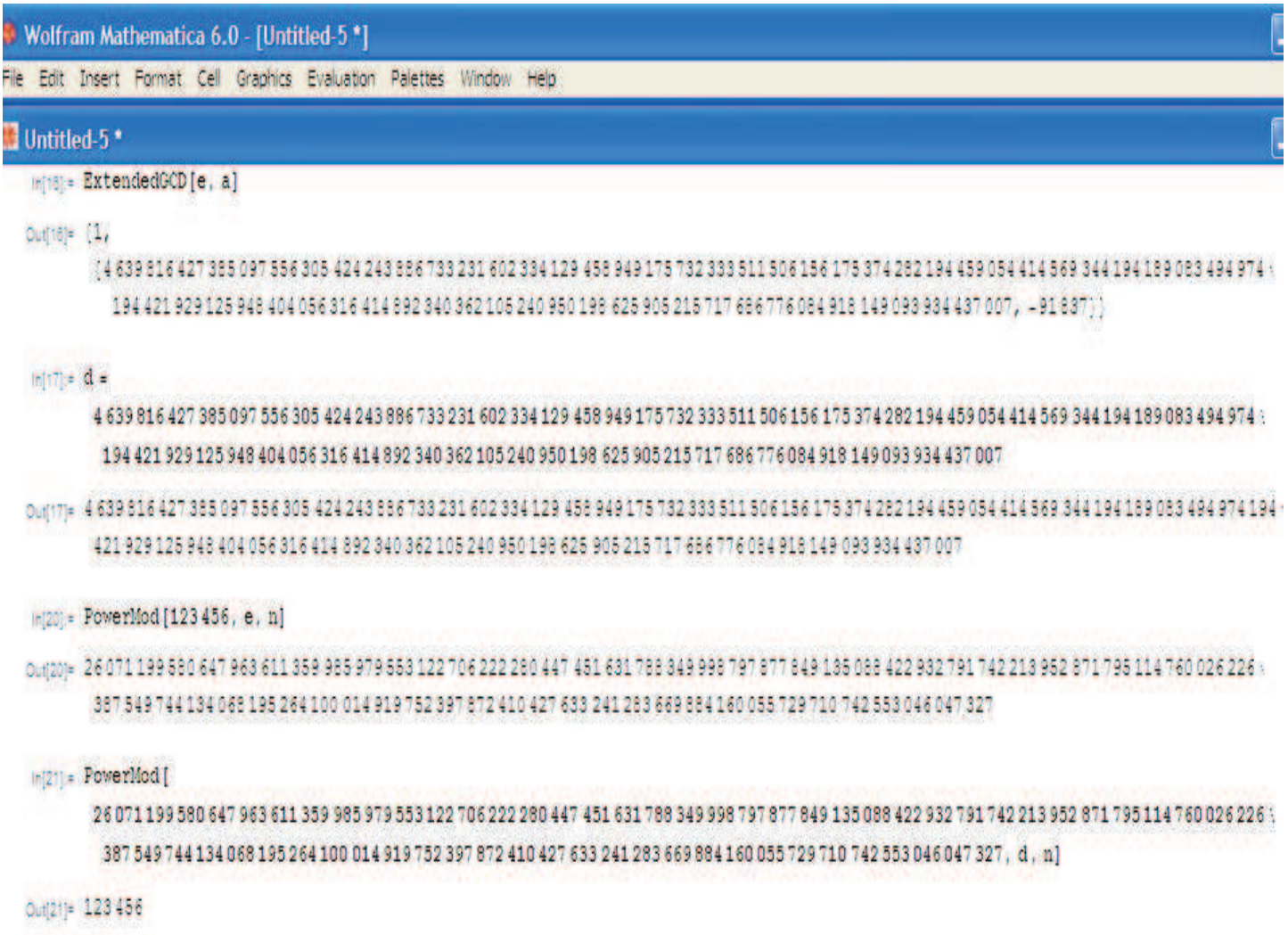
- Alice maakt haar openbare sleutelcombinatie e en n bekend, maar houdt haar geheime sleutelcombinatie d en $\phi(n)$ (en dus ook p en q) uiteraard geheim.
  Voorbeeld: $n = 493$ en $e = 55$.

