Geheim?

Cryptografie en getaltheorie

Uitwerkingen

Uitwerkingen bij de module voor Wiskunde D (vwo)
Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven

2009

Samenstelling:
Kerngroep vo-wo Wiskunde D i.s.m. Ernst Lambeck (versie september 2009 - variant B 270809)

1 Wat is cryptografie?

1 Het eerste woord is waarschijnlijk het woord DE. Dan moet FKG (in de tweede regel) waarschijnlijk DIE zijn. Het derde woord in de eerste regel heb je dan ook al bijna: *EI*E*. Je zult dan al snel kunnen denken dat dat woord KEIZER moet zijn. Zo doorgaand vind je (hopelijk) "DE ROMEINSE KEIZER JULIUS CAESAR HAD VEEL VIJANDEN. DE BOODSCHAPPEN DIE HIJ AAN ZIJN LEGERS STUURDE MOESTEN DAAROM GECODEERD WORDEN. HET SYSTEEM DAT DE KEIZER DAARVOOR GEBRUIKTE IS OOK BIJ DEZE TEKST GEBRUIKT. ZIE JE DE SLEUTEL?."

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

3 Het aantal plaatsen waarover werd verschoven is gelijk aan 2.

4 De 'a' wordt een 'c', dus de sleutel is C.

5 Je kunt de 'a' vervangen door een 'a', 'b', ..., 'z'. Er zijn dus 26 sleutels mogelijk. (Hiervan is sleutel A uiteraard zeer flauw.)

6 D wordt J, E wordt K, enzovoort. Dit geeft als cijfertekst: JK NUULJYZGJ BGT TKJKXRGTJ OY GSYZKXJGS.

7 Verschuif de letters van het begin van de zin over één plaats, over twee plaatsen, enzovoort, tot er iets zinvols tevoorschijn komt. Je krijgt dan achtereenvolgens:

TOLOQ BSTZD; UPMPR CTUAE; VQNQS DUVBF; WRORT EVWCG;
XSPSU FWXDH; YTQTV GXYEI; ZURUW HYZFJ; AVSVX IZAGK;
BWTWY JABHL; CXUXZ KBCIM; DYVYA LCDJN; EZWZB MDEKO;
FAXAC NEFLP; GBYBD OFGMQ; HCZCE PGHNR; IDADF QHIOS;
JEBEG RIJPT; KFCFH SJKQU; LGDGI TKLRV; MHEHJ ULMSW;
NIFIK VMNTX; OJGJL WNOUY; PKHKM XOPVZ; QLILN YPQWA;
RMJMO ZQRXB; SNKNP ARSYC.

Alleen het vetgedrukte fragment is zinvol. Als je de gehele zin volgens de daarbij behorende verschuiving verschuift, dan krijg je de klare tekst "JEBEG RIJPT NUHOP ELIJK DATHE TCAES ARSYS TEEMG EMAKK ELIJK TEONT CIJFE RENIS", dus "je begrijpt nu hopelijk dat het Caesarsysteem gemakkelijk te ontcijferen is".

8 -

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

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

11 Nu is QB waarschijnlijk DE, dus elke Q is een D en elke B is een E. Vanwege de 1-0 gaat het waarschijnlijk over een sportwedstrijd, dus zal waarschijnlijk ZBJWCPLBF het woord GEWONNEN, VERLOREN, GEKLOPT of VERSLAGEN voorstellen. Van deze woorden past alleen VERSLAGEN. Maar dan zou de Z een V moeten zijn, de J een R, de W een S, de C een L, de P een A, de L een G en de F een N. Als je dat overal gaat invullen, dan zie je al snel de tekst "De Nederlandse hockeyvrouwen hebben na de wereldtitel van afgelopen jaar nu ook de Champions Trophy veroverd. In de eindstrijd werd gastland Argentinië met 1-0 verslagen. Maartje Paumen maakte het enige doelpunt. Zij scoorde al na twee minuten."

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

13 a. De 26 letters van het alfabet in één of andere volgorde gezet, b.v. rqbadsckzfoymtjlxpuevgwhin. Je vervangt in dat geval elke a door een r, elke b door een q, elke c door een b, enzovoort.

b. Er zijn $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 2 \cdot 1 = 26! \approx 4 \cdot 10^{26}$ sleutels te maken.

14 Tip: kijk welke letters vaak voorkomen.

15 Als we de letters tellen, dan zien we dat de P het meeste voorkomt (15 keer), gevolgd door de E (8 keer), de H (6 keer) en de L (6 keer). Vervang daarom allereerst de P door de E. Je krijgt dan (de vervangen letters zijn klein geschreven): "eGFeG eEEeL THAWe EHGDH QeEXZ LSETe LTHAJ eASZZ LeeAT HYEeH ASeLe GeEEe LNCKU".

De E wordt waarschijnlijk een N, A of T. In het tweede en het eennalaatste vijftal zie je twee keer het paar EE tussen twee e's. Dus de E kan zeer waarschijnlijk geen A zijn. Aangezien in het Nederlands de paren TE en ET samen vaker voorkomen dan de paren NE en NE, proberen we de E te vervangen door een T. We krijgen dan: "eGFeG etteL THAWe tHGDH QetXZ LStTe LTHAJ eASZZ LeeAT HYteH ASeLe Gette LNCKU".

We zien nu twee keer "GetteL", dat zou wel eens het woord "letter" kunnen zijn. We vervangen dus G door een L en de L door een R. Dit levert het volgende op: "elFel etter THAWe tHlDH QetXZ rStTe rTHAJ eASZZ reeAT HYteH ASere lette rNCKU".

Het eerste woord zou nu wel eens "elke" kunnen zijn. We vervangen daarom de F door een K: "elkel etter THAWe tHlDH QetXZ rStTe rTHAJ eASZZ reeAT HYteH ASere lette rNCKU".

Als we op zoek gaan naar de lidwoorden "de", "het" en "een" die je toch ook vaak tegenkomt, dan is "een" alleen mogelijk bij "eeA". Laten we nu eens de A door een N

vervangen: "elkel etter THnWe tHlDH QetXZ rStTe rTHnJ enSZZ reenT HYteH nSere lette rNCKU".

Kijken we nu naar het woord voor de laatste "letter", dan zouden we kunnen vermoeden dat dat eindigt met "dere", misschien is het woord wel "andere". Vervang H door A en S door D: "elkel etter TanWe talDa QetXZ rdtTe rTanJ endZZ reenT aYtea ndere lette rNCKU".

Het drietal "Tan"zien we nu ook twee keer, dit is waarschijnlijk "van". We gaan T vervangen door V: "elkel etter vanWe talDa QetXZ rdtve rvanJ endZZ reenv aYtea ndere lette rNCKU".

"WetalDaQet"zou "het alfabet"kunnen voorstellen. Vervang dus W door H, D door F en Q door B: "elkel etter vanhe talfa betXZ rdtve rvanJ endZZ reenv aYtea ndere lette rNCKU".

Kijk je nu naar "vervanJen dZZr" dan krijg je het vermoeden dat dit wel eens "vervangen door"zou kunnen zijn. Vervang dus J door G en Z door O: "elkel etter vanhe talfa betXo rdtve rvang endoo reenv aYtea ndere lette rNCKU".

Nu zie je de klare tekst hopelijk al: "elke letter van het alfabet wordt vervangen door een vaste andere letter." De laatste vier letters in de cijfertekst (NCKU) zijn alleen maar opgeschreven om het vijftal vol te maken.

16 Als je de letters telt, dan krijg je de volgende tabel.

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
9	14	59	0	25	40	32	14	15	46	13	7	130	9	11	39	9	11	11	19	0	45	37	0	12	8

Op grond van deze aantallen vermoed je allereerst dat de M een E zal voorstellen en de C een N. In de eerste regel kom je drie keer de combinatie VM tegen. Waarschijnlijk zal dit nu DE voorstellen. Vervang daarom de V door een D. In de eerste regel staat nu LeEPT deFWe nnede JIGnd eJEdP enRNn YPPdE ZRGTT.

De J is ook één van de meest voorkomende letters en zal nu vermoedelijk de A, de T of de R voorstellen. Nemen we de R voor de J, dan wordt de eerste regel LeEPT deFWe nnede rIGnd erEdP enRNn YPPdE ZRGTT, waardoor we het woord "nederlanders"kunnen herkennen in nede rIGnd erE. We vervangen nu de I door de L, de G door de A en de E door de S.

In de eerste regel kunnen we nu na "nederlandersdPen"lezen. De P stelt dus waarschijnlijk de O voor. Vervolgens merken we op dat de letters F en W nu de meest voorkomende letters zijn die we nog niet hebben vervangen. Op grond van de frequentietabellen zou je nu kunnen vermoeden dat deze de letters T en I moeten voorstellen, immers alle overige vaak voorkomende letters hebben we al gebruikt. Als je nu naar het begin van de eerste regel kijkt dan ligt het voor de hand om de F te vervangen door een T en de W door een I (je krijgt dan het woord "tien").

Aan het eind van de zevende regel zien we nu staan: QBtdi nsdaH. De H stelt dus ongetwijfeld een G voor. De laatste regel eindigt met iQdeS inBel, waar we aan het eind het woord "winkel"herkennen. De S stelt dus een W voor en de B een K. Ook kom je

enkele keren "onder Loeke rs"tegen. De L zal dus een Z moeten zijn. Nu is het begin van de tekst duidelijk: "zes op de tien nederlanders", de T stelt dus een P voor.

Het begin van de vierde regel luidt nu "respe ZtieK eliQk". Dat moet het woord "respectievelijk"zijn. Dus de Z stelt een C voor, de K een V en de Q een J. Ook herken je nu het woord "boodschappen", dus de R moet een H worden en de Y een B. Je kunt de tekst nu ongetwijfeld lezen:

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

Er is dus vercijferd met de volgende sleutel (we weten alleen niet waar de D, de U en de X voor staan):

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
F	K	N	-	S	T	A	G	L	R	V	Z	E	U	M	O	J	H	W	P	-	D	I	-	B	C

17 -

18 -

19 De sleutel W vercijfert een W tot een S, de sleutel I vercijfert een I tot een Q, enzovoort. Je vindt op deze manier het sleutelwoord "wiskunde".

20

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

Zo doorgaand vinden we de volgende cijfertekst (in groepjes van vijf letters): "WCHMW SGKIC NSZVZ ODKRL KBBEW GCXHE FSXAL MVZMY KZRIG BCKKE OAUVR OBUGS DSTH"

21 Het heeft geen zin om te tellen hoe vaak iedere letter voorkomt. Verschillende letters kunnen op verschillende plaatsen tot een zelfde letter versleuteld worden (zie in de vorige opgave bijvoorbeeld de eerste en de vijfde letter: beiden worden een W).

22 a. zlpywopwarjwyleiauaq

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

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

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

e. Zie de tekst na de opgave.

23 a. $P(\text{twee gelijke letters}) = \text{P(twee a's)} + \text{P(twee b's)} + \ldots + \text{P(twee z's)} = 0,075 \cdot 0,075 + 0,014 \cdot 0,014 + \ldots + 0,014 \cdot 0,014 \approx 0,078878$.

b. Als het sleutelwoord willekeurig is gekozen, dan heeft elke willekeurige letter een even grote waarschijnlijkheid om bij een vercijfering te voorschijn te komen. Dus is de kans dat deze letters hetzelfde zijn gelijk aan $P(\text{twee gelijke letters}) = \text{P(twee a's)} + \text{P(twee b's)} + \ldots + \text{P(twee z's)} = \frac{1}{26} \cdot \frac{1}{26} + \frac{1}{26} \cdot \frac{1}{26} + \ldots + \frac{1}{26} \cdot \frac{1}{26} = 26 \cdot \frac{1}{26} \cdot \frac{1}{26} = \frac{1}{26}$.

24 De kans op een overeenkomst bij het verschuiven over een ander aantal plaatsen is volgens b. van de vorige opgave gelijk aan $\frac{1}{26} \approx 0,0385$. Bij het verschuiven over 4, over 8 letters, enzovoort, heb je een overeenkomst als de oorspronkelijke letters gelijk waren (ze worden immers op precies dezelfde manier versleuteld). De kans hierop is volgens a. van de vorige opgave 0,078878. Je mag dus meer overeenkomsten verwachten bij het verschuiven over een viervoud plaatsen.

25 Het aantal overeenkomsten is het grootst bij het verschuiven over 20 en over 35 plaatsen. Je mag dus, denk aan de vorige opgaven, redelijkerwijs verwachten dat het sleutelwoord 20 of 35 letters lang is. Het sleutelwoord zou ook 5 letters lang kunnen zijn omdat zowel 20 als 35 een veelvoud van 5 is.

26 5 wordt genoemd omdat 20 en 35 beide veelvouden van 5 zijn.

27 We verschuiven over alle mogelijke aantallen plaatsen en tellen de overeenkomsten. Dit geeft de volgende tabel.

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

We zien dat het grootste aantal overeenkomsten 6 is (bij 10 en bij 40 plaatsen verschuiven) en verder zien we een flink aantal keren 5 overeenkomsten (bij 4, bij 8, bij 12, bij 16, bij 20 en bij 28 overeenkomsten). Omdat op de genoemde 10 na alle aantallen deelbaar zijn door 4, mogen we concluderen dat het sleutelwoord waarschijnlijk 4 letters lang is, maar gezien de 10 en de 40 plaatsen lijkt 10 misschien ook nog mogelijk.

28 Afstanden die een veelvoud zijn van de lengte van het sleutelwoord zullen vaker voorkomen. Zoek dus alle afstanden. Getallen waarvan veelvouden vaak als afstand voorkomen zijn dan mogelijke lengten van het sleutelwoord.

29 Ze worden op precies dezelfde wijze vercijferd. De O beide keren met de tweede letter van het sleutelwoord, de P beide keren met de derde letter.

30 a. Het is mogelijk dat twee willekeurige paren letters bij vercijfering tot hetzelfde letterpaar worden vercijferd. Uiteraard is dan de afstand van dat letterpaar niet gelijk aan een veelvoud van de lengte van het sleutelwoord. Immers paren letters die precies zo'n veelvoud uit elkaar liggen worden met dezelfde sleutel vercijferd.

b. Bovenstaande methoden werken beter voor een lange tekst. Er kunnen immers toevallige overeenkomsten optreden. Bij een lange tekst zullen er veel systematische overeenkomsten zijn, waardoor de rol van het toeval minder groot is.

