Cryptografie

Monique Stienstra
Harm Bakker

Voorwoord

Deze lessenserie cryptografie is geschreven als lesmateriaal voor het keuze-onderwerp cryptografie voor wiskunde D voor VWO-leerlingen in opdracht van cTWO, de commissie tweede fase wiskundeonderwijs, en gesubsidiëerd door cTWO en het Stedelijk Gymnasium Nijmegen. De lessenserie is geschreven door Monique Stienstra en Harm Bakker, het materiaal is een aantal keer herzien en is getest in lesgroepen in de bovenbouw van het vwo.

De illustratie op de voorpagina is een bewerking van een opname van de Enigma, een codeermachine uit de tweede wereldoorlog.

Inhoudsopgave

1 Inleiding

Al eeuwenlang sturen mensen elkaar berichten. Soms moet de inhoud van deze berichten geheim blijven. Je kunt hierbij denken aan de inhoud van een brief of vertrouwelijke stukken van defensie, maar ook bijvoorbeeld aan het doen van bankzaken via internet, aan het geld opnemen bij een pinautomaat of aan mobiele telefonie. Onder andere door de opkomst van computernetwerken en internet is er steeds meer behoefte aan de beveiliging van berichten. De kunst van het beveiligen van berichten noemt men cryptografie. Het woord “cryptografie” stamt uit het Grieks: κρυπτος = geheim, γραφειν = schrijven.

Je kunt ervoor zorgen dat een ander je boodschap niet kan lezen door de boodschap te verstoppen. Dit noemt men steganografie. Herodotus vertelt hoe rond 440 voor Christus een vorst het hoofd van een slaaf liet kaalscheren en daarna een tatoeage liet aanbrengen. De boodschap bevatte een waarschuwing voor Griekenland over de geplande invasie door Perzië. Toen het haar weer teruggroeide was de informatie verborgen voor de buitenwereld en kon weer zichtbaar gemaakt worden door het scheren van het hoofdhaar.

Een andere techniek in het oude Griekenland, ook beschreven door Herodotus, was het schrijven van boodschappen op hout, en ze dan te bedekken met een laag was, zodat het leek of het een ongebruikt tablet was. Van oudsher kent men ook manieren om boodschappen te schrijven op papier met onzichtbare inkt. Tijdens de Tweede Wereldoorlog gebruikten Duitsland en andere spionnen microdots om informatie te verzenden. Deze microdots waren ongeveer zo groot als de punt getypt met een schrijfmachine, en ze bevatten minuscule informatie op fotografische wijze verkleind.

Vandaag de dag zijn er verschillende mensen die de techniek gebruiken om hun eigendom te beveiligen of geheime informatie te versturen via internet. Door bijvoorbeeld een watermerk aan te brengen kan de auteur zijn unieke stempel drukken op een afbeelding of geluidsbestand. Ook kunnen mensen via afbeeldingen op webpagina's publiekelijk informatie versturen, terwijl alleen ingewijden de informatie kunnen achterhalen.

In deze lessenserie zullen we ons niet bezig gaan houden met het *verbergen* van boodschappen, maar met het *versleutelen* ervan.: op de letters van de oorspronkelijke boodschap worden eerst bepaalde bewerkingen uitgevoerd, waarna de bewerkte boodschap wordt verstuurd. In principe kan iedereen het bericht lezen, maar voor de niet-ingewijde lezer staat er alleen onzin. Verderop zullen we uitgebreider bekijken hoe Julius Caesar al gebruik maakte van deze techniek. Hij verving iedere letter uit het oorspronkelijke bericht door de letter die drie posities verder in het alfabet staat. Het versleutelde bericht ziet er dan (in eerste instantie) totaal onbegrijpelijk uit.

In de 18^{e} eeuw had elke Europese grootmacht zijn eigen zogenoemde “Zwarte Kamer”, een soort geheime dienst waar een team van codebrekers dagelijks geheime berichten ontcijferden. Met de komst van de elektrische telegraaf in 1843 ontstond ook de interesse van het grote publiek om te vermijden dat de telegrafist alle bijzonderheden van het bericht zou meelezen. De komst van de radio rond 1900 maakte het versturen van berichten over grote afstanden makkelijker voor het leger, maar vereiste ook een verbetering van de versleuteling van de berichten omdat de vijand op elk moment kon meeluisteren. Tot in de Eerste Wereldoorlog gebruikte men

uitsluitend zogenaamde handcoderingen, ook wel pen-en-papiercodes genoemd of veldcoderingen als het om militaire toepassingen gaat. Nadien ontstonden de eerste elektromechanische coderingen, waarbij machines gebruikt werden om de letters om te zetten in code. De meest bekende codeermachine is de in 1920 in Duitsland ontwikkelde Enigma, die lange tijd de tegenstanders tot wanhoop dreef. Uiteindelijk werd de code van de Enigma toch gekraakt door de Polen en de Britten door gebruik te maken van (voorlopers van) de computer. De Engelse wiskundige Alan Turing vervulde hierbij een belangrijke rol. Het breken van de Enigma-code heeft bijna zeker de nederlaag van de Duitsers versneld.

Naast de Enigma had Duitsland nog een andere machine op berichten te coderen: de Lorenz-machine, die werd gebruikt voor de communicatie tussen Hitler en zijn generaals; deze was nog moeilijker te breken dan de Enigma-code. De Engelsen bouwden hiervoor een elektronische machine, de Colossus. Deze machine wordt vaak gezien als de eerste echte computer. Een code die in de Tweede Wereldoorlog nooit gebroken werd, is er een van de Verenigde Staten die het Navajo, een indianentaal, gebruikten in de oorlog tegen Japan. Ze hadden daarvoor een team van Navajo's opgeleid die niets anders deden dan boodschappen via de radio aan elkaar doorgeven.

Met de komst van de computer werd het mogelijk de versleuteling zeer snel uit te voeren. Men probeerde hierbij tot een standaard te komen. Een van de belangrijkste standaarden werd de Data Encryption Standard (DES),een opvolger van het Lucifer-algoritme van IBM.

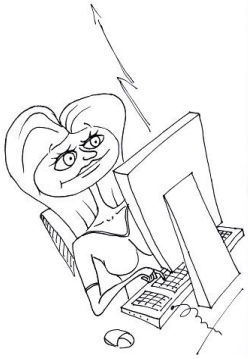
Een probleem bij het gebruik van computerversleuteling bleek het doorgeven van sleutels: de (extra) informatie die aangeeft hoe er precies wordt versleuteld. Voor belangrijke organisaties werd dit lange tijd noodgedwongen door middel van koeriers gedaan. Whitfield Diffie en Martin Hellman ontwikkelden hiervoor samen in Amerika het Diffie-Hellman-sleuteluitwisselingsprotocol Met dit protocol is het mogelijk sleutels op veilig wijze volledig elektronisch uit te wisselen, zelfs als de communicatie wordt afgetapt. Zij legden hiermee de grondslag voor de cryptografie met publieke sleutels

Beveiligen van berichten omvat meer dan alleen zorgen dat een ander de berichten niet kan lezen, of beter: kan ontcijferen. Wanneer je een bericht krijgt, dan wil je zeker weten dat het echt door degene gestuurd is die als afzender vermeld staat. Dit noemt men de handtekeningfunctie van beveiliging of authenticatie. Tot slot wil een ontvanger graag zeker weten dat er onderweg niet met de inhoud van het bericht geknoeid is, hij wil overtuigd zijn van de integriteit van het bericht.

Wiskunde is erg belangrijk in de moderne cryptografie. In deze lessenserie zullen we bestuderen *welke* wiskunde in de cryptografie wordt gebruikt en *hoe* ze daar wordt gebruikt.

2 Begrippen en afspraken

In de cryptografie bekijken we methoden waarop personen (of machines) op een veilige manier boodschappen kunnen uitwisselen. De namen Alice en Bob worden meestal gebruikt voor de personen die elkaar een boodschap sturen. Over de veiligheid hoef je je pas druk te maken als er een derde persoon in het spel is die probeert boodschappen af te luisteren en te ontcijferen. Deze derde persoon krijgt de naam Eve. Het Engelse woord *eavesdropper* betekent luistervink. Soms wordt ook Oscar (van *opponent*) of Mallory (van *malicious*) als actieve kraker opgevoerd. Eve is meer een passieve afluisteraar; de anderen proberen echt in te breken in de communicatie tussen Alice en Bob.



Oscar of Mallory **Alice** **Bob** **Eve**

De volgende tabel geeft een overzicht van een aantal begrippen die we in het vervolg gebruiken.

- *Alfabet:* De verzameling symbolen (letters, punten, komma's, enz.) die in een boodschap gebruikt mogen worden.
- *Vercijferen* of *versleutelen:* Een boodschap omzetten in een gecodeerde boodschap. (Engels: *encrypt*).
- *Ontcijferen:* De gecodeerde boodschap omzetten naar de oorspronkelijke boodschap. (Engels: *decrypt).*
- *Klare tekst:* De oorspronkelijke, niet vercijferde tekst. (Engels: *plaintext*).
- *Cijfertekst:* De vercijferde tekst. (Engels: *ciphertext*).
- *Cryptosysteem:* De methode waarmee een tekst vercijferd en ontcijferd wordt.
- *Sleutel:* Geheime informatie die je nodig hebt om te ontcijferen.
- *Sleutelruimte:* De verzameling van verschillende sleutels die bij een bepaald cryptosysteem mogelijk zijn.

Voorbeeld:
We geven een voorbeeld van een heel simpel cryptosysteem.
Als eerste wordt geëist dat de boodschap wordt geschreven met alleen hoofdletters, leestekens en spaties. Kies vervolgens een (niet te groot) geheel getal k.

Versleutelen:

- Verwijder eerst alle leestekens en spaties.
- Verdeel daarna je tekst in blokjes van k letters.
- Schrijf de tekst per blokje achterstevoren op.
- Voeg alle blokjes weer bij elkaar tot één lange tekst.
- Verdeel de tekst in blokjes van 5 letters (dit laatste is gebruikelijk in de cryptografie).
- Vul het laatste blokje aan met willekeurige letters tot het lengte 5 heeft.

Ontcijferen:

- Voeg alle blokjes bij elkaar tot één lange tekst.
- Verdeel de tekst in blokjes van lengte k.
- Schrijf de tekst per blokje achterstevoren op.
- Voeg de blokjes samen tot één lange tekst.
- Lees de tekst goed door en voeg spaties en leestekens toe.

Opgave 1

a) Formuleer een bericht, bestaande uit hoofdletters, leestekens en spaties.
b) Kies een getal k en versleutel de boodschap op de manier zoals in het voorbeeld staat beschreven.
c) Vertel iemand anders hoe je je bericht hebt versleuteld, maar zonder de waarde van k te onthullen. Vraag hem of haar je bericht te ontcijferen.

In het voorbeeld bestaat het alfabet voor de klare tekst uit hoofdletters, leestekens en spaties; het alfabet voor de cijfertekst bestaat uit alleen hoofdletters. De sleutel bij dit systeem is het getal k. Als je weet welke methode gebruikt is, maar niet welke sleutel er is gebruikt, dan kan het ontcijferen nog een hele klus zijn. Ken je ook de sleutel, dan kun je de boodschap eenvoudig ontcijferen.

De sleutel $k = 1$ doet eigenlijk niets met de tekst en heeft dus niet veel zin. De grootste lengte van de blokjes die je kunt nemen is de lengte van de tekst. Stel dat de tekst n letters bevat, dan is de sleutel één van de getallen $1,2, \ldots, n$. De sleutelruimte is dus de verzameling $\{1,2, \ldots, n\}$.

Het cryptosysteem uit het voorbeeld is natuurlijk een erg slecht cryptosysteem. Als je de sleutel niet kent, kun je hem makkelijk achterhalen door maar wat te proberen. Tenminste, als je weet welk cryptosysteem gebruikt wordt. In de cryptografie hanteren we het principe van Kerckhoff dat zegt dat als Alice en Bob elkaar een vercijferde boodschap sturen, ze er vanuit moeten gaan dat een mogelijke afluisteraar Eve weet welk cryptosysteem ze gebruiken. Natuurlijk houden ze de sleutel geheim.

De redenen voor aanname van dit principe van Kerckhoff zijn de volgende:

- Een methode zit meestal ingebouwd in apparatuur en/of programmatuur (software). Daardoor is hij niet eenvoudig te vervangen. Een sleutel kan wel makkelijk veranderd worden.
- Vaak wordt gebruikgemaakt van gestandaardiseerde software in bijv. webbrowsers en email-programma's. Deze standaarden kunnen natuurlijk niet geheim gehouden worden.
- Bij de ontwerpers van een methode is de methode uiteraard bekend. Toch wil je dat zij je berichten ook niet kunnen lezen.
- Op deze manier hoef je zo weinig mogelijk informatie geheim te houden en dat is eenvoudiger dan veel informatie geheim houden.
- Als een methode bekend is, kan er door andere cryptografen openlijk over de veiligheid ervan gepubliceerd worden.

Tot slot spreken we af om voorlopig een vercijferde boodschap te noteren in groepjes van vijf letters om geen informatie over de lengte van woorden en de zinsopbouw prijs te geven. Vaak wordt de tekst aangevuld met een paar willekeurige letters om het aantal letters een veelvoud van vijf te laten zijn. Voor de duidelijkheid: we vercijferen dus eerst de boodschap en het resultaat schrijven we op in blokjes van vijf letters.

3 Symmetrische cryptografie

De oudste cryptosystemen zijn symmetrische cryptosystemen. Dat wil zeggen dat je voor het versleutelen en voor het ontcijferen dezelfde sleutel nodig hebt. Bij deze systemen bestaat de vercijfering van de boodschap uit een reeks eenvoudig omkeerbare stappen, zoals het optellen van twee getallen. Ontcijfering van de boodschap bestaat er dan uit dat de omgekeerde operaties in omgekeerde volgorde worden uitgevoerd, waardoor de versleuteling ongedaan wordt gemaakt. Dit zag je ook in het voorbeeld in het vorige hoofdstuk. We zullen in dit hoofdstuk een aantal van dit soort systemen bekijken

3.1 Caesarcryptografie

Een van de eerste bekende cryptosystemen is het Caesarcryptosysteem, het systeem dat Julius Caesar gebruikte.

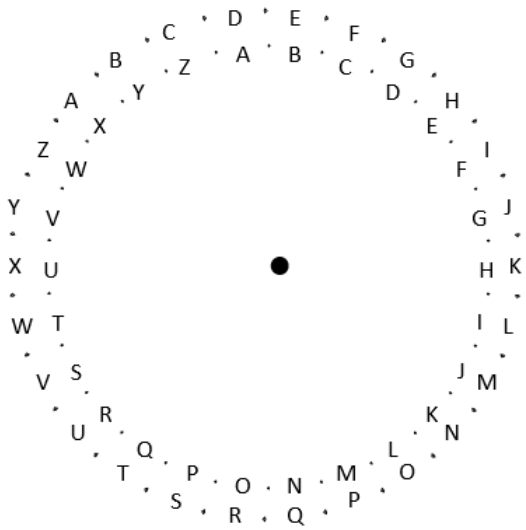
Opgave 1

De beroemde uitspraak "ALEA IACTA EST" (de teerling is geworpen) van Julius Caesar wordt met het Caesarcryptosysteem vercijferd tot "DOHDL DFWDH VWAXQ".

Probeer te achterhalen hoe Caesar zijn berichten vercijferde.

In opgave 1 zul je waarschijnlijk vrij snel ontdekt hebben dat Caesar iedere letter drie plaatsen in het alfabet opschoof. Een A werd dus een D, een B een E, …, een Y een B en een Z een C. De ontvanger wist hoe Caesar de boodschap vercijferd had en kon de oorspronkelijke boodschap ontcijferen. Helaas kon een spion dat ook zeer eenvoudig.

Het systeem van Caesar is een speciaal geval van het schuifsysteem. Bij dit cryptosysteem wordt iedere letter een vast aantal plaatsen in het alfabet opgeschoven. Het cryptosysteem is dus: "kies een geheel getal *k* en schuif iedere letter *k* plaatsen op in het alfabet". De sleutel is het getal *k*; deze is bekend bij zowel de schrijver als de ontvanger, maar moet verder geheim blijven. Bij het ontcijferen schuif je iedere letter weer *k* plaatsen in het alfabet terug.



Wanneer je een boodschap met een schuifsysteem wilt vercijferen, is het handig om twee cirkels met het alfabet met een splitpen op elkaar te maken. Je draait de cirkels zo ten opzichte van elkaar, dat naast iedere letter zijn vercijfering staat.

Opgave 2

- **a)** Wanneer je een bericht dat vercijferd is met een schuifsysteem wilt ontcijferen, kun je alle 26 sleutels uitproberen. Kun je een snellere manier verzinnen?
- **b)** Probeer de sleutel waarmee onderstaande tekst vercijferd is te vinden. De tekst is vercijferd met een schuifsysteem.

  JNAAR REWRR RAGRX FGQVR IREPV WSREQ VFZRG RRAFP UHVSF LFGRR ZJVYG BAGPV WSRER AVFUR GUNAQ VTRRE FGGRX VWXRA ANNEQ RYRGG REFQV RURGZ RRFGR IBBEX BZRAM BNYFQ RRARA GKDMK

In het bovenstaande zijn we uitgegaan van een alfabet van 26 letters. Dit is geen noodzaak. Je zou ook kunnen afspreken om bijvoorbeeld leestekens, spaties en cijfers aan je alfabet toe te voegen en zo op een groter aantal “letters” uitkomen. Uiteraard moet wel bij beide partijen bekend zijn welk alfabet gebruikt wordt. In dit hoofdstuk beperken we ons tot het standaard alfabet met de 26 (hoofd-)letters. In latere hoofdstukken zullen we de verzameling van beschikbare tekens uitbreiden.

3.2 Affiene cryptografie

Het vercijferen van boodschappen komt vaak neer op het uitvoeren van berekeningen met de letters van de boodschap. Je zet dan de letters eerst om in rangnummers en met die rangnummers ga je rekenen. De A krijgt rangnummer 0, de B rangnummer 1 en zo ga je door tot de Z met rangnummer 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Als je berekeningen uitvoert met rangnummers, krijg je al gauw getallen die niet meer in het gebied [0 .. 25] zitten. Om deze getallen toch terug te vertalen naar symbolen uit het alfabet, schrijven we in gedachten het alfabet oneindig vaak achter elkaar:

...	W	X	Y	Z	A	B	C	D	...	X	Y	Z	A	B	C	...	Y	Z	A	B	C	...
...	-4	-3	-2	-1	0	1	2	3	...	23	24	25	26	27	28	...	50	51	52	53	54	...

Maar dat is gemakkelijker te representeren met een cirkel, net als bij een klok. We winden al die kopieën van het alfabet rond de cirkel. Om nu bij een getal het betreffende symbool terug te vinden is het aantal keer dat je rond de cirkel bent gelopen niet van belang; alleen het reststukje bepaalt waar je uitkomt op de cirkel. Je berekent dus eigenlijk de rest bij deling door het aantal letters in je alfabet. Bij een gewone klok werkt dit net zo: na elke 12 uur begin je weer op 0. Als je 100 uur verder telt op een klok, is de afstand die je eigenlijk opschuift gelijk aan de rest die je overhoudt als je 100 deelt12. Je telt dus 4 uur verder, want 100:12 = 8 rest 4. Op dezelfde manier vind je dat op de letterstrook hierboven bij het getal 85 de letter H hoort: 85:26 = 3 rest 7, dus bij het getal 85 staat dezelfde letter als bij het getal 7 en dat is de H.

Opgave 3

- **a)** Welke letter hoort bij het getal 133?
- **b)** Hoe zie je direct dat bij de getallen 1000 en 1026 dezelfde letters horen?

c) Welke letter hoort er bij het getal 2662?
d) Welke letter hoort er bij het getal -22?

Nu we een koppeling hebben gemaakt tussen getallen en letters van het alfabet, zijn we in staat om de versleuteling en ontcijfering met formules te beschrijven. Daarvoor moet bij een letter eerst zijn rangnummer in het alfabet worden bepaald. Op dit rangnummer wordt een wiskundige functie toegepast. Het resultaat leidt dan met behulp van de letterstrook tot de versleutelde letter.

Een functie die beschrijft hoe we bij het rangnummer van een letter uit de klare tekst het rangnummer van de letter uit de cijfertekst berekenen heet een *encryptiefunctie*. Meestal geven we de encryptiefunctie aan met de letter E, waarbij de waarde van de sleutel als parameter wordt genoteerd.

Voorbeeld
De manier waarop Julius Caesar zijn boodschap versleutelde kunnen we beschrijven met de encryptiefunctie $E_3(x) = x + 3$. Voor deze functie geldt $E_3(\text{'A'}) = E_3(0) = 0 + 3 = 3 = \text{'D'}$ en $E_3(\text{'Y'}) = E_3(24) = 24 + 3 = 27 = \text{'B'}$
Merk op dat de waarde van de sleutel, in dit geval 3, als subscript wordt genoteerd.

Opgave 4
a) Hoe ziet de definitie van de encryptiefunctie eruit als je in plaats van 3 nu 7 posities op wilt schuiven?
b) Geef de definitie van de encryptiefunctie die hoort bij een verschuiving van 9 posities naar links.
c) Hoe ziet in het algemeen de encryptiefunctie eruit bij een schuifsysteem?

De functie die je nodig hebt om vanuit cijfertekst te ontcijferen tot de klare tekst heet een *decryptiefunctie* , meestal aangegeven met de letter D. Nu natuurlijk ook weer voorzien van de sleutel.

Opgave 5
a) Geef een decryptiefunctie die hoort bij de encryptiefunctie $E_3(x) = x + 3$.
b) Geef een decryptiefunctie die hoort bij de encryptiefunctie $E_k(x) = x + k$.

De algemene vorm van een encryptiefunctie in een schuifsysteem is $E_k(x) = x + k$.
We spreken van een affien systeem als de encryptiefunctie van de vorm $E_{(a,b)}(x) = a \cdot x + b$ is, dus een willekeurige lineaire functie. Merk op dat je nu twee waarden moet weten om de versleuteling uit te voeren, de waarde van a en de waarde van b. Anders gezegd: de sleutel is nu het paar (a, b).
Bij een schuifsysteem blijven de letters van het alfabet na versleuteling keurig naast elkaar staan; bij een affien systeem wordt deze volgorde verstoord.

Opgave 6
Neem de volgende tabel over en bepaal de versleutelingen van de letters van het alfabet onder de drie encryptiefuncties $E_{11}(x) = x + 11$, $E_{(5,6)}(x) = 5 \cdot x + 6$ en $E_{(9,2)}(x) = 9 \cdot x + 2$.

	A	B	C	D	E	. . .	V	W	X	Y	Z
	0	1	2	3	4		21	22	23	24	25
$E_{11}(x) = x + 11$	L	M								J	K
$E_{(5,6)}(x) = 5 \cdot x + 6$	G	L								W	B
$E_{(9,2)}(x) = 9 \cdot x + 2$	C										T

Opgave 7
In deze opgave werken we met het affiene systeem met sleutel $a = 5$ en $b = 6$.

a) Vercijfer het bericht "VANAVOND OM TIEN UUR GAAT HET GEBEUREN." met deze sleutel.
b) Ontcijfer het bericht "UEBGJ ANBU ZTATV NGGKA ATKAA JEGTG NUADG ETIMW" dat met deze sleutel vercijferd is.

Opgave 8
Wat gebeurt er als je $a = 0$ en $b = 3$ kiest?

Opgave 9
Welke waarden moet je voor *a* en *b* kiezen als je de encryptiefunctie $E_{(a,b)}$ hetzelfde wilt laten zijn als de encryptiefunctie E_k die hoort bij een schuifcryptosysteem?

Opgave 10

a) Vercijfer de woorden "INPUT" en "VACHT" met het affiene systeem met de sleutel (4,3).
b) Vercijfer het alfabet met het affiene systeem met sleutel de (4,3).
c) Wat gaat er mis?
d) Leg uit waarom het verkeerd gaat.

Kennelijk moeten we een extra eis stellen aan de sleutel om te zorgen dat alle letters verschillend vercijferd worden. We gaan nu onderzoeken welke eis dat moet zijn. Wat we willen is dat, als we voor *x* in het voorschrift $y = a \cdot x + b$ de gehele getallen van 0 tot en met 25 invullen en we bepalen de rest bij deling van y door 26 dat daar dan alle getallen van 0 tot en met 25 precies één keer voorkomen.

Voorbeeld:
We nemen weer $a = 4$ en $b = 3$. Als we achtereenvolgens 0, 1, 2, 3, … invullen, komt er 3, 7, 11, 15, … uit. Dit zijn allemaal viervouden plus 3, dus allemaal oneven. De resten bij deling door 26 zijn dan allemaal ook oneven, waaruit we al kunnen concluderen dat de even getallen niet als resultaat voorkomen.
Als je de rij van resten bekijkt dan zie je de zichzelf herhalende rij 3, 7, 11, 15, 19, 23, 1, 5, 9, 13, 17, 21, 25, 3, 7, 11, … . Dit zijn de viervouden plus 3 en de viervouden plus 1 kleiner dan 26.

Opgave 11
De bedoeling van deze opgave is om na te gaan aan welke eisen de waarden van a en b moeten voldoen opdat (a, b) een bruikbare sleutel is in een affien cryptosysteem.

a) Leg uit dat het geen zin heeft om een andere waarde voor b te nemen.
Neem in de rest van de opgave steeds $b = 0$.

b) Kies $a = 2$. Onderzoek of je alle getallen van 0 t/m 25 als uitkomst krijgt.

c) Kies $a = 3$. Onderzoek of je alle getallen van 0 t/m 25 als uitkomst krijgt.

d) Kies $a = 13$. Onderzoek of je alle getallen van 0 t/m 25 als uitkomst krijgt.

e) Onderzoek voor welke waarden van $a \leq 25$ je wel precies alle getallen van 0 t/m 25 als uitkomst krijgt.

f) Laat door $E_{(a+26,b)}(x)$ uit te schrijven zien dat vercijfering met het affiene systeem met sleutel (a, b) hetzelfde oplevert als met sleutel $(a + 26, b)$.

Opgave 12
We hebben gezien dat er 26 sleutels zijn bij een schuifcryptosysteem over een alfabet met 26 letters.

a) Hoeveel daarvan leveren een vercijfering die niet identiek aan de klare tekst is?

b) Onderzoek hoeveel sleutels, dus paren (a, b), er zijn bij een affien cryptosysteem over een alfabet met 26 letters waarmee verschillende zinvolle vercijferingen te maken zijn.

Opgave 13
Wanneer we weten hoe 2 letters vercijferd worden, kunnen we het paar (a, b) achterhalen door deze gegevens in de encryptiefunctie in te vullen. We kunnen de sleutel dus kraken zonder alle sleutels te proberen. In deze opgave gaan we dit doen voor het paar (a, b) waarbij we weten dat een D vercijferd wordt tot een Q en een N tot een O.

a) Leg uit: uit het gegeven dat een D wordt vercijferd tot een Q volgt dat er een geheel getal p is dat voldoet aan $3a + b = 16 + 26p$.

b) Welke conclusie kun je trekken uit het gegeven dat een N wordt vercijferd tot een O?

c) Leg uit dat je het sleutelpaar (a, b) gevonden hebt, als je het stelsel vergelijkingen $\begin{cases} 3a + b = 16 + 26p \\ 13a + b = 14 + 26q \end{cases}$ hebt opgelost.

d) Vind het sleutelpaar (a, b) door het stelsel vergelijkingen op te lossen.