- Een boodschap x aan Alice vercijfer je nu tot het te verzenden $y = x^e \bmod n$.
  Voorbeeld: $x = 111$ geeft $y = 111^{55} \equiv 342 \pmod{493}$

- Het ontvangen bericht y ontcijfert Alice weer tot $x = y^d \bmod n$.
  Voorbeeld: Ontcijferen geeft $x = 342^{391} \equiv 111 \pmod{493}$



Figuur 3.1 Alice maakt met het computeralgebrapakket Mathematica een openbare RSA-sleutel met p en q allebei 100 cijfers lang.



Figuur 3.2 Alice berekent haar d, Bob vercijfert de boodschap '123456' met behulp van de sleutel van Alice, waarna Alice het bericht van Bob ontcijfert.

In de volgende opgave kruip je even in de rol van Eva. Zij heeft een bericht van Bob aan Alice onderschept. Alice is niet slim geweest, zij heeft een kleine n gebruikt.

12 Bob heeft Alice een met haar openbare sleutel vercijferde boodschap gestuurd. Jij hebt de boodschap, het getal 84 onderschept. De openbare sleutelcombinatie van Alice is $n = 221$, $e = 175$. Bereken $\phi(n)$, d en de oorspronkelijke boodschap.

We zijn nu bijna zo ver dat we al onze boodschappen kunnen vercijferen met behulp van RSA. Er rest nog één probleem. RSA rekent getallen om, maar normaal gesproken zijn onze boodschappen stukken tekst.

13 Probeer een of meerdere oplossingen te verzinnen voor genoemd probleem.

Een mogelijke oplossing voor het probleem zou kunnen zijn om elke letter te vervangen door zijn rangnummer van het alfabet, dus A = 1, B = 2, enzovoort, waarna je elk getal apart gaat vercijferen. Een aardige oplossing, maar met name het vercijferen van elk rangnummer apart is niet zo handig: je bent dan eigenlijk weer aan het vercijferen volgens het systeem van enkelvoudige substitutie.

14 Leg uit waarom je dan eigenlijk weer bezig bent met enkelvoudige substitutie.

Het vervangen van letters door hun rangnummer heeft ook nog een ander nadeel. Je kunt geen leestekens en cijfers mee vercijferen. Eén van de mogelijke oplossingen is het gebruiken van de ASCII-code: je vervangt elke letter, cijfer en leesteken door de bijbehorende ASCII-code. Een tabel van de ASCII-code vind je hieronder. We hebben daarbij voor elke code 3 cijfers gebruikt. De tabel is ontleend aan http://www.asciitabel.nl/. De codes 000 t/m 031 zijn bestemd voor systeemopdrachten (als bijvoorbeeld ”start of text”, ”carriage return”, enzovoort). Daarom begint deze tabel met de code 032. De codes na 127 zijn voor speciale tekens. Deze hebben we hieronder niet opgenomen, onder andere omdat er geen standaardafspraken over bestaan. Normaliter hebben we deze ook niet nodig.

032	spatie	064	@	096	‘
033	!	065	A	097	a
034	”	066	B	098	b
035	#	067	C	099	c
036	$	068	D	100	d
037	%	069	E	101	e
038	&	070	F	102	f
039	’	071	G	103	g
040	(	072	H	104	h
041	)	073	I	105	i
042	*	074	J	106	j
043	+	075	K	107	k
044	,	076	L	108	l
045	-	077	M	109	m
046	.	078	N	110	n
047	/	079	O	111	o
048	0	080	P	112	p
049	1	081	Q	113	q
050	2	082	R	114	r
051	3	083	S	115	s
052	4	084	T	116	t
053	5	085	U	117	u
054	6	086	V	118	v
055	7	087	W	119	w
056	8	088	X	120	x
057	9	089	Y	121	y
058	:	090	Z	122	z
059	;	091	[	123	{
060	<	092	\	124	|
061	=	093	]	125	}
062	>	094	^	126	~
063	?	095	_	127	DEL

15 a. Schrijf van de zin ”Wat heb je aan cryptografie?”de bijbehorende ASCII-codes op.

b. De ASCII-codering van een zin is: 075 117 110 032 106 101 032 100 105 116 032 108 101 122 101 110 063. Hoe luidt de zin?