31 BX (5, 20 en 25), CV (24), HB (54), HC (10), HN (40), NS (8, 40 en 48), NW (16), OH (3, 37 en 40), WY (16), XH (8) en YH (44) zijn de letterparen die vaker voorkomen. Tussen haakjes staan de afstanden. Van deze afstanden zijn er 7 een veelvoud van 5 en 11 een veelvoud van 4. Dus waarschijnlijk is de lengte van het sleutelwoord 4.

32 Verdeel de letters in blokken van 4. Kijk vervolgens alleen naar de eerste letters: NBNNOOWNKCEDNFOSB. De twee letters die hierin het vaakst voorkomen zijn de N en de O. Eén van deze twee zal waarschijnlijk een vercijferde E zijn. De eerste letter van het sleutelwoord is dus een J (als de E vercijferd is tot een N) of een K (als de E vercijferd is tot een O).

Kijk vervolgens alleen naar de tweede letters: SGSWHBHWBQFKSOHG. De twee letters die hierin het vaakst voorkomen zijn de H en de S. Eén van deze twee zal waarschijnlijk een vercijferde E zijn. De tweede letter van het sleutelwoord is dan een D (als de E vercijferd is tot een H) of een O (als de E vercijferd is tot een S).

Kijk vervolgens naar de derde letters: YNOYYECYXBXYCHBX. De twee letters die hierin het vaakst voorkomen zijn de X en de Y. Eén van deze twee zal waarschijnlijk een vercijferde E zijn. Dit geeft als mogelijke derde letter voor het sleutelwoord een U of een T.

Tenslotte kijken we naar de vierde letters: HHUMJRVYHXHHVKXA. De H komt hier verre weg het vaakst voor. Dit zal waarschijnlijk een vercijferde E zijn. Dit geeft als vierde letter van het sleutelwoord een D.

Samenvattend: het sleutelwoord is J/K - D/O - U/T - D. Als het sleutelwoord een bestaand woord is, dan is er maar één mogelijkheid over, namelijk KOUD. Laten we daarom proberen te ontcijferen met als sleutelwoord KOUD.

Laten we beginnen met het blok NSYHB. De N is ontstaan uit een vercijfering met sleutel K, dus afkomstig van een D. De S is ontstaan uit een vercijfering met sleutel O, dus afkomstig van een E. De Y is ontstaan uit een vercijfering met sleutel U, dus afkomstig van een E. Zo kun je doorgaan. Je vindt dan de tekst: DEEER STEDE URDIE JETEG ENKOM TISDI EVAND ESCHU URDET WEEDE ISVAN HETHU ISDXR, dus de boodschap luidt 'De eerste deur die je tegenkomt is die van de schuur, de tweede is van het huis.'

33 Allereerst verschuiven we de gehele tekst over 1, over 2, over 3, enzovoort, tot en met 72 plaatsen en we tellen de overeenkomsten. De aantallen overeenkomsten zijn het grootst bij verschuivingen over 12 plaatsen (15 overeenkomsten), 24 plaatsen (17 overeenkomsten), 36 plaatsen (16 overeenkomsten), 60 plaatsen (17 overeenkomsten) en 72 plaatsen (17 overeenkomsten). Alle andere verschuivingen leveren nooit meer dan 13 overeenkomsten. Het lijkt er dus op dat het sleutelwoord 12 letters lang zou kunnen zijn.

Als we de afstanden tussen dezelfde letterparen bekijken, dan krijgen we 59 afstanden waarvan er 24 deelbaar zijn door 12. We mogen er dus redelijkerwijs van uitgaan dat het sleutelwoord 12 letters heeft.

Als we de tekst nu opdelen in blokken van 12 en vervolgens alle eerste letters, alle tweede letters, enzovoort, bekijken en we gaan er van uit dat de meest voorkomende letter telkens een vercijferde E voorstelt, dan vinden we voor de diverse letters van het sleutelwoord de volgende mogelijkheden: S - X/G/T - A/R - I - P - C - E - R - Q - A - A/P - K/L (voor de tweede letter zijn er dus nog drie mogelijkheden, de X, G of T; voor de derde nog twee, de A of de R; enzovoort). Dit lijkt wel erg veel op het woord STRIPVERHAAL. Als we daarmee gaan ontcijferen, dan vinden we de volgende tekst: 'EENTR EINNE THA-

LE NISSI NDSDE NIEUW EDIEN STREG ELING VANDE NSMOE ILIJK GEWOR DENDE TREIN DEURE NGAAN VIJFT IENSE CONDE NEERD ERDIC HTDAN DEREI ZIGER GEWEN DWASD ENSHE EFTDE REGEL SVOOR VERTR EKAAN GESCH ERPTM AARHE EFTDE REIZI GERHI EROVE RNIET INGEL ICHTX', ofwel "EEN TREIN NET HALEN IS SINDS DE NIEUWE DIENSTREGELING VAN DE NS MOEILIJK GEWORDEN. DE TREINDEUREN GAAN VIJFTIEN SECONDEN EERDER DICHT DAN DE REIZIGER GEWEND WAS. DE NS HEEFT DE REGELS VOOR VERTREK AANGESCHERPT, MAAR HEEFT DE REIZIGER HIEROVER NIET INGELICHT."(de laatste letter was ter opvulling van een vijftal)

34 -

35

- Caesar

  vercijferen Elke letter van het alfabet wordt een vast aantal plaatsen doorgeschoven. Bijvoorbeeld de A gaat naar de D, de B naar de E, enzovoort. Bij dit voorbeeld is de sleutel D (altijd de letter waar de A naar toe wordt geschoven).

  ontcijferen Schuif alle letters van het alfabet 1 plaats op en kijk of er een zinnige tekst komt. Zo niet, schuif dan nog een keer 1 plaats door. Na eventueel nog een aantal keren herhalen kom je de boodschap tegen.

  veilig Dit systeem is absoluut het onveiligst van de drie hier genoemde systemen. Je hoeft alleen maar door te schuiven, na maximaal 25 keer schuiven heb je de boodschap ontcijferd.

- Enkelvoudige substitutie

  vercijferen Elke zelfde letter wordt door een andere, telkens dezelfde letter vervangen (bijvoorbeeld de A telkens door de K, de B telkens door de R, enzovoort).

  ontcijferen Tel het aantal keren dat elke letter voorkomt (we maken dus een frequentietabel: een tabel waarin voor elke letter het aantal keren dat hij voorkomt is te lezen). Omdat in Nederlandse teksten de E gemiddeld het vaakst voorkomt, zal naar alle waarschijnlijkheid de meest voorkomende letter in de cijfertekst de E moeten voorstellen. Na de E komen de D en mogelijk de A, T, R gemiddeld het vaakst voor. Dit betekent dat naar alle waarschijnlijkheid de letters, die in de cijfertekst als tweede, derde, vierde en vijfde het vaakst voorkomen, waarschijnlijk de D, A, T en R voorstellen (in een of andere volgorde). Deze proberen geeft meestal binnen enkele pogingen flarden herkenbare tekst. Dan weet je ook de nog niet bekende letters in die flarden, deze weer invullen, enzovoort, geeft tamelijk snel het resultaat.

  veilig Het zal duidelijk zijn dat dit systeem veiliger is dan het vorige, maar ook hier heb je al snel de ontcijfering te pakken.

- Vigenère

vercijferen Dit systeem maakt gebruik van een sleutelwoord, bijvoorbeeld ZESTIG. Vervolgens wordt de eerste letter van de klare tekst volgens het Caesarsysteem vercijferd met als sleutel de eerste letter van het sleutelwoord (hier dus de Z). De tweede letter wordt vercijferd met Caesarsysteem met als sleutel de tweede letter van het sleutelwoord (in het voorbeeld dus sleutel E), enzovoort. Als elke letter van het sleutelwoord aan de beurt is geweest, dan beginnen we weer met de eerste letter van het sleutelwoord. (In het voorbeeld volgt dus na G als zesde sleutel weer de Z als sleutel.)

ontcijferen Verschuif de gehele tekst 1 plaats naar rechts. Tel hoevaak op een plaats dezelfde letter als voor de verschuiving staat (de zogenaamde 1-letter frequentie) en hoevaak op twee plaatsen naast elkaar hetzelfde letterpaar staat (de 2-letter frequentie). Verschuif nu weer 1 naar rechts, totaal heb je de tekst dus 2 plaatsen verschoven. Tel weer de 1- en 2-letterfrequenties, vergeleken met de oorspronkelijke tekst (de tekst voordat je begonnen bent met het verschuiven). Dit doe je telkens weer. Je krijgt dan een lijst met frequenties bij in totaal 1 keer verschuiven, in totaal 2 keer verschuiven, enzovoort. De aantallen verschuivingen waarbij de frequenties het grootst zijn, zijn meestal deelbaar door de lengte van het sleutelwoord.

Als je de lengte van het sleutelwoord kent, deel dan de letters op in evenveel groepen als die lengte. Elke eerste letter in groep 1, elke tweede letter in groep 2, elke derde letter in groep 3, enzovoort. Je kunt dan per groep letterfrequentie toepassen. De meest voorkomende letter in een groep stelt dan waarschijnlijk de E voor. Je weet dan de bijbehorende Caesarverschuiving, dus de sleutel van die verschuiving, en daarmee de bijbehorende letter van het sleutelwoord.

veilig Deze is waarschijnlijk het veiligst van de drie, maar zeker ook nog goed te ontcijferen. Je moet wel wat meer werk verrichten dan bij enkelvoudige substitutie (dus veiliger), maar goed tellen geeft je vrij veel informatie. Als je eenmaal het sleutelwoord hebt, dan is het een peuleschil (maar nog wel veel werk) om de cijfertekst te ontcijferen.

2 Getaltheorie

1 a. Ieder krijgt 25 euro.

b. Er blijft 2 euro over.

2 a. $41 : 7 = 5$ *rest* 6

b. $73 : 11 = 6$ *rest* 7

c. $219 : 17 = 12$ *rest* 15

3 a. 14/17265\1233 dus $17265 : 14 = 1233$ *rest* 3

```
14
 32
 28
  46
  42
   45
   42
    3
```

b. 11/213736\19430 dus $213736 : 11 = 19430$ *rest* 6

```
11
103
 99
  47
  44
   33
   33
    06
     0
     6
```

c. 321/123456\384 dus $123456 : 321 = 384$ *rest* 192

```
 963
 2715
 2568
  1476
  1284
   192
```

4 $2|9$ is niet waar, want $\frac{9}{2} = 4\frac{1}{2}$ is geen geheel getal.

$8|24$ is waar, want $24 = 3 \cdot 8$.

$17|17$ is waar, want $17 = 1 \cdot 17$.

$3|7$ is niet waar, want $\frac{7}{3} = 2\frac{1}{3}$ is geen geheel getal.

$4|0$ is waar, want $0 = 0 \cdot 4$.

$100|25$ is niet waar, want $\frac{25}{100} = \frac{1}{4}$ is geen geheel getal.

5 a. $24 = 1 \cdot 24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6$, dus de delers van 24 zijn 1, 2, 3, 4, 6, 8, 12 en 24.

b. $3 = 1 \cdot 3$, de delers van 3 zijn dus 1 en 3.

c. 3 heeft alleen 1 en zichzelf als deler, 24 heeft behalve 1 en zichzelf nog meer delers.

6 Een getal > 1 heeft in ieder geval 1 en zichzelf als delers, dus minimaal 2 delers.

7 De echte delers van 36 zijn 2, 3, 4, 6, 9, 12 en 18.

8 7, 17 en 19 hebben geen echte delers. $8 = 2 \cdot 4$, $9 = 3 \cdot 3$ en $18 = 2 \cdot 9$, dus 8, 9 en 18 hebben wel echte delers.

9 De priemgetallen onder de 15 zijn 2, 3, 5, 7, 11 en 13.

10

- Nadat 1 is doorgestreept, is 2 het kleinste getal dat nog niet is doorgestreept. We markeren **2** dus als een priemgetal. We strepen nu alle veelvouden van 2 door, dus 4, 6, 8, 10, enzovoort.
- Nu is 3 het kleinste nog niet doorgestreepte of gemarkeerde getal. We markeren **3** als priemgetal en strepen alle veelvouden van 3 door, dus 6, 9, 12, 15, enzovoort.
- Vervolgens is 5 het kleinste nog niet doorgestreepte of gemarkeerde getal. **5** wordt daarom gemarkeerd als priemgetal en alle veelvouden van 5 (dus 10, 15, 20, enzovoort, worden doorgestreept.
- Zo gaan we verder, we vinden dan de volgende priemgetallen: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

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

12 a. $49 + 21 = 70 = 7 \cdot 10$, dus 7 is ook een deler van $49 + 21$.

b. $49 - 21 = 28 = 7 \cdot 4$, dus 7 is ook een deler van $49 - 21$.

13 a. $20 + 44 = 64 = 4 \cdot 16$, dus 4 is ook een deler van $20 + 44$.

b. $20 - 44 = -24 = 4 \cdot -6$, dus 4 is ook een deler van $20 - 44$.

14 a. $d|a$ en $d|b$, dus er zijn m en n zodanig dat $a = m \cdot d$ en $b = n \cdot d$.

b. $b + a = n \cdot d + m \cdot d$ en $b - a = n \cdot d - m \cdot d$.

c. $b + a = n \cdot d + m \cdot d = (n + m) \cdot d$ en $b - a = n \cdot d - m \cdot d = (n - m) \cdot d$.

15 a. Omdat $d_1|a$ en $d_1|b$ volgt uit de vorige opgave dat $d_1|(b - a)$.

b. d_1 is een gemeenschappelijke deler van a en $b - a$. Maar d_2 is de grootste gemeenschappelijke deler van a en $b - a$, dus $d_1 \leq d_2$.

c. $d_2 = \text{ggd}(a,b-a)$, dus $d_2|a$ en $d_2|b-a$. Maar dan ook $d_2|b$ (zie de vorige opgave, bedenk dat $a + (b - a) = b$) en d_2 is dus een gemeenschappelijke deler van a en b.

Aangezien $d_1 = \text{ggd}(a,b)$ moet $d_2 \leq d_1$.

d. Uit a. en b. volgt dat $d_1 = d_2$, ofwel $\text{ggd}(a,b)=\text{ggd}(a,b - a)$.

16 ggd(20,28)=ggd(20,8)=ggd(12,8)=ggd(4,8)=ggd(4,4)=4.

17 ggd(177,15)=ggd(162,15)=ggd(147,15)=ggd(132,15)=ggd(117,15)=ggd(102,15)=ggd(87,15) =ggd(72,15)=ggd(57,15)=ggd(42,15)=ggd(27,15)=ggd(12,15)=ggd(12,3) =ggd(9,3)=ggd(6,3) =ggd(3,3)=3.