Opgave 14
Oscar heeft bij een met affiene cryptografie vercijferde tekst afgeluisterd hoe twee letters vercijferd worden: de C blijkt als F vercijferd te worden en de F als E. Achterhaal de sleutel (a, b) waarmee de tekst vercijferd is.

3.3 Monoalfabetische substitutie

Werd bij het affiene cryptosysteem het alfabet nog volgens een bepaald systeem gehusseld, bij monoalfabetische substitutie wordt het alfabet op een willekeurige manier door elkaar gegooid. Netter gezegd: bij monoalfabetische substitutie is de sleutel een willekeurige permutatie toegepast op de letters van het alfabet.

Voorbeeld:

x	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
$E(x)$	B	M	Y	K	Z	A	S	C	R	L	N	I	E	O	D	P	W	J	Q	U	H	X	T	V	G	F

Opgave 15

Hoeveel sleutels zijn er bij monoalfabetische substitutie bij een alfabet van 26 letters?

Het aantal sleutels in het monoalfabetische substitutie is veel te groot om ze allemaal uit te proberen. De methode om een sleutel te vinden door alle sleutels uit te proberen heet “Exhaustive key search”. Je zou misschien denken dat het dus een veilige manier is om je berichten te vercijferen. Dat is toch niet zo. Doordat in een taal bepaalde letters veel vaker voorkomen dan andere letters, is het systeem vrij eenvoudig te kraken als je gebruik maakt van een letterfrequentietabel. Hieronder staat een letterfrequentietabel voor de Nederlandse taal.

E 19.06%	N 9.41%	T 6.74%	A 6.72%	R 6.45%	I 6.44%	D 5.91%
O 5.87%	S 4.00%	L 3.94%	G 3.14%	V 2.90%	M 2.41%	H 2.32%
K 2.28%	U 1.93%	B 1.80%	C 1.60%	P 1.59%	W 1.57%	J 1.49%
Z 1.18%	F 0.74%	Y 0.29%	Q 0.11%	X 0.11%		

Als je dus alle letters “*e*” vervangt door de letter “*h*”, dan zal ongeveer 19% van de letters van je vercijferde tekst een “*h*” zijn. Je hoeft dus alleen te tellen hoe vaak iedere letter voorkomt en vervolgens met behulp van de frequentietabel te kijken voor welke letter iedere letter staat. Uiteraard zal dit alleen werken als je tekst lang genoeg is, maar dat blijkt al vrij snel het geval te zijn.

Op de website www.math.rug.nl/crypto vind je diverse programma’s die je werk uit handen kunnen nemen. Zo is er het programma “Frequentie-analyse” dat een overzicht maakt met bij elk symbool het aantal keer dat het in een ingegeven tekst voorkomt. Met het programma “Codetabel” kun je een tekst vercijferen en ontcijferen met monoalfabetische substitutie met een door jou ingegeven sleutel.

Opgave 16

Leg uit dat zowel het schuifcryptosysteem als het affiene cryptosysteem speciale gevallen van monoalfabetische substitutie zijn.

Opgave 17

Ontcijfer de Nederlandse tekst hieronder die vercijferd is met monoalfabetische substitutie.

ZDLCD ZDFYM VDDVZ BAGDV ZJCCU AQYFD QDPAW ICVUD YFDZD VHMVU XMMFG CCVUW DAQGC WBAQU AVZDQ PCCUO DOPDZ DVDVM PQWDD YDVFD IDVUH DDUWD HMUZM UEDUD IDVUC JGAWV XCCTZ DDVOF CUDEB APDVH DPZBA GDVZQ CIWDQ YBAP

3.4 Vigenère

Het Vigenère-cryptosysteem werd in 1553 bedacht door Giovanni Batista Belaso, maar werd bekend door de Fransman Blaise de Vigenère. Vigenère schreef zelf in zijn "Traité des Chiffres" over een verbeterde versie waar we aan het einde van deze paragraaf nog aandacht aan besteden. Het systeem dat bedoeld wordt met de naam "Vigenère-systeem" is dus niet van Vigenère, maar van Belaso.

Blaise de Vigenère (1523-1596)

Wanneer je een tekst gaat vercijferen met het Vigenèresysteem, kies je eerst een sleutelwoord. Dat sleutelwoord schrijf je herhaald onder je tekst. Vervolgens tel je van de letters die onder elkaar staan de rangnummers in het alfabet bij elkaar op. Bij deze som bepaal je weer met behulp van de letterstrook het resultaat.

Voorbeeld:
Wanneer je als sleutelwoord "WISKUNDE" gebruikt en je wilt de tekst "DEZE TEKST VERCIJFEREN WE MET VIGENERE" vercijferen, dan tel je voor de eerste letter de rangnummers in het alfabet van de "D" en de "W" bij elkaar op. Dat zijn 3 en 22. De eerste vercijferde letter is dus de letter met positie 25, dus de "Z". Zie hieronder de vercijfering voor de hele zin.

DEZE TEKST VERCIJFEREN WE MET VIGENERE
WISK UNDEW ISKUNDEWISK UN DEW ISKUNDEW
ZMRO NRNWP EWBWVMJAZWX QR PIP DAQYAHVA

In groepjes van 5 letters wordt de cijfertekst dus:
ZMRON RNWPE WBWVM JAZWX QRPIP DAQYA HVAQX.

Natuurlijk hoef je geen bestaand woord als sleutel te nemen. Sterker nog, het komt de veiligheid van je systeem niet ten goede wanneer je een bestaand woord of bijvoorbeeld de naam van je geliefde neemt, omdat de sleutelruimte er ernstig door beperkt wordt en de sleutel bovendien makkelijker te raden is.

De tabel op de volgende bladzij heet een *Vigenèretabel*. Voor ieder tweetal letters is de som bepaald. Je kunt deze tabel gebruiken bij de opgaven.

Vigenère-tabel bij het standaard alfabet

	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

Opgave 18

Kies een sleutelwoord en versleutel daarmee met het Vigenére-cryptosysteem de boodschap "JE GELE KANARIEPAK OK ALS JE JE DUIKBRIL MAAR MEENEEMT".

Opgave 19

De boodschap "JE GELE KANARIEPAK OK ALS JE JE DUIKBRIL MAAR MEENEEMT" wordt vercijferd met Vigenére tot "ESMIW ZYGRL MWKTL FCQEW NXKNP YIOOM MWRQL VFSIP JSKQE".

Achterhaal het sleutelwoord. Leg duidelijk uit hoe je dit hebt aangepakt.

Opgave 20

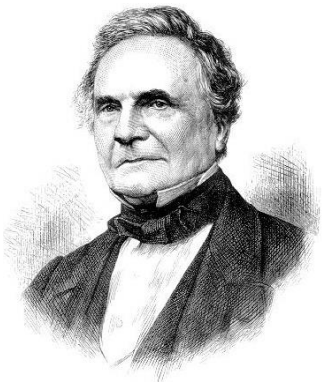
a) Het ontcijferen van een boodschap die vercijferd is met Vigenère is niet zo eenvoudig als het ontcijferen van een boodschap die vercijferd is met mono-alfabetische substitutie. Leg uit waarom het zo lastig is.

b) Leg uit dat de sleutel vinden in principe niet moeilijk is, d.w.z. met behulp van computers goed te doen, als je weet hoe lang de sleutel is.

c) Leg uit waarom het toch nog heel lastig is de boodschap "QAGQO XVKFV JGARH XOWVL ERAIN KPRLT NNBAH TNTAR TTYSF VJGXA GNRBR PTXNT GWHED MQKMX" ontcijferen

ook al weet je dat hij vercijferd is met Vigenère en een sleutelwoord van lengte 3.

Men heeft lang gedacht dat het Vigenèresysteem niet te kraken was tot in 1863 de Pruisische legerofficier Friedrich Kasiski een methode ontwikkelde om de sleutellengte te achterhalen en zo het systeem te kraken. De Britse wiskundige Charles Babbage had enkele jaren eerder dezelfde methode ontwikkeld om de sleutellengte te achterhalen, maar had dit niet gepubliceerd.



Charles Babbage (1791 – 1871)

Het achterhalen van de sleutellengte kan op verschillende manieren. We bekijken eerst een andere methode en vervolgens de methode van Kasiski.
De eerste methode berust op het volgende idee. In een taal komen bepaalde letters vaker voor. Wanneer de letters van een alfabet een bepaald aantal plaatsen verschoven worden, komen er weliswaar andere letters het meest voor maar zijn er dus nog steeds letters die vaker voorkomen dan andere letters.

Opgave 21

- **a)** Laat met behulp van de letterfrequentietabel uit paragraaf 3.3 zien dat de kans dat twee willekeurige letters in een Nederlandse tekst hetzelfde zijn ongeveer gelijk is aan 0,075.
- **b)** In een cijfertekst die vercijferd is met een willekeurig sleutelwoord van 6 letters, dat dus geen bestaand woord hoeft te zijn en meerdere keren dezelfde letter mag bevatten, bekijken we twee letters die niet op 6, 12, 18, … plaatsen uit elkaar liggen. Wat is de kans dat deze twee letters hetzelfde zijn?
- **c)** Dezelfde vraag voor een willekeurig sleutelwoord dat uit 6 verschillende letters bestaat.
- **d)** Leg uit waarom de kans op twee dezelfde letters groter is als de letters een veelvoud van de sleutellengte uit elkaar staan.

Als je in Vigenère een sleutelwoord hebt van bijv. 6 letters, dan zijn in de cijfertekst de letters op plaats 1, 7, 13, 19, … met dezelfde sleutel vercijferd. Op deze plaatsen zullen dezelfde letters vaker voorkomen. Ook de letters op plaats 2, 8, 14, 20, … zijn met dezelfde sleutel vercijferd. Hier komen andere letters vaker voor dan op plaats 1, 7, 13, 19, … (behalve als de 1^e en de 2^e letter van de sleutel hetzelfde zijn), maar binnen deze plaatsen zijn er natuurlijk wel weer een paar vaste letters die vaker voorkomen.

Onder de cijfertekst ga je nu de cijfertekst nog een keer opschrijven. Nu verschuif je de onderste tekst één plaats naar rechts en tel je hoe vaak dezelfde letters boven elkaar staan. Dan verschuif je de onderste tekst nog een plaats naar rechts en tel je weer hoe vaak dezelfde letters boven elkaar staan, enz. Al deze uitkomsten van het tellen houd je bij in een tabel. Wanneer het aantal plaatsen dat de onderste tekst verschoven is een veelvoud van de sleutellengte is, zal het aantal keer dat dezelfde letters boven elkaar staat groter zijn.

Voorbeeld:
De volgende tekst over belasting op wegwerpeetstokjes in China is vercijferd met Vigenère:

DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE TKRVF HLREV LRCPH PCGWM PUJIJ SYIPC SIGBD EPHDP DWMDQ BGITS SVQRX GVSQS PRHVF WHTTC GYEHH RXOOP GBGIK BFLKB DENCP ZGFWI ISQAQ CUHKR JIYSJ AGFSI GHVXQ YMIUR HFGZD VVWQK KGHVQ DJITW FLVAH RUSQQ KZLIW PHAWG WITCP XGZDX GBJEC BPIVG FLCOU WGUUS PRVXQ TIIPN RENGK SWHKB EVLRC KRVFH MECFO MLYVX YSHQK ZMSGB NYDWH OGAHX GFKSW HWSVS HXUGW SMXHW XSUAG FNXTL

We gaan nu proberen de sleutellengte te achterhalen. Als voorbeeld laat ik voor een deel van de eerste regel zien hoe je te werk gaat. Dit laten zien voor de hele tekst kost te veel tijd en voegt niets toe. De uitkomst van analyse op de hele tekst is te zien in de tabel onderaan.

- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DSME UHLRI CSIGH VXQYM IUGLR FGHIP OSV
  1 positie verschoven, 0 overeenkomsten.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DSM EUHLR ICSIG HVXQY MIUGL RFGHI POSV
  2 posities verschoven, 0 overeenkomsten.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DS MEUHL RICSI GHVXQ YMIUG LRFGH IPOSV
  1
  3 posities verschoven, 1 overeenkomst.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  D SMEUH LRICS IGHVX QYMIU GLRFG HIPOS V
  1
  4 posities verschoven, 1 overeenkomst.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SV
  1
  5 posities verschoven, 1 overeenkomst.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DSME UHLRI CSIGH VXQYM IUGLR FGHIP OSV
  6 posities verschoven, 0 overeenkomsten.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DSM EUHLR ICSIG HVXQY MIUGL RFGHI POSV
  7 posities verschoven, 0 overeenkomsten.
- DSMEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
  DS MEUHL RICSI GHVXQ YMIUG LRFGH IPOSV
  1 2
  8 posities verschoven, 2 overeenkomsten.

Gaan we nu de hele tekst vergelijken met de verschoven tekst, dan vinden we de resultaten die in onderstaande tabel staan.

Aantal posities verschoven	1	2	3	4	5	6	7	8
Aantal overeenkomsten	10	6	6	20	9	11	9	20

Je ziet dat de overeenkomsten groter zijn bij 4 posities verschoven en bij 8 posities verschoven.

Opgave 22

Welke sleutellengte denk je dat de sleutel heeft die voor de vercijfering in het voorbeeld gebruikt is? Waarom?

De methode van Kasiski om de sleutellengte te achterhalen 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.

Opgave 23

Stel dat het sleutelwoord inderdaad uit 4 letters bestaat. In een stuk te vercijferen tekst staat het letterpaar "IN" meerdere keren. Het letterpaar "IN" staat een keer op de 7^e en 8^e positie van de tekst, en een keer op 23^e en 24^e positie van de tekst.

a) Wat gebeurt er met de beide IN's als je gaat vercijferen?
b) Leg uit wat je hier aan hebt.
c) Deze methode werkt alleen als de letterparen een veelvoud van de sleutellengte uit elkaar liggen. Waarom?

Opgave 24

a) Onderzoek in de tekst over de Chinese eetstokjes met bovenstaande methode of er reden is om aan te nemen dat de lengte van het sleutelwoord 4 is.
Tip: kijk bijvoorbeeld naar het letterpaar "LR".
b) Achterhaal het codewoord dat gebruikt is om de tekst over de Chinese eetstokjes te vercijferen.

Opgave 25

Zoals je gezien hebt, is het mogelijk de sleutellengte te achterhalen.

Hoe kun je de sleutel kiezen als je toch Vigenère zou willen gebruiken en een niet al te groot risico wilt lopen dat je bericht ontcijferd wordt?

3.5 Polyalfabetische substitutie en het autokey-systeem

Polyalfabetische substitutie is een verbetering van het Vigenèresysteem. Bij Vigenère wordt eigenlijk een aantal keer het schuifcryptosysteem gebruikt, bij polyalfabetische substitutie is dat een aantal keer een monoalfabetische substitutie die steeds herhaald wordt. Je hebt dan bijvoorbeeld 4 keer een gepermuteerd (=gehusseld) alfabet. Voor de vercijfering van de eerste letter gebruik je de eerste permutatie van het alfabet, voor de tweede letter de tweede permutatie van het alfabet, voor de derde letter de derde permutatie van het alfabet, voor de vierde letter de vierde permutatie van het alfabet, voor de vijfde letter weer de eerste permutatie van het alfabet, voor de zesde letter weer de tweede permutatie van het alfabet, enz.

Opgave 26

Is een boodschap die vercijferd is met de polyalfabetische substitutie veel moeilijker om te ontcijferen dan een boodschap die vercijferd is met Vigenère of valt dat wel mee? Leg je antwoord uit.

Het cryptosysteem dat Vigenère wel beschreef wordt *autoclave-* , *autokey-* of *autosleutelsysteem* genoemd. Dit systeem lijkt erg veel op het Vigenèresysteem. Het verschil is dat dit systeem het sleutelwoord slechts één keer aan het begin van de tekst gebruikt. Daarna gebruikt men in plaats van het sleutelwoord de oorspronkelijke tekst. Doordat nu niet steeds het sleutelwoord herhaald wordt, is het systeem moeilijker te kraken.

Voorbeeld:
We vercijferen hieronder de zin "AUTOCLAVE IS EEN VERBETERING VAN VIGENERE" met behulp van het sleutelwoord "BETER".

AUTOC LAVEI SEENV ERBET ERING VANVI GENÈR EXQXQ
BETER AUTOC LAVEI SEENV ERBET ERING VANVI GENER
BYMST LUOSK DEZRD WVFRO IIJRZ ZRVIO BEAZZ KBFBH

Opgave 27

Waarom is dit systeem moeilijker te kraken dan het Vigenèresysteem van Belaso?

Dit systeem is ongeveer 200 jaar ongekraakt gebleven. Uiteindelijk heeft Charles Babbage ook dit systeem gekraakt. Als je wilt weten hoe hij dat deed, kun je dat opzoeken op *http://en.wikipedia.org/wiki/Autokey_cipher*.

4 Coderen

Bij diverse cryptosystemen die we in het vorige hoofdstuk hebben bekeken, was het nodig om de symbolen van de klare tekst eerst om te zetten naar getallen. De zender en ontvanger moeten op dezelfde manier tekens en getallen met elkaar in verband brengen, maar de manier waarop ze dat doen hoeft niet geheim te blijven. Sterker nog: je kunt veel beter gebruik maken van een (internationale) standaard. Dan hoef je ook niet met alle partijen waar je mee wilt communiceren afzonderlijk af te spreken welke koppeling tussen symbolen en getallen je gaat gebruiken. Eigenlijk valt dit deel van het uitwisselen van berichten dus niet onder cryptografie. We geven het daarom een andere naam: onder coderen verstaan we het omzetten van symbolen naar getallen; het terugvertalen van getallen naar symbolen noemen we decoderen.

De internationale standaard die we in de rest van deze lessenserie gaan gebruiken is de ASCII-codering. De term ASCII is een afkorting van American Standard Code for Information Interchange. Computers begrijpen alleen getallen, dus een ASCII code is de numerieke weergave van een karakter zoals de 'a' of '@' of een of andere actie. De codes 000 t/m 031 zijn bestemd voor systeemopdrachten (als bijvoorbeeld ”start of text”, ”carriage return”, enzovoort). De codes na 126 zijn voor speciale tekens.

Voorbeeld
De zin

> Ik wou dat ik 2 hondjes was.

wordt gecodeerd in de volgende rij gehele getallen

> 073 107 032 119 111 117 032 100 097 116 032 105 107 032 050 032 104 111 110 100 106 101 115 032 119 097 115 046

Opgave 1

> Tel het aantal tekens in de zin uit het voorbeeld en het aantal getallen in de codering. Is dit gelijk? Zo niet, wat heb je dan bij het tellen over het hoofd gezien?

Op de volgende bladzijde staat een tabel met voor een groot aantal tekens het bijbehorende getal. Zo zie je bijvoorbeeld dat bij de hoofdletter ‘A’ het getal vijfenzestig hoort. Om er echter voor te zorgen dat alle symbolen een code krijgen van dezelfde lengte, schrijven we 065.

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

Opgave 2

Codeer de zin “Tussen Keulen en Parijs.”.

Cryptosystemen die een boodschap letter voor letter versleutelen zijn kwetsbaar. We hebben al gezien dat een eenvoudige methode als frequentieanalyse zulke systemen vaak kan kraken. Dit wordt ondervangen door steeds een vast aantal getallen uit de codering aan elkaar te plakken en de versleuteling uit te voeren op deze (grote) getallen. In de praktijk zijn dat er meer, maar wij zullen ons beperken tot steeds twee getallen samennemen. Dat maakt aan de ene kant het kraken met behulp van frequentie-analyse al een stuk lastiger en aan de andere kant blijft het nog net hanteerbaar: een deel van de berekeningen is nog uit te voeren met behulp van de grafische rekenmachine. Als we verderop berekeningen moeten maken waar de grafische rekenmachine het niet meer aankan, dan stappen we terug naar losse letters of we zetten de computer in.

Opgave 3

Decodeer de volgende boodschap:
079112 032077 097114 115032 105115 032119 097116 101114 032103 101118 111110 100101 110033

Opgave 4

Leg uit waarom het bij deze manier van werken nodig is dat alle getallen door evenveel cijfers worden weergegeven.

5 Getaltheorie

Moderne cryptosystemen maken veel gebruik van wiskunde. Met name priemgetallen en modulo-rekenen spelen een belangrijke rol. We beginnen daarom in dit hoofdstuk met twee paragrafen over delers en priemgetallen. Daarna halen we onze kennis over verzamelingen kort op. Tot slot zullen we uitgebreid ingaan op wat modulo-rekenen is en welke regels er gelden voor modulo-rekenen.

We zullen hier over het algemeen niet bewijzen waarom de regels die we vinden gelden. In hoofdstuk 7 doen we dat wel.

5.1 Delers en priemgetallen

Een geheel getal a is een *deler* van een geheel getal b als het getal a precies een geheel aantal keer in het getal b past. Meer wiskundig: een geheel getal a is een *deler* van een geheel getal $b$als er een geheel getal k is, zodanig dat er geldt $a \cdot k = b$.

In de wiskunde is er een notatie voor “deler zijn van”. Deze notatie is een verticale rechte streep: |. Wanneer je schrijft $a|b$, bedoel je dus dat a een deler is van b.

Opgave 1
Geef voor elk van de onderstaande beweringen aan of hij waar of niet waar is.

- **a)** $5|345$
- **b)** $25|5$
- **c)** $5|0$
- **d)** $7|25$
- **e)** $6|8$
- **f)** $6|6$
- **g)** $1|7$

Opgave 2

- **a)** Hoeveel delers hebben, 8, 81 en 49?
- **b)** Hoeveel delers heeft $8 \cdot 81 \cdot 49$?

Opgave 3

Hoeveel delers heeft een positief geheel getal dat groter is dan 1 minimaal?

Een *priemgetal* is een positief geheel getal ≥ 2dat precies twee positieve delers heeft, namelijk 1 en zichzelf.

Opgave 4

Geef de eerste 10 priemgetallen.

Alle priemgetallen kleiner dan een zeker getal n vinden, is niet zo heel moeilijk. Het kost alleen behoorlijk wat tijd als het getal n groot is. Een systematische manier om priemgetallen te vinden is "*de zeef van Eratosthenes*". De zeef van Eratosthenes werkt als volgt:

1. Schrijf de getallen van 2 t/m n op.
2. Omcirkel het kleinste getal dat niet doorgestreept of omcirkeld is.
3. Streep alle veelvouden van het getal dat je net omcirkeld hebt door.
4. Ga naar stap 2 als er nog getallen zijn die niet doorgestreept of omcirkeld zijn. Als alle getallen doorgestreept of omcirkeld zijn, ben je klaar. Alle omcirkelde getallen zijn priemgetallen.

Opgave 5

Geef met behulp van de zeef van Eratosthenes alle priemgetallen kleiner dan 100.

Opgave 6

a) Waarom begin je bij stap 1 met opschrijven bij de 2 en niet lager?
b) Waarom weet je zeker dat priemgetallen niet doorgestreept worden?
c) Waarom weet je zeker dat getallen die geen priemgetallen zijn doorgestreept worden?

Positieve gehele getallen ≥ 2 met meer dan twee positieve delers heten *samengesteld.* Ieder positief geheel getal ≥ 2 kun je schrijven als een product van priemgetallen. Een *veelvoud* van *a* is een getal dat *a* als deler heeft.

Voorbeeld:
$24 = 3 \cdot 2 \cdot 2 \cdot 2 = 3 \cdot 2^3$. We zeggen dat 24 twee *priemdelers* heeft, nl. 2 en 3, en vier *priemfactoren* omdat 24 het product is van vier priemgetallen. Een getal schrijven als een product van priemgetallen noemen we *ontbinden in priemfactoren.*

Opgave 7

1, 41, 91, 101, 121, 231.

a) Welke van de bovenstaande getallen zijn samengesteld en welke zijn priemgetallen?
b) Geef van de samengestelde getallen de priemfactoren.

Marin Mersenne (1588-1648)

In de moderne cryptografie zijn priemgetallen erg belangrijk. Dit komt doordat het voor producten van twee heel grote priemgetallen van bijvoorbeeld elk 150 cijfers lang, heel erg moeilijk is de priemfactorontbinding te bepalen. Van de priemgetallen die nodig zijn voor moderne cryptografie zijn er heel veel bekend. Zoveel zelfs dat je ze niet allemaal kunt gaan proberen om een ontbinding van $m$te vinden. Veel grotere priemgetallen van bijvoorbeeld miljoenen cijfers lang vinden, is niet eenvoudig. De grootste bekende priemgetallen zijn Mersenne-priemgetallen, genoemd naar de Franse wiskundige Marin Mersenne. Deze priemgetallen zijn van de vorm $2^p - 1$, waarbij $p$een priemgetal is. Maar niet alle getallen van deze vorm zijn priemgetallen. Voor getallen van deze vorm bestaan testen om te onderzoeken of ze priem zijn. Het grootste priemgetal dat op het moment

dat deze lessenserie geschreven wordt bekend is, is $2^{32582657} - 1$. Dit getal is het 44e Mersenne-priemgetal, bestaat uit 9808358 cijfers en is in september 2006 door wetenschappers van de Central Missouri State University, in het kader van het GIMPS (Great Internet Mersenne Prime Search project) gevonden.

Priemfactoren van een groot samengesteld getal vinden is nog veel moeilijker. Zo is bijvoorbeeld wel bekend dat het getal $2^{2^{14}} + 1$ niet priem is, maar is er geen enkele priemfactor van bekend.

5.2 Grootste gemene delers en het algoritme van Euclides

In deze paragraaf gaan we dieper in op eigenschappen van delers die getallen gemeenschappelijk hebben. Ook zullen we een methode bekijken om eenvoudig de grootste gemeenschappelijke deler van getallen te kunnen vinden.

Opgave 8

- **a)** Geef de positieve delers van 120.
- **b)** Geef de positieve delers van 112.
- **c)** Wat zijn de gemeenschappelijke delers van 120 en 112?
- **d)** Wat is grootste gemeenschappelijke deler van 120 en 112?

In hoofdstuk 3 hadden we het al even over de grootste gemene deler. De grootste gemene deler van *a* en *m* is het grootste gehele getal dat deler is van zowel *a* als *m*. We noteren dit als ggd(*a*,*m*).

Wanneer je de grootste gemene deler van twee getallen groter dan of gelijk aan 2 zoekt, kun je als volgt te werk gaan. Je zoekt de priemfactoren die in beide getallen voorkomen en schrijft daarom de priemfactorontbinding van beide getallen op. Vervolgens neem je het product van de factoren die in beide ontbindingen voorkomen.