Het vercijferen van elke code apart komt ook weer neer op enkelvoudige substitutie en is dus niet verstandig.

16 Hoe zou je een ASCII-codering van een boodschap dan wel kunnen vercijferen?

Wat je bijvoorbeeld kan doen is zoveel mogelijk ASCII-codes achter elkaar te schrijven en als één getal te schrijven en deze vervolgens met RSA te vercijferen.

17

a. Als je zoveel mogelijk ASCII-codes achter elkaar hebt opgeschreven, dan krijg je bij het ontcijferen weer een lange reeks cijfers terug. Hoe kun je daar de diverse ASCII-codes weer uit halen en dus de boodschap vinden?

b. Is er een maximaal aantal ASCII-codes wat je achter elkaar kunt zetten om er één getal van te maken? Zo ja, waarom en hoeveel, zo nee, waarom niet?

Natuurlijk is er een maximum aan het aantal ASCII-codes wat je achter elkaar kunt zetten om er een getal van te maken. Als bijvoorbeeld de n die je in je RSA-code gebruikt 20 cijfers lang is, dan kun maar 6 ASCII-codes achter elkaar zetten: je krijgt anders een getal wat groter is dan n. Er is echter ook een getal kleiner dan n wat gelijk is aan dat grote getal modulo n. Beide getallen geven dan bij de vercijfering hetzelfde getal als cijfertekst: je kunt niet meer ontcijferen! Het maximaal aantal codes achter elkaar is dus zodanig dat het ontstane getal nog kleiner is dan n.

18 Je hebt een paar sleutels gemaakt voor het RSA-systeem. Daarbij heb je de volgende keuze gemaakt: $p = 1013$, $q = 401$ en $e = 123$. Je mag in deze opgave voor je berekeningen gebruik maken van de programma's die bij deze module behoren.

a. Bepaal de bijbehorende n, $\phi(n)$ en d.

b. Je ontvangt van ons (de schrijvers van deze module) een boodschap, vercijferd met jouw openbare sleutel:41835 218629 385915. Ontcijfer de ontvangen cijfertekst.

19 Kies een paar priemgetallen (ongeveer 50 cijfers, gebruik het programma **Priem**). Kies daarna een vercijferingsexponent e. Dit is de basis van je sleutels in het RSA-systeem. Geef de openbare sleutel aan je docent. Hij stuurt je met behulp van dit systeem een boodschap. Aan jou de taak om deze te ontcijferen. Ook nu kun je voor je berekeningen gebruik maken van de programma's horend bij deze module.

In deze paragraaf heb je kennis gemaakt met het RSA-systeem. Dit systeem wordt veelal gebruikt bij beveiligde internetverbindingen, zit veelal geprogrammeerd in bankpasjes en creditcards, kortom wordt vooral toegepast in de wereld van getallen. Omdat het systeem getallen omzet in getallen zijn boodschappen in de vorm van tekst minder geschikt voor RSA. Hierboven hebben we de ASCII-codes gebruikt om de teksten om te zetten in getallen, er zijn zeker ook andere mogelijkheden. Maar hoe dan ook, het feit dat je eerst teksten om moet zetten in getallen maakt RSA in dat opzicht minder geschikt. Daarom wordt RSA ook veel gebruikt om alleen op een veilige manier sleutels uit te wisselen, waarna vervolgens met een ander cryptosysteem de daadwerkelijke vercijfering plaats vindt.

Hoofdstuk 4

Antwoorden

Hoofdstuk 1. Wat is cryptografie?

1 DE ROMEINSE KEIZER JULIUS CAESAR HAD VEEL VIJANDEN. DE BOODSCHAPPEN DIE HIJ AAN ZIJN LEGERS STUURDE MOESTEN DAAROM GECODEERD WORDEN. HET SYSTEEM DAT DE KEIZER DAARVOOR GEBRUIKTE IS OOK BIJ DEZE TEKST GEBRUIKT. ZIE JE DE SLEUTEL?.