18 $5148 - 12 \cdot 420 = 108$
$420 - 3 \cdot 108 = 96$
$108 - 1 \cdot 96 = 12$
$96 - 8 \cdot 12 = 0$.

Terugrekenend krijgen we:
$12 = 108 - 1 \cdot 96$
$= 108 - 1 \cdot (420 - 3 \cdot 108)$
$= 4 \cdot 108 - 1 \cdot 420$
$= 4 \cdot (5148 - 12 \cdot 420) - 1 \cdot 420$
$= 4 \cdot 5148 - 49 \cdot 420$
dus $\text{ggd}(5148,420) = 12 = 4 \cdot 5148 - 49 \cdot 420$.

19 $4284 - 4 \cdot 924 = 588$
$924 - 1 \cdot 588 = 336$
$588 - 1 \cdot 336 = 252$
$336 - 1 \cdot 252 = 84$
$252 - 3 \cdot 84 = 0$.

Terugrekenend krijgen we:

$$\begin{aligned}84 &= 336 - 1 \cdot 252\\ &= 336 - 1 \cdot (588 - 1 \cdot 336)\\ &= 2 \cdot 336 - 1 \cdot 588\\ &= 2 \cdot (924 - 1 \cdot 588) - 1 \cdot 588\\ &= 2 \cdot 924 - 3 \cdot 588\\ &= 2 \cdot 924 - 3 \cdot (4284 - 4 \cdot 924)\\ &= 14 \cdot 924 - 3 \cdot 4284\end{aligned}$$

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

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

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

22 a. Het priemgetal p heeft maar twee delers, namelijk 1 en p. Daarom is ggd(p,a) gelijk aan 1 of p. Maar p is geen deler van a, dus geen gemeenschappelijke deler van p en a. Derhalve is ggd(p,a)=1.

b. ggd(p,a)=1, zodat $1 = ak + pl$ voor zekere gehele getallen k en l.

c. $p|ab$ (gegeven), dus $p|abk$. Maar ook $p|bpl$, dus p deelt ook de som van deze twee, ofwel b. Uit a., b. en c. volgt dat als p geen deler van a is, dan is p een deler van b. Dus $p|a$ of $p|b$.

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

24 De getallen 12, 18 en 45 kun je niet ook nog op een andere manier schrijven als een product van priemgetallen: 12 kun je alleen delen door de priemgetallen 2 en 3, 18 alleen door de priemgetallen 2 en 3 en 45 alleen door de priemgetallen 3 en 5.

25 Als een getal $n > 1$ geen priemgetal is, dan heeft het een echte deler. Neem de kleinste echte deler p van n, dit moet een priemgetal zijn: een echte deler d van deze kleinste echte deler p is zelf ook weer een deler van n en kleiner dan p, hetgeen uiteraard niet kan. Dus $n = p \cdot k$ voor een priemgetal p en een zeker getal k. Bovendien is $k < n$. Herhaal dit verhaal nu voor k: k is of een priemgetal (en dan is n het product van twee priemgetallen) of het product van een priemgetal en een nog kleiner getal (en n is het product van twee priemgetallen en dat kleinere getal). Zo kunnen we doorgaan en omdat de getallen steeds kleiner worden, stopt het een keer. Je hebt dan n geschreven als een product van priemgetallen.

26 a. Het priemgetal q_1 deelt een product, dus moet het één van de factoren delen. Met andere woorden, q_1 deelt één van de priemgetallen $p_1, \ldots, p_n$. Maar een priemgetal heeft alleen 1 en zichzelf als delers, dus moet q_1 één van de priemgetallen $p_1, \ldots, p_n$ zijn.

b. Deel links en rechts zoveel mogelijk factoren $p_i = q_1$ weg. Als $l_1 > k_i$, dan houden we rechts nog een factor q_1 over, die dan gelijk moet zijn aan één van de priemfactoren links. Omdat daar geen p_i meer over is, moet q_1 ook nog gelijk zijn aan een ander priemgetal, hetgeen natuurlijk onmogelijk is. Hetzelfde verhaal als $l_1 < k_i$, dan houden we links nog een factor p_i over, die dan gelijk moet zijn aan één van de andere priemfactoren rechts, hetgeen uiteraard ook niet kan. Dus $l_1 = k_i$.

c. Als we a. en b. uitvoeren voor alle priemfactoren $q_1, \ldots, q_m$, en vervolgens al deze factoren wegdelen, dan krijgen rechts een 1. Links moeten we dan ook 1 krijgen: dus beide priemfactorontbindingen zijn dezelfde.

27 a. $40 = 2^3 \cdot 5 = 2^3 \cdot 5^1$, $28 = 2^2 \cdot 7 = 2^2 \cdot 7^1$ en ggd(40,28)$= 4 = 2^2$. De priemfactor 2 is de enige gemeenschappelijke priemfactor van 28 en 40. De exponent 2 van 2 in de priemfactorontbinding van de ggd is de kleinste exponent van 2 in de priemfactorontbindingen van 28 en 40.

b. $60 = 2^2 \cdot 3 \cdot 5 = 2^2 \cdot 3^1 \cdot 5^1$, $192 = 2^6 \cdot 3 = 2^6 \cdot 3^1$ en ggd(60,192)$= 12 = 2^2 \cdot 3 = 2^2 \cdot 3^1$. De priemfactoren 2 en 3 zijn de enige gemeenschappelijke priemfactoren in alle priemfactorontbindingen. Ook hier zijn de exponenten van 2 en 3 in de priemfactorontbinding van de ggd de kleinste van de exponenten van 2 en 3 in de priemfactorontbindingen van 60 en 192.

28 $13475 = 5^2 \cdot 7^2 \cdot 11$, $936 = 2^3 \cdot 3^2 \cdot 13$ en ggd(13475,936)$= 1$. De getallen 13475 en 936 hebben geen gemeenschappelijke priemfactor.

29 $610 = 2 \cdot 5 \cdot 61$, $987 = 3 \cdot 7 \cdot 47$, dus ggd(610,987)=1.

30 $2382 = 2 \cdot 3 \cdot 397$, $237 = 3 \cdot 79$, dus ggd(2382,237)=3.

31 Als a en b geen priemgetal gemeenschappelijk hebben in hun priemfactorontbinding, dan moet ggd(a,b)=1. Als er immers een getal $d > 1$ is dat beiden deelt, dan zal een priemgetal in de priemfactorontbinding van d ook een deler zijn van a en van b, dus voorkomen in beide priemfactorontbindingen.

Als d een deler van a is, dan is de priemfactorontbinding van d een deel van die van a (immers de priemfactorontbinding van a is eenduidig, dus moet vanwege $a = d \cdot k$ de priemfactorontbinding van d wel in die van a passen). Als d een deler is van a en van b, dan moet de priemfactorontbinding van d een deel zijn van de priemfactorontbindingen van a en van b, dus een gemeenschappelijk deel van beide priemfactorontbindingen. Dus de priemfactorontbinding van ggd(a,b) is een deel van beide priemfactorontbindingen. Omdat de ggd de grootste gemeenschappelijke deler is, moet het ook het grootste gemeenschappelijke deel van beide priemfactorontbindingen hebben, dus alles wat gemeenschappelijk is.

32 a. $2^3 \cdot 3^3 = 3 \cdot (2^3 \cdot 3^2)$, ofwel $216 = 3 \cdot 72$.

b. $2^3 \cdot 3^3 = 2 \cdot (2^2 \cdot 3^3)$, ofwel $216 = 2 \cdot 108$.

c. De veelvouden van 72 zijn 72, 144, 216, enzovoort; de veelvouden van 108 zijn 108, 216, enzovoort. Er is dus geen kleiner gemeenschappelijk veelvoud.

33 Als het priemgetal p a keer voorkomt in de priemfactorontbinding van n, dan komt p ook minimaal a keer voor in elk veelvoud van n. Als p b keer voorkomt in de priemfactorontbinding van m, dan komt p ook minimaal b keer voor in elk veelvoud van m. Het kleinste gemene veelvoud van m en n bevat dus op zijn minst a, maar ook b, priemfactoren p, dus minimaal het grootste van de twee. Maar omdat het het kleinste gemene veelvoud van m en n moet zijn, bevat het ook niet meer priemfactoren p.

34 $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, $5148 = 2^2 \cdot 3^2 \cdot 11 \cdot 13$, dus kgv(420,5148)$= 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 180180$.
$924 = 2^2 \cdot 3 \cdot 7 \cdot 11$, $4284 = 2^2 \cdot 3^2 \cdot 7 \cdot 17$, dus kgv(924,4284)$= 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 17 = 47124$.
$30 = 2 \cdot 3 \cdot 5$, $192 = 2^6 \cdot 3$, dus kgv(30,192)$=2^6 \cdot 3 \cdot 5 = 960$.

35 a. $a \cdot b = 420 \cdot 5148 = 2162160$, ggd($a$,$b$)$\cdot$kgv($a$,$b$)$= 12 \cdot 180180 = 2162160$.

b. $a \cdot b = 924 \cdot 4284 = 3958416$, ggd($a$,$b$)$\cdot$kgv($a$,$b$)$= 84 \cdot 47124 = 3958416$.

c. $a \cdot b = 30 \cdot 192 = 5760$, ggd($a$,$b$)$\cdot$kgv($a$,$b$)$= 6 \cdot 960 = 5760$.

d. Telkens is $a \cdot b = \text{ggd}(a,b) \cdot \text{kgv}(a,b)$. Dit is logisch als je gebruik maakt van de stelling inzake priemfactorontbindingen. Als $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, $b = p_1^{l_1} p_2^{l_2} \dots p_n^{l_n}$, dan volgt $\text{ggd}(a,b) = p_1^{\min\{k_1,l_1\}} p_2^{\min\{k_2,l_2\}} \dots p_n^{\min\{k_n,l_n\}}$ en $\text{kgv}(a,b) = p_1^{\max\{k_1,l_1\}} p_2^{\max\{k_2,l_2\}} \dots p_n^{\max\{k_n,l_n\}}$. Nu is $a \cdot b = p_1^{k_1+l_1} p_2^{k_2+l_2} \dots p_n^{k_n+l_n}$ en voor het product van ggd en kgv vinden we dan $\text{ggd}(a,b) \cdot \text{kgv}(a,b) = p_1^{\min\{k_1,l_1\}+\max\{k_1,l_1\}} p_2^{\min\{k_2,l_2\}+\max\{k_2,l_2\}} \dots p_n^{\min\{k_n,l_n\}+\max\{k_n,l_n\}}$. Maar voor elk tweetal getallen a en b geldt dat $\min\{a,b\} + \max\{a,b\} = a + b$, zodat inderdaad $a \cdot b = \text{ggd}(a,b) \cdot \text{kgv}(a,b)$

36 Vanwege ggd(k,n)=1 volgt dat er gehele (positief of negatief) getallen a en b zijn met $1 = a \cdot k + b \cdot n$. Evenzo moet gelden dat er gehele (positief of negatief) getallen c en d zijn met $1 = c \cdot m + d \cdot n$. Maar dan is ook $1 = 1 \cdot 1 = (ak + bn)(cm + dn) = akcm + akdn + bncm + bndn = (ac)(km) + (akd + bcm + bnd)n$. Nu deelt ggd$(km,n)$ zowel km als n, dus deelt het ook $(ac)(km) + (akd + bcm + bnd)n = 1$ en moet dus wel 1 zijn.

37 Omdat ggd(m,n)=1, komen er geen gemeenschappelijke priemfactoren voor in de priemfactorontbindingen van m en n (als er wel een gemeenschappelijke priemfactor zou zijn, dan zou deze ook de ggd van m en n moeten delen). Aangezien $m|a$, is de priemfactorontbinding van m een deel van de priemfactorontbinding vam a (a is immers een veelvoud van m). Hetzelfde geldt voor de priemfactorontbinding van n. In de priemfactorontbinding van a komen dus zowel die van m als die van n voor. Deze laatste twee zijn echter volledig verschillend, dus komen ze naast elkaar voor. Maar samen zijn ze precies de priemfactorontbinding van $m \cdot n$, dus moet $a = mn \cdot b$ voor een zeker getal b, anders gezegd $mn|a$.

38 a. $264 = 2^3 \cdot 3 \cdot 11$, $432 = 2^4 \cdot 3^3$, $\text{kgv}(264, 432) = 2^4 \cdot 3^3 \cdot 11 = 4752$,
dus $\frac{5}{264} + \frac{7}{432} = \frac{90}{4752} + \frac{77}{4752} = \frac{167}{4752}$

b. $605 = 5 \cdot 11^2$, $77 = 7 \cdot 11$, $\text{kgv}(605, 77) = 5 \cdot 7 \cdot 11^2 = 4235$,
dus $\frac{3}{605} + \frac{6}{77} = \frac{21}{4235} + \frac{330}{4235} = \frac{351}{4235}$

c. $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, $910 = 2 \cdot 5 \cdot 7 \cdot 13$, $\text{kgv}(1155, 910) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$,
dus $\frac{13}{1155} + \frac{11}{910} = \frac{338}{30030} + \frac{363}{30030} = \frac{701}{30030}$

39 Neem een interval met als lengte een gemeenschappelijk veelvoud van beide perioden. Dan hebben beide functies dezelfde functiewaarde aan het begin en aan het eind van het interval, dus de som ook. De periode is de lengte van het kleinste interval waarvoor dit geldt en moet dus de kgv zijn.

40 De ggd van de coëfficiënten van x, dus ggd(8,12), is gelijk aan 4. De periode is $\frac{2\pi}{4}$. Je zou de kgv kunnen gebruiken als beide perioden een geheel getal of een geheel aantal keren π zijn. Als beide coëfficiënten van x gehele getallen zijn, dan zou je de ggd kunnen gebruiken.

41 a. ggd(16,40)=8, dus de periode van f is $\frac{2\pi}{8} = \frac{1}{4}\pi$.

b. De periode van $\cos\frac{1}{8}x$ is $\frac{2\pi}{\frac{1}{8}} = 16\pi$, de periode van $\cos\frac{1}{10}x$ is $\frac{2\pi}{\frac{1}{10}} = 20\pi$. kgv(16,20)=80, dus de periode van g is 80π.

c. ggd(22,28)=2, dus de periode van h is $\frac{2\pi}{2} = \pi$.

d. De periode van $\cos\frac{2}{90}x$ is $\frac{2\pi}{\frac{2}{90}} = 90\pi$, de periode van $\sin\frac{1}{30}x$ is $\frac{2\pi}{\frac{1}{30}} = 60\pi$. kgv(90,60)=180, dus de periode van j is 180π.