Voorbeeld:
Bereken ggd(980, 504). $980 = 2^2 \cdot 5 \cdot 7^2$, $504 = 2^3 \cdot 3^2 \cdot 7$. In beide priemfactorontbindingen zit twee keer de priemfactor 2 en een keer de priemfactor 7, dus $ggd(980{,}504) = 2^2 \cdot 7 = 28$.

Opgave 9

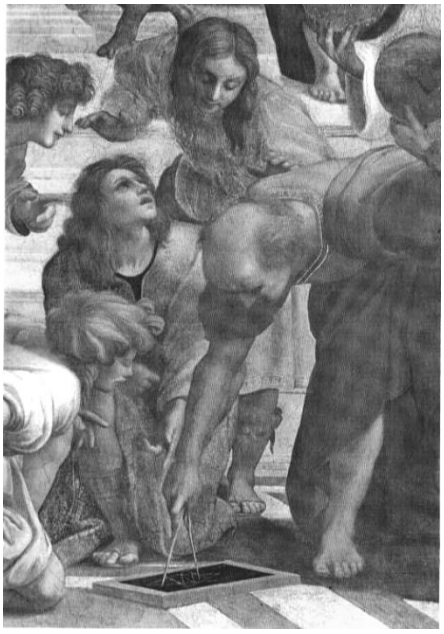
- **a)** Bereken ggd(252, 198).
- **b)** Bereken ggd(6466, 5429).
- **c)** Bereken ggd(47, 0).
- **d)** Geef ggd(*a*, 0) met $a \neq 0$.

Deze methode is goed te doen voor kleine getallen, maar voor grote getallen is de priemfactorontbinding erg moeilijk te vinden en kun je deze methode dus niet gebruiken.


Euclides van Alexandrië

De Griek Euclides van Alexandrië (niet te verwarren met Euclides van Megara, de leerling van Socrates!) heeft een methode beschreven waarmee je de grootste gemene deler wel voor grote getallen kunt berekenen. Euclides is één van de belangrijkste wiskundigen van de afgelopen 2400 jaar.

In de derde eeuw voor Chr. schreef Euclides op basis van de voorschriften van Plato zijn wereldberoemde werk ‘De Elementen’, een boek waarin hij de eigenschappen van geometrische vormen en gehele getallen afleidt uit een verzameling axioma’s. Axioma’s zijn uitgangspunten die niet bewezen worden, maar als grondslag aanvaard zijn. Uit een aantal axioma’s worden andere stellingen afgeleid. Euclides wordt daarom wel beschouwd als een voorloper van de axiomatische methode in de moderne wiskunde. Veel van de resultaten die Euclides in ‘De Elementen’ beschreef, waren afkomstig van eerdere wiskundigen. Het is echter een grote prestatie van Euclides om dit in één logisch coherent raamwerk te verbinden. Tot de 20ste eeuw was dit boek samen met de bijbel één van de meest gedrukte boeken.



Hiernaast zie je een fragment uit ‘De school van Athene’, een beroemd werk van Rafael (Italië, 1483-1520). Op dit fragment zie je Euclides aan het werk.

Van de wiskunde die Euclides in ‘De Elementen’ beschreef, gebruiken we in de cryptografie niets. Het algoritme van Euclides dat we nu gaan bespreken is wel een belangrijke stelling in de cryptografie.

Opgave 10
Het getal 11 is deler van 66 en 33.

- **a)** Is het getal 11 ook deler van $66 + 33$?
- **b)** Is het getal 11 ook deler van $66 - 33$?
- **c)** Is het getal 11 ook deler van $33 - 66$?

Opgave 11
Het getal d is deler van de getallen a en m.

- **a)** Leg uit dat er getallen v en w zijn waarvoor geldt dat $a = v \cdot d$ en $m = w \cdot d$.
- **b)** Druk $a + m$ en $a - m$ uit in v, w en d.
- **c)** Leg uit dat $d|(a + m)$ en $d|(a - m)$.

Opgave 12
Gegeven is dat $d = ggd(a, m)$. Het getal q is een geheel getal.

- **a)** Leg uit dat $d|(a - q \cdot m)$.
- **b)** Leg uit dat m en $(a - q \cdot m)$ geen grotere deler dan d gemeenschappelijk kunnen hebben en dat er dus geldt dat $d = ggd(m, a - q \cdot m)$.

We hebben nu gezien dat we de grootste gemene deler van een paar getallen kunnen vinden, zonder eerst alle delers op te moeten schrijven. We trekken telkens het kleinste getal een aantal keer van het grootste getal af. Omdat we graag met zo klein mogelijke getallen rekenen, kunnen we het kleinste getal het beste zo vaak mogelijk van het grootste getal aftrekken, maar wel zo dat de uitkomst positief blijft.

Opgave 13
Bereken op bovenstaande manier:

a) $ggd(252,198)$
b) $ggd(6466,5429)$
c) $ggd(47,0)$

Opgave 14
Gegeven zijn de positieve gehele getallen a, m en q, zodanig dat $a > m$ en dat q het grootste getal is waarvoor geldt dat $a - q \cdot m \geq 0$. Er geldt dus $a - qm = rest(a:m)$.

a) Leg uit dat $ggd(a,m) = ggd(m, rest(a:m))$.
b) Onderzoek of $ggd(a,m) = ggd(m, rest(a:m))$ ook geldt als $m > a$.

De methode om een grootste gemene deler snel te berekenen die we in de bovenstaande opgaven ontdekt hebben, heet het "Algoritme van Euclides".

Algoritme van Euclides:
Voor alle positieve gehele getallen a is ggd$(a, 0) = a$ en als m een positief geheel getal is, dan geldt $ggd(a,m) = ggd(m, rest(a:m))$. Dit wordt herhaald tot de rest 0 is.

Voorbeeldje:
Bereken ggd(99, 45) met behulp van het algoritme van Euclides.

- 99 : 45 = 2 rest 9, want $99 = 2 \cdot 45 + 9$,
  dus ggd(99, 45) = ggd(45, 9).
- 45 : 9 = 5 rest 0, want $45 = 5 \cdot 9 + 0$,
  dus ggd(45, 9) = ggd(9,0) = 9 (want ggd(a, 0) = a).

Hieruit volgt dus ook ggd(99, 45) = 9.

Voor een berekening met kleine getallen kun je de berekening wel als hierboven opschrijven. Voor grote getallen wordt het wat onoverzichtelijk. We zetten de tussenstappen daarom in een tabel. We willen de 2 en de 9 uit de uitkomst 2 rest 9 graag in twee verschillende kolommen zetten. De 9 is de rest na deling. De rest geven we aan met de letter r. De 2 is het gehele deel van het quotiënt. Dit gehele deel geven we aan met de letter q.

a	m	q	r
99	45	2	9
45	9	5	0
9	0		

Op elke regel is de$ggd(a,m)$ gelijk, dus $ggd(99,45) = ggd(45,9) = ggd(9,0) = 9$.

Voorbeeld:
Bereken $ggd(148104,47223)$.
Het algoritme van Euclides toepassen levert:

a	m	q	r
148104	47223	3	6435
47223	6435	7	2178
6435	2178	2	2079
2178	2079	1	99
2079	99	21	0
99	0		

Opgave 15

a) Waar vind je de grootste gemene deler in de tabel?
b) Wat is dus ggd(148104,47223)?

Opgave 16

a) Bereken ggd(96, 22) met behulp van het algoritme van Euclides.
b) Bereken ggd(484, 576).
c) Bereken ggd(47957, 32395).

Wanneer je dit voor echt grote getallen moet doen, doe je het natuurlijk niet met de hand, maar wordt er een computerprogramma geschreven dat het werk voor je doet. Dit is niet zo moeilijk en je zou het eens kunnen proberen als je informatica hebt gekozen.

5.3 Modulo-rekenen

In het vorige hoofdstuk hebben we een onderscheid aangebracht tussen coderen en versleutelen. Doordat we het omzetten van rijtjes symbolen naar getallen en omgekeerd op een van tevoren afgesproken manier gaan doen, kunnen we ons bij het beschrijven van de cryptosystemen beperken tot het werken met getallen. In de systemen die we in hoofdstuk 3 hebben bekeken, hadden we maar 26 symbolen en daarmee hadden we aan de getallen 0 tot en met 25 genoeg. De bewerkingen die we met deze getallen hebben uitgevoerd lieten zich eenvoudig informeel beschrijven. Nu we de beschikking hebben over meer symbolen en we ook nog gaan werken met rijtjes symbolen, krijgen we te maken met veel grotere getallen. En omdat we ons niet vast willen leggen op welke getallen er in onze boodschappen voor zullen komen, is het nodig wat gestructureerder naar de bewerkingen met gehele getallen te kijken.

Bij affiene cryptografie was het nodig om bij elke uitkomst van een berekening te bepalen wat de rest bij deling door 26 was. Op die manier bestond zowel de onbewerkte als de versleutelde boodschap uit een rij van getallen uit de verzameling $0,1,\ldots,25$. In de komende paragrafen wordt dat idee uitgebreid.

Hoeveel pootjes van 25 cm kun je zagen uit een balk van 240 cm? Het antwoord dat de rekenmachine geeft bij de deling $240:25$ is in dit geval onzin: als je pootjes van 25 cm nodig hebt, dan heb je niets aan het laatste stukje dat toch te klein is. Als k het (grootste) aantal pootjes van 25 cm is dat we uit de balk van 240 cm kunnen zagen, dan is k het grootste gehele getal dat voldoet aan $25 \cdot k \leq 240$. In dit geval is dat dus 9.

Om onderscheid te maken tussen de 'breukdeling' $240:25$ (= 9,6) en de geheeltallige deling noteren we deze laatste als 240 div 25 (= 9). Voor positieve gehele getallen a en m verstaan we onder $a\ div\ m$ dus het geheel aantal keren dat m in a past.

Voor negatieve gehele getallen a is het wat lastiger in te zien wat $a\ div\ m$ zou moeten zijn. Bij de positieve gehele a zochten we de grootste gehele k die voldeed aan $k \cdot m \leq a$. We spreken af dat we dat voor negatieve gehele a net zo doen. Wanneer we $(-240)\ div\ 25$ berekenen, komt daar dus -10 uit, want $-10 \cdot 25 = -250$ en dat is kleiner dan -240. De uitkomst -9 is niet goed, want $-9 \cdot 25 = -225$ en dat is meer dan -240.

Formeel kunnen we de operator div dus als volgt vastleggen:

Voor gehele getallen a en positieve gehele getallen m is $a\ div\ m$ het grootste gehele getal k dat voldoet aan $k \cdot m \leq a$.

Opgave 17
Bereken:

- **a)** 17 div 5.
- **b)** 944 div 13.
- **c)** 91 div 7.
- **d)** (-22) div 7.

Zoals je bij het zagen van pootjes uit een balk in het algemeen iets overhoudt, blijft er bij geheeltallige deling in het algemeen een rest over. Bij deling van 25 door 7 is het resultaat 3. Maar $3 \cdot 7$ maakt de 25 niet vol. Er blijft als rest over: $25 - 3 \cdot 7 = 25 - 21 = 4$. Deze rest noteren we als $25 \bmod 7$. We spreken dit uit als: "25 modulo 7". De rest van een geheel getal bepalen na deling door m, noemen we a reduceren modulo m.

In het algemeen is voor gehele getallen a en positieve gehele getallen m het getal $a\ mod\ m$ de rest bij geheeltallige deling van a door m. Formeel:

Voor gehele getallen a en positieve gehele getallen m is $a\ mod\ m = a - m \cdot (a\ div\ m)$, de rest bij geheeltallige deling van a door m.

Opgave 18
Bereken:

- **a)** $17 \bmod 5$.
- **b)** $944 \bmod 13$.
- **c)** $91 \bmod 7$.
- **d)** $(-22) \bmod 7$.

De operatoren div en mod voldoen aan de volgende eigenschappen:

Voor gehele getallen a en positieve gehele getallen m geldt (1) $a = m \cdot (a \text{ div } m) + (a \bmod m)$ (2) $0 \leq a\ mod\ m < m$

Opgave 19

- **a)** Controleer deze eigenschappen voor $a = 17$ en $m = 5$.
- **b)** Controleer deze eigenschappen voor $a = -22$ en $m = 7$.
- **c)** Leg uit hoe deze twee eigenschappen volgen uit de definities van div en mod.

Als we berekeningen modulo een bepaald getal moeten uitvoeren, kunnen we gebruik maken van een aantal rekenregels. We zullen deze regels hier aan de hand van voorbeelden aannemelijk maken, maar ze niet bewijzen. In hoofdstuk 7 kom je precies te weten waarom de rekenregels kloppen.

Opgave 20
We hebben een balk van 240 cm en een balk van 190 cm en we gaan daar zo veel mogelijk pootjes van 25 cm afzagen.

a) Hoeveel cm houden we bij elke balk over?
b) Het is niet verrassend dat we dezelfde lengte overhouden. Waarom niet?

We zagen in deze opgave dat het verschil van twee getallen een veelvoud is van m als de twee getallen dezelfde rest hebben na deling door m. Dit resulteert in de volgende regel:

Voor gehele getallen a en b en positieve gehele getallen m geldt:
$a \bmod m = b \bmod m$ precies dan als $(a - b) \bmod m = 0$.

Opgave 21

a) Controleer deze eigenschap voor $a = 17$, $b = 32$ en $m = 5$.
b) Laat zien dat het drietal $a = 22$, $b = 35$ en $m = 11$ niet voldoet.
c) Geef een m zodanig dat het drietal $a = 22$, $b = 35$ en m wel voldoet.

Opgave 22
We hebben een balk van 240 cm en een balk van 155 cm. We plakken de balken aan elkaar en zagen hier pootjes van 25 cm van.

a) Hoe lang is het stukje balk dat we uiteindelijk overhouden?

We doen hetzelfde nog een keer, maar nu met een balk van 190 cm en een balk van 305 cm.

b) Hoe lang is nu het stukje balk dat we uiteindelijk overhouden?
c) Leg uit waarom de uitkomsten bij **a)** en **b)** hetzelfde zijn.

Opgave 23
We nemen 7 balken van 240 cm en zagen er pootjes van 25 cm van. Vervolgens plakken we alle restanten aan elkaar en zagen daar ook weer pootjes van 25 cm van.

a) Hoe lang is het stukje balk dat we uiteindelijk overhouden?

We doen hetzelfde met 7 balken van 190 cm.

b) Hoe bereken je makkelijk hoe lang het stukje is dat we uiteindelijk overhouden?

Weer hetzelfde, dit keer met 32 balken van 240 cm.

c) Hoe bereken je nu makkelijk hoe lang het stukje is dat we uiteindelijk overhouden?
d) Waarom doen die 25 balken extra er niet toe?

In opgaven 22 en 23 hebben we een idee gekregen hoe het optellen en vermenigvuldigen bij modulo-rekenen werkt. Inderdaad blijkt er een somregel en een productregel voor het modulo-rekenen te zijn:

Voor gehele getallen a, b, c en d en positieve gehele getallen m geldt:
als $a \bmod m = b \bmod m$ en $c \bmod m = d \bmod m$ dan
Somregel: $(a + c) \bmod m = (b + d) \bmod m$
Productregel: $(a \cdot c) \bmod m = (b \cdot d) \bmod m$

Opgave 24
Bereken de volgende uitdrukkingen. Doe dit zonder je rekenmachine te gebruiken en geef steeds aan welke rekenregel je gebruikt.

a) $(123 + 456)\ mod\ 10$.
b) $(113 \cdot 222)\ mod\ 10$.
c) $17 \cdot (355 + 773)\ mod\ 7$.

In het hoofdstuk over symmetrische cryptografie rekenden we met de getallen 0 tot en met 25, de rangnummers van de 26 letters in het alfabet. Liep je door de rekenkundige bewerkingen (optellen en vermenigvuldigen) uit dit domein, dan bracht je met behulp van modulo-rekenen het resultaat terug tot een getal in dit domein, ook al noemden we dat nog niet zo. Wanneer het duidelijk is dat we modulo m rekenen, laten we het "$mod\ m$" soms weg.

In de wiskunde noemen we twee getallen a en b *congruent modulo* m als ze dezelfde rest hebben bij deling door het gehele getal m, waarbij $m \geq 1$. We noteren dit als volgt: $a \bmod m = b \bmod m$ ofwel $a \equiv_m b$. Congruent modulo m zijn geeft dus een relatie aan tussen getallen.
We verdelen de gehele getallen nu in verzamelingen getallen in, die dezelfde rest hebben na deling door m. Zo'n verzameling van getallen die dezelfde rest hebben na deling door m noemen we een *restklasse*. We noteren een restklasse als een getal uit de restklasse tussen rechte haken, met als index het getal m. Als er geen misverstand kan zijn over wat het getal m is, wordt een restklasse aangegeven door een streepje boven een getal uit de restklasse te zetten.

Voorbeeld:
Als je modulo 7 rekent, geldt $\overline{2} = \{\ldots, -12, -5, 2, 9, \ldots\}$ want alle getallen in de verzameling $\{\ldots, -12, -5, 2, 9, \ldots\}$ hebben rest 2 als je ze door 7 deelt. Je kunt dit ook noteren als $\bar{2} = \{x \in \mathbb{Z} | x \equiv_7 2\}$. Je bedoelt hiermee dat alle getallen in de restklasse $\overline{2}$ gehele getallen zijn (het stukje "$x \in \mathbb{Z}$" voor de streep) en dat je bovendien de extra eis stelt dat alle getallen modulo 7 congruent zijn met 2 (het stukje "$x \equiv_7 2$ na de streep).

De verzameling van alle restklassen modulo m noemen we $\mathbb{Z}_m$. Je kunt $\mathbb{Z}_m$ dus als volgt weergeven: $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-2}, \overline{m-1}\}$.
Als je modulo 7 rekent is de restklasse $\overline{2}$ dezelfde restklasse als $\overline{9}$ en $\overline{51}$. De getallen 2, 9 en 51 hebben immers dezelfde rest na deling door 7. De getallen 2, 9 en 51 zijn in $\mathbb{Z}_7$ voorbeelden van *representanten* van de restklasse $\overline{2}$.
Wanneer we in $\mathbb{Z}_m$ werken kan bijvoorbeeld de restklasse $\overline{2}$ geschreven worden als de representant 2.

Voorbeeld:
Bereken $7 \cdot 5$ in $\mathbb{Z}_{12}$.
Berekening: $(7 \cdot 5)\ mod\ 12 = 35\ mod\ 12 = 11$ ofwel $7 \cdot 5 \equiv 11$ in $\mathbb{Z}_{12}$.

Opgave 25
Vul onderstaande tabellen in $\mathbb{Z}_5$ in.

+	0	1	2	3	4
0					
1					
2					
3					
4					

·	0	1	2	3	4
0					
1					
2					
3					
4					

Opgave 26
Los de volgende vergelijkingen op:
- **a)** In $\mathbb{Z}_5$: $3 + x = 1$
- **b)** In $\mathbb{Z}_8$: $3 + x = 1$
- **c)** In $\mathbb{Z}_{19}$: $14 + x = 5$
- **d)** In $\mathbb{Z}_{19}$: $11 + x = 0$

Het oplossen van vergelijkingen van het type zoals in de vorige opgave zal niet zoveel problemen geven. Ook zonder dat je de hele opteltabel hebt uitgeschreven lukt het wel $14 + x = 5$ op te lossen in $\mathbb{Z}_{19}$. In $\mathbb{Z}_{19}$ kun je $14 + x = 5$ eenvoudig oplossen door $x = (5 - 14) mod 19 = -9 mod 19 = 10$.

Je kunt het ook als volgt zien: in $\mathbb{Z}_{19}$ betekent $14 + x = 5$ eigenlijk $(14 + x)\ mod\ 19 = 5$ en dat wil zeggen dat je rest 5 overhoudt als je $14 + x$ door 19 deelt. Er is dus een k zodanig dat $14 + x - 19 \cdot k = 5$, ofwel $9 + x = 19 \cdot k$. Voor $k = 0$ levert dit $9 + x = 0$, dit geeft $x = -9 = 10\ mod\ 19$, voor $k = 1$ levert dit $9 + x = 19$, dus $x = 10$, etc. Voor elke waarde van *k* levert de vergelijking een *x*-waarde op welke representant is van de restklasse $\overline{10}$.

Opgave 27
Los de volgende vergelijkingen op:
- **a)** In $\mathbb{Z}_{23}$: $16 + x = 7$
- **b)** In $\mathbb{Z}_{1278}$: $756 + x = 341$

Je ziet dat een vergelijking met een optelling oplossen niet zo moeilijk is. Wanneer er een vermenigvuldiging in de vergelijking zit, is een oplossing vinden minder eenvoudig. Een van de problemen is het volgende.

Als je niet modulo-rekent, kun je concluderen dat als $ac = bc$, dat dan daaruit $a = b$ volgt. Bij modulo-rekenen geldt niet altijd dat als $a \cdot c = b \cdot c$ in $\mathbb{Z}_m$ dat dan $a = b$ in $\mathbb{Z}_m$.

Opgave 28

- **a)** Ga dit na voor $a = 12, b = 7, c = 6$ en $m = 10$.
- **b)** Leg uit waarom het in dit voorbeeld niet geldt.
- **c)** Wat voor een getal moet *m* zijn om wel te laten gelden dat $a = b$ in $\mathbb{Z}_m$ als $a \cdot c = b \cdot c$ in $\mathbb{Z}_m$?

Afgezien daarvan is het ook lastig omdat je niet eenvoudig links en rechts door hetzelfde getal kunt delen.

Opgave 29

- **a)** Codeer de tekst "NIJMEGEN" op de manier zoals die in hoofdstuk 4 is aangegeven.
- **b)** Versleutel deze boodschap met de encryptiefunctie $E(x) = (1234 \cdot x + 192731) \ mod \ 437217$.

Opgave 30

Een boodschap is op de afgesproken manier gecodeerd en daarna versleuteld met de encryptiefunctie $E(x) = (x + 398843) \ mod \ 468713$. De versleutelde boodschap is 466957 027229 034246 031240.

Ontcijfer en decodeer deze boodschap.

In de volgende paragraaf gaan we bekijken wanneer een vergelijking van de vorm $(a \cdot x) \, mod \, m = 1$ een oplossing heeft en hoe we die kunnen vinden.

5.4 Inverse

Opgave 31

Los de volgende vergelijkingen op in $\mathbb{Z}_{37}$:

- **a)** $10x = 4$
- **b)** $10x = 5$

Het oplossen van vergelijkingen waarin vermenigvuldigingen voorkomen zijn lastig en vragen in ieder geval veel werk. We kijken eens hoe we een dergelijke vergelijking oplossen als we niet modulo-rekenen.

Om de vergelijking $5 \cdot x = 3$op te lossen ga je als volgt te werk:

$$5 \cdot x = 3$$
$$\tfrac{1}{5} \cdot 5 \cdot x = \tfrac{1}{5} \cdot 3$$
$$x = \tfrac{3}{5}$$

Het getal $\frac{1}{5}$ is het *omgekeerde* van 5: het getal waarmee je 5 moet vermenigvuldigen om 1 te krijgen. In plaats van omgekeerde spreken we ook wel van multiplicatieve inverse. Hiermee geven we duidelijk aan dat we de inverse bedoelen bij vermenigvuldigen.

De multiplicatieve inverse van 5 in $\mathbb{Z}_{34}$ is 7 (ga na!). Het oplossen van de vergelijking $5 \cdot x = 3$ in $\mathbb{Z}_{34}$ gaat nu als volgt:

$$\begin{aligned} 5 \cdot x &= 3 \\ 7 \cdot 5 \cdot x &= 7 \cdot 3 \\ 1 \cdot x &= 7 \cdot 3 \\ x &= 21 \end{aligned}$$

Wat we nu in feite hebben geïntroduceerd is delen in $\mathbb{Z}_m$. We zullen echter eigenlijk nooit expliciet spreken over delen. Bij het oplossen van vergelijkingen delen we niet; we vermenigvuldigen met de multiplicatieve inverse.

Opgave 32

a) Ga na dat $10 \cdot 6 = 1$ in $\mathbb{Z}_{59}$

Los de volgende vergelijkingen op in $\mathbb{Z}_{59}$:

b) $10x = 4$

c) $10x = 5$

d) Waarom is opgave 32 veel makkelijker dan opgave 31?

Afgezien van dat we een oplossing van de vergelijking $a \cdot x = 1$ in $\mathbb{Z}_m$ kunnen gebruiken om vergelijkingen van de vorm $a \cdot x = b$ in $\mathbb{Z}_m$ op te lossen, is de vergelijking $a \cdot x = 1$ in $\mathbb{Z}_m$ een hele belangrijke vergelijking in de cryptografie. In hoofdstuk 6 zullen we zien waarom dat zo is. Nu bekommeren we ons eerst om de vraag of de vergelijking wel voor iedere a en m een oplossing heeft.

We hebben nu gezien dat twee getallen elkaars multiplicatieve inverse heten als hun product 1 is. Er bestaan ook andere soorten inverses, maar die gebruiken we in deze lessenserie niet. We zullen daarom in het vervolg spreken over de "inverse" omdat het toch duidelijk is over wat voor een soort inverse we het hebben.

Als we niet modulo-rekenen, maar "gewoon" rekenen, is het niet moeilijk om bij een gegeven getal a zijn inverse b te vinden zodat $a \cdot b = 1$. Neem voor b het getal $\frac{1}{a}$ en je hebt een inverse van $a$gevonden. Wanneer we modulo-rekenen is het niet zo eenvoudig. We rekenen daar immers alleen met gehele getallen en kunnen dus niet zomaar de omgekeerde van een getal nemen.

We gaan ons buigen over de volgende twee vragen. Ten eerste: heeft ieder getal a wel een inverse in $\mathbb{Z}_m$? Ten tweede: hoe vind je zo'n inverse? De eerste vraag beantwoorden we in deze paragraaf, de tweede vraag in de volgende paragraaf.

Voorbeeld:
We gaan onderzoeken welke getallen een inverse hebben als we modulo 4 rekenen.
We zoeken bij a zijn inverse b in $\mathbb{Z}_4$. Er moet dus gelden $a \cdot b = 1$.
$a = 0$: Er is geen b zodat $0 \cdot b = 1$want voor iedere $b$geldt dat $0 \cdot b = 0$, dus 0 heeft geen inverse in $\mathbb{Z}_4$.
$a = 1$: Als $b = 1$ staat er $1 \cdot 1 = 1$, dus is 1 een inverse van 1 in $\mathbb{Z}_4$.
$a = 2$: $2 \cdot b$ is altijd even en dus nooit 1 in $\mathbb{Z}_4$, dus 2 heeft geen inverse in $\mathbb{Z}_4$.
$a = 3$: Als $b = 3$ staat er $3 \cdot 3 = 1$, dus is 3 een inverse van 3 in $\mathbb{Z}_4$.

Opgave 33

a) Welk getal heeft voor geen enkele m een inverse in $\mathbb{Z}_m$?

b) Welk getal heeft voor iedere m een inverse in $\mathbb{Z}_m$?

Opgave 34

a) In de volgende tabel rekenen we in $\mathbb{Z}_5$. Vul de inverse in als die er is.