2 Elke letter van het alfabet is over een vast aantal plaatsen verschoven.

3 2

4 C

5 26

6 JK NUULJYZGJ BGT TKJKXRGTJ OY GSYZKXJGS

7 "Je begrijpt nu hopelijk dat het Caesarsysteem gemakkelijk te ontcijferen is."

8 -

9 Je schrijft een boodschap om het leger bijvoorbeeld naar een bepaalde plaats te sturen. Vervolgens verschuif je elke letter een vast aantal plaatsen. Omdat Julius Caesar dit systeem van vercijferen gebruikt, lijkt het alsof de boodschap van hem komt.

10 Cryptografie wordt onder meer gebruikt in bankpasjes, bij beveiligde internetverbindingen, bij mobiele telefoons, enzovoort.

11 "De Nederlandse hockeyvrouwen hebben na de wereldtitel van afgelopen jaar nu ook de Champions Trophy veroverd. In de eindstrijd werd gastland Argentinië met 1-0 verslagen. Maartje Paumen maakte het enige doelpunt. Zij scoorde al na twee minuten."

12 Elke letter is vervangen door een vaste andere letter (systeem). De

sleutel is A=U, B=E, C=L, D=B, E=C, F=N, G=P, H=I, I=Y, J=R, L=G, N=T, O=H, P=A, Q=D, R=W, S=O, T=Z, U=J, V=F, W=S, X=K, Y=M en Z=V. De K en de M moeten de Q en de X voorstellen, maar die hebben we in deze tekst niet gezien, we weten dus niet welke van deze twee bij welke hoort.

13 a. De 26 letters van het alfabet in één of andere volgorde gezet.

b. $26! \approx 4 \cdot 10^{26}$ sleutels

14 -

15 "Elke letter van het alfabet wordt vervangen door een vaste andere letter."

16 "Zes op de tien Nederlanders doen hun boodschappen met de auto. Bijna 25 procent fietst en de rest neemt de benenwagen. Daarmee worden respectievelijk 150, 520 en 640 calorien per week verbruikt, als twee tot drie keer per week boodschappen worden gedaan. Dat blijkt dinsdag uit onderzoek van de Erasmus Universiteit Rotterdam en het Centraal Bureau Levensmiddelenhandel. In de strijd tegen overgewicht roepen de onderzoekers mensen op om vaker te lopen of fietsen als ze boodschappen gaan doen. Wel moeten de supermarkten dan goed per fiets bereikbaar zijn. De onderzoekers pleiten onder meer voor goede fietspaden en betere parkeergelegenheid voor fietsen bij de winkel."

17 -

18 -

19 "wiskunde"

20 WCHMW SGKIC NSZVZ ODKRL KBBEW GCXHE FSXAL MVZMY KZRIG BCKKE OAUVR OBUGS DSTH

21 -

22 a. zlpywopwarjwyleiauaq

b. Alle oneven letters zijn vercijferd met de Caesarverschuiving met sleutel W.

c. Alle even letters zijn vercijferd met de Caesarverschuiving met sleutel D.

d. Alle oneven letters zijn vercijferd met dezelfde Caesarverschuiving (zelfde sleutel). Ook alle even letters zijn met dezelfde Caesarverschuiving (zelfde sleutel).

e. Zie de tekst na de opgave.

23 a. $\approx 0,078878$

b. $\frac{1}{26}$

24 -

25 5, 20 of 35.

26 -

27 Waarschijnlijk 4 letters lang

28 -

29 -

30 -

31 Waarschijnlijk 4 letters lang.

32 "De eerste deur die je tegenkomt is die van de schuur, de tweede is van het huis."

33 "Een trein net halen is sinds de nieuwe dienstregeling van de ns moeilijk geworden de treindeuren gaan vijftien seconden eerder dicht dan de reiziger gewend was de ns heeft de regels voor vertrek aangescherpt maar heeft de reiziger hierover niet ingelicht."