43 Doortellen levert dat het over 8 uur 3 uur is. Terugtellen levert dat het 10 uur geleden 9 uur was.

44 a. $7 + 9 = 16 \equiv 4 \pmod{12}$

b. $3 - 11 = -8 \equiv 4 \pmod{12}$

c. $6 + 6 = 12 \equiv 0 \pmod{12}$

d. $3 \cdot 7 = 21 \equiv 9 \pmod{12}$

e. $5 \cdot 5 = 25 \equiv 1 \pmod{12}$

f. $5^2 = 25 \equiv 1 \pmod{12}$

g. $6^3 = 216 \equiv 0 \pmod{12}$

h. $5^5 = 3125 \equiv 5 \pmod{12}$

45 Je berekent $5^3 = 125$ en trekt vervolgens van het antwoord zo vaak mogelijk 15 af. Dit geeft $125 - 8 \cdot 15 = 5$, dus $5^3 \equiv 125 \equiv 5 \pmod{15}$

46 $125 : 15 = 8$ *rest* 5 betekent $125 = 8 \cdot 15 + 5$, ofwel $125 - 5 = 8 \cdot 15$: het verschil van 125 en de rest 5 is deelbaar door 15.

47 $a \equiv b \pmod{k}$ betekent dat $a - b$ deelbaar is door k, of, anders gezegd, dat $a = b + nk$ voor een zeker geheel getal n.

48 a. $94 \equiv 1 \pmod 3$

b. $94 \equiv 4 \pmod 5$

c. $94 \equiv 3 \pmod 7$

d. $17 + 39 = 56 \equiv 8 \pmod{24}$

e. $3 - 41 = -38 \equiv 22 \pmod{30}$

f. $26 + 26 = 52 \equiv 15 \pmod{37}$

g. $3 \cdot 7 = 21 \equiv 7 \pmod{14}$

h. $5 \cdot 19 = 95 \equiv 15 \pmod{40}$

i. $3^2 = 9 \equiv 2 \pmod 7$

j. $3^4 = 81 \equiv 4 \pmod 7$

k. $2^2 \equiv 4 \pmod 7$

49 a. $3^4 = (3^2)^2 = (2 + 7k)^2 = 2^2 + 2 \cdot 2 \cdot 7k + (7k)^2 = 2^2 + 4 \cdot 7k + 49k^2 = 2^2 + 7(4k + 7k^2)$, dus$3^4 \equiv 2^2 \pmod 7$.

b. $17 = 7 + 1 \cdot 10$, $15 = 5 + 1 \cdot 10$, dus $17 \cdot 15 = (7 + 1 \cdot 10)(5 + 1 \cdot 10) =$
$7 \cdot 5 + 7 \cdot 1 \cdot 10 + 5 \cdot 1 \cdot 10 + 1 \cdot 10 \cdot 1 \cdot 10 = 7 \cdot 5 + 10(7 + 5 + 10)$, dus $17 \cdot 15 \equiv 7 \cdot 5 \pmod{10}$.

c. Als $a \equiv c \pmod k$ en $b \equiv d \pmod k$, dan is $a = c + km$ en $b = d + kn$. Vermenigvuldigen geeft dan $ab = (c + km)(d + kn) = cd + ckn + dkm + k^2mn = cd + k(cn + dm + kmn)$, dus $ab \equiv cd \pmod k$.

50 a. $23^2 = 529 \equiv 132 \pmod{397}$, $23^4 \equiv 132^2 \equiv 17424 \equiv 353 \pmod{397}$

b. $23^8 \equiv 353^2 \equiv 124609 \equiv 348 \pmod{397}$

c. $23^{16} \equiv 348^2 \equiv 121104 \equiv 19 \pmod{397}$

d. $23^{32} \equiv 19^2 \equiv 361 \pmod{397}$

51 a. $23^{48} = 23^{32} \cdot 23^{16} \equiv 361 \cdot 19 \equiv 6859 \equiv 110 \pmod{397}$

b. $23^{56} = 23^{48} \cdot 23^8 \equiv 110 \cdot 348 \equiv 38280 \equiv 168 \pmod{397}$

c. $23^{57} = 23^{56} \cdot 23^1 \equiv 168 \cdot 23 \equiv 3864 \equiv 291 \pmod{397}$

52 a. $97^2 = 9409 \equiv 256 \pmod{1017}$

$97^4 \equiv 256^2 \equiv 65536 \equiv 448 \pmod{1017}$

$97^8 \equiv 448^2 \equiv 200704 \equiv 355 \pmod{1017}$

$97^{16} \equiv 355^2 \equiv 126025 \equiv 934 \pmod{1017}$

$97^{32} \equiv 934^2 \equiv 872356 \equiv 787 \pmod{1017}$

$97^{64} \equiv 787^2 \equiv 619369 \equiv 16 \pmod{1017}$

dus $97^{97} = 97^{64} \cdot 97^{32} \cdot 97^1 \equiv 16 \cdot 787 \cdot 97 \equiv 388 \cdot 97 \equiv 7 \pmod{1017}$

b. $891^2 = 793881 \equiv 256 \pmod{907}$

$891^4 \equiv 256^2 \equiv 65536 \equiv 232 \pmod{907}$

$891^8 \equiv 232^2 \equiv 53824 \equiv 311 \pmod{907}$

$891^{16} \equiv 311^2 \equiv 96721 \equiv 579 \pmod{907}$

$891^{32} \equiv 579^2 \equiv 335241 \equiv 558 \pmod{907}$

$891^{64} \equiv 558^2 \equiv 311364 \equiv 263 \pmod{907}$

$891^{128} \equiv 263^2 \equiv 69169 \equiv 237 \pmod{907}$

dus $891^{133} = 891^{128} \cdot 891^4 \cdot 891^1 \equiv 237 \cdot 232 \cdot 891 \equiv 564 \cdot 891 \equiv 46 \pmod{907}$

c. $17^2 = 289 \equiv 72 \pmod{217}$

$17^4 \equiv 72^2 \equiv 5184 \equiv 193 \pmod{217}$

$17^8 \equiv 193^2 \equiv 37249 \equiv 142 \pmod{217}$

$17^{16} \equiv 142^2 \equiv 20164 \equiv 200 \pmod{217}$

$17^{32} \equiv 200^2 \equiv 40000 \equiv 72 \pmod{217}$

$17^{64} \equiv 72^2 \equiv 5184 \equiv 193 \pmod{217}$

dus $17^{117} = 17^{64} \cdot 17^{32} \cdot 17^{16} \cdot 17^4 \cdot 17^1 \equiv 193 \cdot 72 \cdot 200 \cdot 193 \cdot 17 \equiv 8 \cdot 200 \cdot 193 \cdot 17$

$\equiv 81 \cdot 193 \cdot 17 \equiv 9 \cdot 17 \equiv 153 \pmod{217}$

53 a. Probeer $x = 0$: $5 \cdot 0 = 0 \not\equiv 3 \pmod{7}$.

Probeer $x = 1$: $5 \cdot 1 = 5 \not\equiv 3 \pmod{7}$.

Probeer $x = 2$: $5 \cdot 2 = 10 \equiv 3 \pmod{7}$.

Dus $x = 2$ voldoet.

b. Probeer $x = 0$: $7 \cdot 0 + 5 = 5$, $2 \cdot 0 - 1 = -1$ en $5 \not\equiv -1 \pmod 9$
Probeer $x = 1$: $7 \cdot 1 + 5 = 12$, $2 \cdot 1 - 1 = 1$ en $12 \not\equiv 1 \pmod 9$
Probeer $x = 2$: $7 \cdot 2 + 5 = 19$, $2 \cdot 2 - 1 = 3$ en $19 \not\equiv 3 \pmod 9$
Probeer $x = 3$: $7 \cdot 3 + 5 = 26$, $2 \cdot 3 - 1 = 5$ en $26 \not\equiv 5 \pmod 9$
Probeer $x = 4$: $7 \cdot 4 + 5 = 33$, $2 \cdot 4 - 1 = 7$ en $33 \not\equiv 7 \pmod 9$
Probeer $x = 5$: $7 \cdot 5 + 5 = 40$, $2 \cdot 5 - 1 = 9$ en $40 \not\equiv 9 \pmod 9$
Probeer $x = 6$: $7 \cdot 6 + 5 = 47$, $2 \cdot 6 - 1 = 11$ en $47 \equiv 11 \pmod 9$
Dus $x = 6$ voldoet.

c. Probeer $x = 0$: $0^5 = 0 \not\equiv 10 \pmod{11}$
Probeer $x = 1$: $1^5 = 1 \not\equiv 10 \pmod{11}$
Probeer $x = 2$: $2^5 = 32 \equiv 10 \pmod{11}$
Dus $x = 2$ voldoet.

d. Probeer $x = 0$: $5^0 = 1 \not\equiv 4 \pmod{11}$
Probeer $x = 1$: $5^1 = 5 \not\equiv 4 \pmod{11}$
Probeer $x = 2$: $5^2 = 25 \not\equiv 4 \pmod{11}$
Probeer $x = 3$: $5^3 = 125 \equiv 4 \pmod{11}$
Dus $x = 3$ voldoet.

54 Probeer $x = 0$: $0 \not\equiv 1 \pmod 2$.
Probeer $x = 1$: $1 \not\equiv 2 \pmod 5$.
Probeer $x = 2$: $2 \not\equiv 1 \pmod 2$.
Probeer $x = 3$: $3 \not\equiv 1 \pmod 3$.
Probeer $x = 4$: $4 \not\equiv 1 \pmod 2$.
Probeer $x = 5$: $5 \not\equiv 1 \pmod 3$.
Probeer $x = 6$: $6 \not\equiv 1 \pmod 2$.
Probeer $x = 7$: $7 \equiv 1 \pmod 2$, $7 \equiv 1 \pmod 3$ en $7 \equiv 2 \pmod 5$.
Dus $x = 7$ voldoet.

55 a. $10x \equiv 25 \pmod{35}$ betekent $10x = 25 + 35k$ voor een zeker getal k. Delen door 5 geeft nu $2x = 5 + 7k$, zodat $2x \equiv 5 \pmod 7$.

b. $10x \equiv 24 \pmod{35}$ betekent $10x = 24+35k$ voor een zeker getal k. Omdat ggd(24,35)=1 kun je nu niet door een getal > 1 delen en een vergelijking met gehele getallen overhouden.

56 a. Laat g =ggd(a,k), dan is $a = cg$ en $k = mg$. Stel ggd(c,m)= $n > 1$, dan geldt $n|c$, dus $ng|cg = a$. Evenzo geldt $ng|mg = k$. Met andere woorden ng is een gemeenschappelijke deler van a en k, dus $ng \leq g$ =ggd(a,k). Maar $ng > g$ (immers $n > 1$). Tegenspraak, dus moet ggd(c,m)= 1. Maar dan zijn er getallen d en e zodanig dat $cd + em = 1$, ofwel $cd = 1 - em$. Dus is er een veelvoud van c (namelijk cd) dat gelijk is aan 1 (mod m).

b. $ax \equiv b \pmod{k}$ betekent $ax = b + km$ voor een zeker getal m. Als g =ggd(a,k), dan $g|a$ en $g|k$. Maar dan ook $g|ax$, $g|km$ en $g|(ax - km)$, dus $g|b$. Als de vergelijking een oplossing heeft, dan moet derhalve b een veelvoud van de ggd van a en k zijn. Is b geen veelvoud van de ggd van a en k, dan heeft de vergelijking dus geen oplossing.

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

Vermenigvuldigen met 3 (want $5 \cdot 3 = 15 \equiv 1 (\text{mod } 7)$) geeft: $x \equiv 9 \equiv 2 \pmod{7}$.

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

$5x \equiv -6 \pmod{9}$

Vermenigvuldigen met 2 (want $5 \cdot 2 = 10 \equiv 1 (\text{mod } 9)$) geeft: $x \equiv -12 \equiv 6 \pmod{9}$.

58 a. Voor elke i met $1 \leq i \leq k$ geldt $x_1 + x_2 + \ldots + x_k \equiv a_i \pmod{m_i}$, immers alle $x_1, x_2, \ldots, x_k$ zijn equivalent met 0 modulo m_i, behalve x_i, waarvoor geldt $x_i \equiv a_i \pmod{m_i}$. Neem dus $x = x_1 + x_2 + \ldots + x_k$.

b. $x_1 \equiv 0 \pmod{m_2}$ betekent dat m_2 een deler is van x_1. Evenzo is m_3 een deler van x_1. Maar dan is $m_2 \cdot m_3$ ook een deler van x_1 volgens een eerdere opgave. Vanwege ggd(m_2, m_4)=1 en ggd(m_3, m_4)=1 is ook ggd($m_2 \cdot m_3, m_4$)=1 (ook volgens een eerdere opgave). Daarmee weten we op dezelfde manier als hiervoor dat nu ook $m_2 \cdot m_3 \cdot m_4$ een deler van x_1. Zo doorredenerend krijgen we dat $m_2 \cdot m_3 \cdot \ldots \cdot m_k = \frac{m}{m_1}$ een deler van x_1 is.

c. Nee, dat hoeft niet. m en m_1 zeggen niets over a_1. a_1 kan in principe elk getal van 0 tot m_1 voorstellen. Het zou dan ook erg toevallig zijn als het waar zou zijn. Door bijvoorbeeld $a_1 = 4, a_2 = 2, m_1 = 7, m_2 = 5$ te nemen, zie je dat het ook niet klopt. De bewering $\frac{m}{m_1} \equiv a_1 \pmod{m_1}$ wordt dan de onjuiste bewering $5 \equiv 4 \pmod{7}$.

d. Als in vraag b. kun je beredeneren dat ggd($\frac{m}{m_1}, m_1$)=1. Maar dan moeten er gehele getallen r en s bestaan zodat $r \cdot \frac{m}{m_1} + s \cdot m_1 = 1$, ofwel $r \cdot \frac{m}{m_1} = 1 - s \cdot m_1 \equiv 1 \pmod{m_1}$. Je kunt dus $b_1 = r$ nemen.

e. $x_1 = a_1 \cdot b_1 \cdot \frac{m}{m_1} \equiv a_1 \cdot 1 = a_1 \pmod{m_1}$. Voor alle $i \neq 1$ geldt $x_1 = a_1 \cdot b_1 \cdot \frac{m}{m_1} \equiv a_1 \cdot b_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_k \equiv a_1 \cdot b_1 \cdot 0 = 0 \pmod{m_i}$. Deze x_1 voldoet aan alle eisen in a. aan x_1 gesteld.

f. Op dezelfde manier als in b. tot en met e. kun je ook $x_2, x_3, \ldots, x_k$ vinden. Daarna kun je $x \equiv x_1 + x_2 + \ldots + x_k \pmod{m}$ nemen.