Getal	0	1	2	3	4
Inverse					

b) In de volgende tabel rekenen we in $\mathbb{Z}_6$. Vul de inverse in als die er is.

Getal	0	1	2	3	4	5
Inverse						

c) In de volgende tabel rekenen we in $\mathbb{Z}_7$.Vul de inverse in als die er is.

Getal	0	1	2	3	4	5	6
Inverse							

d) In de volgende tabel rekenen we in $\mathbb{Z}_8$. Vul de inverse in als die er is.

Getal	0	1	2	3	4	5	6	7
Inverse								

e) In de volgende tabel rekenen we in $\mathbb{Z}_9$. Vul de inverse in als die er is.

Getal	0	1	2	3	4	5	6	7	8
Inverse									

f) In de volgende tabel rekenen we in $\mathbb{Z}_{10}$.Vul de inverse in als die er is.

Getal	0	1	2	3	4	5	6	7	8	9
Inverse										

g) In de volgende tabel rekenen we in $\mathbb{Z}_{11}$. Vul de inverse in als die er is.

Getal	0	1	2	3	4	5	6	7	8	9	10
Inverse											

h) Heb je al een vermoeden wanneer a wel een inverse in $\mathbb{Z}_m$ heeft en wanneer niet? Zo ja, formuleer je vermoeden.

Opgave 35

Als je de tabel bij opgave 36 goed hebt ingevuld, zie je dat steeds geldt dat de inverse van $m-1$ in $\mathbb{Z}_m$ het getal $m-1$ zelf is, dus dat $(m-1)^2 = 1$.

Laat dit zien door $(m-1)^2$ uit te werken.

Wanneer de grootste gemene deler van twee getallen 1 is, noemen we deze getallen *copriem* of *relatief priem* ofwel *onderling ondeelbaar*. Deze getallen hebben dus geen andere positieve deler dan 1 gemeenschappelijk. Dit hoeft niet te betekenen dat de getallen priemgetallen zijn.

Opgave 36

a) Noem een getal dat relatief priem is met 24.

b) Kan een even getal relatief priem zijn met 24?

c) Is ieder oneven getal relatief priem met 24?

Waarschijnlijk is het je in opgave 36 wel opgevallen dat a alleen een inverse in $\mathbb{Z}_m$ heeft als a en m relatief priem zijn. Dat dit in het algemeen zo is, volgt uit de volgende gedachtegang.

Je zoekt een inverse b zodanig dat $a \cdot b = 1$, dus geldt $m|ab-1$.

Dus is er een getal k zó dat $mk = ab - 1$, dus $ab - mk = 1$.
De grootste gemene deler van a en m noemen we d.
Dan is er dus een getal v zodanig dat $a = vd$ en een getal w zó dat $m = wd$.
Als a nu een inverse b in $\mathbb{Z}_m$ heeft, geldt er dus dat $vdb - wdk = 1$.
En dus ook dat $(vb - wk)d = 1$.
Maar dat kan alleen als $d = 1$. Dus heeft a alleen een inverse in $\mathbb{Z}_m$ hebben als a en m relatief priem zijn, dus als $ggd(a, m) = 1$.
Er geldt: a heeft een inverse in $\mathbb{Z}_m \leftrightarrow ggd(a, m) = 1$.

Opgave 37

Waarom kan $(vb - wk)d = 1$ alleen als $d = 1$?

We zoeken nu dus getallen b en k zodanig dat $ab - mk = 1$. In de volgende paragraaf zullen we het uitgebreide algoritme van Euclides bekijken. Met behulp van deze uitbreiding kunnen we op een handige manier de getallen b en k vinden.

5.5 Het uitgebreide algoritme van Euclides

In het deze paragraaf zullen we het uitgebreide algoritme van Euclides bekijken. Dit is een handige methode om de vergelijking $ab - mk = 1$ die we in de vorige paragraaf moesten oplossen, op te lossen.

Met de uitbreiding van het algoritme van Euclides kunnen we getallen b, k en d berekenen, zodanig dat $ggd(a, m) = d$ en $a \cdot b + m \cdot k = d$.

Opgave 38

Leg uit hoe we met behulp van de oplossing van de vergelijking $ab + mk = 1$ de oplossing op de vergelijking $ab - mk = 1$ kunnen vinden.

Laten we eens gaan kijken hoe het uitgebreide algoritme van Euclides werkt. We nemen de tabel uit het laatste voorbeeld van paragraaf 5.2 er nog eens bij. We berekenden daar de grootste gemene deler van 148104 en 47223. De letter q gebruiken we voor $a\ div\ m$, de letter r voor de rest $a\ mod\ m$.

a	m	$a\ div\ m = q$	$a\ mod\ m = r$
148104	47223	3	6435
47223	6435	7	2178
6435	2178	2	2079
2178	2079	1	99
2079	99	21	0
99	0		

Bedenk hierbij de volgende zaken:

- De waarde van r is gelijk aan de waarde van $m$een regel lager.
- De waarde van m is gelijk aan de waarde van $a$een regel lager.
- In de tabel geldt dat $ggd(a, m)$ op iedere regel hetzelfde is.
- Op iedere regel in de tabel geldt $a - q \cdot m = r$.

Opgave 39

Ga dit laatste punt na.

De uitbreiding van het algoritme van Euclides zegt dat er altijd gehele getallen b en k bestaan, zodanig dat $ab + mk = ggd(a,m)$. Omdat op iedere regel de grootste gemene deler van de getallen a en m hetzelfde is, zijn er dus op iedere regel een getal$b$en een getal$k$te vinden zodat $a \cdot b + m \cdot k = d$, waarbij $d = ggd(a,m)$.

We voegen nu twee kolommen aan de tabel toe om daarin de getallen b en k bij te houden. Er geldt $ab + mk = ggd(a,m)$ en we gaan proberen de b en k op de bovenste regel te vinden. We beginnen echter onderaan en gaan de tabel van onder naar boven vullen.

De onderste regel is niet moeilijk om in te vullen.

a	m	$a\ div\ m = q$	$a\ mod\ m = r$	b	k
148104	47223	3	6435		
47223	6435	7	2178		
6435	2178	2	2079		
2178	2079	1	99		
2079	99	21	0		
99	0				

Opgave 40

- **a)** Wat was de grootste gemene deler van 148104 en 47223 ook al weer?
- **b)** Vul de op één na onderste regel in.
- **c)** Op welke plek in de tabel is $ggd(a,m)$ altijd te vinden?
- **d)** Welke getallen kun je dus altijd op de één na onderste regel invullen?

Nu moeten we naar boven gaan werken. Als we op een regel b en k gevonden hebben, kunnen we deze waarden gebruiken om b en k op de regel daarboven te vinden, als volgt:

a	m	$a\ div\ m = q$	$a\ mod\ m = r$	b	k
A	M	Q	R	B	K
$A' = M$	$M' = R$	Q'	R'	B'	K'

We gaan uit van de situatie dat we B' en K' weten en B en K te weten willen komen. We weten dus dat $ggd(a,m) = A' \cdot B' + M' \cdot K'$ en het doel is om waarden/uitdrukkingen te vinden voor B en K zo, dat $ggd(a,m) = A \cdot B + M \cdot K$. Als we bedenken dat de rest bij deling voldoet aan $R = A - Q \cdot M$ en dat $M = A'$ en $R = M'$, dan vinden we

$$\begin{aligned} \text{ggd}(a,m) &= A' \cdot B' + M' \cdot K' \\ &= M \cdot B' + R \cdot K' \\ &= M \cdot B' + (A - Q \cdot M) \cdot K' \\ &= M \cdot B' + A \cdot K' - Q \cdot M \cdot K' \\ &= A \cdot K' + M \cdot (B' - Q \cdot K'). \end{aligned}$$

Uit deze laatste regel is af te lezen dat $B = K'$ en $K = B' - Q \cdot K'$. Hiermee zijn dus de twee meest rechtse kolommen eenvoudig te vullen en door dit naar boven toe steeds uit te voeren vinden we op de bovenste regel de getallen b en k zodanig dat $ab + mk = d$.

Opgave 41

De derde regel van onder is in dit geval ook eenvoudig in te vullen: $\text{ggd}(a, m) = 99 = b \cdot 2178 + k \cdot 2079$, dus $b =\ldots$ en $k =\ldots$

Opgave 42

We gaan weer een regel omhoog. De al ingevulde getallen op die regel geven: $2079 = 6435 - 2 \cdot 2178$.

a) Vul de lege plekken in onderstaande berekening in:

$$ggd(a, m) = 99 =\ldots\cdot 2178+\ldots\cdot 2079$$
$$=\ldots\cdot 2178+\ldots\cdot (6435 - 2 \cdot 2178)$$
$$=\ldots\cdot 6435+\ldots\cdot 2178, \text{ dus } b =\ldots \text{ en } k =\ldots$$

b) Bereken op dezelfde manier de één na bovenste regel.

c) Bereken tot slot de bovenste regel.

d) Controleer of de vergelijking $ab + mk = d$ klopt voor de gevonden b, k en d en de gegeven a en m.

Opgave 43

a) Bereken $ggd(724{,}804)$

b) Los op $804b + 724k = ggd(724{,}804)$

c) Los op $47957b + 32395k = ggd(47957{,}32395)$

Opgave 44

Los op:

a) $65x + 23y = 1$

b) $65x + 23y = -1$

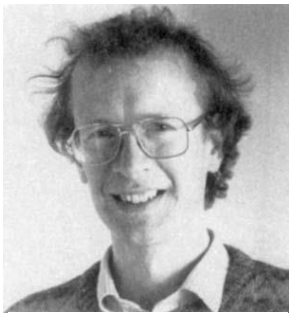
c) $65x + 23y = 3$

Een veeltermvergelijking die alleen gehele getallen als oplossing mag hebben, wordt een Diophantische vergelijking genoemd. Diophantische vergelijkingen van de vorm $ax + by = c$hebben we in deze paragraaf bekeken. Andere Diophantische vergelijkingen zijn bijv. de vergelijkingen met Pythagoreïsche drietallen als oplossing: $x^2 + y^2 = z^2$ en de vergelijking uit de 'laatste' stelling van Fermat: $x^n + y^n = z^n$.

De Diophantische vergelijkingen zijn genoemd naar Diophantes van Alexandrië. Diophantes was een Griekse wiskundige die waarschijnlijk in het midden van de derde eeuw na Chr. leefde. De exacte periode is niet bekend. De meeste Griekse wiskundigen hielden zich voornamelijk met meetkunde en wiskunde die daarmee samenhangt bezig. Diophantes echter hield zich hoofdzakelijk met algebra bezig. Diophantes schreef zijn werk op in de "*Arithmetika"*. Dit bestond uit 13 delen, waarvan echter lange tijd slechts 6 delen (1-3 en 8-10) bekend waren. Pas in 1982 werden 4 verdere delen (4-7) teruggevonden, zij het in Arabische vertaling. De laatste 3 delen zijn verdwenen.

Pierre de Fermat (1601-1665)

In de kantlijn van Diophantes' Arithmetika schreef Fermat zijn beroemde 'laatste' stelling. Fermat schreef dat hij bewezen had dat de vergelijking $x^n + y^n = z^n$ geen oplossing had voor $n \geq 3$, maar dat er in de kantlijn geen ruimte was voor het bewijs. Eeuwenlang hebben wiskundigen geprobeerd zijn stelling te bewijzen. Pas in 1994 is Andrew Wiles (1953) hierin geslaagd. Het bewijs van Wiles bevat echter veel wiskunde die in de tijd van Fermat nog niet bekend was. Men neemt tegenwoordig aan dat in het bewijs van Fermat een fout moet hebben gezeten, maar dat de stelling desondanks wel waar is. Van Fermat zullen we later in deze lessenserie een andere stelling bekijken.



Andrew Wiles (1953-…)

We gaan weer even terug naar de inverse, daar was dit alles ons immers om te doen. Aan het eind van de vorige paragraaf constateerden we dat we de getallen b en k moesten vinden zodanig dat $ab - mk = 1$ omdat b de inverse van a in $\mathbb{Z}_m$ is. Met behulp van het uitgebreide algoritme van Euclides kunnen we inmiddels de vergelijking $ab + mk = 1$ oplossen. Nu we dat kunnen, is het vinden van de inverse een koud kunstje.

Opgave 45

- **a)** Ga met het algoritme van Euclides na dat $ggd(23,72) = 1$.
- **b)** Bereken met het uitgebreide algoritme van Euclides een oplossing van de lineaire Diophantische vergelijking $23b + 72k = ggd(23,72)$.
- **c)** Laat zien dat 47 de inverse van 23 in $\mathbb{Z}_{72}$ is.

Opgave 46

- **a)** Bereken $ggd(105, 291)$ met het algoritme van Euclides.
- **b)** Bereken een oplossing van de lineaire Diophantische vergelijking $105b + 291k = ggd(105,291)$.
- **c)** Leg uit waarom 105 geen inverse in $\mathbb{Z}_{291}$ heeft.

Opgave 47

- **a)** Bereken $ggd(130, 231)$.
- **b)** Bereken een oplossing van de lineaire Diophantische vergelijking $130b + 231k = 1$.
- **c)** Bereken de inverse van 130 in $\mathbb{Z}_{231}$.

Opgave 48

- **a)** Bereken de inverse van 27 in $\mathbb{Z}_{64}$.
- **b)** Bereken de inverse van 153 in $\mathbb{Z}_{2164}$.

Opgave 49
Een boodschap is gecodeerd met de ASCII-tabel. Daarna is ze letter voor letter versleuteld met de encryptie-functie $E(x) = (117 \cdot x)\ mod\ 5\,00$. De versleutelde boodschap is 073 317 338 136 285 402 019 244 200 317 136 317 370 361.

- **a)** Laat met een berekening zien dat de eerste letter van de boodschap een 'E' is.
- **b)** Welke vergelijking moet je oplossen om het tweede symbool te ontcijferen?
- **c)** En het derde?
- **d)** Bereken $(453 \cdot 117)\ mod\ 5\,00$.
- **e)** Leg met behulp van je antwoord op de vragen **b)** en **d)** uit dat het ontcijferen van het tweede symbool neerkomt op het berekenen van $(453 \cdot 317)\ mod\ 5\,00$. Ontcijfer en decodeer het tweede symbool.
- **f)** Ontcijfer op dezelfde manier het derde symbool.
- **g)** Ontcijfer en decodeer nu de hele boodschap.

Opgave 50
Een boodschap is gecodeerd met de ASCII-tabel. Daarna is ze letter voor letter versleuteld met de encryptie-functie $E(x) = (143 \cdot x)\ mod\ 5\,00$. De versleutelde boodschap is 298 373 444 300 443 087 373 302 088

- **a)** Leg uit waarom we graag een oplossing willen hebben van de vergelijking $(b \cdot 143)\ mod\ 5\,00 = 1$.
- **b)** Vind met behulp van de inverse een oplossing van de vergelijking in vraag **a)**.
- **c)** Ontcijfer en decodeer de versleutelde boodschap.

5.6 Machtsverheffen

In paragraaf 5.3 heb je de somregel en de productregel voor het modulo-rekenen geleerd. We herhalen ze nog even:

Voor gehele getallen a, b, c en d en positieve gehele getallen m geldt:
als $a\ mod\ m = b\ mod\ m$ en $c\ mod\ m = d\ mod\ m$ dan
Somregel: $(a + c)\ mod\ m = (b + d)\ mod\ m$
Productregel: $(a \cdot c)\ mod\ m = (b \cdot d)\ mod\ m$

In deze paragraaf richten we onze aandacht op het machtsverheffen.

Opgave 51

- **a)** Leg uit dat we voor kwadrateren geen aparte regel nodig hebben.
- **b)** Leg uit dat als je kunt kwadrateren en twee getallen kunt vermenigvuldigen, dat je dan ook weet hoe je tot de derde en de vierde macht moet verheffen.
- **c)** Leg uit dat je dan dus ook weet hoe je getallen tot een hogere macht kunt verheffen.

Na het maken van opgave 51 voel je de juistheid van de machtenregel wel aan:

Voor gehele getallen x en y en positieve gehele getallen k en d geldt:
als $x \bmod d = y \bmod d$ dan $x^k \bmod d = y^k \bmod d$.

Opgave 52

Vul de tabel in $\mathbb{Z}_5$ in. Met het teken "^" bedoelen we "tot de macht", dus $1\text{^}2 = 1^2$.

^	0		1	2	3	4
0						
1				1		
2						
3						
4						

Met behulp van de somregel, de productregel en vooral de machtenregel kunnen we berekeningen die erg moeilijk lijken toch vrij eenvoudig uitvoeren.

Voorbeeld:

Bereken 17^{25} in $\mathbb{Z}_{26}$.

(1) $17^{25} = 17^{24} \cdot 17 = (17^2)^{12} \cdot 17$ → *herschrijven om machtenregel toe te passen.*

(2) $17^2 = 3$ → $17^2 \; mod \; 26 = 289 \; mod \; 26 = 3$

(3) $(17^2)^{12} \cdot 17 = 3^{12} \cdot 17$ → *volgt uit (1) en (2).*

(4) $3^{12} \cdot 17 = (3^3)^4 \cdot 17$ → *zie stap (1).*

(5) $3^3 = 1$ → $3^3 \; mod \; 26 = 27 \; mod \; 26 = 1$

(6) $3^{12} \cdot 17 = (3^3)^4 \cdot 17 = 1^4 \cdot 17 = 17$ → *zie stap (3), (4) en (5)*

(7) Dus $17^{25} = 17$ in $\mathbb{Z}_{26}$.

Opgave 53

a) Bereken 2^{25} in $\mathbb{Z}_{31}$.

b) Bereken 3^{301} in $\mathbb{Z}_{25}$.

c) Bereken 18^{96} in $\mathbb{Z}_{325}$.

Opgave 54

a) Bereken 17^{33} in $\mathbb{Z}_{553}$.

b) Bereken 12^{40} in $\mathbb{Z}_{1000}$.

c) Bereken 7^{3843} in $\mathbb{Z}_{640}$.

Opgave 55

a) Bepaal de rest van 2^{47} bij deling door 47.

b) Bepaal het laatste cijfer van 3^{81}. (Tip: reken modulo 10)

c) Onderdeel **b)** kan ook anders. Hoe?

5.7 Euler en Fermat

Leonhard Euler (1707-1783)

Leonhard Euler (1707-1783) wordt beschouwd als de belangrijkste wiskundige van de achttiende eeuw en is de wiskundige die het meest gepubliceerd heeft. Zijn verzameld werk beslaat zo'n zeventig delen. Euler heeft onder andere de symbolen *e*, *i* en π en de goniometrische functies sin, cos en tan geïntroduceerd.

De postzegels hieronder vermelden twee van zijn stellingen: $e - k + f = 2$ (Ecken -Kanten + Flächen = 2 (= hoekpunten – ribben + vlakken)) en $e^{ix} = cos(x) + i \cdot sin(x)$. Van de laatste is de Euleridentiteit $e^{\pi i} + 1 = 0$ een speciaal geval.

In deze paragraaf zullen we de stelling van Euler bekijken die ons goed van pas komt als we naar wat moderne cryptosystemen gaan kijken. De stelling van Euler gaat over machtsverheffen en maakt het rekenen met grote machten eenvoudiger.
Het aantal natuurlijke getallen *a* waarvoor geldt $0 \leq a \leq m - 1$ en $ggd(a, m) = 1$, heet de *Eulerindicator* en geven we aan met $\phi(m)$. De Eulerindicator wordt ook wel de *Eulerfunctie* of de *totiëntfunctie* genoemd. Dit aantal is vanzelfsprekend gelijk aan het aantal getallen *k* waarvoor geldt dat $0 \leq k \leq m - 1$ en dat *k* een inverse in $\mathbb{Z}_m$ heeft.

Opgave 56
Bepaal

- **a)** $\phi(12)$
- **b)** $\phi(5)$
- **c)** $\phi(7)$
- **d)** $\phi(p)$ als p een priemgetal is.

Voor de Eulerindicator gelden bepaalde wetmatigheden. We zagen er al één in opgave 56d. In de volgende twee opgaven zullen we er nog twee bekijken.

Opgave 57

- **a)** Bepaal $\phi(35)$.
- **b)** $\phi(p \cdot q)$ als $p$en q priem zijn en $p \neq q$. Leg uit hoe je aan je antwoord komt.
- **c)** Laat zien dat $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$ als p en q priem zijn en $p \neq q$.

De regel uit 57c geldt ook als p en q relatief priem zijn. We zullen dit hier niet bewijzen, maar je kunt het natuurlijk zelf proberen.

Opgave 58

- **a)** Bepaal $\phi(25)$.
- **b)** Bepaal $\phi(125)$.
- **c)** Bepaal $\phi(625)$.
- **d)** Leg uit dat $\phi(p^r) = (p-1) \cdot p^{r-1}$.

Met de twee regels voor de Eulerindicator kunnen we nu voor alle getallen de Eulerindicator berekenen. Om van een getal de Eulerindicator te vinden, schrijven we het getal eerst als product van machten van zijn priemfactoren. Die machten van priemfactoren zijn onderling vanzelfsprekend relatief priem en daarom mogen we de regel uit opgave 57c toepassen. Om de Eulerindicator van de machten van de priemfactoren zelf te vinden, passen we de regel uit opgave 58d toe.

Voorbeeld:
Bereken $\phi(18000)$.
$18000 = 2^4 \cdot 3^2 \cdot 5^3$. Omdat 2^4, 3^2 en 5^3relatief priem zijn, kunnen we de regel uit opgave 58c gebruiken. Voor de Eulerindicator van de machten van de priemfactoren gebruiken we de regel uit opgave 58d.

$\phi(18000) = \phi(2^4) \cdot \phi(3^2) \cdot \phi(5^3) = (1 \cdot 2^3) \cdot (2 \cdot 3^1) \cdot (4 \cdot 5^2) = 8 \cdot 6 \cdot 100 = 4800$.

Opgave 59

- **a)** Bepaal $\phi(640)$.
- **b)** Bepaal $\phi(49000)$.
- **c)** Bepaal $\phi(245025)$.

We zouden de Eulerindicator van m ook graag willen uitrekenen zonder m eerst in factoren te ontbinden. Helaas is niet bekend hoe dat zou moeten. In feite is het uitrekenen van de Eulerindicator equivalent met het ontbinden van m in factoren. In het volgende hoofdstuk zullen we zien dat functies die heel erg moeilijk te berekenen zijn als je niet over extra informatie, zoals de ontbinding van een getal, beschikt en juist makkelijk te berekenen zijn als je wel over extra informatie beschikt, heel nuttig zijn voor de cryptografie.

De Eulerindicator komt voor in de stelling van Euler en deze stelling helpt ons bij het rekenen met machten. De stelling van Euler bewijzen we in hoofdstuk 7.

De stelling van Euler:
Voor alle gehele getallen a en m met $ggd(a,m) = 1$ geldt dat $a^{\varphi(m)} = 1$ in $\mathbb{Z}_m$.

Dit is een resultaat waarmee we grote machten heel snel kunnen reduceren!

Voorbeeld:
Bereken 3^{300}in $\mathbb{Z}_{25}$.
Er geldt $ggd(3,25) = 1$, dus we mogen de stelling van Euler gebruiken.
$\phi(25) = 20$, dus $3^{20} = 1$ in $\mathbb{Z}_{25}$.
$3^{300} = (3^{20})^{15} = 1^{15} = 1$.

Opgave 60

Bereken:

a) 7^{3843} in $\mathbb{Z}_{640}$.

b) 16^{1033} in $\mathbb{Z}_{81}$.

c) 25^{2999} in $\mathbb{Z}_{99}$ en bereken de inverse van 25 in $\mathbb{Z}_{99}$.

Uit de stelling van Euler volgt de kleine stelling van Fermat:

De kleine stelling van Fermat:
Als p een priemgetal is en a een positief geheel getal en $ggd(a, p) = 1$, dan geldt $a^{p-1} = 1$ in $\mathbb{Z}_p$.

Opgave 61

Laat zien dat de kleine stelling van Fermat uit de stelling van Euler volgt.

Opgave 62

Nederlandse bankrekeningnummers bestaan uit 9 cijfers. Wanneer je een overschrijving doet, wordt gecontroleerd of een opgegeven getal een bankrekeningnummer kan zijn. Dit werkt als volgt. Het eerste cijfer doe je keer 9, het tweede keer 8, het derde keer 7, en zo verder. Deze uitkomsten tel je bij elkaar op. Het laatste cijfer is controlecijfer en wordt zo gekozen dat het resultaat van de berekening 0 is modulo 11. De eerste 4 cijfers vormen overigens het nummer van de bank.

a) Van een Nederlands bankrekeningnummer is bekend dat de eerste 8 cijfers 15783035 zijn. Bereken het laatste cijfer.

Belgische bankrekeningnummers zijn ook met behulp van modulo-rekening te controleren. Belgische bankrekeningnummers bestaan uit 12 cijfers. De eerste 3 cijfers vormen het nummer van de bank. De laatste 2 cijfers zijn zo gekozen dat het getal dat gevormd wordt door de eerste 10 cijfers gelijk is aan het getal dat gevormd wordt door de laatste 2 cijfers modulo 97. Voor rekeningnummer 235-0351345-23 geldt dus dat $2350351345 \; mod \; 97 = 23$.

b) Bereken de controlecijfers opdat het rekeningnummer 235-7350912-.. een geldig Belgisch rekeningnummer is.

In de volgende drie opgaven zijn de symbolen uit de boodschap gecodeerd met de ASCII-tabel en daarna twee aan twee zijn samengenomen om de lijst getallen te krijgen.

Opgave 63

Ontcijfer en decodeer boodschap “200421 002305 016291 000291 010306 011289 004306 163424 012222 180365 163415 001288 014307 228427 005236” als je weet dat er is versleuteld met de encryptiefunctie $E(c) = (c + 131313) \; mod \; 231123$.

Opgave 64
De volgende boodschap is versleuteld met de encryptiefunctie $E(t) = (243 \cdot t + 1234)\ mod\ 372281$:

365727 280785 196732 328613 142588 293674 360792
167787 369540 260438 225669

a) Leg uit dat je voor het ontcijferen van het eerste getal de vergelijking $372281 \cdot k - 243 \cdot t = -364493$ op moet lossen.
b) Leg uit dat bovenstaande vergelijking oplossen neerkomt op de vergelijking$372038 \cdot t = 7788$ in $\mathbb{Z}_{372281}$ oplossen.
c) Welke vergelijking moet je oplossen om het tweede getal te ontcijferen?
d) Leg uit dat je met behulp van de inverse van 372038 in $\mathbb{Z}_{372281}$ de boodschap kunt ontcijferen.
e) Bereken de inverse van 372038 in $\mathbb{Z}_{372281}$.
f) Ontcijfer en decodeer het eerste getal van de boodschap.
g) Ontcijfer en decodeer de hele boodschap.

Opgave 65
De boodschap is "234865 191995 268496 180839 173080 038870 067994 048415 268496 044027" is versleuteld met de encryptiefunctie
$E(t) = (1719 \cdot t)\ mod\ 2\ 94808$.
Ontcijfer en decodeer dit bericht.