34 -

35 Het antwoord op deze opgave staat in de uitwerkingenbundel. Vraag je leraar.

Hoofdstuk 2. Getaltheorie.

1 a. 25 euro

b. 2 euro

2 a. 5 *rest* 6

b. 6 *rest* 7

c. 12 *rest* 15

3 a. 1233 *rest* 3

b. 19430 *rest* 6

c. 384 *rest* 192

4 8|24, 17|17 en 4|0.

5 a. 1, 2, 3, 4, 6, 8, 12 en 24

b. 1 en 3

c. 3 heeft alleen zichzelf en 1 als deler.

6 2

7 2, 3, 4, 6, 9, 12 en 18.

8 7, 17 en 19

9 2, 3, 5, 7, 11 en 13.

10 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

11 De delers van 20 zijn 1, 2, 4, 5, 10 en 20. De delers van 28 zijn 1, 2, 4, 7, 14 en 28. De gemeenschappelijke delers zijn 1, 2 en 4. De grootste gemeenschappelijke deler is 4.

12 a. ja

b. ja

13 a. ja

b. ja

14 -

15 -

16 4

17 3

18 ggd(5148,420)=12, $12 = 4 \cdot 5148 - 49 \cdot 420$

19 ggd(4284,924)=84, $84 = 14 \cdot 924 - 3 \cdot 4284$

20 Alleen $6|8 \cdot 9$ is waar.

21 $7|21 \cdot 11$ en $7|21$ zijn waar.

22 -

23 $12 = 2^2 \cdot 3$, $18 = 2 \cdot 3^2$ en $45 = 3^2 \cdot 5$.

24 nee

25 -

26 -

27 a. $40 = 2^3 \cdot 5 = 2^3 \cdot 5^1$, $28 = 2^2 \cdot 7 = 2^2 \cdot 7^1$ en ggd(40,28)= $4 = 2^2$

b. $60 = 2^2 \cdot 3 \cdot 5 = 2^2 \cdot 3^1 \cdot 5^1$, $192 = 2^6 \cdot 3 = 2^6 \cdot 3^1$ en ggd(60,192)= $12 = 2^2 \cdot 3 = 2^2 \cdot 3^1$

28 $13475 = 5^2 \cdot 7^2 \cdot 11$, $936 = 2^3 \cdot 3^2 \cdot 13$ en ggd(13475,936)= 1

29 1

30 3

31 -

32 -

33 -

34 kgv(420,5148)=180180, kgv(924,4284)=47124 en kgv(30,192)=960

35 a. beiden 2162160

b. beiden 3958416

c. beiden 5760

d. -

36 -

37 -

38 a. $\frac{167}{4752}$

b. $\frac{351}{4235}$

c. $\frac{701}{30030}$

39 -

40 -

41 a. $\frac{1}{4}\pi$.

b. 80π.

c. π.

d. 180π.

42 -

43 3 uur, 9 uur

44 a. 4 (mod 12)

b. 4 (mod 12)

c. 0 (mod 12)

d. 9 (mod 12)

e. 1 (mod 12)

f. 1 (mod 12)

g. 0 (mod 12)

h. 5 (mod 12)

45 -

46 -

47 -

48 a. 1 (mod 3)

b. 4 (mod 5)

c. 3 (mod 7)

d. 8 (mod 24)

e. 22 (mod 30)

f. 15 (mod 37)

g. 7 (mod 14)

h. 15 (mod 40)

i. 2 (mod 7)

j. 4 (mod 7)

k. 4 (mod 7)

49 -

50 a. 353 (mod 397)

b. 348 (mod 397)

c. 19 (mod 397)

d. 361 (mod 397)

51 a. 110 (mod 397)

b. 168 (mod 397)

c. 291 (mod 397)

52 a. 7 (mod 1017)

b. 46 (mod 907)

c. 153 (mod 217)

53 a. 2

b. 6

c. 2

d. 3

54 7

55 -

56 -

57 a. 2 (mod 7)

b. 6 (mod 9)

58 a. $x = x_1 + x_2 + \ldots + x_k$

b. -

c. Nee. Neem bijvoorbeeld $a_1 = 4, a_2 = 2, m_1 = 7, m_2 = 5$.

d. -

e. -

f. -

59 a. 4336 (mod 24871)

b. 4218 (mod 9240)

60 113

61 -

62 -

63 a. 0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7.

b. 0, 3, 6, 2, 5, 1, 4.

c. 0, 3, 6, 9, 0, 3, 6, 9, 0, 3, 6, 9.

d. 0, 0, 0, 0, 0.

e. Bij a. en b. zijn alle antwoorden verschillend, bij c. en d. zijn er gelijke.