59 a. $m = 7 \cdot 11 \cdot 17 \cdot 19 = 24871$

$\frac{m}{m_1} = \frac{24871}{7} = 3553$, $\frac{m}{m_2} = \frac{24871}{11} = 2261$, $\frac{m}{m_3} = \frac{24871}{17} = 1463$ en $\frac{m}{m_4} = \frac{24871}{19} = 1309$

$3553b_1 \equiv 1 \pmod{7}$ geeft $b_1 \equiv 2 \pmod{7}$

$2261b_2 \equiv 1 \pmod{11}$ geeft $b_2 \equiv 2 \pmod{11}$

$1463b_3 \equiv 1 \pmod{17}$ geeft $b_3 \equiv 1 \pmod{17}$

$1309b_4 \equiv 1 \pmod{19}$ geeft $b_4 \equiv 9 \pmod{19}$

$x = 3553 \cdot 2 \cdot 3 + 2261 \cdot 2 \cdot 2 + 1463 \cdot 1 \cdot 1 + 1309 \cdot 9 \cdot 4 = 78949 \equiv 4336 \pmod{24871}$

Alternatieve oplossing:

Uit $x \equiv 3 \pmod{7}$ volgt $x = 3 + 7y$ voor een zekere y

Invullen in $x \equiv 2 \pmod{11}$ geeft $3 + 7y \equiv 2 \pmod{11}$, ofwel

$7y \equiv -1 \pmod{11}$ en $y \equiv 56y = 8 \cdot 7y \equiv -8 \equiv 3 \pmod{11}$,

dus is er een z met $y = 3 + 11z$ en $x = 3 + 7y = 3 + 7(3 + 11z) = 24 + 77z$.

Substitutie hiervan in $x \equiv 1 \pmod{17}$ geeft $24 + 77z \equiv 1 \pmod{17}$, ofwel

$7 + 9z \equiv 1 \pmod{17}$, $9z \equiv -6 \pmod{17}$ en $z \equiv 18z = 2 \cdot 9z \equiv -12 \equiv 5 \pmod{17}$,

dus $z = 5 + 17k$ voor een zekere k en $x = 24 + 77z = 24 + 77(5 + 17k) = 409 + 1309k$.

Substitueren in $x \equiv 4 \pmod{19}$ geeft $409 + 1309k \equiv 4 \pmod{19}$, ofwel

$10 + 17k \equiv 4 \pmod{19}$, $17k \equiv -6 \pmod{19}$ en

$k \equiv 153k = 9 \cdot 17k \equiv -54 \equiv 3 \pmod{19}$.

We krijgen nu dat voor een zekere l moet gelden $k = 3 + 19l$ en

$x = 409 + 1309(3 + 19l) = 4336 + 24871l$, zodat ook nu volgt $x \equiv 4336 \pmod{24871}$

b. $m = 8 \cdot 15 \cdot 7 \cdot 11 = 9240$

$\frac{m}{m_1} = \frac{9240}{8} = 1155$, $\frac{m}{m_2} = \frac{9240}{15} = 616$, $\frac{m}{m_3} = \frac{9240}{7} = 1320$ en $\frac{m}{m_4} = \frac{9240}{11} = 840$

$1155b_1 \equiv 1 \pmod{8}$ geeft $b_1 \equiv 3 \pmod{8}$

$616b_2 \equiv 1 \pmod{15}$ geeft $b_2 \equiv 1 \pmod{15}$

$1320b_3 \equiv 1 \pmod 7$ geeft $b_3 \equiv 2 \pmod 7$

$840b_4 \equiv 1 \pmod{11}$ geeft $b_4 \equiv 3 \pmod{11}$

$x = 1155 \cdot 3 \cdot 2 + 616 \cdot 1 \cdot 3 + 1320 \cdot 2 \cdot 4 + 840 \cdot 3 \cdot 5 \equiv 31938 \equiv 4218 \pmod{9240}$

Alternatieve oplossing:

Uit $x \equiv 2 \pmod 8$ volgt $x = 2 + 8y$ voor een zekere y

Invullen in $x \equiv 3 \pmod{15}$ geeft $2 + 8y \equiv 3 \pmod{15}$, ofwel

$8y \equiv 1 \pmod{15}$ en $y \equiv 16y = 2 \cdot 8y \equiv 2 \pmod{15}$,

dus is er een z met $y = 2 + 15z$ en $x = 2 + 8y = 2 + 8(2 + 115z) = 18 + 120z$.

Substitutie hiervan in $x \equiv 4 \pmod 7$ geeft $18 + 120z \equiv 4 \pmod 7$, ofwel

$4 + z \equiv 4 \pmod 7$, $z \equiv 0 \pmod 7$ en

dus $z = 7k$ voor een zekere k en $x = 18 + 120z = 18 + 120 \cdot 7k = 18 + 840k$.

Substitueren in $x \equiv 5 \pmod{11}$ geeft $18 + 840k \equiv 5 \pmod{11}$, ofwel

$7 + 4k \equiv 5 \pmod{11}$, $4k \equiv -2 \pmod{11}$ en

$k \equiv 12k = 3 \cdot 4k \equiv -6 \equiv 5 \pmod{11}$.

We krijgen nu dat voor een zekere l moet gelden $k = 5 + 11l$ en

$x = 18 + 840(5 + 11l) = 4218 + 9240l$, zodat ook nu volgt $x \equiv 4218 \pmod{9240}$

60 Dit verhaal komt neer op het vinden van de kleinste oplossing van het stelsel

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

We lossen nu eerst dit stelsel op.

$m = 3 \cdot 7 \cdot 11 = 231$

$\frac{m}{m_1} = \frac{231}{3} = 77$, $\frac{m}{m_2} = \frac{231}{7} = 33$, $\frac{m}{m_3} = \frac{231}{11} = 21$

$77b_1 \equiv 1 \pmod 3$ geeft $b_1 \equiv 2 \pmod 3$

$33b_2 \equiv 1 \pmod 7$ geeft $b_2 \equiv 3 \pmod 7$

$21b_3 \equiv 1 \pmod{11}$ geeft $b_3 \equiv 10 \pmod{11}$

$x = 77 \cdot 2 \cdot 2 + 33 \cdot 3 \cdot 1 + 21 \cdot 10 \cdot 3 \equiv 1037 \equiv 113 \pmod{231}$

Dus zitten er minstens 113 toffees in de zak van grootvader.

Alternatieve oplossing voor het stelsel vergelijkingen:

Uit $x \equiv 2 \pmod 3$ volgt $x = 2 + 3y$ voor een zekere y

Invullen in $x \equiv 1 \pmod 7$ geeft $2 + 3y \equiv 1 \pmod 7$, ofwel

$3y \equiv -1 \pmod 7$ en $y \equiv 15y = 5 \cdot 3y \equiv -5 \equiv 2 \pmod 7$,

dus is er een z met $y = 2 + 7z$ en $x = 2 + 3y = 2 + 3(2 + 7z) = 8 + 21z$.

Substitutie hiervan in $x \equiv 3 \pmod{11}$ geeft $8 + 21z \equiv 3 \pmod{11}$, ofwel

$8 + 10z \equiv 3 \pmod{11}$, $10z \equiv -5 \pmod{11}$ en
$z \equiv 100z = 10 \cdot 10z \equiv -50 \equiv 5 \pmod{11}$,
dus $z = 5 + 11k$ voor een zekere k en $x = 8 + 21z = 8 + 21(5 + 11k) = 113 + 231k$.
We krijgen ook nu $x \equiv 113 \pmod{231}$ en concluderen wederom dat er minstens 113 toffees in de zak van grootvader zitten.

61 a. $x - y \equiv a_1 - a_1 = 0 \pmod{m_1}$.

b. ggd(m_1, m_2)= 1. Dus is $x-y$ deelbaar door $m_1 \cdot m_2$. Uit ggd(m_1, m_3)= 1 en ggd(m_2, m_3)= 1 volgt ggd$(m_1 \cdot m_2, m_3)$= 1. Maar dan moet ook $m_1 \cdot m_2 \cdot m_3$ een deler zijn van $x - y$. Zo kunnen we verder gaan tot $m|(x - y)$.

c. Het verschil van elk tweetal oplossingen van het stelsel is deelbaar door m, dus modulo m hetzelfde. Modulo m is er dus maximaal één oplossing. Hiervoor hadden we al gezien dat er minstens één is, dus is er precies één oplossing modulo m.

62 Vervang de letter a door 1, de letter b door 2, enzovoort, tot en met de z door 26 (of 0). Als je nu over een vast aantal plaatsen (zeg 5) gaat verschuiven, dan tel je overal 5 bij op. Alle antwoorden reken je uit modulo 26. Vervang je nu de antwoorden weer door de bijbehorende letters, dan heb je precies de Caesarverschuiving over 5 letters gemaakt. Zo gaat bijvoorbeeld de a (=1) naar de f (=6) en $1 + 5 = 6$, en de y (=25) naar de d (=4) en $25 + 5 = 30 \equiv 4 \pmod{26}$.

63 a. Als we $0, 1, 2, \ldots, 10$ met 15 vermenigvuldigen, dan krijgen we $0, 15, 30, \ldots, 150$. Als we deze getallen modulo 11 nemen dan krijgen we $0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7$.

b. Als we $0, 1, 2, \ldots, 6$ met 10 vermenigvuldigen, dan krijgen we $0, 10, 20, \ldots, 60$. Als we deze getallen modulo 7 nemen dan krijgen we $0, 3, 6, 2, 5, 1, 4$.

c. Als we $0, 1, 2, \ldots, 11$ met 15 vermenigvuldigen, dan krijgen we $0, 15, 30, \ldots, 165$. Als we deze getallen modulo 12 nemen dan krijgen we $0, 3, 6, 9, 0, 3, 6, 9, 0, 3, 6, 9$.

d. Als we $0, 1, 2, 3, 4$ met 10 vermenigvuldigen, dan krijgen we $0, 10, 20, 30, 40$. Als we deze getallen modulo 5 nemen dan krijgen we $0, 0, 0, 0, 0$.

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

64 a. Het lijkt er op dat de antwoorden allemaal verschillend zijn als de ggd van de vermenigvuldigingsfactor en de modulus gelijk is aan 1. Als die ggd geen 1 is, dan zijn er gelijke antwoorden.

b. ggd (11,15)=1, dus moet $i = j$.

(of als de getallen willekeurig groot mogen zijn $i \equiv j \pmod{11}$.)

65 a. Als $ai \equiv aj \pmod{p}$, dan is $ai = aj + kp$ voor een zeker geheel getal k. Hieruit volgt $ai - aj = kp$, dus is p een deler van $ai - aj$.

b. Het priemgetal p is een deler van $ai - aj = a(i-j)$, dus $p|a$ of $p|(i-j)$. Omdat gegeven is dat a niet deelbaar is door p, moet p derhalve een deler zijn van $i-j$.

c. Als $p|(i-j)$, dan is er een geheel getal n zodanig dat $i - j = np$, ofwel $i = j + np$. Dit betekent dat $i \equiv j \pmod{p}$.

66 a. $15 \equiv 4 \pmod{11}$

$15^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$

$15^4 \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$

$15^8 \equiv 3^2 \equiv 9 \pmod{11}$

dus $15^{10} = 15^8 \cdot 15^2 \equiv 9 \cdot 5 \equiv 45 \equiv 1 \pmod{11}$.

b. $10 \equiv 3 \pmod{7}$

$10^2 \equiv 3^2 \equiv 9 \equiv 2 \pmod{7}$

$10^4 \equiv 2^2 \equiv 4 \pmod{7}$

dus $10^6 = 10^4 \cdot 10^2 \equiv 4 \cdot 2 \equiv 8 \equiv 1 \pmod{7}$.

c. $15 \equiv 3 \pmod{12}$

$15^2 \equiv 3^2 \equiv 9 \pmod{12}$

$15^4 \equiv 9^2 \equiv 9 \pmod{12}$

$15^8 \equiv 9^2 \equiv 9 \pmod{12}$

dus $15^{11} = 15^8 \cdot 15^2 \cdot 15^1 \equiv 9 \cdot 9 \cdot 3 \equiv 9 \cdot 3 \equiv 3 \pmod{12}$.

d. $10 \equiv 0 \pmod{5}$

$10^2 \equiv 0^2 \equiv 0 \pmod{5}$

$10^4 \equiv 0^2 \equiv 0 \pmod{5}$

dus $10^6 = 10^4 \cdot 10^2 \equiv 0 \cdot 0 \equiv 0 \pmod{5}$

e. $6^2 = 36$

$6^4 = 36^2 = 1296 \equiv 26 \pmod{127}$

$6^8 \equiv 26^2 \equiv 676 \equiv 41 \pmod{127}$

$6^{16} \equiv 41^2 \equiv 1681 \equiv 30 \pmod{127}$

$6^{32} \equiv 30^2 \equiv 900 \equiv 11 \pmod{127}$

$6^{64} \equiv 11^2 \equiv 121 \pmod{127}$

$$\begin{aligned}\text{dus } 6^{126} &= 6^{64} \cdot 6^{32} \cdot 6^{16} \cdot 6^8 \cdot 6^4 \cdot 6^2 \equiv 121 \cdot 11 \cdot 30 \cdot 41 \cdot 26 \cdot 36 \\ &\equiv 61 \cdot 30 \cdot 41 \cdot 26 \cdot 36 \equiv 52 \cdot 41 \cdot 26 \cdot 36 \equiv 100 \cdot 26 \cdot 36 \equiv 60 \cdot 36 \equiv 1 \pmod{127}\end{aligned}$$

67 Bij de berekeningen met antwoord 1 was de ggd van grondtal en modulus 1, bij de berekeningen met een antwoord ongelijk aan 1 was de ggd van grondtal en modulus ongelijk aan 1.

68 a. Als $ai \equiv aj \pmod{p}$, dan is $i \equiv j \pmod{p}$. De getallen $1, 2, \ldots, p-1$ zijn modulo p verschillend, dus de getallen $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ zijn modulo p ook allemaal verschillend.

b. Modulo p heb je alleen maar de getallen $0, 1, 2, \ldots, p-1$. Dat zijn er p, waarvan dus $p-1$ verschillend van 0. De $p-1$ getallen $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ zijn modulo p allemaal verschillend. Bovendien zijn ze allemaal ongelijk aan 0 modulo p, je kunt ze immers niet door p delen - het priemgetal p is geen deler van a, noch van de getallen $1, 2, \ldots, p-1$. Dus de getallen $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ zijn modulo p dezelfde (misschien wel in een andere volgorde) als de getallen $1, 2, \ldots, p-1$. Maar dan zijn hun producten gelijk.

c. $1 \cdot a \cdot 2 \cdot a \cdot \ldots \cdot (p-1) \cdot a = a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1)$.

d. $(1 - a^{p-1}) \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 0 \pmod{p}$ betekent dat p een deler moet zijn van $(1 - a^{p-1}) \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1)$

e. p deelt het product $(1 - a^{p-1}) \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1)$, dus één van de factoren. Aangezien p de getallen $1, 2, \ldots, p-1$ niet kan delen, moet p wel een deler zijn van $1 - a^{p-1}$.

f. Dit betekent dat $a^{p-1} \equiv 1 \pmod{p}$.