5.8 Modulo-rekenen op de grafische rekenmachine

De grafische rekenmachine heeft geen mod-operator, maar we kunnen er wel een maken. Onder de knop MATH in het submenu NUM zit de functie int. Deze functie rondt een getal naar beneden af op een geheel getal. En dat komt zo ongeveer overeen met wat wij met de div-operator hebben gedaan: $a\,div\,m = int(\,a/m)$
Maar dan kunnen we de mod-operator ook wel nabouwen: $a\,mod\,m = a - (a\,div\,m) \cdot m = a - int(\,a/m) \cdot m$

Dit kun je in je grafische rekenmachine programmeren:

- Toets PRGM
- Kies "NEW"
- Er staat nu "PROGRAM:" in je scherm.
- Typ als naam "MOD" en druk op ENTER (letters krijg je met behulp van de groene toets ALPHA).
- Nu staat er een dubbele punt. Hierachter kun je een programmaregel invoeren.
- Kies bij PRGM voor "I/O" en vervolgens voor "Prompt".
- Typ achter "Prompt" de naam van je eerste variabele "A" en weer op ENTER.
- Typ weer "Prompt" en vervolgens de naam van je tweede variabele "M" en druk weer op ENTER.
- Typ op de volgende regel "A-int(A/M)*M→U". Dit wijst de uitkomst van
- A-int(A/M)*M toe aan U. Het pijltje krijg je met de knop STO→ en "int" vind je bij op MATH onder "num".
- Druk weer op ENTER.
- Zet op de volgende regel "Disp", dit vind je bij PRGM onder "I/O", met daarachter ""A MOD M IS",U". Dit zorgt ervoor dat de uitkomst op je scherm komt te staan.
- Als je nu bijvoorbeeld $523\ mod\ 17$ wilt berekenen, kies je in je rekenscherm PRGM en dan EXEC bij je programma MOD.
- In je rekenscherm komt dan "prgmMOD" te staan. Als je op ENTER drukt kun je voor A het getal 523 invoeren en voor M het getal 17.
- Als uitkomst krijg je nu de tekst "A MOD M IS 13".

Opgave 66

a) Voer het programma in in je GR.
b) Bereken $76325\ mod\ 632$.

5.9 Samenvatting

In dit hoofdstuk heb je veel nieuwe termen, notaties en regels geleerd. We zetten ze daarom de belangrijkste nog een keer op een rij.

Definities en notaties:
$\boldsymbol{a \mid b}$: a is een deler van b.
$a \; div \; m$: het grootste gehele getal k dat voldoet aan $k \cdot m \leq a$.
$a \; mod \; m$: $a - m \cdot (a \; div \; m)$, de rest bij geheeltallige deling van a door m.
$\mathbb{Z}_m$: Verzameling van niet negatieve gehele getallen van 0 t/m m – 1, dus $\{0,1,\ldots,m-1\}$.
Eulerindicator $\phi(m)$: het aantal gehele getallen a waarvoor geldt $0 \leq a \leq m-1$ en $ggd(a,m) = 1$

Euclides:
Voor positieve gehele getallen a en m geldt dat $\text{ggd}(a,0) = a$ en dat $ggd(a,m) = ggd(m, rest(a:m))$.
Bovendien zijn er getallen b en k te vinden zodanig dat $ab + mk = ggd(a,m)$.
Als $ggd(a,m) = 1$, dan zijn $b \; mod \; m$ en $a \; mod \; m$ elkaars inverse in $\mathbb{Z}_m$.

Regels:
Voor alle positieve gehele getallen $\boldsymbol{m}$ en $\boldsymbol{n}$ geldt:

Als a en b gehele getallen zijn, geldt $a \; mod \; m = b \; mod \; m$ precies dan als $(a - b) \; mod \; m = 0$.

Somregel
Als a, b, c, d gehele getallen zijn en $a \; mod \; m = b \; mod \; m$ en $c \; mod \; m = d \; mod \; m$ dan
$(a + c) \; mod \; m = (b + d) \; mod \; m$.

Productregel
Als a, b, c, d gehele getallen zijn en $a \; mod \; m = b \; mod \; m$ en $c \; mod \; m = d \; mod \; m$ dan $(a \cdot c) \; mod \; m = (b \cdot d) \; mod \; m$

Machtenregel
Als a en b gehele getallen zijn, dan geldt $a^n \; mod \; m = b^n \; mod \; m$.

Regels voor de Eulerindicator
$\varphi(p) = p - 1$ als $p$een priemgetal is.
$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$ als p en q relatief priem zijn.
$\phi(p^r) = (p-1) \cdot p^{r-1}$ als p een priemgetal is.

Stelling van Euler
Voor alle gehele getallen a met $ggd(a,m) = 1$ geldt dat $\boldsymbol{a^{\varphi(m)} = 1}$ in $\mathbb{Z}_m$ **.**

De kleine stelling van Fermat:
Als $p$een priemgetal is, a een positief geheel getal is en $ggd(a,p) = 1$,
dan geldt $a^{p-1} = 1$ in $\mathbb{Z}_p$.

6 Public key cryptografie

6.1 Inleiding

In hoofdstuk 3 hebben we gekeken naar diverse symmetrische cryptosystemen. Bij een symmetrisch cryptosysteem hebben de zendende en de ontvangende partij sleutels nodig die eenvoudig van elkaar af te leiden zijn, zonder dat de tegenpartij over deze sleutelparen beschikt. Dit is lastig om verschillende redenen:

- Als een gezelschap wil communiceren en samen één sleutelpaar deelt, moeten de gebruikers allemaal het sleutelpaar geheim houden. Hoe groter de groep is, des te moeilijker dit is. Ook kan iedereen de berichten van alle anderen lezen en als iemand de groep verlaat, moet je het sleutelpaar vervangen anders kan hij alles blijven lezen.
- Als een gezelschap wil communiceren en voor ieder tweetal een apart sleutelpaar wil hebben, heb je voor een groot gezelschap erg veel sleutelparen nodig. Bovendien moet je erg veel sleutelparen verspreiden met alle risico's van dien.
- De sleutels wil je regelmatig wisselen omdat een afluisteraar iedere keer wat informatie krijgt als hij een boodschap onderschept. Maar hoe spreek je veilig een sleutel af als je nog geen sleutel en dus nog geen veilige manier van communiceren hebt?

Opgave 1
Een gezelschap van n personen wil voor alle tweetallen aparte sleutelparen hebben.

a) Hoeveel sleutelparen heeft iedere deelnemer in zijn bezit?
b) Hoeveel sleutelparen worden er in het totaal uitgewisseld?

Bij public-key cryptografie delen gebruikers geen sleutels die voor anderen geheim zijn. Een public-key cryptosysteem is een systeem dat werkt met sleutelparen die bestaan uit een privé-sleutel en een publieke sleutel. Iedere gebruiker van het systeem kiest zo'n privé-sleutel. De privé-sleutel houdt de gebruiker geheim. De publieke berekent hij op een afgesproken manier. Kan dat zo maar? Als je weet hoe een boodschap is versleuteld, dan is in principe toch ook duidelijk hoe de boodschap moet worden ontcijferd? Anders gezegd: als je de encryptie-functie kent, dan ligt de decryptie-functie toch ook vast? Het antwoord daarop is: ja, in principe wel! Maar er zijn functies die niet moeilijk zijn om te berekenen, maar waarvoor het voor grote getallen ondoenlijk is om terug te rekenen.

Bij moderne public-key cryptosystemen is de berekening om uit de geheime sleutel de publieke te berekenen niet moeilijk uit te voeren, maar als je uit de uitkomst de beginwaarde wilt berekenen is dat heel moeilijk. Hier berust de veiligheid op. Een voorbeeld is dat een getal tot een macht verheffen niet zo moeilijk is, maar dat een hogere-machtswortel trekken niet zo eenvoudig lukt. De publieke sleutel wordt bekend gemaakt, bijvoorbeeld op een website. Er hoeven dus geen sleutels verstuurd te worden en iedereen heeft maar één sleutel die geheim gehouden moet worden.

Wanneer Alice een boodschap wil versturen aan Bob, zoekt ze de publieke sleutel van Bob op. De boodschap vercijfert ze met behulp van de publieke sleutel van Bob. Vervolgens verstuurt ze de boodschap naar Bob. Bob ontcijfert de boodschap met

behulp van zijn privé-sleutel. Als Bob een antwoord wil sturen, gebruikt hij de publieke sleutel van Alice om het antwoord te vercijferen en ontcijfert Alice de boodschap met haar privé-sleutel.

Het vercijferingsalgoritme en het ontcijferingsalgoritme van een public-keycryptosysteem moeten aan twee belangrijke voorwaarden voldoen:

- Het vercijferingsalgoritme en het ontcijferingsalgoritme mogen niet te veel rekentijd en geheugenruimte van de computer gebruiken.
- Het moet onmogelijk zijn om de vercijferde boodschap te ontcijferen zonder kennis van de geheime sleutel of om de geheime sleutel af te leiden uit de publieke sleutel.

Een algoritme dat voldoet aan deze eigenschappen, is een “trapdoor one-way algoritme”. Een one-way algoritme is een algoritme dat eenvoudig uit te voeren is, maar waarvan het inverse algoritme zeer moeilijk is om uit te voeren. Een voorbeeld hiervan is een nummer bij een naam opzoeken in een telefoonboek. Het nummer vinden is niet moeilijk doordat de namen alfabetisch gerangschikt staan. Een naam bij een nummer vinden is veel minder eenvoudig.

Een trapdoor one-way algoritme is een one-way algoritme waarvoor het inverse algoritme met wat extra informatie wel goed uit te voeren is. Om trapdoor one-way algorimtes te maken heb je behoorlijk wat wiskundige kennis nodig.

In het hoofdstuk over getaltheorie bekeken we wiskunde die veel gebruikt wordt in de public-key cryptografie. In dit hoofdstuk laten we een manier zien om het gebruik van symmetrische en public key cryptosystemen te combineren en bekijken we enkele public-key cryptosystemen met bijbehorende algoritmes.

6.2 Diffie-Hellman sleutelprotocol

In deze paragraaf zullen we bekijken hoe het machtsverheffen in $\mathbb{Z}_m$ gebruikt kan worden in de cryptografie.

Een nadeel van public key cryptosystemen ten opzichte van symmetrische cryptosystemen is dat de algoritmes die in de public key cryptosystemen gebruikt worden vaak meer rekentijd kosten dan de algoritmes die in de symmetrische cryptosystemen gebruikt worden. Men combineert daarom vaak de beide soorten systemen. De sleutel die voor symmetrische cryptografie veilig tussen gebruikers moet kunnen worden uitgewisseld, wordt met behulp van een public key cryptosysteem verstuurd. Voor het public key cryptosysteem hoeven geen sleutels uitgewisseld te worden en zo kunnen de gebruikers veilig de sleutel van het symmetrische cryptosysteem aan elkaar laten weten. De eigenlijke boodschap kan dan met behulp van symmetrische cryptografie vercijferd worden. Dat voor het vercijferen en ontcijferen van de sleutel wat meer rekentijd nodig is, is niet erg aangezien de sleutel over het algemeen veel korter zal zijn dan de boodschap die verstuurd moet worden.

In 1976 publiceerden Whitfield Diffie en Martin Hellman een methode om op een veilige manier een sleutel af te spreken. Ook al onderschept een afluisteraar de hele communicatie over deze sleutel, hij zal daar de sleutel zelf niet uit kunnen afleiden.

Tenminste, als de gebruikte getallen flink groot zijn. Hun methode wordt het Diffie-Hellman-sleutelprotocol genoemd. We leggen eerst het protocol uit; daarna volgt een voorbeeld. De getallen in het voorbeeld zijn voor praktisch gebruik veel te klein, maar de methode wordt zo wel duidelijk.

Het systeem rekent modulo een priemgetal p en maakt gebruik van een publiek bekende restklasse $\overline{g}$. Elke gebruiker kiest als geheime sleutel een getal t en berekent zijn publieke sleutel in $\mathbb{Z}_p$, de restklasse $\overline{T} = \overline{g}^t$. Deze publieke sleutel $\overline{T}$ maakt hij bekend.

Als Alice met Bob een sleutel wil afspreken, dan kiest ze eerst een priemgetal p en een restklasse $\overline{g}$ in $\mathbb{Z}_p$. Vervolgens kiest Alice een getal a dat ze geheim houdt en ze berekent $\overline{A} = \overline{g}^a$ in $\mathbb{Z}_p$. De combinatie $\left(p, \overline{g}, \overline{A}\right)$ is haar publieke sleutel en ze stuurt die aan Bob.
Bob kiest, nadat hij p en $\overline{g}$ van Alice heeft ontvangen, een getal b dat hij geheim houdt en hij berekent $\overline{B} = \overline{g}^b$ in $\mathbb{Z}_p$. Deze restklasse $\overline{B}$ is, samen met de al bekende p en $\overline{g}$, zijn publieke sleutel en hij stuurt $\overline{B}$ aan Alice.
Alice berekent nu $\overline{K} = \overline{B}^a$ in $\mathbb{Z}_p$ en Bob berekent $\overline{K} = \overline{A}^b$ in $\mathbb{Z}_p$. Deze $\overline{K}$ is nu de afgesproken sleutel.

Opgave 2
Hierboven staat dat de twee uitkomsten gelijk zijn. Dat gaan we even na.

Vul de lege plekken in: $\overline{K} = \overline{B}^a = (\overline{g}^{\cdots})^a = \overline{g}^{\cdots \cdot \cdots} = \overline{g}^{\cdots \cdot b} = (\ldots)^b = \ldots^{\cdots} = \overline{K}$.

Op deze manier hebben Alice en Bob een sleutel afgesproken zonder directe onderlinge communicatie.

Voorbeeld:
Alice kiest $\overline{g} = 11$ en $p = 59$ en als geheime sleutel $a = 12$.
Haar publieke sleutel$\overline{A}$ is dus 21, kijk maar: $\overline{11}^{12} = \left(\overline{11}^2\right)^6 = \overline{121}^6 = \overline{3}^6 = \overline{3}^4 \cdot \overline{3}^2 = \overline{81} \cdot \overline{9} = \overline{22} \cdot \overline{9} = \overline{198} = \overline{21}$.
Alice stuurt Bob de combinatie $(p, \overline{g}, \overline{a}) = (59, \overline{11}, \overline{21})$.

Bob heeft als geheime sleutel $b = 24$ en als publieke sleutel $\overline{B} = \overline{28}$ want $\overline{11}^{24} = \left(\overline{11}^{12}\right)^2 = \overline{21}^2 = \overline{441} = \overline{28}$.
Alice berekent hun sleutel door de publieke sleutel van Bob tot de macht haar geheime sleutel te verheffen modulo 59: $\overline{B}^a = \overline{28}^{12} = \overline{20}$.
Bob berekent hun sleutel door de publieke sleutel van Alice tot de macht zijn geheime sleutel te verheffen modulo 59: $\overline{A}^b = \overline{21}^{24} = \overline{20}$.
Dat $\overline{A}^b = \overline{B}^a$ zie je ook als volgt: $\overline{A}^b = \overline{21}^{24} = \left(\overline{11}^{12}\right)^{24} = \overline{11}^{12 \cdot 24} = \overline{11}^{24 \cdot 12} = \left(\overline{11}^{24}\right)^{12} = \overline{28}^{12} = \overline{B}^a$.

Opgave 3
Gegeven is $\overline{g} = 7$ en $p = 47$. Als geheime sleutel kiezen we $x = 5$.

a) Bereken de publieke sleutel $\overline{X}$.

We willen een sleutel afspreken met Yvonne die als publieke sleutel $\overline{Y} = 14$ heeft.

b) Bereken de sleutel die we met Yvonne afspreken.

Gegeven is dat de geheime sleutel $y$van Yvonne kleiner dan 5 is.

c) Probeer een getal te vinden dat de geheime sleutel van Yvonne zou kunnen zijn.

d) Controleer dat Yvonne dezelfde sleutel vindt als wij bij onderdeel **b)** gevonden hebben.

Wanneer het Diffie-Hellman-sleutelprotocol in het echt gebruikt wordt, neemt men natuurlijk niet zo'n kleine$p$als wij nu genomen hebben. Je moet dan aan een $p$denken van een paar honderd cijfers lang. Gewoon even wat machten proberen is dus geen optie.

We gaan nu bekijken welk probleem Oscar moet oplossen om de sleutel die Alice en Bob afspreken te achterhalen. Oscar kent de $\overline{g}$, p, $\overline{A}$ en $\overline{B}$.

Opgave 4

a) Oscar weet dat de restklassen Aen B anders te schrijven zijn. Hoe?

b) Hoe kan de sleutel die Alice en Bob afspreken als macht van g geschreven worden?

Oscar zoekt dus naar een methode om een getal $g^{a \cdot b}$ te vinden als je g^a en g^b modulo p kent. Laten we eerst kijken hoe je een getal a vindt als je $g$en g^a kent. In de volgende opgave doen we dit eerst zonder modulo te rekenen en daarna als we wel modulo p rekenen.

Opgave 5
Los op:

a) $3^x = 243$

b) $10^x = 100000000000$

c) $17^x = 2390724356851513248471 53$

d) $356^x = 45118016$

e) In $\mathbb{Z}_5$: $3^x = 2$

f) In $\mathbb{Z}_{11}$: $5^x = 1$

Opgave 6

a) Met onderdeel **a)** tot en met **d)** in de vorige opgave had je waarschijnlijk weinig moeite. Hoe pakte je het aan?

b) Onderdeel **e)** en **f)** waren lastiger. Waarom?

Omdat er bij machtsverheffen twee getallen zijn die een geheel verschillende rol spelen (het grondtal en de exponent), zijn er twee geheel verschillende vragen. We gaan bij beide vragen uit van de machtsverheffing $g^a = b$ in $\mathbb{Z}_m$.

- Gegeven g en b. Gevraagd te berekenen de (kleinste positieve) waarde x waarvoor $g^x = b$.

Voor reële getallen komt dit neer op $x = ^g log\ b$. In analogie daarmee wordt het oplossen van de vergelijking in $\mathbb{Z}_m$ het *discrete logaritme probleem* genoemd. Discreet wil zeggen dat je alleen met gehele getallen werkt. Discrete wiskunde is de tak van wiskunde die over gehele getallen gaat.

- Gegeven a en b. Gevraagd te berekenen de waarde van y waarvoor $y^a = b$. Dit is het oplossen van een *hogeremachtsvergelijking* in $\mathbb{Z}_m$.

In beide gevallen zou je de oplossing kunnen vinden door voor x respectievelijk y de waarden $1, 2, 3, ...$ te proberen, totdat je de oplossing hebt gevonden. Voor grote waarden van m is dat natuurlijk ondoenlijk.

Er zijn wel methoden die het aanzienlijk beter doen. Maar al die methoden laten het ook afweten als de getallen heel groot worden. Op dit moment worden in de praktijk getallen gebruikt van 150 tot 200 cijfers. Alle methoden die nu bekend zijn, vragen bij getallen van deze grootte zelfs op de snelste computers rekentijden die vergelijkbaar zijn met de leeftijd van het heelal. Het is juist deze ondoenlijkheid die de basis vormt van veel crypto-systemen die vandaag de dag in de praktijk worden gebruikt.

Terug naar het probleem van Oscar. Oscar zoekt een methode om een restklasse $\overline{g}^{a \cdot b}$ te vinden als je $\overline{g}^a$ en $\overline{g}^b$ in $\mathbb{Z}_p$ kent. De restklasse $\overline{g}$is bekend, de getallen a en $b$niet. Als we uit $\overline{g}$ en $\overline{g}^a$ konden afleiden wat a was of uit $\overline{g}$ en $\overline{g}^b$ wat b was, waren we klaar.

Opgave 7

Waarom zouden we dan klaar zijn?

Maar deze getallen $a$en b kunnen we niet vinden. Dit komt namelijk neer op het oplossen van het discrete logaritme probleem en daar is nog geen methode voor gevonden die bij grote getallen snel genoeg werkt. Het vinden van zo'n restklasse $\overline{g}^{a \cdot b}$in $\mathbb{Z}_p$ staat bekend als het Diffie-Hellman-completeringsprobleem.

Over de restklasse $\overline{g}$ moet nog iets opgemerkt worden. Niet iedere restklasse in $\mathbb{Z}_p$ is geschikt om als $\overline{g}$ gebruikt te worden. In de volgende opgaven zullen we ontdekken wat het probleem bij het gebruik van bepaalde $\overline{g}$'s is.

Opgave 8

a) Bob heeft gepubliceerd: $p = 811$, $\overline{g} = \overline{339}$. Alice kiest $a = 78$. Welke restklasse $\bar{A}$ stuurt Alice naar Bob?

b) Bob kiest $b = 129$. Welke waarde stuurt Bob naar Alice?

c) Eva onderschept de restklasse $\bar{A}$ die Alice stuurt. Om de waarde van a te achterhalen probeert ze achtereenvolgens $1, 2, ...$. Welke waarde voor a vindt ze?

d) Eva onderschept ook de restklasse $\bar{B}$ die Bob stuurt. Laat zien dat Eva nu de sleutel kan achterhalen, ondanks het feit dat ze niet dezelfde waarde voor a heeft als Alice.

De uitkomst van vraag **c)** hierboven geeft aan dat je met het kiezen van de restklasse $\bar{g}$ op moet passen. Niet elke waarde in $\mathbb{Z}_p$ is even geschikt. De volgende opgaven laten zien waar je op moet letten.

Opgave 9

- **a)** Neem de waarden uit de vorige opgave. Bereken $\bar{g}^5$.
- **b)** Leg uit hoe je nu heel snel kunt zien dat $\bar{g}^3 \equiv_{811} \bar{g}^{78}$.
- **c)** Hoeveel verschillende restklassen kom je met de gekozen waarden voor p en $\bar{g}$ tegen als je $\bar{g}^x$ uitrekent voor $x = 1, 2, 3, ...$?

Opgave 10

- **a)** Bereken in $\mathbb{Z}_7$ de volgende machten: $\overline{6}^1, \overline{6}^2, \overline{6}^3, \overline{6}^4, \overline{6}^5$ en $\overline{6}^6$.
- **b)** Bereken in $\mathbb{Z}_7$ de volgende machten: $\overline{5}^1, \overline{5}^2, \overline{5}^3, \overline{5}^4, \overline{5}^5$ en $\overline{5}^6$.
- **c)** Welke restklasse zou je liever als $\overline{g}$ kiezen, $\overline{5}$ of $\overline{6}$? Waarom?

De restklasse $\overline{5}$ heet een *voortbrenger* van $\mathbb{Z}_7$. Een restklasse $\overline{g}$ is een voortbrenger van $\mathbb{Z}_p$ als de machten $\overline{g}^1, \overline{g}^2, \overline{g}^3, \ldots, \overline{g}^{p-1}$ in $\mathbb{Z}_p$ alle restklassen van $\overline{1}$ tot en met $\overline{p-1}$ een keer als oplossing hebben. Voortbrengers zijn geschikte kandidaten voor de restklasse $\overline{g}$ omdat er zo veel verschillende sleutels te maken zijn. In de praktijk blijkt het ook mogelijk te zijn om een $\overline{g}$ te kiezen die geen voortbrenger is als de machten van $\overline{g}$ samen de helft van alle restklassen (uitgezonderd $\overline{0}$) als uitkomsten hebben.

Opgave 11

- **a)** Bepaal de voortbrengers van $\mathbb{Z}_{11}$.
- **b)** Welke restklassen van $\mathbb{Z}_{11}$ die geen voortbrenger zijn, zouden toch in aanmerking komen om als restklasse $\overline{g}$ te dienen?

6.3 RSA

Het bekendste en meest gebruikte public-keycryptosysyteem is RSA. RSA is in 1978 gepubliceerd door Ron Rivest, Adi Shamir en Leonard Adleman. We gaan in deze paragraaf kijken hoe het systeem werkt.

Het RSA-vercijferingsalgoritme voert berekeningen uit in $\mathbb{Z}_m$. Iedere gebruiker moet een publieke en een geheime sleutel kiezen. Dit gaat als volgt:

1. Kies priemgetallen p en q, waarbij $p \neq q$.
2. Bereken $m = p \cdot q$ en $\phi(m)$.
3. Kies een restklasse $\bar{e}$ die een inverse in $\mathbb{Z}_{\phi(m)}$ heeft.
4. Bereken de restklasse $\bar{d}$ die de inverse is van $\bar{e}$ in $\mathbb{Z}_{\phi(m)}$.
5. Vernietig de getallen p, q en $\phi(m)$!
6. De publieke sleutel is het paar $(m, \bar{e})$ en de geheime sleutel is het paar $(m, \bar{d})$.

Wanneer je het bericht $\bar{b}$ wilt vercijferen als cijfertekst $\bar{c}$, bereken je $\bar{c} = \bar{b}^e$ in $\mathbb{Z}_m$. Het bericht $\bar{c}$ ontcijfer je door $\bar{b} = \bar{c}^d$ in $\mathbb{Z}_m$ te berekenen.

Opgave 12

Gegeven is dat $m = p \cdot q$.

a) Druk $\phi(m)$ uit in p en q.

b) Welke eigenschap bezitten de restklassen $\bar{e}$ die een inverse hebben in $\mathbb{Z}_{\phi(m)}$?

Voorbeeld:

1. $p = 71,\ q = 73$
2. $m = p \cdot q = 71 \cdot 73 = 5183,\ \phi(m) = \phi(5183) = \phi(71) \cdot \phi(73) = 70 \cdot 72 = 5040$
3. $\bar{e} = \overline{17}$
4. $\bar{d} = \overline{593}$
5. Publieke sleutel:$(5183,17)$, geheime sleutel: $(5183,593)$.

Opgave 13

a) Voer de berekening uit die in stap 4. nodig is om $\bar{d}$ te vinden.

b) Ga na dat in $\mathbb{Z}_{5183}$ inderdaad geldt dat $(\bar{b}^{17})^{593} = \bar{b}$ als $ggd(b, 5138) = 1$.

c) Ga na dat in $\mathbb{Z}_m$ met m, $\bar{e}$ en $\bar{d}$ als beschreven in het RSA-algoritme geldt dat $(\bar{b}^{e})^{d} = \bar{b}$ als $ggd(b, m) = 1$.

Opgave 14

a) Bepaal met de waarden uit het voorbeeld tot welke waarde het getal 41 wordt versleuteld.

b) Ga met een berekening na dat de waarde die je bij vraag **a)** hebt gevonden door de decryptiefunctie weer tot 41 wordt ontcijferd.

Wanneer je een bericht met RSA wilt vercijferen, zet je het bericht eerst om naar een bericht dat bestaat uit getallen. Je kunt bijvoorbeeld de ASCII-codes van de tekens van het toetsenbord nemen. Als we deze codes achter elkaar zetten en vervolgens opsplitsen in blokken van een bepaalde lengte, kunnen we deze blokken vercijferen met het RSA-algoritme. De lengte l van deze blokken wordt zo gekozen dat $10^l < m$, maar niet al te veel kleiner.