64 -

65 -

66 a. 1 (mod 11)

b. 1 (mod 7)

c. 3 (mod 12)

d. 0 (mod 5)

e. 1 (mod 127)

67 -

68 -

69 a. 1 (mod 97)

b. 1 (mod 101)

c. 57 (mod 101)

d. 87 (mod 101)

e. 461 (mod 1009)

f. 5801 (mod 9973)

g. 109 (mod 439)

h. 1 (mod 563)

70 a. 6

b. 6

c. 4

d. 10

e. 12

f. 20

71 -

72 -

73 -

74 -

75 -

76 -

77 a. 16

b. 24

c. 864

d. 32

e. 1600

f. 960

g. 6576

h. 137088

78 a. 1 (mod 32)

b. 1 (mod 72)

c. 0 (mod 72)

d. 0 (mod 96)

e. 1 (mod 32)

f. 1 (mod 48)

g. 49 (mod 56)

h. 1 (mod 100)

79 -

80 -

81 a. 1 (mod 3528)

b. 25 (mod 3528)

c. 2141 (mod 3528)

d. 1 (mod 880)

e. 49 (mod 880)

f. 2 (mod 7623)

g. 10201 (mod 26299)

82 a. 337 (mod 637)

b. 181 (mod 637)

c. 475 (mod 1573)

d. 729 (mod 1571)

e. 1027 (mod 1571)

f. 1486 (mod 49005)

g. 2971 (mod 49005)

h. 47521 (mod 49005)

i. 2545 (mod 3528)

j. 1 (mod 3528)

83 a. 001

b. 267

c. 361

d. 713

84 a. 25 *rest* 65

b. 4522 *rest* 31

c. 4658 *rest* 61

d. 41516 *rest* 118

85 a. $2 = 400 \cdot 2714 - 369 \cdot 2942$

b. $9 = 509 \cdot 3213 - 164 \cdot 9972$

c. $15 = 20 \cdot 4035 - 33 \cdot 2445$

d. $11 = 6 \cdot 2761 - 5 \cdot 3311$

e. $14 = 3 \cdot 1414 - 1 \cdot 4228$

f. $3 = 3617 \cdot 12345 - 822 \cdot 54321$

g. $3 = 731 \cdot 456 - 33 \cdot 10101$

h. $4 = 224 \cdot 5364 - 131 \cdot 9172$

86 a. $35640 = 2^3 \cdot 3^4 \cdot 5 \cdot 11$
$1907400 = 2^3 \cdot 3 \cdot 5^2 \cdot 11 \cdot 17^2$
$\text{ggd}(35640, 1907400) = 2^3 \cdot 3 \cdot 5 \cdot 11 = 1320$
$\text{kgv}(35640, 1907400) = 2^3 \cdot 3^4 \cdot 5^2 \cdot 11 \cdot 17^2 = 51499800$

b. $166320 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$
$2608515 = 3^2 \cdot 5 \cdot 7^3 \cdot 13^2$
$\text{ggd}(166320, 2608515) = 3^2 \cdot 5 \cdot 7 = 315$
$\text{kgv}(166320, 2608515) = 2^4 \cdot 3^3 \cdot 5 \cdot 7^3 \cdot 11 \cdot 13^2 = 1377295920$

c. $1524 = 2^2 \cdot 3 \cdot 127$
$254 = 2 \cdot 127$
$\text{ggd}(1524, 254) = 2 \cdot 127 = 254$
$\text{kgv}(1524, 254) = 2^2 \cdot 3 \cdot 127 = 1524$