69 a. 33 is niet deelbaar door het priemgetal 97, dus $33^{96} \equiv 1 \pmod{97}$.

b. 57 is niet deelbaar door het priemgetal 101, dus $57^{100} \equiv 1 \pmod{101}$.

c. $57^{101} = 57^{100} \cdot 57^1 \equiv 1 \cdot 57 \equiv 57 \pmod{101}$.

d. $57^2 = 3249 \equiv 17 \pmod{101}$
$57^4 \equiv 17^2 \equiv 87 \pmod{101}$
dus $57^{104} = 57^{100} \cdot 57^4 \equiv 1 \cdot 87 \equiv 87 \pmod{101}$.

e. 991 is niet deelbaar door het priemgetal 1009, dus $991^{1008} \equiv 1 \pmod{1009}$.
$991^2 = 982081 \equiv 324 \pmod{1009}$
$991^4 \equiv 324^2 \equiv 104976 \equiv 40 \pmod{1009}$
$991^8 \equiv 40^2 \equiv 1600 \equiv 591 \pmod{1009}$
dus $991^{1017} = 991^{1008} \cdot 991^8 \cdot 991^1 \equiv 1 \cdot 591 \cdot 991 \equiv 585681 \equiv 461 \pmod{1009}$.

f. 871 is niet deelbaar door het priemgetal 9973, dus $871^{9972} \equiv 1 \pmod{9973}$
$871^2 = 758641 \equiv 693 \pmod{9973}$
$871^4 \equiv 693^2 \equiv 480249 \equiv 1545 \pmod{9973}$

$871^8 \equiv 1545^2 \equiv 2387025 \equiv 3478 \pmod{9973}$

$871^{16} \equiv 3478^2 \equiv 12096484 \equiv 9208 \pmod{9973}$

dus $871^{10000} = 871^{9972} \cdot 871^{16} \cdot 871^8 \cdot 871^4$

$\equiv 1 \cdot 9208 \cdot 3478 \cdot 1545 \equiv 2121 \cdot 1545 \equiv 5801 \pmod{9973}$.

g. 72 is niet deelbaar door het priemgetal 439, dus $72^{438} \equiv 1 \pmod{439}$

$72^2 = 5184 \equiv 355 \pmod{439}$

$72^4 \equiv 126025 \equiv 32 \pmod{439}$

dus $72^{443} = 72^{438} \cdot 72^4 \cdot 72^1 \equiv 1 \cdot 32 \cdot 72 \equiv 2304 \equiv 109 \pmod{439}$.

h. 991 is niet deelbaar door het priemgetal 563, dus $991^{562} \equiv 1 \pmod{563}$.

70 a. $i \leq 7$ en ggd(i,7)=1 geldt voor $i = 1, 2, 3, 4, 5, 6$, dus $\phi(7) = 6$.

b. $i \leq 9$ en ggd(i,9)=1 geldt voor $i = 1, 2, 4, 5, 7, 8$, dus $\phi(9) = 6$.

c. $i \leq 10$ en ggd(i,10)=1 geldt voor $i = 1, 3, 7, 9$, dus $\phi(10) = 4$.

d. $i \leq 11$ en ggd(i,11)=1 geldt voor $i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$, dus $\phi(11) = 10$.

e. $i \leq 21$ en ggd(i,21)=1 geldt voor $i = 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$, dus $\phi(21) = 12$.

f. $i \leq 25$ en ggd(i,25)=1 geldt voor $i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24$, dus $\phi(25) = 20$.

71 a. Als m priem is, dan is $\phi(m) = m - 1$. Waarschijnlijk geen toeval, zie de volgende opgaven.

b. Als m een kwadraat is, zeg $m = n^2$, dan is $\phi(m) = m - n$. Waarschijnlijk geen toeval, zie de volgende opgaven.

c. Als m het product is van twee verschillende priemgetallen, laten we zeggen $m = pq$, dan is $\phi(m) = (p - 1)(q - 1)$. Waarschijnlijk geen toeval, zie de volgende opgaven.

72 De getallen $1, 2, \ldots, p - 1$ hebben allemaal een ggd gelijk aan 1 met p. Dat zijn er $p - 1$, dus $\phi(p) = p - 1$.

73 a. $10 = 2 \cdot 5$

b. De getallen 2, 4, 6, 8 en 10 zijn deelbaar door 2. Dat zijn er 5 - dit had je ook kunnen vinden uit $\frac{10}{2} = 5$. Evenzo zijn er $\frac{10}{5} = 2$ getallen deelbaar door 5. Het getal 10 is deelbaar door zowel 2 als 5.

c. Van $1, 2, 3, \ldots, 10$ hebben $10 - 5 - 2 + 1 = 4$ getallen een ggd gelijk aan 1 met 10. De 5 getallen deelbaar door 2 moet je niet meetellen, de 2 getallen deelbaar door 5 ook niet. Je hebt het getal 10 nu twee keer niet meegeteld, dus je hebt er 1 teveel afgehaald. Dus $\phi(10) = 4$.

d. $21 = 3 \cdot 7$

e. Er zijn $\frac{21}{3} = 7$ getallen deelbaar door 3 en $\frac{21}{7} = 3$ getallen deelbaar door 7. Het getal 21 is deelbaar door zowel 3 als 7.

f. Van $1, 2, 3, \ldots, 21$ hebben $21 - 7 - 3 + 1 = 12$ getallen een ggd gelijk aan 1 met 21. De 7 getallen deelbaar door 3 moet je niet meetellen, de 3 getallen deelbaar door 7 ook niet. Je hebt het getal 21 nu twee keer niet meegeteld, dus je hebt er 1 teveel afgehaald. Dus $\phi(21) = 12$.

g. Er zijn $\frac{m}{p} = q$ getallen deelbaar door p en $\frac{m}{q} = p$ getallen deelbaar door q. Het getal m is deelbaar door zowel p als q.

h. Van $1, 2, 3, \ldots, pq$ hebben $pq - q - p + 1$ getallen een ggd gelijk aan 1 met $m = pq$. De q getallen deelbaar door p moet je niet meetellen, de p getallen deelbaar door q ook niet. Je hebt het getal $m = pq$ nu twee keer niet meegeteld, dus je hebt er 1 teveel afgehaald. Dus $\phi(pq) = pq - q - p + 1 = (p - 1)(q - 1)$.

74 a. $9 = 3^2$

b. De getallen 3, 6 en 9 zijn deelbaar door 3. Dat zijn $\frac{9}{3} = 3$ getallen.

c. Er zijn $9 - 3 = 6$ getallen die een ggd gelijk aan 1 met 9 hebben. $\phi(9) = 6$.

d. $25 = 5^2$

e. $\frac{25}{5} = 5$ getallen zijn deelbaar door 5.

f. Er zijn 25-5=20 getallen die een ggd gelijk aan 1 met 25 hebben. $\phi(25) = 20$.

g. Er zijn $\frac{p^2}{p} = p$ getallen deelbaar p.

h. $p^2 - p = p(p - 1)$ getallen hebben een ggd gelijk aan 1 met p. Dus $\phi(p^2) = p(p - 1)$.

i. Er zijn $\frac{p^k}{p} = p^{k-1}$ getallen deelbaar p.

j. $p^k - p^{k-1} = p^{k-1}(p - 1)$ getallen hebben een ggd gelijk aan 1 met p.
Dus $\phi(p^k) = p^{k-1}(p - 1)$.

75 a. Er zijn $\phi(m)$ getallen a kleiner dan m die geen echte deler met m gemeen hebben. Er zijn $\phi(n)$ getallen b kleiner dan n die geen echte deler met n gemeen hebben.

b. Er zijn $\phi(m) \cdot \phi(n)$ van deze stelsels mogelijk.

c. Volgens de Chinese reststelling heeft het stelsel precies één oplossing modulo mn. Er is dus precies één oplossing x kleiner dan mn.

Als er een gemeenschappelijke echte deler van x en mn zou zijn, dan zou er ook een priemgetal p zijn dat zowel x als mn deelt. Maar dan zou p een deler van m of van n moeten zijn, zeg van m. In dat geval deelt p zowel x als m, dus vanwege $x \equiv a \pmod{m}$ ook $p|a$. Dit laatste is niet mogelijk, immers ggd(a,m)=1.

Dus hebben de oplossing x en mn geen gemeenschappelijke echte delers.

d. Er is maar één a kleiner dan m met de eigenschap dat $x \equiv a \pmod{m}$, namelijk de rest als je x door m deelt. Voor deze a geldt bovendien dat ggd(a,m)=1, want als $x \equiv a \pmod{m}$, dan moet iedere gemeenschappelijke deler van a en m ook x delen en x en m hebben geen echte delers gemeen.

Evenzo is er maar één b kleiner dan n met de eigenschap dat $x \equiv b \pmod{n}$ en ggd(b,n)=1.

Er is dus maar één dergelijk stelsel mogelijk.

e. Er zijn volgens b. $\phi(m)\phi(n)$ stelsels mogelijk. Er zijn $\phi(mn)$ getallen x kleiner dan mn die geen echte deler met mn gemeen hebben. Bij iedere dergelijke x hoort zo'n stelsel en omgekeerd, dus $\phi(mn) = \phi(m)\phi(n)$.

76 $\phi(n) = \phi(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \dots \phi(p_k^{a_k}) =$
$p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1) \cdot \dots \cdot p_k^{a_k-1}(p_k-1)$.

77 a. $32 = 2^5$, dus $\phi(32) = 2^4 \cdot (2-1) = 16$.

b. $72 = 2^3 \cdot 3^2$, dus $\phi(72) = 2^2 \cdot (2-1) \cdot 3^1 \cdot (3-1) = 24$.

c. $1976 = 2^3 \cdot 13 \cdot 19$, dus $\phi(1976) = 2^2 \cdot (2-1) \cdot (13-1) \cdot (19-1) = 864$.

d. $96 = 2^5 \cdot 3$, dus $\phi(96) = 2^4 \cdot (2-1) \cdot (3-1) = 32$.

e. $3232 = 2^5 \cdot 101$, dus $\phi(3232) = 2^4 \cdot (2-1) \cdot (101-1) = 1600$.

f. $3600 = 2^4 \cdot 3^2 \cdot 5^2$, dus $\phi(3600) = 2^3 \cdot (2-1) \cdot 3^1 \cdot (3-1) \cdot 5^1 \cdot (5-1) = 960$.

g. $12345 = 3 \cdot 5 \cdot 823$, dus $\phi(12345) = (3-1) \cdot (5-1) \cdot (823-1) = 6576$.

h. $543210 = 2 \cdot 3 \cdot 5 \cdot 19 \cdot 953$, dus $\phi(543210) = 1 \cdot 2 \cdot 4 \cdot 18 \cdot 952 = 137088$.

78 a. $11^2 = 121 \equiv 25 \pmod{32}$
$11^4 \equiv 25^2 \equiv 625 \equiv 17 \pmod{32}$
$11^8 \equiv 17^2 \equiv 289 \equiv 1 \pmod{32}$
$11^{\phi(32)} = 11^{16} \equiv 1^2 \equiv 1 \pmod{32}$.

b. $11^2 = 121 \equiv 49 \pmod{72}$
$11^4 \equiv 49^2 \equiv 2401 \equiv 25 \pmod{72}$
$11^8 \equiv 25^2 \equiv 625 \equiv 49 \pmod{72}$
$11^{16} \equiv 49^2 \equiv 2401 \equiv 25 \pmod{72}$
$11^{\phi(72)} = 11^{24} = 11^{16} \cdot 11^8 \equiv 25 \cdot 49 \equiv 1225 \equiv 1 \pmod{72}$.

c. $6^2 = 36$
$6^4 \equiv 36^2 \equiv 1296 \equiv 0 \pmod{72}$
$6^8 \equiv 0^2 \equiv 0 \pmod{72}$
$6^{16} \equiv 0^2 \equiv 0 \pmod{72}$
$6^{\phi(72)} = 6^{24} = 6^{16} \cdot 6^8 \equiv 0 \cdot 0 \equiv 0 \pmod{72}$.

d. $6^2 = 36$
$6^4 \equiv 36^2 \equiv 1296 \equiv 48 \pmod{96}$
$6^8 \equiv 48^2 \equiv 2304 \equiv 0 \pmod{96}$
$6^{16} \equiv 0^2 \equiv 0 \pmod{96}$
$6^{\phi(96)} = 6^{32} \equiv 0^2 \equiv 0 \pmod{96}$.

e. $13^2 = 169 \equiv 9 \pmod{32}$
$13^4 \equiv 9^2 \equiv 81 \equiv 17 \pmod{32}$
$13^8 \equiv 17^2 \equiv 289 \equiv 1 \pmod{32}$
$13^{\phi(32)} = 13^{16} \equiv 1^2 \equiv 1 \pmod{32}$.

f. $\phi(48) = \phi(2^4 \cdot 3) = 2^3 \cdot 1 \cdot 2 = 16$
$7^2 = 49 \equiv 1 \pmod{48}$
$7^4 \equiv 1^2 \equiv 1 \pmod{48}$
$7^8 \equiv 1^2 \equiv 1 \pmod{48}$
$7^{\phi(48)} = 7^{16} \equiv 1^2 \equiv 1 \pmod{48}$.

g. $\phi(56) = \phi(2^3 \cdot 7) = 2^2 \cdot 1 \cdot 6 = 24$
$7^2 = 49$
$7^4 = 49^2 = 2401 \equiv 49 \pmod{56}$
$7^8 \equiv 49^2 \equiv 2401 \equiv 49 \pmod{56}$
$7^{16} \equiv 49^2 \equiv 2401 \equiv 49 \pmod{56}$
$7^{\phi(56)} = 7^{24} = 7^{16} \cdot 7^8 \equiv 49 \cdot 49 \equiv 2401 \equiv 49 \pmod{56}$.

h. $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$

$11^2 = 121 \equiv 21 \pmod{100}$

$11^4 \equiv 21^2 \equiv 441 \equiv 41 \pmod{100}$

$11^8 \equiv 41^2 \equiv 1681 \equiv 81 \pmod{100}$

$11^{16} \equiv 81^2 \equiv 6561 \equiv 61 \pmod{100}$

$11^{32} \equiv 61^2 \equiv 3721 \equiv 21 \pmod{100}$

$11^{\phi(100)} = 11^{40} = 11^{32} \cdot 11^8 \equiv 21 \cdot 81 \equiv 1701 \equiv 1 \pmod{100}$.