Opgave 15

In deze opgave geven we de letters van het alfabet hun rangnummer als code. De letter *a* is dus 00, de letter *b* 01, enz. Alice wil Bob het bericht “rsa” sturen.

a) Geef de code voor “rsa”.

Alice splitst de code in blokken van lengte 3 en vercijfert de blokken met de publieke sleutel (5183,17) van Bob.

b) Bereken de vercijferde boodschap.

Vervolgens ontcijfert Bob het bericht met zijn geheime sleutel (5183,593).

c) Voer deze ontcijfering uit.

In opgave 15 zie je dat de lengte van de blokken in de cijfertekst niet hetzelfde is als de lengte van de blokken in de originele boodschap. In de praktijk zul je gewoonlijk niet een heel bericht met RSA vercijferen. De rekentijd is hiervoor te lang. RSA wordt meestal gebruikt om een sleutel te versturen van een symmetrisch cryptosysteem waarbij vercijfering minder tijd kost. Naast de sleutel wordt eventueel wat aanvullende informatie verstuurd om te zorgen dat je zeker weet dat niemand wijzigingen in je bericht heeft aangebracht. De lengte van de boodschap die je wilt

versturen is hierdoor korter dan de lengte van de p. Het is dan niet nodig de boodschap op te splitsen in blokken en je hoeft dus ook niet een aantal blokken afzonderlijk te vercijferen. Hierdoor maakt het niet uit als de originele tekst en de cijfertekst niet even lang zijn.

Opgave 16
De publieke sleutel van Bob is (209,13).

a) Achterhaal de geheime sleutel van Bob.

Wijzer geworden door deze ervaring kiest Bob de publieke sleutel (1040257,1361). De geheime sleutel van Bob vinden, zal je nu niet zo snel lukken zonder computer.

b) Wat is er zo moeilijk aan?

Voor kleine p en q is het niet moeilijk om de geheime sleutel uit de publieke sleutel af te leiden, voor (hele) grote p en q wel. Daarom gebruikt men voor p en q getallen van ongeveer 150 cijfers. Het getal m bestaat dan uit ongeveer 300 cijfers. Een getal dat zo groot is, is momenteel zelfs met de allersnelste computers niet binnen een mensenleven te ontbinden. Hierop berust de veiligheid van RSA. Wanneer je de getallen p en q zou kunnen vinden, zou je $\phi(m)$ eenvoudig kunnen berekenen en de inverse $\bar{d}$ van $\bar{e}$ met het uitgebreide algoritme van Euclides kunnen berekenen. Je zou dan de vercijferde boodschap kunnen ontcijferen door hem tot de macht $\bar{d}$ te verheffen.

6.4 Digitale handtekeningen

We hebben in de afgelopen lessen gezien hoe we cryptografie kunnen gebruiken om boodschappen veilig te versturen. In deze paragraaf kijken we naar een andere, maar niet minder belangrijke, toepassing van cryptografie.

Wanneer we een boodschap ontvangen, willen we graag zeker weten dat de afzender inderdaad de persoon is die hij zegt dat hij is. Stel dat een bank een opdracht krijgt waarin staat dat er geld van een bepaalde rekening overgeschreven moet worden naar een andere rekening. De bank wil dan wel graag zeker weten dat de persoon die die opdracht geeft daartoe gemachtigd is. Hiervoor gebruikt de bank een crypto-systeem. De opdrachtgever moet bepaalde informatie geven die alleen een gemachtigd persoon kan weten.

Door het meesturen van een digitale handtekening kan zekerheid verkregen worden over of de afzender van een bericht is wie hij zegt dat hij is.

Alice verstuurt een bericht aan Bob. Ze stuurt een digitale handtekening mee. De digitale handtekening mag alleen door Alice gemaakt kunnen worden. Dit betekent dat Alice er bepaalde geheime informatie voor nodig moet hebben om de handtekening te kunnen maken. Bob moet de handtekening kunnen controleren en dus heeft hij enige kennis over de informatie van Alice hebben. Hij moet de handtekening immers kunnen onderscheiden van valse handtekeningen. Misschien herken je hierin al de geheime en publieke sleutel die we eerder in de public-key cryptografie tegenkwamen.

Het RSA-cryptosysteem kunnen we gebruiken om een digitale handtekening te maken. De geheime en publieke sleutel worden gekozen als gebruikelijk. Als Alice

een geheime boodschap wil versturen aan Bob en ze bovendien wil dat Bob kan zien dat de boodschap echt van haar komt, gaat ze als volgt te werk.

1. Alice vercijfert haar boodschap $\bar{s}$ met haar geheime sleutel (m_a, a), ze berekent dus $\bar{t} \equiv_{m_a} \bar{s}^a$.
2. Vervolgens vercijfert ze het bericht $\bar{t}$ met de publieke sleutel (m_b, B) van Bob, ze berekent dus $\bar{c} \equiv_{m_b} \bar{t}^B$.

Opgave 17

a) Leg uit waarom dit bericht alleen door Alice verstuurd kan zijn.
b) Beschrijf hoe het ontcijferen in zijn werk gaat.
c) Leg uit waarom dit bericht alleen door Bob gelezen kan worden.

Opgave 18

Alice gaat Bob een bericht voorzien van handtekening sturen. Alice kiest als haar priemgetallen $p_a = 5$ en $q_a = 13$. Bob heeft de priemgetallen $p_b = 7$ en $q_b = 11$ gekozen.

a) Bereken $\phi(m_a)$ en $\phi(m_b)$.
De geheime sleutel van Alice is 19 en de geheime sleutel van Bob is 17.
b) Bereken de publieke sleutels van Alice en Bob.
Alice wil het geheime bericht "6" versturen aan Bob en voorzien van een digitale handtekening.
c) Bereken welk bericht Alice aan Bob gaat sturen.
d) Voor de ontcijfering van het bericht voor Bob uit.

7 De bewijzen

In de wiskunde kijken we wat anders aan tegen het modulo-rekenen dan we in het vorige hoofdstuk gedaan hebben. In dit hoofdstuk zullen wij op deze wiskundige manier het modulo-rekenen behandelen. We gaan nu ook in op waarom de rekenregels gelden.

7.1 Verzamelingen

In de wiskunde gebruikt men de termen '*verzameling*' en '*element*'. In een verzameling zitten elementen. In de cryptografie werken we alleen met gehele getallen. Daarom zijn de verzamelingen $\mathbb{N}$ en $\mathbb{Z}$ belangrijk voor ons:

- $\mathbb{N}$: de verzameling van de natuurlijke getallen bestaat uit de elementen 0, 1, 2, 3, …
- $\mathbb{Z}$: de verzameling van de gehele getallen bestaat uit de elementen …, -2, -1, 0, 1, 2, …

Er zijn veel meer verzamelingen getallen, bijvoorbeeld de complexe getallen, de getallen in $\mathbb{Z}$ die oplossing zijn van de vergelijking $0 = x^2 - 1$ of de vijfvouden.

Een verzameling kan genoteerd worden door alle elementen op te sommen (gescheiden door komma's) en deze opsomming te omgeven door accolades. In plaats van alle elementen op te sommen, kun je ook puntjes zetten om aan te geven dat de rij elementen verder gaat zoals je dat zou verwachten. De verzameling van de natuurlijke getallen kun je in plaats van met de $\mathbb{N}$ dus ook schrijven als $\{0,1,2,3,\dots\}$.
Met een schuine streep geven we aan dat bepaald deel van de verzameling er niet bij hoort: $\mathbb{N}\backslash\{0\} = \{1,2,3,\dots\}$.
Om aan te geven dat een x een element is van een verzameling wordt het symbool $\in$ gebruikt: we schrijven $x \in \mathbb{N}$. Om aan te geven dat iets geen element is van een verzameling gebruikt men het symbool $\notin$. Bijv.: $2\frac{1}{2} \notin \mathbb{N}$.
Je kunt een verzameling ook beschrijven door aan te geven waar de elementen aan moeten voldoen, bijv. $\{x \in \mathbb{Z} | x = 5z, z \in \mathbb{Z}\}$, dit is de verzameling van 5-vouden. Bij deze manier van noteren gaat het om de elementen links van de streep die een eigenschap hebben die rechts van de streep staat beschreven. Dat is in het voorbeeld ook te zien. Er staat namelijk voor de streep uit welke verzameling de elementen komen, dat is hier uit de gehele getallen. Na de streep staat aan welke voorwaarde de elementen moeten voldoen: hier moet het zo zijn dat ieder element is te schrijven als 5 keer een geheel getal. Dat kan alleen als ieder element een 5-voud is.

Alle symbolen nogmaals bij elkaar:

- $V = \{2,4,6\}$: V is de verzameling die bestaat uit de getallen 2, 4 en 6.
- $2 \in V$: 2 is een element van de verzameling V.
- $1 \notin V$: 1 is geen element van de verzameling V.
- $W = \{k \in \mathbb{Z} | -3 \leq k \leq 7\}\backslash\{0\}$: W is de verzameling die bestaat uit de gehele getallen van -3 tot en met 7, uitgezonderd 0.

Opgave 1

a) Leg uit wat het verschil is tussen $\{a \in \mathbb{Z} \mid -3 \leq a \leq 3\}$ en $\{a \in \mathbb{N} \mid -3 \leq a \leq 3\}$.

b) Geef in de verzamelingennotatie de verzameling van de even getallen tussen 101 en 1001.

Opgave 2

Geef aan of de volgende beweringen waar of niet waar zijn.

a) $\pi \in \mathbb{Z}$

b) $\mathbb{N} = \{a \in \mathbb{Z} | a \geq 0\}$

7.2 Modulo-rekenen als equivalentierelatie

In hoofdstuk 5 definieerden we "$a \, mod \, m$" als de rest van a bij deling door m.
In de wiskunde noemen we twee getallen $a$en b *congruent modulo* $m$als ze dezelfde rest hebben bij deling door het gehele getal m, waarbij $m \geq 1$. We noteren dit als volgt: $a \equiv_m b$.

Opgave 3

Gegeven is dat $a = 30, \ b = 93$.

a) Zijn *a* en *b* congruent modulo 7? Licht je antwoord toe met een berekening.

b) Zijn *a* en *b* congruent modulo 8? Licht je antwoord toe met een berekening.

c) Kun je nog een getal *m* vinden waarvoor geldt dat *a* en *b* congruent modulo *m* zijn?

Opgave 4

Gegeven is dat $a = 38, \ m = 5$.

a) Geef 8 mogelijke waarden van *b* zodat geldt dat *a* en *b* congruent modulo *m* zijn.

b) Leg uit dat $b = 38 - k \cdot 5$, waarbij *k* een geheel getal is.

c) Leg uit dat als *a* en *b* congruent modulo *m* zijn er een geheel getal *k* moet zijn zodanig dat $b = a - k \cdot m$.

Opgave 5

Gegeven is dat *a* en *b* congruent modulo *m* zijn.

Laat zien dat $m | a - b$.

Je ziet dat congruent modulo m zijn niet een bewerking is die we uitvoeren op een getal, maar dat het een relatie aangeeft tussen getallen. Bij een bewerking voer je een berekening uit op getallen. Je telt bijvoorbeeld twee getallen bij elkaar op of je neemt de logaritme van een getal. Bij een relatie deel je getallen in in verzamelingen getallen met een bepaalde eigenschap. We verdelen de gehele getallen nu in verzamelingen getallen in, die dezelfde rest hebben na deling door m. Zo'n verzameling van getallen die dezelfde rest hebben na deling door m noemen we een *restklasse*. We noteren een restklasse als een getal uit de restklasse tussen rechte haken, met als index het getal m. Als er geen misverstand kan zijn over wat het getal m is, wordt een restklasse ook vaak aangegeven door een streepje boven een getal uit de restklasse te zetten.

Voorbeeld:

Als je modulo 7 rekent, geldt $[2]_7 = \overline{2} = \{\ldots, -12, -5, 2, 9, \ldots\}$want alle getallen in de verzameling $\ldots, -12, -5, 2, 9, \ldots$ hebben rest 2 als je ze door 7 deelt. Je kunt dit ook

noteren als $\bar{2} = \{x \in \mathbb{Z} | x \equiv_7 2\}$. Je bedoelt hiermee dat alle getallen in de restklasse $\overline{2}$ gehele getallen zijn (het stukje "$x \in \mathbb{Z}$" voor de streep) en dat je bovendien de extra eis stelt dat alle getallen modulo 7 congruent zijn met 2 (het stukje "$x \equiv_7 2$ na de streep).

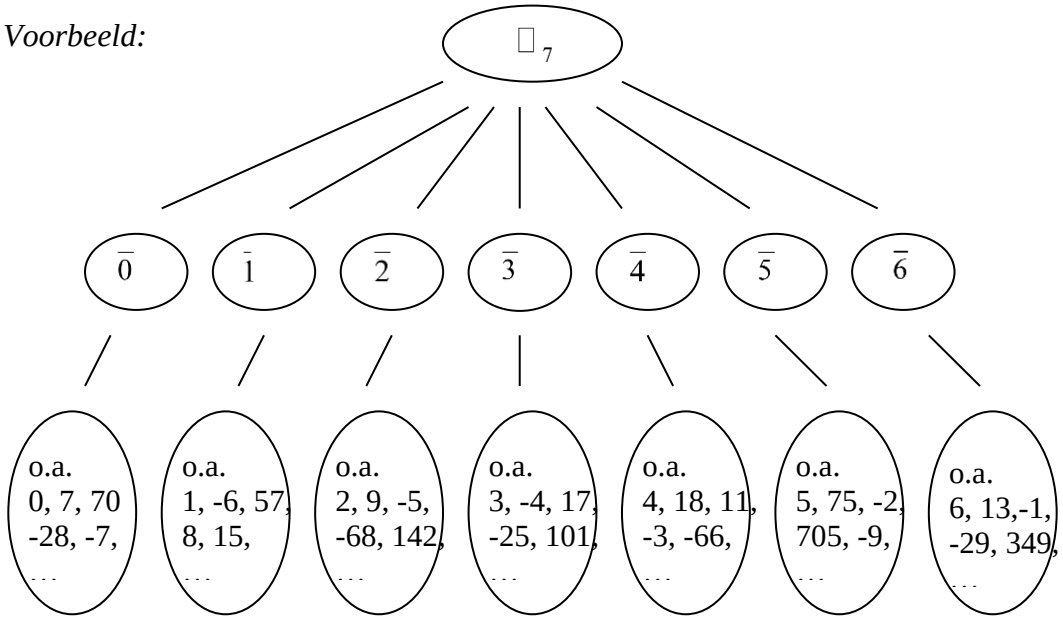
Opgave 6

In deze opgave rekenen we modulo 7.

- **a)** Welke verschillende restklassen zijn er modulo 7?
- **b)** Beschrijf deze restklassen op twee manieren met de verzamelingennotatie als in het voorbeeld hierboven.
- **c)** Leg uit dat je elk geheel getal kunt indelen in één van deze restklassen.

De verzameling van alle restklassen modulo $m$noemen we $\mathbb{Z}_m$. $\mathbb{Z}_m$ kun je dus als volgt weergeven: $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-2]_m, [m-1]_m\}$ of $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-2}, \overline{m-1}\}$. Als je modulo 7 rekent is de restklasse $\overline{2}$ dezelfde restklasse als $\overline{9}$ en $\overline{51}$. De getallen 2, 9 en 51 hebben immers dezelfde rest na deling door 7. De getallen 2, 9 en 51 zijn in $\mathbb{Z}_7$ *representanten* van de restklasse $\overline{2}$. $\mathbb{Z}_m$ kun je dus ook weergeven als bijvoorbeeld $\mathbb{Z}_m = \{\overline{m}, \overline{m+1}, \overline{m+2}, \ldots, \overline{2m-2}, \overline{2m-1}\}$of $\mathbb{Z}_m = \{\overline{m}, \overline{1}, \overline{5m+2}, \ldots, \overline{-m-2}, \overline{2m-1}\}$. Al zijn deze schrijfwijzen natuurlijk wel minder overzichtelijk en daarom minder gebruikelijk.

Voorbeeld:



Voorbeeld:
Als we modulo 5 rekenen, zijn er de restklassen$\bar{0}, \bar{1}, \bar{2}, \bar{3}$en $\bar{4}$. Dus $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Maar alle verschillende resten die mogelijk zijn na deling door 5 komen ook voor als we de restklassen $\overline{15}, \overline{6}, \overline{32}, \overline{623}$ en $\overline{1024}$ kiezen, dus is $\mathbb{Z}_5 = \{\overline{15}, \overline{6}, \overline{32}, \overline{623}, \overline{1024}\}$ hetzelfde.

Een verzameling getallen die van elke restklasse in $\mathbb{Z}_m$ precies één representant bevat, noemen we een *representantensysteem.* We kiezen vaak voor het representantensysteem $\{0,1,\ldots,m-1\}$. De getallen in dit representantensysteem zijn precies alle verschillende resten die je kunt krijgen als je getallen door *m* deelt.

7.3 Bewijzen van de rekenregels

We gaan nu een aantal rekenregels in $\mathbb{Z}_m$ bekijken. Als we gaan rekenen met restklassen, rekenen we eigenlijk met representanten van restklassen. We willen graag dat het voor de uitkomsten dezelfde restklasse terecht komen, ongeacht welke representant we gebruiken. Als we bijvoorbeeld modulo 7 de som $2+4$ uitrekenen, moet de uitkomst in dezelfde restklasse zitten als de uitkomst van $9+11$. De restklassen $\overline{2}$ en $\overline{9}$ zijn immers dezelfde restklasse in $\mathbb{Z}_7$, net als de restklassen $\overline{4}$ en $\overline{11}$. Deze regel heet, weinig verrassend, de somregel.

De somregel:
Als $a \equiv_m b$ en $c \equiv_m d$, dan geldt $a + c \equiv_m b + d$.

In de volgende opgave gaan we de somregel bewijzen.

Opgave 7
Gegeven: $a \equiv_m b$ en $c \equiv_m d$
Te bewijzen: $a + c \equiv_m b + d$
Bewijs: **(1)** $m|a-b$ want
(2) $m|c-d$ …. $a \equiv_m b$

a) Geef het argument bij stap **(2)**

(3) Er is een *v* zodat $vm = a - b$ **(1)**

b) Leg uit hoe stap **(3)** uit stap **(1)** volgt.

(4) Er is een *w* zodat $wm = \ldots$ **(2)**

c) Maak stap **(4)** af.

(5) $(a-b)+(c-d) = vm + wm = (v+w)m$ **(3,4)**
(6) $(a+c)-(b+d) = (a-\ldots)+(\ldots-\ldots) = (v+w)m$ **(5)**

d) Maak stap **(6)** af.

(7) $m|\ldots$ **(6)**
(8) $a + c \equiv_m b + d$ **(7)**

e) Maak stap **(7)** zodanig af dat je de conclusie bij **(8)** inderdaad uit **(7)** kunt trekken.

Uit de somregel volgt nu dat we de optelling op $\mathbb{Z}_m$ als volgt kunnen definiëren:

Voor alle $\overline{a}, \overline{b} \in \mathbb{Z}_m$ geldt dat $\overline{a} + \overline{b} = \overline{a + b}$.

Opgave 8
Vul in de tabel voor optelling in $\mathbb{Z}_5$ in.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

Een zelfde soort regel als de somregel willen we ook graag hebben voor het product. Als we twee representanten van twee restklassen met elkaar vermenigvuldigen, willen we graag dat de uitkomst altijd hetzelfde is ongeacht welke representanten we van de restklasse kiezen.

De productregel:
Als $a \equiv_m b$ en $c \equiv_m d$, dan geldt $a \cdot c \equiv_m b \cdot d$.

Opgave 9
In deze opgave gaan we de productregel bewijzen.
Gegeven: $a \equiv_m b$ en $c \equiv_m d$
Te bewijzen: $a + c \equiv_m b + d$

Bewijs:		
	(1) $m \mid a - b$	want $a \equiv_m b$
	(2) …	…
	(3) Er is een *v* zodat $vm = a - b$	**(1)**
	(4) Er is een *w* zodat …	…
	(5) $vm \cdot c = \ldots$	…
	(6) …	…
	(7) $(a-b) \cdot c + (c-d) \cdot b = \ldots = \ldots$	**(5,6)**
	(8) $(a-b) \cdot c + (c-d) \cdot b = ac - bd = (vc + wb) \cdot m$	**(7)**
	(9) $m \mid \ldots$	**(8)**
	(10) $a \cdot c \equiv_m b \cdot d$	**(9)**

Vul zelf de ontbrekende stappen en argumenten aan.

Uit de productregel volgt nu dat we de vermenigvuldiging op $\mathbb{Z}_m$ als volgt kunnen definiëren:

Voor alle $\overline{a}, \overline{b} \in \mathbb{Z}_m$ geldt dat $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Opgave 10
Vul de tabel voor vermenigvuldiging in $\mathbb{Z}_5$ in.

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

7.4 Bewijzen van de stellingen van Euler en Fermat

We richten ons eerst op de kleine stelling van Fermat.

Opgave 11

a) Vul de vermenigvuldigingstabel in $\mathbb{Z}_7$ in.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$						
$\bar{2}$						
$\bar{3}$						
$\bar{4}$						
$\bar{5}$						
$\bar{6}$						

b) Wat valt je op als je naar de uitkomsten in de verschillende rijen kijkt?

Bij het bewijs van de kleine stelling van Fermat maken we gebruik van de eigenschap die in opgave 11 opviel:

"Als p een priemgetal is en a een geheel getal dat geen p-voud is, geldt dat $\overline{a} \cdot \overline{0}, \overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \ldots, \overline{a} \cdot \overline{p-1}$ allen verschillende restklassen zijn."

Opgave 12
We gaan bovenstaande eigenschap in deze opgave bewijzen.

a) Waarom mag a geen p-voud zijn?
b) De getallen $a, 2a, \ldots, (p-1)a$ zijn allen geen p-voud. Hoe weet je dat?
c) Waarom hebben de getallen $a, 2a, \ldots, (p-1)a$ na deling door p allen een andere rest?
d) Leg uit dat hieruit volgt dat $\{\overline{a} \cdot \overline{0}, \overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \ldots, \overline{a} \cdot \overline{p-1}\} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$.

Deze eigenschap gebruiken we in het bewijs van de kleine stelling van Fermat in de volgende opgave. We herhalen de kleine stelling van Fermat nog even.

De kleine stelling van Fermat:
Als $p$een priemgetal is en $a \in \mathbb{N}\backslash\{0\}$en $ggd(a,p) = 1$, dan geldt $a^{p-1} \equiv_p 1$, oftewel dat $\bar{a}^{p-1} = \overline{1}$ in $\mathbb{Z}_p$.

Opgave 13
Uit opgave 12 blijkt dat $\overline{a} \cdot \overline{0}, \overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \ldots, \overline{a} \cdot \overline{p-1}$ allen verschillende restklassen zijn. We gaan nu het product $(\overline{a} \cdot \overline{1}) \cdot (\overline{a} \cdot \overline{2}) \cdot \ldots \cdot (\overline{a} \cdot \overline{p-1})$ in $\mathbb{Z}_p$ berekenen.

a) Laat zien dat $(\overline{a} \cdot \overline{1}) \cdot (\overline{a} \cdot \overline{2}) \cdot \ldots \cdot (\overline{a} \cdot \overline{p-1}) = \overline{a}^{p-1}(\overline{p-1})!$ in $\mathbb{Z}_p$.

b) Leg uit dat $(\overline{a} \cdot \overline{1}) \cdot (\overline{a} \cdot \overline{2}) \cdot \ldots \cdot (\overline{a} \cdot \overline{p-1}) = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}$ in $\mathbb{Z}_p$.

c) Leg uit dat uit onderdeel **a)** en **b)** volgt dat $\bar{a}^{p-1} = 1$ in $\mathbb{Z}_p$.

Nu we de kleine stelling van Fermat bewezen hebben, richten we ons op de stelling van Euler. De stelling van Euler is algemener omdat die niet alleen kijkt naar $\mathbb{Z}_p$ met p priem, maar ook naar machten van a in $\mathbb{Z}_m$, zolang a en m relatief priem zijn.

Opgave 14

a) Vul de vermenigvuldigingstabel in $\mathbb{Z}_8$ in.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$							
$\bar{2}$							
$\bar{3}$							
$\bar{4}$							
$\bar{5}$							
$\bar{6}$							
$\bar{7}$							

b) Wat valt je nu op als je naar de uitkomsten in de verschillende rijen kijkt?

In opgave 14 valt de eigenschap op dat $\overline{a} \cdot \overline{0}, \overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \ldots, \overline{a} \cdot \overline{m-1}$ verschillende restklassen zijn als a en m relatief priem zijn. Het bewijs hiervan loopt analoog aan het bewijs in opgave 15 en geven we hier niet.

We gaan nu de stelling van Euler bewijzen nadat we hem nog een keer herhaald hebben.

De stelling van Euler:
Voor alle $a \in \mathbb{Z}$ met $ggd(a,m) = 1$ geldt dat $\bar{a}^{\phi(m)} = \overline{1}$ in $\mathbb{Z}_m$.

Bij deling door m zijn er $\phi(m)$ mogelijke resten $a_1, a_2, \ldots, a_{\phi(m)}$ die relatief priem zijn met m. Vermenigvuldigen we deze getallen met a, dan krijgen we opnieuw $\phi(m)$ getallen die relatief priem zijn met m en die verschillende resten hebben bij deling door m. Ook deze resten zijn weer relatief priem met m, en omdat ze verschillend zijn, zijn het dezelfde resten als waarmee we begonnen, alleen mogelijk in een andere volgorde.

Opgave 15

Leg uit door $(\overline{a} \cdot \overline{a_1}) \cdot (\overline{a} \cdot \overline{a_2}) \cdot \ldots \cdot \left(\overline{a} \cdot \overline{a_{\phi(m)}}\right)$ te herschrijven en te vergelijken met $\overline{a_1} \cdot \overline{a_2} \cdot \ldots \cdot \overline{a_{\phi(m)}}$ dat $\overline{a}^{\phi(m)} = \overline{1}$ in $\mathbb{Z}_m$.

De kleine stelling van Fermat kan ook geformuleerd worden zonder gebruik te maken van modulo-rekenen.

Nogmaals de kleine stelling van Fermat:
Als p een priemgetal is en $n \in \mathbb{N}$, dan geldt $p | n^p - n$.

Opgave 16
Leg uit dat beide formuleringen inderdaad gelijkwaardig zijn. (M.a.w. dezelfde stelling opleveren.)

8 Praktische opdrachten

Praktische opdracht 1, horend bij hoofdstuk 2.

Zoek informatieover het symmetrische cryptosysteem “Playfair” dat in 1854 door Charles Wheatstone bedacht werd. Beschrijf hoe het werkt en probeer te achterhalen hoe je het kunt kraken. Ontcijfer vervolgens onderstaand bericht.