87 a. $38 \pmod{45}$

b. $231 \pmod{2001}$

c. $1744 \pmod{3101}$

d. $81 \pmod{100}$

e. $89 \pmod{97}$

f. $199 \pmod{200}$

g. $29 \pmod{105}$

h. $33 \pmod{91}$

88 a. $9 \pmod{45}$

b. $10 \pmod{31}$

c. $4 \pmod{51}$

d. $3 \pmod{5}$

e. niet oplosbaar

f. $14 \pmod{39}$

89 a. 3 (mod 385)

b. 6 (mod 418)

c. 5 (mod 255)

90 6

91 a. 3

b. 13

c. 313

92 a. -

b. -

c. Ja

93 -

94 a. Door geen van de drie deelbaar.

b. Door geen van de drie deelbaar.

c. Alleen deelbaar door 3.

d. Door geen van de drie deelbaar.

e. Alleen deelbaar door 3.

f. Alleen deelbaar door 11.

g. Deelbaar door 3 en door 9.

h. Alleen deelbaar door 11.

95 a. 0, 1, 4 en 9.

b. 0, 5, 8 en 9.

c. 0, 4 en 8.

d. 0, 1, 4, 5, 8 en 9.

e. $23 \equiv 11 \pmod{12}$

96 -

97 -

Hoofdstuk 3. Moderne cryptografische systemen.

1 a. Bob moet $\frac{20}{5} = 4$ noemen.

b. Bob moet $\sqrt{119}$ noemen.

c. Bob moet $\ln 7$ noemen.

2 Bij cryptografie moet je de werking van een sleutel opheffen, dus de inverse functie van de sleutel gebruiken bij het ontcijferen.

3 Alice vertelt dat ze de e-macht van het cijfer aan Bob gaat vertellen. Bob moet daarna de ln van het door Alice genoemd getal nemen.

4 a. Alice stuurt $O_B(x)$: ze vercijfert de boodschap x met O_B. Omdat alleen Bob de inverse van O_B kent (dat is immers zijn geheime sleutel G_B), kan alleen Bob de boodschap lezen.

b. Alice stuurt $G_A(y)$: ze vercijfert de boodschap y met G_A. Omdat alleen Alice haar geheime sleutel G_A kent en er alleen bij ontcijfering met O_A een zinvolle tekst ontstaat, kan alleen Alice deze boodschap hebben verstuurd.

c. Alice stuurt nu $G_A(O_B(z))$ of $O_B(G_A(z))$: ze vercijfert de boodschap z zowel met O_B als met G_A. Omdat alleen Alice haar geheime sleutel G_A kent en er alleen bij ontcijfering met O_A een zinvolle tekst ontstaat, kan alleen Alice deze boodschap hebben verstuurd. Omdat alleen Bob de inverse van O_B kent (dat is immers zijn geheime sleutel G_B), kan alleen Bob de boodschap lezen.

5 a. Eva kan de boodschap alleen ontcijferen als ze G_B kent.

b. Eva kan alleen een boodschap, die zogenaamd afkomstig is van Alice versturen, als ze G_A kent.

c. Eva moet nu dus G_A en G_B kennen.

6 -

7 $(x^e)^d \equiv x \pmod{n}$, dus zo kun je x terugvinden.

8 -

9 Als $n = p_1^{k_1} \cdot {}_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ de priemfactorontbinding van n is,
dan is $\phi(n) = p_1^{k_1-1} \cdot (p_1 - 1) \cdot p_2^{k_2-1} \cdot (p_2 - 1) \cdot \ldots \cdot p_m^{k_m-1} \cdot (p_m - 1)$.

10 -

11 -

12 $\phi(n) = 192$, $d \equiv 79 \pmod{192}$ en de boodschap is 33.

13 -

14 -

15 a. 087 097 116 032 104 101 100 032 106 101 032 097 097 110 032 099 114 121 112 116 111 103 114 097 102 105 101 063

b. Kun je dit lezen?

16 -

17 -

18 a. $n = 406213$, $\phi(n) = 404800$, $d \equiv 115187 \pmod{404800}$

b. Goed!

19 -