79 Het antwoord was 1 als de ggd van grondtal en modulus gelijk was aan 1.

80 a. Als een priemgetal q een gemeenschappelijke deler is van m en ai, dan moet q een gemeenschappelijke deler zijn van i en m (immers als $q|ai$, dan moet $q|a$ of $q|i$ en ggd(a,m)=1, dus $q \not| a$.) Maar dat betekent dat zo'n getal i niet in G kan zitten. Dus voor elk getal i in G geldt dat ai ook geen echte deler met m gemeen heeft en modulo m gelijk is aan een of ander getal uit G.

Als $ai \equiv aj \pmod{m}$, dan is $ai - aj = a(i-j)$ deelbaar door m. Elk priemgetal q dat m deelt, moet $i - j$ delen. Maar dat betekent dat de volledige priemfactorontbinding van m terug te vinden is in de priemfactorontbinding van $i-j$, dus $i-j$ is een veelvoud van m, ofwel $i \equiv j \pmod{m}$. Als i en j beiden in G zitten, dan kan dat alleen als $i = j$.

Dus alle getallen uit P zijn modulo m verschillend en komen allemaal ook voor in G. Omdat P evenveel getallen als G bevat, moeten beide collecties modulo m dus hetzelfde zijn.

b. Modulo m zijn beide collecties hetzelfde, dus het product van alle getallen uit de collectie P is modulo m gelijk aan het product van alle getallen uit de collectie G.

c. Modulo m is elk getal uit de collectie P gelijk aan a maal een getal uit de collectie G. Er zijn $\phi(m)$ getallen in beide collecties. Als je alle factoren a uit het product p apart neemt, dan krijg je $\phi(m)$ factoren a, gevolgd door alle getallen uit de collectie G, ofwel $p{=}a^{\phi(m)} \cdot g$. Met $p \equiv g \pmod{m}$ krijgen we dan $a^{\phi(m)} \cdot g \equiv g \pmod{m}$

d. $(1 - a^{\phi(m)}) \cdot g \equiv 0 \pmod{m}$ betekent dat $(1 - a^{\phi(m)}) \cdot g$ een veelvoud is van m.

e. Elk priemgetal dat m deelt moet $1 - a^{\phi(m)}$ delen, want dat priemgetal kan g niet delen (g was immers het product van alle getallen uit $1, 2, \ldots, m-1$ die geen echte deler met m gemeen hadden). Maar dat betekent dat de volledige priemfactorontbinding van m terug te vinden is in de priemfactorontbinding van $1 - a^{\phi(m)}$: m deelt dus $1 - a^{\phi(m)}$, ofwel $a^{\phi(m)} \equiv 1 \pmod{m}$.

81 a. $\phi(3528) = \phi(2^3 \cdot 3^2 \cdot 7^2) = 2^2 \cdot 1 \cdot 3^1 \cdot 2 \cdot 7^1 \cdot 6 = 1008$.

Dus $5^{1008} \equiv 1 \pmod{3528}$.

b. $5^{1010} = 5^{1008} \cdot 5^2 \equiv 1 \cdot 25 \equiv 25 \pmod{3528}$.

c. $5^2 = 25$
$5^4 = 25^2 = 625$
$5^8 = 625^2 = 390625 \equiv 2545 \pmod{3528}$
$5^{1017} = 5^{1008} \cdot 5^8 \cdot 5^1 \equiv 1 \cdot 2545 \cdot 5 \equiv 2141 \pmod{3528}$.

d. $\phi(880) = \phi(2^4 \cdot 5 \cdot 11) = 2^3 \cdot 1 \cdot 4 \cdot 10 = 320$.
Dus $7^{320} \equiv 1 \pmod{880}$.

e. $7^{322} = 7^{320} \cdot 7^2 \equiv 1 \cdot 49 \equiv 49 \pmod{880}$.

f. $\phi(7623) = \phi(3^2 \cdot 7 \cdot 11^2) = 3^1 \cdot 2 \cdot 6 \cdot 11^1 \cdot 10 = 3960$
$2^{3961} = 2^{3960} \cdot 2^1 \equiv 1 \cdot 2 \equiv 2 \pmod{7623}$.

g. $\phi(26299) = \phi(7 \cdot 13 \cdot 17^2) = 6 \cdot 12 \cdot 17^1 \cdot 16 = 19584$
$3^2 = 9$
$3^4 = 9^2 = 81$
$3^8 = 81^2 = 6561$
$3^{16} = 6561^2 = 43046721 \equiv 21557 \pmod{26299}$
$3^{32} \equiv 21557^2 \equiv 464704249 \equiv 919 \pmod{26299}$
$3^{64} \equiv 919^2 \equiv 844561 \equiv 2993 \pmod{26299}$
$3^{128} \equiv 2993^2 \equiv 8958049 \equiv 16389 \pmod{26299}$
$3^{256} \equiv 16389^2 \equiv 268599321 \equiv 7634 \pmod{26299}$
$3^{20000} = 3^{19584} \cdot 3^{256} \cdot 3^{128} \cdot 3^{32} \equiv 1 \cdot 7634 \cdot 16389 \cdot 919 \equiv 9283 \cdot 919 \equiv 10201 \pmod{26299}$.

82 a. $\phi(637) = \phi(7^2 \cdot 13) = 7^1 \cdot 6 \cdot 12 = 504$.
$25^2 = 625$
$25^{507} = 25^{504} \cdot 25^2 \cdot 25^1 \equiv 1 \cdot 625 \cdot 25 \equiv 337 \pmod{637}$.

b. $90^2 = 8100 \equiv 456 \pmod{637}$
$90^4 \equiv 456^2 \equiv 207936 \equiv 274 \pmod{637}$
$90^8 \equiv 274^2 \equiv 75076 \equiv 547 \pmod{637}$
$90^{513} = 90^{504} \cdot 90^8 \cdot 90^1 \equiv 1 \cdot 547 \cdot 90 \equiv 181 \pmod{637}$.

c. $\phi(1573) = \phi(11^2 \cdot 13) = 11^1 \cdot 10 \cdot 12 = 1320$

$7^2 = 49$

$7^4 = 49^2 = 2401 \equiv 828 \pmod{1573}$

$7^8 \equiv 828^2 \equiv 685584 \equiv 1329 \pmod{1573}$

$7^{16} \equiv 1329^2 \equiv 1766241 \equiv 1335 \pmod{1573}$

$7^{32} \equiv 1335^2 \equiv 1782225 \equiv 16 \pmod{1573}$

$7^{64} \equiv 16^2 \equiv 256 \pmod{1573}$

$7^{128} \equiv 256^2 \equiv 65536 \equiv 1043 \pmod{1573}$

$7^{1573} = 7^{1320} \cdot 7^{128} \cdot 7^{64} \cdot 7^{32} \cdot 7^{16} \cdot 7^8 \cdot 7^4 \cdot 7^1 \equiv 1 \cdot 1043 \cdot 256 \cdot 16 \cdot 1335 \cdot 1329 \cdot 828 \cdot 7 \equiv$
$1171 \cdot 16 \cdot 1335 \cdot 1329 \cdot 828 \cdot 7 \equiv 1433 \cdot 1335 \cdot 1329 \cdot 828 \cdot 7 \equiv 287 \cdot 1329 \cdot 828 \cdot 7 \equiv$
$757 \cdot 828 \cdot 7 \equiv 742 \cdot 7 \equiv 475 \pmod{1573}$.

d. 1571 is een priemgetal, dus $9^{1570} \equiv 1 \pmod{1571}$.

$9^2 = 81$

$9^{1573} = 961570 \cdot 9^2 \cdot 9^1 \equiv 1 \cdot 81 \cdot 9 \equiv 729 \pmod{1571}$.

e. 1571 is een priemgetal, dus $10^{1570} \equiv 1 \pmod{1571}$.

$10^2 = 100$

$10^4 = 10000 \equiv 574 \pmod{1571}$

$10^{1575} = 10^{1570} \cdot 10^4 \cdot 10^1 \equiv 1 \cdot 574 \cdot 10 \equiv 1027 \pmod{1571}$.

f. $\phi(49005) = \phi(3^4 \cdot 5 \cdot 11^2) = 3^3 \cdot 2 \cdot 4 \cdot 11^1 \cdot 10 = 23760$

$28^2 = 784$

$28^4 = 784^2 = 614656 \equiv 26596 \pmod{49005}$

$28^8 \equiv 26596^2 \equiv 707347216 \equiv 9046 \pmod{49005}$

$28^{16} \equiv 9046^2 \equiv 81830116 \equiv 40771 \pmod{49005}$

$28^{32} \equiv 40771^2 \equiv 1662274441 \equiv 24841 \pmod{49005}$

$28^{64} \equiv 24841^2 \equiv 617075281 \equiv 4321 \pmod{49005}$

$28^{128} \equiv 4321^2 \equiv 18671041 \equiv 136 \pmod{49005}$

$28^{256} \equiv 136^2 \equiv 18496 \pmod{49005}$

$28^{512} \equiv 18496^2 \equiv 342102016 \equiv 47116 \pmod{49005}$

$28^{1024} \equiv 47116^2 \equiv 2219917456 \equiv 39961 \pmod{49005}$

$28^{25000} = 28^{23760} \cdot 28^{1024} \cdot 28^{128} \cdot 28^{64} \cdot 27^{16} \cdot 28^8 \equiv 1 \cdot 39961 \cdot 136 \cdot 4321 \cdot 40771 \cdot 9046 \equiv$
$44146 \cdot 4321 \cdot 40771 \cdot 9046 \equiv 274006 \cdot 40771 \cdot 9046 \equiv 7021 \cdot 9046 \equiv 1486 \pmod{49005}$.

g. $28^{50000} \equiv 1486^2 \equiv 2208196 \equiv 2971 \pmod{49005}$.

h. $28^{47520} = (28^{23760})^2 \equiv 1^2 \equiv 1 \pmod{49005}$.
$28^{47600} = 28^{47520} \cdot 28^{64} \cdot 28^{16} \equiv 1 \cdot 4321 \cdot 40771 \equiv 47521 \pmod{49005}$.

i. $\phi(3528) = \phi(2^3 \cdot 3^2 \cdot 7^2) = 2^2 \cdot 1 \cdot 3^1 \cdot 2 \cdot 7^1 \cdot 6 = 1008$.
$5^{3024} = (5^{1008})^3 \equiv 1^3 \equiv 1 \pmod{3528}$
$5^2 = 25$
$5^4 = 25^2 = 625$
$5^8 = 625^2 = 390625 \equiv 2545 \pmod{3528}$
$5^{16} \equiv 2545^2 \equiv 6477025 \equiv 3145 \pmod{3528}$
$5^{32} \equiv 3145^2 \equiv 9891025 \equiv 2041 \pmod{3528}$
$5^{64} \equiv 2041^2 \equiv 4165681 \equiv 2641 \pmod{3528}$
$5^{128} \equiv 2641^2 \equiv 6974881 \equiv 25 \pmod{3528}$
$5^{3200} = 5^{3024} \cdot 5^{128} \cdot 5^{32} \cdot 5^{16} \equiv 1 \cdot 25 \cdot 2041 \cdot 3145 \equiv 1633 \cdot 3145 \equiv 2545 \pmod{3528}$

j. $5^{4032} = (5^{1008})^4 \equiv 1^4 \equiv 1 \pmod{3528}$

83 a. Om de laatste 3 cijfers van 3^{400} te weten, moeten we modulo 1000 gaan rekenen. Nu is $\phi(1000) = \phi(2^3 \cdot 5^3) = 2^2 \cdot 1 \cdot 5^2 \cdot 4 = 400$, dus $3^{400} \equiv 1 \pmod{1000}$, zodat 3^{400} eindigt op 001.

b. $27^{400} \equiv 1 \pmod{1000}$
$27^2 = 729$
$27^4 = 729^2 = 531441 \equiv 441 \pmod{1000}$
$27^8 \equiv 441^2 \equiv 194481 \equiv 481 \pmod{1000}$
$27^{16} \equiv 481^2 \equiv 231361 \equiv 361 \pmod{1000}$
$27^{32} \equiv 361^2 \equiv 130321 \equiv 321 \pmod{1000}$
$27^{64} \equiv 321^2 \equiv 103041 \equiv 41 \pmod{1000}$
$27^{513} = 27^{400} \cdot 27^{64} \cdot 27^{32} \cdot 27^{16} \cdot 27^1 \equiv 1 \cdot 41 \cdot 321 \cdot 361 \cdot 27 \equiv$
$161 \cdot 361 \cdot 27 \equiv 121 \cdot 27 \equiv 267 \pmod{1000}$,
zodat 27^{513} eindigt op 267.

c. $19^{400} \equiv 1 \pmod{1000}$
$19^{800} = (19^{400})^2 \equiv 1^2 \equiv 1 \pmod{1000}$
$19^2 = 361$
$19^4 = 361^2 = 130321 \equiv 321 \pmod{1000}$

$19^8 \equiv 321^2 \equiv 103041 \equiv 41 \pmod{1000}$

$19^{16} \equiv 41^2 \equiv 1681 \equiv 681 \pmod{1000}$

$19^{32} \equiv 681^2 \equiv 463761 \equiv 761 \pmod{1000}$

$19^{64} \equiv 761^2 \equiv 579121 \equiv 121 \pmod{1000}$

$19^{128} \equiv 121^2 \equiv 14641 \equiv 641 \pmod{1000}$

$19^{1002} = 19^{800} \cdot 19^{128} \cdot 19^{64} \cdot 19^8 \cdot 19^2 \equiv 1 \cdot 641 \cdot 121 \cdot 41 \cdot 361 \equiv$
$561 \cdot 41 \cdot 361 \equiv 1 \cdot 361 \equiv 361 \pmod{1000}$,
zodat 19^{1002} eindigt op 361.

d. $33^{1200} = (33^{400})^3 \equiv 1^3 \equiv 1 \pmod{1000}$

$33^2 = 1089 \equiv 89 \pmod{1000}$

$33^4 \equiv 89^2 \equiv 7921 \equiv 921 \pmod{1000}$

$33^8 \equiv 921^2 \equiv 848241 \equiv 241 \pmod{1000}$

$33^{16} \equiv 241^2 \equiv 58081 \equiv 81 \pmod{1000}$

$33^{32} \equiv 81^2 \equiv 6561 \equiv 561 \pmod{1000}$

$33^{64} \equiv 561^2 \equiv 314721 \equiv 721 \pmod{1000}$

$33^{128} \equiv 721^2 \equiv 519841 \equiv 841 \pmod{1000}$

$33^{256} \equiv 841^2 \equiv 707281 \equiv 281 \pmod{1000}$

$33^{1513} = 33^{1200} \cdot 33^{256} \cdot 33^{32} \cdot 33^{16} \cdot 33^8 \cdot 33^1 \equiv 1 \cdot 281 \cdot 561 \cdot 81 \cdot 241 \cdot 33 \equiv$
$641 \cdot 81 \cdot 241 \cdot 33 \equiv 921 \cdot 241 \cdot 33 \equiv 961 \cdot 33 \equiv 713 \pmod{1000}$,
zodat 33^{1513} eindigt op 713.