LPPIM WMDCY CACZT FFLOS EMATQ SACHU EFZHS FQLCA SNPYF GAGMD UWEIN ANAXA NALQP LLFHM MDAOC PEFSM UYEIN AGRCM DQHMI FMSMI FIAGL MCAUN HUIOM IMIFI BFFTF BPSEZ BFCYM YLTEF MCMVM BSTCM IFMSX GODMI FIZHS FTDEM UTSMM IFIDF FYDID SMBIY IFACC ASENA MIFIE FFOPR NSYPU DGHSN GSNSB FSQTU DFFYZ HFYID UYHPV XIZHU YLWLF IFIBF LWIZG PEMTF PKZCM WMDHF XBDMT QIVIB XIQYX

Antwoorden cryptografie

3 Symmetrische cryptografie

Opgave 1

Iedere letter wordt vervangen door een letter die drie plaatsen verder in het alfabet staat.

Opgave 2

a) Wanneer je een tekst die vercijferd is met een schuifsysteem wilt ontcijferen, is het handig eerst te kijken naar de letters die het meeste voorkomen zoals de e, n en t. Als je bijvoorbeeld weet welke letter de e is, kun je de rest eenvoudig herleiden.

b) K=13

Opgave 3

a) $133 - 5 \cdot 26 = 3$, dus "D".

b) Verschillen 26.

c) $2662 - 2652 = 10$, dus "K".

d) $-22 + 26 = 4$, dus "E".

Opgave 4

a) $E_7(x) = x + 7$

b) $E_{-9}(x) = x - 9$

c) $E_k(x) = x + k$

Opgave 5

a) $D_3(x) = x - 3$

b) $D_k(x) = x - k$

Opgave 6

	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
$E_{11}(x) = x + 11$	L	M	N	O	P	Q	R	S	T	U	V	W	X
$E_{(5,6)}(x) = 5 \cdot x + 6$	G	L	Q	V	A	F	K	P	U	Z	E	J	O
$E_{(9,2)}(x) = 9 \cdot x + 2$	C	L	U	D	M	V	E	N	W	F	O	X	G

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
$E_{11}(x) = x + 11$	Y	Z	A	B	C	D	E	F	G	H	I	J	K
$E_{(5,6)}(x) = 5 \cdot x + 6$	T	Y	D	I	N	S	X	C	H	M	R	W	B
$E_{(9,2)}(x) = 9 \cdot x + 2$	P	Y	H	Q	Z	I	R	A	J	S	B	K	T

Opgave 7

a) HGTGH YTVYO XUATC CNKGG XPAXK ALACN ATRWB

b) Ik zal er zijn en draag een geel kanariepak.

Opgave 8

Dan worden alle letters vercijferd als de letter *d*.

Opgave 9

$a = 1$ en $b = k$.

Opgave 10

a) VDVFB en JDLRB.

a) DHLPTXBFJNRVZ DHLPTXBFJNRVZ

b) Je krijgt slechts de helft van de letters terug in het vercijferde alfabet.

c) De functie $y = 4x + 3$ heeft alleen oneven uitkomsten, ook als je er een veelvoud van 26 aftrekt. Hierdoor kun je niet op alle posities terecht komen.

Opgave 11

a) Je krijgt of alle oneven of alle even getallen < 26, maar nooit alle getallen < 26.

b) Je krijgt alleen even uitkomsten, nee dus.

c) Als we achtereenvolgens 0, 1, 2, 3, … invullen, krijgen we er 0, 3, 6, 9, 12, 15, 18, 21, 24, 1, 4, 7, 10, 13, 16, 19, 22, 25, 2, 5, 8, 11, 14, 17, 20, 23 uit, dus eerst de drievouden, dan de drievouden +1 en dan de drievouden +2. Dus alle getallen van 0 t/m 25.

d) Nee, je krijgt er alleen 0 en 13 uit.

e) Voor a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. (Dus voor alle oneven getallen behalve 13.)

f) $E_{(a+26,b)}(x) = \text{rest}((x\cdot(a+26)+b):26) = \text{rest}((ax+26x+b):26) = \text{rest}((ax+b):26)$

$E_{(a,b)}(x) = \text{rest}((ax+b):26)$.

Opgave 12

a) 25, bij $m = 0$ is de cijfertekst identiek aan de klare tekst.

b) In opgave 11 zagen we dat er voor a 12 mogelijke getallen zijn, b kan gekozen worden uit de getallen 0 t/m 25. Vercijfering met $a = 1$ en $b = 0$ levert de klare tekst en heeft dus geen zin. Er zijn dus $12 \cdot 26 - 1 = 311$ sleutelparen.

Opgave 13

a) $E_{(a,b)}(3) = 16$, $E_{(a,b)}(13) = 14$

b) Als je $ax + b$ deelt door 26 krijg je $E_{(a,b)}(x)$ als rest, dus is er een getal k zodanig dat $ax + b = 26k + E_{(a,b)}(x)$.

c) De eerste vergelijking krijg je door in de vergelijking van onderdeel **b)** voor x en $E_{(a,b)}(x)$ de posities van D en Q te nemen, dus 3 resp. 16. Voor de tweede vergelijking neem je op dezelfde manier 13 en 14.

d)

$$\begin{cases} 3a + b = 16 + 26k \\ 13a + b = 14 + 26l \end{cases}$$
$$\begin{cases} b = 16 - 3a + 26k \\ b = 14 - 13a + 26l \end{cases}$$
$$16 - 3a + 26k = 14 - 13a + 26l$$
$$10a = -2 + 26(l - k)$$
$$a = 5, l - k = 2$$
$$3 \cdot 5 + b = 16 + 26k$$
$$13 \cdot 5 + b = 14 + 26l$$

$k = 0, l = 2, b = 1$ Dus het sleutelpaar (a, b) is (5,1).

Opgave 14

c = 2, f = 5, e = 4

$$\begin{cases} 5 + 26k = 2a + b \\ 4 + 26l = 5a + b \end{cases}$$
$$\begin{cases} b = 5 - 2a + 26k \\ b = 4 - 5a + 26l \end{cases}$$
$$5 - 2a + 26k = 4 - 5a + 26l$$
$$3a = -1 + 26(l - k)$$
$$a = 17, l - k = 2$$
$$5 + 26k = 2 \cdot 17 + b$$
$$4 + 26l = 5 \cdot 17 + b$$

$k = 2, l = 4, b = 23$ De sleutel is dus (17, 23).

Opgave 15

26!

Opgave 16

Zowel bij het schuifcryptosysteem als bij het affiene cryptosysteem is de sleutel een permutie toegepast op de letters van het alfabet.

Opgave 17

De moeder van een duizendpoot is vreselijk ontevreden, want haar zoontje is zojuist in de sloot gegleden. En als je even rekent, weet je wat dat betekent: op zijn hoofd een grote buil en wel duizend sokjes vuil!

Opgave 19

Vogel.

Opgave 20

a) Je weet niet hoe lang het sleutelwoord is en dus ook niet op welke letters je de frequentie-analyse moet toepassen.

b) Als je weet dat de sleutellengte *n* is, komt het kraken neer op *n* keer een schuifcryptosysteem kraken.

c) Nat.

Opgave 21

a) $P(A) \cdot P(A) + P(B) \cdot P(B) + \ldots + P(Z) \cdot P(Z)$

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

c)

$$\frac{1}{26} \cdot (P(A) \cdot (1 - P(A)) + P(B) \cdot (1 - P(B)) + \ldots + P(Z) \cdot (1 - P(Z))) =$$

$$\frac{1}{26} \cdot ((P(A) - P(A)^2 + P(B) - P(B)^2 + \ldots + P(Z) - P(Z)^2) =$$

$$\frac{1}{26} \cdot (P(A) + P(B) + \ldots + P(Z) - (P(A)^2 + P(B)^2 + \ldots + P(Z)^2) =$$

$$\frac{1}{26} \cdot (1 - (\text{het antwoord van onderdeel a})) =$$

$$\frac{1}{26} \cdot (1 - 0{,}075) = 0{,}036$$

d) Letters die een veelvoud van de sleutellengte uit elkaar staan, komen steeds uit een alfabet dat over hetzelfde aantal posities verschoven is. Omdat bepaalde letters daar vaker voorkomen, is de kans groter dat je juist die letters aantreft.

Opgave 22

Sleutellengte 4, want bij 4 en 8 posities verschoven zijn er meer overeenkomsten en 4 en 8 zijn veelvouden van 4. (Ook van 2 maar dan had je bij 2, 6, 10, enz. meer overeenkomsten verwacht.)

Opgave 23

a) Die worden hetzelfde vercijferd. De "I" wordt namelijk vercijferd met de derde letter van het sleutelwoord en de "N" met de vierde letter omdat 7 een viervoud plus 3 is en 8 een viervoud.

b) Als je op een veelvoud van een vast getal vaak dezelfde letterparen tegenkomt, zijn dat waarschijnlijk in de klare tekst letterparen die veel voorkomen en die over hetzelfde aantal posities in het alfabet verschoven zijn. De sleutellengte zal waarschijnlijk dat vaste getal zijn.

c) Als ze op een andere afstand van elkaar liggen worden ze over een verschillend aantal posities verschoven en leveren ze dus niet hetzelfde letterpaar in de cijfertekst.

Opgave 24

a) LR staat op positie 7,8 en 23,24 en 27,28 en 47,48 en 263,264. Dat is wel redelijk vaak. Het letterpaar GB komt op plaats 73,74 en 121,122 en 221,222 en 289,290 voor. Zo zijn er wel meer letterparen te vinden die regelmatig op viervouden uit elkaar voorkomen.
b) Code.

Opgave 25

Je moet dan een sleutelwoord gebruiken dat heel lang is ten opzichte van de lengte van de tekst. Het beste is het natuurlijk om een sleutelwoord te nemen dat even lang is als de tekst die je wilt vercijferen. Je zou bijvoorbeeld kunnen afspreken dat je als sleutelwoord steeds de volgende bladzijde uit een boek neemt dat je allebei hebt. Je moet dan alleen wel geheim houden waar je je sleutel vandaan haalt…

Opgave 26

Het is wel moeilijker, maar niet veel moeilijker als je bijv. een computer kunt gebruiken. Achterhalen van de sleutellengte werkt hetzelfde als bij Vigenère. Daarna moet je *n* keer een mono-alfabetische substitie ontcijferen i.p.v. *n* keer een schuifsysteem, maar met behulp van letterfrequentie-analyse en/of een computer is het wel binnen niet al te lange tijd te doen.

Opgave 27

Na de sleutel één keer gebruikt te hebben, wordt hij niet meer herhaald. De truuk waarbij je kijkt na hoeveel posities weer met dezelfde sleutel vercijferd wordt is hier dus niet te gebruiken.

4 Coderen

Opgave 1

28. Heb je aan de spaties en punt gedacht?

Opgave 2

084 117 115 115 101 110 032 075 101 117 108 101 110 032 101 110 032 080 097 114 105 106 115 046

Opgave 3

Op Mars is water gevonden!

Opgave 4

Anders weet je niet waar het volgende getal begint.

5 Getaltheorie

Opgave 1

a) Waar
b) Niet waar
c) Waar
d) Niet waar
e) Niet waar
f) Waar
g) Waar

Opgave 2

a) 8: 1, 2, 4, 8 -> 4, 81: 1, 3, 9, 27, 81 -> 5, 49: 1, 7, 49 -> 3.
b) $8 \cdot 81 \cdot 49$: $4 \cdot 5 \cdot 3 = 60$ delers.

Opgave 3

2, namelijk 1 en zichzelf.

Opgave 4

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

Opgave 5

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	97	98	99	10

Dus: 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.

Opgave 6

a) Omdat priemgetallen positief zijn en precies 2 delers hebben. Het getal 1 heeft maar één deler.

b) Omdat ze niet door een ander getal dan 1 en zichzelf deelbaar zijn. Veelvouden van 1 streep je niet door (anders zou je alles doorstrepen). Dus kunnen ze niet doorgestreept worden voor ze omcirkeld worden.

c) Omdat die allemaal een deler hebben die groter is dan 1 en kleiner dan het getal zelf.

Opgave 7

a) Samengesteld: 91, 121, 231, priemgetallen: 41, 101, niet samengesteld en niet priem: 1.

b) $91 = 7 \cdot 13$, $121 = 11^2$, $231 = 3 \cdot 7 \cdot 11$

Opgave 8

a) 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 60, 120.

b) 1, 2, 4, 7, 8, 14, 16, 28, 56, 112.

c) 1, 2, 4, 8.

d) 8.

Opgave 9

a) 18

b) 61

c) 47

d) a

Opgave 10

a) Ja

b) Ja

c) Ja

Opgave 11

a) Als d een deler is van a dan is dus $a{:}\,d$ geheel en dus kan voor v de uitkomst van $a{:}\,d$ genomen worden. Net zo voor w.

b) $a + m = vd + wd = d(v + m)$, $a - m = (vd - wd) = d(v - w)$

c) Zie **b)**.

Opgave 12

a) $a = vd$, $m = wd$, dus $a - qm = vd - qwd = d(v - qw)$ en dus geldt $d|(a - qm)$.

b) Als d niet de ggd van $a - qm$ en m en dus van $d(v - qw)$ en wd is, hebben $v - qw$ en w een deler gemeenschappelijk, zeg c. We weten dat $ggd(v, w) = 1$, want anders hadden a en m een grotere deler gemeenschappelijk gehad dan d. We hebben net gezegd dat de deler c moet een deler van w moet zijn , dus is hij het niet van $v$want $ggd(v, w) = 1$. Maar dan kan hij het niet van $v - qw$ zijn. Dus geldt $ggd(m, a - qm) = d$.

Opgave 13

a) ggd(252, 198) = ggd(198, 54) = ggd(54, 36) = ggd(36, 18) = ggd(18, 0) = 18.

b) ggd(6466, 5429) = ggd(5429, 1037) = ggd(1037, 244) = ggd(244, 61) = ggd(61, 0) = 61.

Opgave 14

a) $a - qm = rest(a{:}m)$. In opgave 12 hebben we gezien dat $ggd(a, m) = ggd(m, a - qm)$, dus geldt ook $ggd(a, m) = ggd(m, rest(a{:}m))$.

b) $rest(a{:}m) = a$ als $m > a$, dus dan geldt $ggd(a, m) = ggd(m, rest(a{:}m)) = ggd(m, a)$ en dat dat klopt zie je meteen.

Opgave 15

a) Op de onderste rij in de kolom onder *a*, op de daarboven onder *b* en op de rij daar weer boven onder *a* mod *b*.

b) 99.

Opgave 16

a) $ggd(96{,}22) = 2$

a	m	q	r
96	22	4	8
22	8	2	6
8	6	1	2
6	2	3	0
2	0		

b) $ggd(484,576) = 4$

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

c) ggd(47957, 32395) = 31

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

Opgave 17

a) 3
b) 72
c) 13
d) -4

Opgave 18

a) 2
b) 8
c) 0
d) 6

Opgave 19

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

Opgave 20

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

Opgave 21

a) $17\ mod\ 5 = 2 = 32\ mod\ 5$, $(32 - 17)\ mod\ 5 = 15\ mod\ 5 = 0$.
b) $22\ mod\ 1\ 1 = 0$, $35\ mod\ 1\ 1 = 3$, $(35 - 22)\ mod\ 1\ 1 = 13\ mod\ 1\ 1 \neq 0$.
c) $m = 13$.

Opgave 22

a) 20 cm.
b) 20 cm.
c) $(240 - 190)\ mod\ 2\ 5 = 0$, $(105 - 155)\ mod\ 2\ 5 = 0$.

Opgave 23

a) 5 cm.
b) $(240 - 190)\ mod\ 2\ 5 = 0$, dus weer 5 cm.
c) Van 25 keer 240 houd je niks over want $25 \cdot 240$ is een 25-voud, dus houd je 7 keer 240 over en daarvan houd je 5 cm over.
d) Zie **c)**.

Opgave 24

a) 9 (som)

b) 6 (product)

c) $17 \cdot (355 + 773) \, mod \, 7 = 3 \cdot (5 + 3) \, mod \, 7 = 24 \, mod \, 7 = 3$ (som en product)

Opgave 25

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Opgave 26

a) 3

b) 6

c) 10

d) 8

Opgave 27

a) $16 + x = 7 \text{ in } \mathbb{Z}_{23}$

$(16 + x) \bmod 23 = 7$

$16 + x - 23 \cdot k = 7$

$9 + x = 23k, \text{ dus } x = 14 \text{ en } k = 1$

b) $756 + x = 341 \text{ in } \mathbb{Z}_{1278}$

$(756 + x) \bmod 1278 = 341$

$756 + x - 1278 \cdot k = 341$

$415 + x = 1278k, \text{ dus } x = 863 \text{ en } k = 1$

Opgave 28

a) $(12 \cdot 6) \, mod \, 10 = 72 \, mod \, 10 = 2, (7 \cdot 6) \, mod \, 10 = 42 \, mod \, 10 = 2$ maar $12 \, mod \, 10 \neq 7 \, mod \, 10$.

b) Het verschil tussen 12 en 7 is 5. Wanneer je deze getallen met een even getal vermenigvuldigd wordt het verschil een veelvoud van 10.

c) Als m geen gemeenschappelijke deler heeft met a, b of c geldt wel dat $a = b$ als $a \cdot c = b \cdot c$.

Opgave 29

a) 078073 074077 069071 069078

b) 347073 225396 169030 177668

Opgave 30

Drachten.

Opgave 31

a) $x = 30$

b) $x = 19$

Opgave 32

a) $10 \cdot 6 \, mod \, 59 = 60 \, mod \, 59 = 1$.

b)
$$\begin{aligned} 10 \cdot x \bmod 59 &= 4 \bmod 59 \\ 6 \cdot 10 \cdot x \bmod 59 &= 6 \cdot 4 \bmod 59 \\ 60 \cdot x \bmod 59 &= 24 \bmod 59 \\ x \bmod 59 &= 24 \bmod 59 \\ x &= 24 \end{aligned}$$

c)
$$\begin{aligned} 10 \cdot x &= 5 \\ 6 \cdot 10 \cdot x &= 6 \cdot 5 \\ x &= 30 \end{aligned}$$

d) Je weet al keer welk getal je 10 moet doen om te zorgen dat de getallen keer elkaar $1 \, mod \, 5 \, 9$zijn.

Opgave 33

a) 0

b) 1

Opgave 34

a)

Getal	0	1	2	3	4
Inverse	-	1	3	2	4

b)

Getal	0	1	2	3	4	5
Inverse	-	1	-	-	-	5

c)

Getal	0	1	2	3	4	5	6
Inverse	-	1	4	5	2	3	6

d)

Getal	0	1	2	3	4	5	6	7
Inverse	-	1	-	3	-	5	-	7

e)

Getal	0	1	2	3	4	5	6	7	8
Inverse	-	1	5	-	7	2	-	4	8

f)

Getal	0	1	2	3	4	5	6	7	8	9
Inverse	-	1	-	7	-	-	-	3	-	9

g)

Getal	0	1	2	3	4	5	6	7	8	9	10
Inverse	-	1	6	4	3	9	2	8	7	5	10

h) Ja, a heeft een inverse modulo m als a en m geen gemeenschappelijke delers hebben.

Opgave 35

$(m-1)^2 = m^2 - 2m + 1 = 1$, want m^2 en $2m$ zijn veelvouden van m.

Opgave 36

a) Bijv. 35.

b) Nee, die zijn allebei deelbaar door 2.

c) Nee, bijv. oneven 3-vouden zijn niet relatief priem met 24 want die zijn ook deelbaar door 3.

Opgave 37

Omdat v, b, w en k gehele getallen zijn en als d groter dan 1 zou zijn dan zou $vb - wk$ een breuk moeten zijn.

Opgave 38

Vervang k door $-k$.

Opgave 39

$148104 - 47223 \cdot 3 = 6435$, enz.

Meer algemeen: $a - q \cdot m = a - (a\,div\,m) \cdot m = a\,mod\,m = r$

Opgave 40

a) 99

b) $b = 0, k = 1$

c) Op de onderste rij in de kolom onder *a*, op de daarboven onder *b* en op de rij daar weer boven onder *a* mod *b*.

d) $b = 0, k = 1$

Opgave 41

$b = 1, k = -1$

Opgave 42

a) $\text{ggd}(a, m) = 99 = 1 \cdot 2178 + -1 \cdot 2079 = 1 \cdot 2178 + -1 \cdot (6435 - 2 \cdot 2178) = -1 \cdot 6435 + 3 \cdot 2178$, dus $b = -1$ en $k = 3$.

b) $\text{ggd}(a, m) = 99 = -1 \cdot 6435 + 3 \cdot 2178 = -1 \cdot 6435 + 3 \cdot (47223 - 7 \cdot 6435) = 3 \cdot 47223 - 22 \cdot 6435$,

dus $b = 3$ en $k = -22$.

c) $\text{ggd}(a, m) = 99 = 3 \cdot 47223 - 22 \cdot 6435 = 3 \cdot 47223 - 22 \cdot (148104 - 3 \cdot 47223) = -22 \cdot 148104 + 69 \cdot 47223$,

dus $b = -22$ en $k = 69$.

d) $a = 148104, m = 47223, d = 99, b = -22, k = 69$,

$ab + mk = 148104 \cdot -22 + 69 \cdot 47223 = 99 = d$, dus klopt.

Opgave 43

a) $ggd(724{,}804) = 4$

a	*m*	$a\,div\,m = q$	$a\,mod\,m = r$	*b*	*k*
804	724	1	80	-9	10
724	80	9	4	1	-9
80	4	20	0	0	1
4	0				

b) Zie laatste twee kolommen bij **a)**. $b = -9, k = 10$.

c) ggd(47957, 32395) = 31, $b = -102, k = 151$, zie de berekening in de tabel.

a	*m*	$a\,div\,m = q$	$a\,mod\,m = r$	*b*	*k*
47957	32395	1	15562	-102	151
32395	15562	2	1271	49	-102
15562	1271	12	310	-4	49
1271	310	4	31	1	-4
310	31	10	0	0	1
31	0				

Opgave 44

a) $ggd(65{,}23) = 1, b = -6, k = 17$, zie tabel.

a	*m*	$a\,div\,m = q$	$a\,mod\,m = r$	*b*	*k*
65	23	2	19	-6	17
23	19	1	4	5	-6
19	4	4	3	-1	5
4	3	1	1	1	-1
3	1	3	0	0	1

1	0				

Controle: $-6 \cdot 65 + 17 \cdot 23 = 1$

b) Omdat de uitkomst -1 ipv 1 moet zijn, vermenigvuldigen we *b* en *k* met -1, dus $b = 6, k = -17$. Controle: $6 \cdot 65 + -17 \cdot 23 = -1$.

c) Omdat de uitkomst 3 ipv 1 moet zijn, vermenigvuldigen we *b* en *k* met 3, dus $b = -18, k = 51$. Controle: $-18 \cdot 65 + 51 \cdot 23 = 3$.

Opgave 45

a)

a	*m*	$a\ div\ m = q$	$a\ mod\ m = r$	*b*	*k*
23	72	0	23	-25	8
72	23	3	3	8	-25
23	3	7	2	-1	8
3	2	1	1	1	-2
2	1	2	0	0	1
1	0				

b) $b = -25, k = 8$, voor berekening zie laatste twee kolommen van de tabel.

c) In dit geval is $m = 72$ en $a = 23$. Je zoekt de waarde van *b* in de vergelijking $23b - 72k = 1$ en hebt de oplossing van de vergelijking $23b + 72k = 1$. Dus neem je $-k$ voor k. De inverse van 23 in $\mathbb{Z}_{72}$ is dus $(-25)\ mod\ 7\ 2$ en dat is 47.

Opgave 46

a) ggd(105, 291) = 3.

a	*m*	$a\ div\ m = q$	$a\ mod\ m = r$	*b*	*k*
105	291	0	105	-36	13
291	105	2	81	13	-36
105	81	1	24	-10	13
81	24	3	9	3	-10
24	9	2	6	-1	3
9	6	1	3	1	-1
6	3	2	0	0	1
3	0				

b) *b* = -36 en *k* = 13, zie tabel.

c) Omdat er wel een oplossing is voor de vergelijking $105b - 291k = 3$, maar niet voor $105b - 291k = 1$ doordat $ggd(291,105) \neq 1$.

Opgave 47

a)

a	*m*	$a\ div\ m = q$	$a\ mod\ m = r$	*b*	*k*
130	231	0	130	16	-9
231	130	1	101	-9	16
130	101	1	29	7	-9
101	29	3	14	-2	7
29	14	2	1	1	-2
14	1	14	0	0	1
1	0				

b) $b = 16, k = -9$**,** zie tabel.

c) In dit geval is $m = 231$ en $a = 130$. Je zoekt de waarde van *b* in de vergelijking $130b - 231k = 1$ en hebt de oplossing van de vergelijking $130b + 231k = 1$. Dus neem je $-k$ voor k. De inverse van 130 in $\mathbb{Z}_{231}$ is dus 16.

Opgave 48

a) Inverse van 27 in $\mathbb{Z}_{64}$ is 19.

b) Inverse van 153 in $\mathbb{Z}_{2164}$ is $-99\ mod\ 2\,164$, dus 2065.

Opgave 49

a) Als eerste letter een "E" is, dan $x = 069$. $(117 \cdot 69)\ mod\ 5\,00 = 8073\ mod\ 5\,00 = 73$.

b) $317 = (117 \cdot x)\ mod\ 5\,00$

c) $338 = (117 \cdot x)\ mod\ 5\,00$

d) $(453 \cdot 117)\ mod\ 5\,00 = 53001\ mod\ 5\,00 = 1$

e)
$$317 = (117 \cdot x) \bmod 500$$
$$453 \cdot 317 \bmod 500 = (453 \cdot 117 \cdot x) \bmod 500$$
$$453 \cdot 317 \bmod 500 = x \bmod 500$$
$$143601 \bmod 500 = x \bmod 500$$
$$101 = x$$

Dus is het tweede symbool van de klare tekst een "e".

f) $338 \cdot 453\ mod\ 5\,00 = 153114\ mod\ 5\,00 = 114$, dus "r".

g) Eerlijk delen!

Opgave 50

a) Als we de oplossing van die vergelijking weten, kunnen we de versleutelde codes vermenigvuldigen met de oplossing en hebben we de boodschap ontcijferd.

b) 143 eindigt op "3", om op "1" te eindigen moeten we vermenigvuldigen met een getal dat op "7" eindigt. $143 \cdot 7\ mod\ 5\,00 = 1001\ mod\ 5\,00 = 1$.

c) Voldemort

Opgave 51

a) Kwadrateren is hetzelfde als een getal met zichzelf vermenigvuldigen.

b) Tot de derde macht verheffen is het kwadraat van een getal met het getal zelf vermenigvuldigen, enz.

c) Herhaald vermenigvuldigen.

Opgave 52

^	0	1	2	3	4
0	1	0	0	0	0
1	1	1	1	1	1
2	1	2	4	3	1
3	1	3	4	2	1
4	1	4	1	4	1

Opgave 53

a) $2^{25} = (2^5)^5 = 32^5 = 1^5 = 1$.

b) $3^{301} = (3^3)^{100} \cdot 3 = 27^{100} \cdot 3 = (2^7)^{14} \cdot 2^2 \cdot 3 = 3^{14} \cdot 4 \cdot 3 =$
$3^{15} \cdot 4 = (3^3)^5 \cdot 4 = 2^5 \cdot 4 = 7 \cdot 4 = 3$

c) $18^{96} = (18^2)^{48} = (324)^{48} = 1$, want $(-1)\ mod\ 3\,25 = 324$, dus $(324)^{48}\ mod\ 3\,25 = (-1)^{48}\ mod\ 3\,25 = 1$

Opgave 54

a) $17^{33} = (17^3)^{11} = (489)^{11} = ((489)^2)^5 \cdot 489 = (225)^5 \cdot 489 =$
$(225^2)^2 \cdot 225 \cdot 489 = (302)^2 \cdot 531 = 512 \cdot 531 = 349$

b) $12^{40} = (12^4)^{10} = ((736)^2)^5 = (696)^5 = ((696)^2)^2 \cdot 696 = (416)^2 \cdot 696 =$
$56 \cdot 696 = 976$

c) $7^{3843} = (7^4)^{960} \cdot 7^3 = (481^2)^{480} \cdot 343 = (321^2)^{240} \cdot 343 = 1^{240} \cdot 343 = 343$

Opgave 55

a)

$$2^{47} = (2^6)^7 \cdot 2^5 = (17)^7 \cdot 32 = (17^2)^3 \cdot 17 \cdot 32 =$$
$$7^3 \cdot 27 = 7^2 \cdot 7 \cdot 27 = 2 \cdot 1 = 2$$

b) $3^{81} = (3^4)^{20} \cdot 3 = 1^{20} \cdot 3 = 3$

c) Van de uitkomsten van de machten van 3 schrijf ik steeds het laatste cijfer op: 3,9,7,1,3,9,7,1,3,…. De uitkomsten van de machten van 3 die een viervoud plus één als macht hebben eindigt steeds op 1, dus 3^{81} ook.

Opgave 56

a) 4 (1,5,7,11)

b) 4 (1,2,3,4)

c) 6 (1,2,3,4,5,6)

d) $p - 1$

Opgave 57

a) 24 (1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34 of 1 t/m 34 behalve 5,10,15,20,25,35,7,14,21,28)

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

c) $\phi(p \cdot q) = p \cdot q - 1 - (p-1) - (q-1) = p \cdot q - p - q + 1 = (p-1)(q-1) = \phi(p) \cdot \phi(q)$

Opgave 58

a) 20 (getallen 1 t/m 25 behalve de 5 vijfvouden.)

b) 100 (getallen 1 t/m 125 behalve de 25 vijfvouden.)

c) 500 (getallen 1 t/m 625 behalve de 125 vijfvouden.)

d) $\phi(p^r) = p^r - p^r/p = p^r - p^{r-1} = p \cdot p^{r-1} - 1 \cdot p^{r-1} = (p-1) \cdot p^{r-1}$.

Opgave 59

a) $\phi(640) = \phi(2^7) \cdot \phi(5) = (1 \cdot 2^6) \cdot 4 = 64 \cdot 4 = 256$

b) $\phi(49000) = \phi(2^3) \cdot \phi(5^3) \cdot \phi(7^2) = (1 \cdot 2^2) \cdot (4 \cdot 5^2) \cdot (6 \cdot 7^1) = 4 \cdot 100 \cdot 42 = 16800$

c) $\phi(245025) = \phi(3^4) \cdot \phi(5^2) \cdot \phi(11^2) = (2 \cdot 3^3) \cdot (4 \cdot 5^1) \cdot (10 \cdot 11^1) = 18 \cdot 20 \cdot 110 = 39600$

Opgave 60

a) $ggd(7,640) = 1, \phi(640) = 256$ (zie 60a), dus m.b.v. Euler: $7^{3843} = (7^{256})^{15} \cdot 7^3 = 1^{15} \cdot 7^3 = 1 \cdot 343 = 343$

b) $ggd(16,81) = 1, \phi(81) = 54$, dus mbv Euler: $16^{1033} = (16^{54})^{19} \cdot 16^7 = 1^{19} \cdot 16^7 = 1 \cdot (16^2)^3 \cdot 16 = 13^3 \cdot 16 = 10 \cdot 16 = 79$

c) $ggd(25,99) = 1, \phi(99) = 60$, dus mbv Euler $25^{3000} = (25^{60})^{50} = 1$, dus geldt $25 \cdot 25^{2999} = 1$, dus is 25^{2999}de inverse van 25 in $\mathbb{Z}_{99}$ en we kunnen met Euclides of door gewoon even te rekenen vinden dat deze 4 is.

Opgave 61

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

Opgave 62

a) 7

b) 70

Opgave 63

Elfstedentocht op 14 februari.

Opgave 64

a)
$$365727 = (243 \cdot t + 1234) \bmod 372281$$
$$365727 + 372281 \cdot k = 243 \cdot t + 1234$$
$$372281 \cdot k - 243 \cdot t = -364493$$

b) $(372281 \cdot k)\ mod\ 372281 = 0$, $(-364493)\ mod\ 372281 = 7788$.

c)
$$280785 = (243 \cdot t + 1234) \bmod 372281$$
$$280785 + 372281 \cdot k = 243 \cdot t + 1234$$
$$372281 \cdot k - 243 \cdot t = -279551$$

Dus $372038 \cdot t = 92730$ in $\mathbb{Z}_{372281}$

d)
$$c = (243 \cdot t + 1234) \bmod 372281$$
$$c + 372281 \cdot k = 243 \cdot t + 1234$$
$$372281 \cdot k - 243 \cdot t = 1234 - c$$

Dus $372038 \cdot t = 1234 - c$ in $\mathbb{Z}_{372281}$

Als je de inverse b van 372038 in $\mathbb{Z}_{372281}$ weet, weet je de oplossing van $372038 \cdot b = 1$ in $\mathbb{Z}_{372281}$.

Vervolgens kun je t berekenen: $t = b \cdot (1234 - c)$.

e)

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

De inverse van 372038 in $\mathbb{Z}_{372281}$ is dus (-148606) mod 372281 = 223675.

f) $t = b \cdot (1234 - c) = 223675 \cdot (1234 - 365727) = 078101$

Dus $t = 078101$ en de eerste twee letters van de boodschap zijn: “Ne”.

g) Newton: actie=-reactie

Opgave 65

$c = (1719 \cdot t)\ mod\ 294808$

Dus $c = 1719 \cdot t$ in $\mathbb{Z}_{294808}$

Als je de inverse b van 1719 in $\mathbb{Z}_{294808}$ weet, weet je de oplossing van $1719 \cdot b = 1$ in $\mathbb{Z}_{294808}$. Vervolgens kun je t berekenen: $t = b \cdot c$.

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

De inverse van 1719 in $\mathbb{Z}_{294808}$ is dus 343, dus $t = 343 \cdot c$.

Boodschap: Loper van B2 naar B5

Opgave 66

b) 485

6 Public key cryptografie

Opgave 1

a) $n-1$

b) $\frac{1}{2} \cdot n \cdot (n-1)$

Opgave 2

$$\overline{K} = \overline{B}^a = \left(\overline{g}^b\right)^a = \overline{g}^{b \cdot a} = \overline{g}^{a \cdot b} = \left(\overline{A}\right)^b = \overline{A}^b = \overline{K}$$

Opgave 3

a) $7^5 \equiv_{47} (7^2)^2 \cdot 7 \equiv_{47} 49^2 \cdot 7 \equiv_{47} 2^2 \cdot 7 \equiv_{47} 28$

b) $14^5 \equiv_{47} (14^2)^2 \cdot 14 \equiv_{47} 196^2 \cdot 14 \equiv_{47} 8^2 \cdot 14 \equiv_{47} 64 \cdot 14 \equiv_{47} 17 \cdot 14 \equiv_{47} 238 \equiv_{47} 3$

c) We zoeken een getal y zodanig dat $7^y \equiv_{47} 14$. We proberen wat: $7^1 \equiv_{47} 7, \quad 7^2 \equiv_{47} 2, \quad 7^3 \equiv_{47} 14$. Dus y zou 3 kunnen zijn.

d) $28^3 \equiv_{47} 21952 \equiv_{47} 3$

Opgave 4

a) $\overline{A} = \overline{g}^a$ en $\overline{B} = \overline{g}^b$.

b) $\overline{g}^{a \cdot b}$.

Opgave 5

a) $x = 5$

b) $x = 11$

c) $x = 19$

d) $x = 3$

e) $x = 3$

f) $x = 5$

Opgave 6

a) Als je $a^x = b$ moet oplossen, neem je $x = \frac{log\, b}{log\, a}$.

b) Je kent geen handige manier en moet dus alle mogelijkheden afgaan.

Opgave 7

$\bar{g}$, $\bar{g}^a$ en $\bar{g}^b$ zijn bekend. Als je daaruit a en b zou kunnen berekenen, kun je vervolgens $(\bar{g}^a)^b$ en $(\bar{g}^b)^a$ en dus de afgesproken sleutel $\bar{K}$ berekenen.

Opgave 8

a) $\overline{A} \equiv_{811} \overline{339}^{78} \equiv_{811} \overline{212}$.

b) $\overline{B} \equiv_{811} \overline{339}^{129} \equiv_{811} \overline{500}$.

c) $a = 3$.

d) $\overline{K} \equiv_{811} \overline{g}^{ab} \equiv_{811} \overline{B}^a \equiv_{811} \overline{500}^{78} \equiv_{811} \overline{570}$, maar ook $\overline{500}^3 \equiv_{811} \overline{570}$.

Opgave 9

a) $\overline{g}^5 \equiv_p \overline{339}^5 \equiv_{811} \overline{1}$.

b) $\overline{g}^{78} \equiv_{811} \left(\overline{g}^5\right)^{15} \cdot \overline{g}^3 \equiv_{811} \overline{1} \cdot \overline{g}^3 \equiv_{811} \overline{g}^3$.

c) 5, want na 5 machten herhaalt de rij uitkomsten zich.

Opgave 10

a) $\overline{6}^1 \equiv_7 \overline{6}, \overline{6}^2 \equiv_7 \overline{1}, \overline{6}^3 \equiv_7 \overline{6}, \overline{6}^4 \equiv_7 \overline{1}, \overline{6}^5 \equiv_7 \overline{6}$ en $\overline{6}^6 \equiv_7 \overline{1}$

b) $\overline{5}^1 \equiv_7 \overline{5}, \overline{5}^2 \equiv_7 \overline{4}, \overline{5}^3 \equiv_7 \overline{6}, \overline{5}^4 \equiv_7 \overline{2}, \overline{5}^5 \equiv_7 \overline{3}$ en $\overline{5}^6 \equiv_7 \overline{1}$

c) $\overline{5}$, meer verschillende uitkomsten mogelijk.

Opgave11

a) $\overline{2}, \overline{6}, \overline{7}, \overline{8}$

b) $\overline{3}, \overline{4}, \overline{5}, \overline{9}$

Opgave 12

a) $\phi(m) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1)$

b) De getallen e en $\phi(m)$ zijn relatief priem.

Opgave 13

a)

$\phi(m)$	e	q	r	k	d
5040	17	296	8	-2	593
17	8	2	1	1	-2
8	1	8	0	0	1
1	0				

b) $\phi(5183) = 5040$, dus $\overline{b}^{5040} \equiv_{5183} \overline{1}$ (Euler). $\overline{17}$ en $\overline{593}$ zijn elkaars inverse in $\mathbb{Z}_{5040}$, dus geldt $\overline{17} \cdot \overline{593} \equiv_{5040} \overline{1}$, m.a.w. er is een k zodanig dat $17 \cdot 593 = k \cdot 5040 + 1$.
$\left(\overline{b}^{17}\right)^{593} \equiv_{5183} \overline{b}^{17 \cdot 593} \equiv_{5183} \overline{b}^{k \cdot 5040 + 1} \equiv_{5183} \left(\overline{b}^{5040}\right)^k \cdot \overline{b} \equiv_{5183} \overline{1}^k \cdot \overline{b} \equiv_{5183} \overline{b}$.

c) $\overline{b}^{\phi(m)} \equiv_m \overline{1}$ (Euler). $\overline{d}$ en $\overline{e}$ zijn elkaars inverse in $\mathbb{Z}_{\phi(m)}$, dus geldt $\overline{e} \cdot \overline{d} \equiv_{\phi(m)} \overline{1}$, m.a.w. er is een k zodanig dat $e \cdot d = k \cdot \phi(m) + 1$.

$$\left(\overline{b}^{e}\right)^{d} \equiv_m \overline{b}^{e \cdot d} \equiv_m \overline{b}^{k \cdot \phi(m) + 1} \equiv_m \left(\overline{b}^{\phi(m)}\right)^k \cdot \overline{b} \equiv_m \overline{1}^k \cdot \overline{b} \equiv_m \overline{b}$$

Opgave 14

a) $\overline{41}^{17} \equiv_{5183} \overline{5021}$

b) $\overline{5021}^{593} \equiv_{5183} \overline{41}$

Opgave 15

a) 17 18 00

b) Code: 171 800. Vercijfering: $\overline{171}^{17}\ \overline{800}^{17}$ in $\mathbb{Z}_{5183}$

$\overline{171}^{17} \equiv_{5183} \left(\overline{171}^2\right)^8 \cdot \overline{171} \equiv_{5183} \left(\overline{3326}^2\right)^4 \cdot \overline{171} \equiv_{5183} \left(\overline{1754}^2\right)^2 \cdot \overline{171} \equiv_{5183}$
$\overline{2997}^2 \cdot \overline{171} \equiv_{5183} \overline{5053} \cdot \overline{171} \equiv_{5183} \overline{3685}$

$\overline{800}^{17} \equiv_{5183} \left(\overline{800}^2\right)^8 \cdot \overline{800} \equiv_{5183} \left(\overline{2491}^2\right)^4 \cdot \overline{800} \equiv_{5183} \left(\overline{1030}^2\right)^2 \cdot \overline{800} \equiv_{5183}$
$\overline{3568}^2 \cdot \overline{800} \equiv_{5183} \overline{1176} \cdot \overline{800} \equiv_{5183} \overline{2677}$

Vercijferd bericht: 3685 2677.

c) $\overline{3685}^{593} \equiv_{5183} \left(\overline{3685}^2\right)^{296} \cdot \overline{3685} \equiv_{5183} \left(\overline{4948}^2\right)^{148} \cdot \overline{3685} \equiv_{5183}$

$\left(\overline{3395}^2\right)^{74} \cdot \overline{3685} \equiv_{5183} \left(\overline{4216}^2\right)^{37} \cdot \overline{3685} \equiv_{5183} \left(\overline{2149}^2\right)^{18} \cdot \overline{2149} \cdot \overline{3685} \equiv_{5183}$

$\left(\overline{148}^3\right)^6 \cdot \overline{4624} \equiv_m \left(\overline{2417}^2\right)^3 \cdot \overline{4624} \equiv_{5183} \overline{648}^3 \cdot \overline{4624} \equiv_{5183} \overline{658} \cdot \overline{4624} \equiv_{5183} \overline{171}$

$\overline{2677}^{593} \equiv_{5183} \left(\overline{2677}^2\right)^{296} \cdot \overline{2677} \equiv_{5183} \left(\overline{3423}^2\right)^{148} \cdot \overline{2677} \equiv_{5183}$

$\left(\overline{3349}^2\right)^{74} \cdot \overline{2677} \equiv_{5183} \left(\overline{4972}^2\right)^{37} \cdot \overline{2677} \equiv_{5183} \left(\overline{3057}^2\right)^{18} \cdot \overline{3057} \cdot \overline{2677} \equiv_{5183}$

$\left(\overline{300}^3\right)^6 \cdot \overline{4815} \equiv_m \left(\overline{1753}^2\right)^3 \cdot \overline{4815} \equiv_{5183} \overline{4673}^2 \cdot \overline{4673} \cdot \overline{4815} \equiv_{5183}$

$\overline{950} \cdot \overline{1092} \equiv_{5183} \overline{800}$

Ontcijferd bericht: 171 800.

Opgave 16

a) $209 = 19 \cdot 11$, dus $\phi(209) = \phi(19) \cdot \phi(11) = 18 \cdot 10 = 180$. Je moet dus de inverse van $\overline{13}$ in $\mathbb{Z}_{180}$ vinden.

$\phi(m)$	e	q	r	k	d
180	13	13	11	6	-83
13	11	1	2	-5	6
11	2	5	1	1	-5
2	1	2	0	0	1
1	0				

$\overline{-83} \equiv_{180} \overline{97}$, de inverse van $\overline{13}$ is dus $\overline{97}$ en de geheime sleutel van Bob is dus (209,97).

b) Het is moeilijk om het getal 1040257 te ontbinden in priemfactoren. Je kunt $\phi(m)$ niet vinden en weet dus niet in welke $\mathbb{Z}_{\phi(m)}$ je de inverse van 1361 moet vinden.

Opgave 17

a) Voor het vercijferen heb je de geheime sleutel van Alice nodig en die weet alleen Alice.

b) Ontcijfer eerst $\bar{c}$ met de geheime sleutel van Bob, dus $\bar{c}^b \equiv_{m_b} (\bar{t}^B)^b \equiv_{m_b} \bar{t}$, dan krijg je $\bar{t}$ en die ontcijfer je met de publieke sleutel van Alice, dus $\bar{t}^A \equiv_{m_a} (\bar{s}^a)^A \equiv_{m_a} \bar{s}$.

c) Voor het ontcijferen heb je de geheime sleutel van Bob nodig en die weet alleen Bob.

Opgave 18

a) $\phi(m_a) = \phi(p_a \cdot q_a) = \phi(5 \cdot 13) = \phi(5) \cdot \phi(13) = 4 \cdot 12 = 48$, $\phi(m_b) = \phi(p_b \cdot q_b) = \phi(7 \cdot 11) = \phi(7) \cdot \phi(11) = 6 \cdot 10 = 60$

b)

$\phi(m_a)$	a	q	r	k	A
48	19	2	10	2	-5
19	10	1	9	-1	2
10	9	1	1	1	-1
9	1	9	0	0	1
1	0				

Publieke sleutel van Alice is $-5 + 48 = 43$.

$\phi(b)$	b	q	r	k	B
60	17	3	9	2	-7
17	9	1	8	-1	2
9	8	1	1	1	-1
8	1	8	0	0	1

1	0				

Publieke sleutel van Bob is $-7 + 60 = 53$.

c) $\overline{6}^{19} \equiv_{65} \overline{46}$, $\overline{46}^{53} \equiv_{77} \overline{30}$.

d) $\overline{30}^{17} \equiv_{77} \overline{46}$, $\overline{46}^{43} \equiv_{65} \overline{6}$.

7 De bewijzen

Opgave 1

a) In de eerste verzameling zitten de getallen -3, -2 en 01, in de tweede niet.

b) $\{101 \leq x \leq 1001 | x = 2k, k \in \mathbb{Z}\}$

Opgave 2

a) Niet waar

b) Waar

Opgave 3

a) Ja, allebei rest 2.

b) Nee, $30 \, mod \, 8 = 4$, $93 \, mod \, 8 = 7$.

c) Ja 9.

Opgave 4

a) Bv. -7, -2, 3, 8, 13, 18, 23, 28.

b) $(38 - k \cdot 5) \, mod \, 5 = 38 \, mod \, 5 - k \cdot 5 \, mod \, 5 = 3 - 0 = 3$.

c) $a = r - x \cdot m$, $b = r - y \cdot m$ want a en b zijn congruent modulo m.

$$\begin{aligned} b &= a - a + r - y \cdot m \\ &= a - (r - x \cdot m) + r - y \cdot m \\ &= a + x \cdot m - y \cdot m \\ &= a + (x - y) \cdot m \\ &= a - (y - x) \cdot m \end{aligned}$$

k is dus $y - x$.

Opgave 5

$a = r - x \cdot m$, $b = r - y \cdot m$ want a en b zijn congruent modulo m.

$$\begin{aligned} a - b &= (r - x \cdot m) - (r - y \cdot m) \\ &= y \cdot m - x \cdot m \\ &= (y - x) \cdot m \end{aligned}$$

Dus $m | a - b$.

Opgave 6

a) $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$

b) $\overline{0} = \{\ldots, -14, -7, 0, 7, \ldots\} = \{x \in \mathbb{Z} | x \equiv_7 0\}$

$\overline{1} = \{\ldots, -13, -6, 1, 8, \ldots\} = \{x \in \mathbf{Z} \mid x \equiv_7 1\}$ $\overline{2} = \{\ldots, -12, -5, 2, 9, \ldots\} =$

$\{x \in \mathbb{Z} | x \equiv_7 2\}$ $\overline{3} = \{\ldots, -11, -4, 3, 10, \ldots\} = \{x \in \mathbf{Z} \mid x \equiv_7 3\}$ $\overline{4} =$

$\{\ldots, -10, -3, 4, 11, \ldots\} = \{x \in \mathbb{Z} | x \equiv_7 4\}$

$\overline{5} = \{\ldots, -9, -2, 5, 12, \ldots\} = \{x \in \mathbf{Z} \mid x \equiv_7 5\}$ $\overline{6} = \{\ldots, -8, -1, 6, 13, \ldots\} =$

$\{x \in \mathbb{Z} | x \equiv_7 6\}$

c) Elk geheel getal heeft na deling door 7 rest 0, 1, 2, 3, 4, 5 of 6 en zit dus in één van deze restklassen.

Opgave 7

a) want $c \equiv_m d$

b) m is een deler van $a - b$, dus is er een getal v waarvoor geldt dat $vm = a - b$.

c) $c - d$.

d) b, c, d.

e) $(a + c) - (b + d)$.

Opgave 8

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Opgave 9

1. $m|a-b$ want $a \equiv_m b$
2. $m|c-d$ want $c \equiv_m d$
3. Er is een *v* zodat $vm = a-b$ (1)
4. Er is een *w* zodat $wm = c-d$ (2)
5. $vm \cdot c = (a-b)\cdot c$ (3)
6. $wm \cdot b = (c-d)\cdot b$ (4)
7. $(a-b)\cdot c + (c-d)\cdot b = vmc + wmb = (vc+wb)\cdot m$ (5,6)
8. $(a-b)\cdot c + (c-d)\cdot b = ac - bd = (vc+wb)\cdot m$ (7)
9. $m|ac-bd$ (8)
10. $a \cdot c \equiv_m b \cdot d$ (9)

Opgave 10

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Opgave 11

a)

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

b) Op iedere rij komen alle restklassen voor.

Opgave 12

a) Omdat dan voor ieder getal b geldt dat $a \cdot b \equiv_p 0$.

b) Omdat a geen *p*-voud is en de getallen $1,2,\ldots,p-1$ook geen *p*-voud kunnen zijn.

c) $a, 2a, \ldots, (p-1)a$ verschillen onderling elk een veelvoud van a dat geen veelvoud van p kan zijn. Als er twee dezelfde rest zouden hebben, zouden het verschil een veelvoud van $p$moeten zijn en dat kan niet zo zijn.

d) Als de getallen$a, 2a, \ldots, (p-1)a$ allen een andere rest hebben, zijn de restklasssen $\overline{a}\cdot\overline{0}, \overline{a}\cdot\overline{1}, \overline{a}\cdot\overline{2}, \ldots, \overline{a}\cdot\overline{p-1}$allen verschillend. In $\{\overline{a}\cdot\overline{0}, \overline{a}\cdot\overline{1}, \overline{a}\cdot\overline{2}, \ldots, \overline{a}\cdot$

$\overline{p-1}\}$komen dan precies alle restklassen uit $\mathbb{Z}_p$ voor en dus geldt $\{\overline{a}\cdot\overline{0},\overline{a}\cdot\overline{1},\overline{a}\cdot\overline{2},\ldots,\overline{a}\cdot\overline{p-1}\}=\{\overline{0},\overline{1},\overline{2},\ldots,\overline{p-1}\}$.

Opgave 13

a) $(\overline{a}\cdot\overline{1})\cdot(\overline{a}\cdot\overline{2})\cdot\ldots\cdot(\overline{a}\cdot\overline{p-1})=\overline{a}^{p-1}\cdot(\overline{1}\cdot\overline{2}\cdot\ldots\cdot\overline{p-1})=\overline{a}^{p-1}(\overline{p-1})!$

b) In opgave 45 hebben we gezien dat de restklassen links dezelfde zijn als de restklassen rechts, dus geldt hier een gelijkheid. Vermenigvuldigen met restklassen komt neer op het vermenigvuldigen van willekeurige elementen uit de betreffende restklassen.

c) $(\overline{a}\cdot\overline{1})\cdot(\overline{a}\cdot\overline{2})\cdot\ldots\cdot(\overline{a}\cdot\overline{p-1})=\overline{a}^{p-1}\cdot(\overline{1}\cdot\overline{2}\cdot\ldots\cdot\overline{p-1})=\overline{a}^{p-1}(\overline{p-1})!$ en $(\overline{a}\cdot\overline{1})\cdot(\overline{a}\cdot\overline{2})\cdot\ldots\cdot(\overline{a}\cdot\overline{p-1})=\overline{1}\cdot\overline{2}\cdot\ldots\cdot\overline{p-1}=(\overline{p-1})!$, dus $\overline{a}^{p-1}(\overline{p-1})!=(\overline{p-1})!$, dus $\bar{a}^{p-1}=1$

Opgave 14

a)

·	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

b) Op de regels waar de restklasse relatief priem is met 8 komen alle restklassen voor, op de andere regels niet.

Opgave 15

$(\overline{a}\cdot\overline{a_1})\cdot(\overline{a}\cdot\overline{a_2})\cdot\ldots\cdot(\overline{a}\cdot\overline{a_{\phi(m)}})=\overline{a}^{\phi(m)}\cdot(\overline{a_1}\cdot\overline{a_2}\cdot\ldots\cdot\overline{a_{\phi(m)}})$en $(\overline{a}\cdot\overline{a_1})\cdot(\overline{a}\cdot\overline{a_2})\cdot\ldots\cdot(\overline{a}\cdot\overline{a_{\phi(m)}})=\overline{a_1}\cdot\overline{a_2}\cdot\ldots\cdot\overline{a_{\phi(m)}}$dus $\overline{a}^{\phi(m)}=1$.

Opgave 16

Als $p|n^p-n$ wil dat zeggen dat $n^p\equiv_p n$, dus dat $n^{p-1}\equiv_p 1$.

Bibliografie

- An introduction to cryptologie – Henk C.A. van Tilborg
- Cryptografie – Gerard Tel
- Dictaat Getallen – Frans Keune
- Dictaat Inleiding in de wiskunde – Frans Keune
- Dictaat Wiskundig Denken – Frans Keune
- Geheim? Cryptografie en getaltheorie – Kerngroep vo-ho Wiskunde D i.s.m. Ernst Lambeck
- Handbook of applied cryptography – Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone
- Kraak de code – Roger Labie, Koen Stulens
- Kun je die code kraken? – Henk C.A. van Tilborg
- Materiaal training Internationale Wiskunde-Olympiade – Thijs Notenboom, Maxim Hendriks
- nl.wikipedia.org
- Rijmpjes en versjes uit de nieuwe doos – Han Hoekstra, Fiep Westendorp
- The art of computer programming volume 2 – Donald E. Knuth
- www.asciitabel.nl
- www.wisfaq.nl

Index