84 a.

313/7890\25 dus $7890 : 313 = 25$ *rest* 65
626
1630
1565
65

b. 47/212565\4522 dus $212565 : 47 = 4522$ *rest* 31

188
245
235
106
94
125
94
31

c. 3949/18394503\4658 dus $18394503 : 3949 = 4658$ *rest* 61

15796
25985
23694
22910
19745
31653
31592
61

d. 701/29102834\41516 dus $29102834 : 701 = 41516$ *rest* 118

2804
1062
701
3618
3505
1133
701
4324
4206
118

85 a. $2942 - 1 \cdot 2714 = 228$
$2714 - 11 \cdot 228 = 206$
$228 - 1 \cdot 206 = 22$
$206 - 9 \cdot 22 = 8$
$22 - 2 \cdot 8 = 6$
$8 - 1 \cdot 6 = 2$
$6 - 3 \cdot 2 = 0$

Terugrekenend krijgen we:
$2 = 8 - 1 \cdot 6$
$= 8 - 1 \cdot (22 - 2 \cdot 8)$
$= 3 \cdot 8 - 1 \cdot 22$
$= 3 \cdot (206 - 9 \cdot 22) - 1 \cdot 22$
$= 3 \cdot 206 - 28 \cdot 22$
$= 3 \cdot 206 - 28 \cdot (228 - 1 \cdot 206)$
$= 31 \cdot 206 - 28 \cdot 228$
$= 31 \cdot (2714 - 11 \cdot 228) - 28 \cdot 228$
$= 31 \cdot 2714 - 369 \cdot 228$
$= 31 \cdot 2714 - 369 \cdot (2942 - 1 \cdot 2714)$
$= 400 \cdot 2714 - 369 \cdot 2942$
dus ggd(2942,2714)=$2 = 400 \cdot 2714 - 369 \cdot 2942$.

b. $9972 - 3 \cdot 3213 = 333$
$3213 - 9 \cdot 333 = 216$
$333 - 1 \cdot 216 = 117$
$216 - 1 \cdot 117 = 99$
$117 - 1 \cdot 99 = 18$
$99 - 5 \cdot 18 = 9$
$18 - 2 \cdot 9 = 0$

Terugrekenend krijgen we:
$9 = 99 - 5 \cdot 18$
$= 99 - 5 \cdot (117 - 1 \cdot 99)$
$= 6 \cdot 99 - 5 \cdot 117$
$= 6 \cdot (216 - 1 \cdot 117) - 5 \cdot 117$
$= 6 \cdot 216 - 11 \cdot 117$
$= 6 \cdot 216 - 11 \cdot (333 - 1 \cdot 216)$
$= 17 \cdot 216 - 11 \cdot 333$
$= 17 \cdot (3213 - 9 \cdot 333) - 11 \cdot 333$
$= 17 \cdot 3212 - 164 \cdot 333$
$= 17 \cdot 3212 - 164 \cdot (9972 - 3 \cdot 3213)$
$= 509 \cdot 3213 - 164 \cdot 9972$
dus ggd(9972,3213)=9$= 509 \cdot 3213 - 164 \cdot 9972$.

c. $4035 - 1 \cdot 2445 = 1590$
$2445 - 1 \cdot 1590 = 855$
$1590 - 1 \cdot 855 = 735$
$855 - 1 \cdot 735 = 120$
$735 - 6 \cdot 120 = 15$
$120 - 8 \cdot 15 = 0$

Terugrekenend krijgen we:
$15 = 735 - 6 \cdot 120$
$= 735 - 6 \cdot (855 - 1 \cdot 735)$
$= 7 \cdot 735 - 6 \cdot 855$
$= 7 \cdot (1590 - 1 \cdot 855) - 6 \cdot 855$
$= 7 \cdot 1590 - 13 \cdot 855$
$= 7 \cdot 1590 - 13 \cdot (2445 - 1 \cdot 1590)$
$= 20 \cdot 1590 - 13 \cdot 2445$
$= 20 \cdot (4035 - 1 \cdot 2445) - 13 \cdot 2445$
$= 20 \cdot 4035 - 33 \cdot 2445$
dus ggd(4035,2445)=15= $20 \cdot 4035 - 33 \cdot 2445$.

d. $3311 - 1 \cdot 2761 = 550$
$2761 - 5 \cdot 550 = 11$
$550 - 50 \cdot 11 = 0$

Terugrekenend krijgen we:
$11 = 2761 - 5 \cdot 550$
$= 2761 - 5 \cdot (3311 - 1 \cdot 2761)$
$= 6 \cdot 2761 - 5 \cdot 3311$
dus ggd(3311,2761)=$11 = 6 \cdot 2761 - 5 \cdot 3311$.

e. $4228 - 2 \cdot 1414 = 1400$
$1414 - 1 \cdot 1400 = 14$
$1400 - 100 \cdot 14 = 0$

Terugrekenend krijgen we:
$14 = 1414 - 1 \cdot 1400$
$\quad = 1414 - 1 \cdot (4228 - 2 \cdot 1414)$
$\quad = 3 \cdot 1414 - 1 \cdot 4228$
dus ggd(1414,4228)=$14 = 3 \cdot 1414 - 1 \cdot 4228$.

f. $54321 - 4 \cdot 12345 = 4941$
$12345 - 2 \cdot 4941 = 2463$
$4941 - 2 \cdot 2463 = 15$
$2463 - 164 \cdot 15 = 3$
$15 - 5 \cdot 3 = 0$

Terugrekenend krijgen we:
$3 = 2463 - 164 \cdot 15$
$\quad = 2463 - 164 \cdot (4941 - 2 \cdot 2463)$
$\quad = 329 \cdot 2463 - 164 \cdot 4941$
$\quad = 329 \cdot (12345 - 2 \cdot 4941) - 164 \cdot 4941$
$\quad = 329 \cdot 12345 - 822 \cdot 4941$
$\quad = 329 \cdot 12345 - 822 \cdot (54321 - 4 \cdot 12345)$
$\quad = 3617 \cdot 12345 - 822 \cdot 54321$
dus ggd(12345,54321)=$3 = 3617 \cdot 12345 - 822 \cdot 54321$.

g. $10101 - 22 \cdot 456 = 69$
$456 - 6 \cdot 69 = 42$
$69 - 1 \cdot 42 = 27$
$42 - 1 \cdot 27 = 15$
$27 - 1 \cdot 15 = 12$
$15 - 1 \cdot 12 = 3$
$12 - 4 \cdot 3 = 0$

Terugrekenend krijgen we:
$3 = 15 - 1 \cdot 12$
$\quad = 15 - 1 \cdot (27 - 1 \cdot 15)$
$\quad = 2 \cdot 15 - 1 \cdot 27$
$\quad = 2 \cdot (42 - 1 \cdot 27) - 1 \cdot 27$
$\quad = 2 \cdot 42 - 3 \cdot 27$
$\quad = 2 \cdot 42 - 3 \cdot (69 - 1 \cdot 42)$
$\quad = 5 \cdot 42 - 3 \cdot 69$

$= 5 \cdot (456 - 6 \cdot 69) - 3 \cdot 69$
$= 5 \cdot 456 - 33 \cdot 69$
$= 5 \cdot 456 - 33 \cdot (10101 - 22 \cdot 456)$
$= 731 \cdot 456 - 33 \cdot 10101$
dus ggd(10101,456)=3 $= 731 \cdot 456 - 33 \cdot 10101$.

h. $9172 - 1 \cdot 5364 = 3808$
$5364 - 1 \cdot 3808 = 1556$
$3808 - 2 \cdot 1556 = 696$
$1556 - 2 \cdot 696 = 164$
$696 - 4 \cdot 164 = 40$
$164 - 4 \cdot 40 = 4$
$40 - 10 \cdot 4 = 0$

Terugrekenend krijgen we:
$4 = 164 - 4 \cdot 40$
$= 164 - 4 \cdot (696 - 4 \cdot 164)$
$= 17 \cdot 164 - 4 \cdot 696$
$= 17 \cdot (1556 - 2 \cdot 696) - 4 \cdot 696$
$= 17 \cdot 1556 - 38 \cdot 696$
$= 17 \cdot 1556 - 38 \cdot (3808 - 2 \cdot 1556)$
$= 93 \cdot 1556 - 38 \cdot 3808$
$= 93 \cdot (5364 - 1 \cdot 3808) - 38 \cdot 3808$
$= 93 \cdot 5364 - 131 \cdot 3808$
$= 93 \cdot 5364 - 131 \cdot (9172 - 1 \cdot 5364)$
$= 224 \cdot 5364 - 131 \cdot 9172$
dus ggd(9172,5364)=4 $= 224 \cdot 5364 - 131 \cdot 9172$.

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

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

c. $1524 = 2^2 \cdot 3 \cdot 127$

$254 = 2 \cdot 127$

$\text{ggd}(1524, 254) = 2 \cdot 127 = 254$

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

87 a. $47 \equiv 2 \pmod{45}$

$47^2 \equiv 2^2 \equiv 4 \pmod{45}$

$47^4 \equiv 4^2 \equiv 16 \pmod{45}$

$47^8 \equiv 16^2 \equiv 256 \equiv 31 \pmod{45}$

$47^{16} \equiv 31^2 \equiv 16 \pmod{45}$

$47^{19} = 47^{16} \cdot 47^2 \cdot 47 \equiv 16 \cdot 4 \cdot 2 \equiv 19 \cdot 2 \equiv 38 \pmod{45}$

b. $231^2 = 53361 \equiv 1335 \pmod{2001}$

$231^4 \equiv 1335^2 \equiv 1782225 \equiv 1335 \pmod{2001}$

$231^8 \equiv 1335^2 \equiv 1782225 \equiv 1335 \pmod{2001}$

$231^{16} \equiv 1335^2 \equiv 1782225 \equiv 1335 \pmod{2001}$

$231^{29} = 231^{16} \cdot 231^8 \cdot 231^4 \cdot 231 \equiv 1335 \cdot 1335 \cdot 1335 \cdot 231$

$\equiv 1335 \cdot 1335 \cdot 231 \equiv 1335 \cdot 231 \equiv 231 \pmod{2001}$

c. $764^2 = 583696 \equiv 708 \pmod{3101}$

$764^4 \equiv 708^2 \equiv 501264 \equiv 2003 \pmod{3101}$

$764^8 \equiv 2003^2 \equiv 4012009 \equiv 2416 \pmod{3101}$

$764^{16} \equiv 2416^2 \equiv 5837056 \equiv 974 \pmod{3101}$

$764^{32} \equiv 974^2 \equiv 948676 \equiv 2871 \pmod{3101}$

$764^{64} \equiv 2871^2 \equiv 8242641 \equiv 183 \pmod{3101}$

$764^{121} = 764^{64} \cdot 764^{32} \cdot 764^{16} \cdot 764^8 \cdot 764 \equiv 183 \cdot 2871 \cdot 974 \cdot 2416 \cdot 764$

$\equiv 1324 \cdot 974 \cdot 2416 \cdot 764 \equiv 2661 \cdot 2416 \cdot 764 \equiv 603 \cdot 764 \equiv 1744 \pmod{3101}$

d. $\phi(100) = \phi(2^2 \cdot 5^2) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$, dus $291^{40} \equiv 1 \pmod{100}$

$291^{320} = (291^{40})^8 \equiv 1^8 \equiv 1 \pmod{100}$

$291 \equiv 91 \pmod{100}$

$291^2 \equiv 91^2 \equiv 8281 \equiv 81 \pmod{100}$

$291^{322} = 291^{320} \cdot 291^2 \equiv 1 \cdot 81 \equiv 81 \pmod{100}$

e. 97 is een priemgetal, dus $95^{96} \equiv 1 \pmod{97}$
$95 \equiv -2 \pmod{97}$
$95^2 \equiv (-2)^2 \equiv 4 \pmod{97}$
$95^{99} = 95^{96} \cdot 95^2 \cdot 95 \equiv 1 \cdot 4 \cdot -2 \equiv -8 \equiv 89 \pmod{97}$

f. $\phi(200) = \phi(2^3 \cdot 5^2) = 2^2 \cdot 1 \cdot 5 \cdot 4 = 80$, dus $39^{80} \equiv 1 \pmod{200}$
$39^2 = 1521 \equiv 121 \pmod{200}$
$39^4 \equiv 121^2 \equiv 14641 \equiv 41 \pmod{200}$
$39^{85} = 39^{80} \cdot 39^4 \cdot 39 \equiv 1 \cdot 41 \cdot 39 \equiv 199 \pmod{200}$

g. $\phi(105) = \phi(3 \cdot 5 \cdot 7) = 2 \cdot 4 \cdot 6 = 48$, dus $74^{48} \equiv 1 \pmod{105}$
$74^2 = 5476 \equiv 16 \pmod{105}$
$74^{51} = 74^{48} \cdot 74^2 \cdot 74 \equiv 1 \cdot 16 \cdot 74 \equiv 29 \pmod{105}$

h. $\phi(91) = \phi(7 \cdot 13) = 6 \cdot 12 = 72$, dus $19^{72} \equiv 1 \pmod{91}$
$19^{864} = (19^{72})^{12} \equiv 1^{12} \equiv 1 \pmod{91}$
$19^2 = 361 \equiv 88 \equiv -3 \pmod{91}$
$19^4 \equiv (-3)^2 \equiv 9 \pmod{91}$
$19^8 \equiv 9^2 \equiv 81 \equiv -10 \pmod{91}$
$19^{16} \equiv (-10)^2 \equiv 100 \equiv 9 \pmod{91}$
$19^{32} \equiv 9^2 \equiv 81 \equiv -10 \pmod{91}$
$19^{919} = 19^{864} \cdot 19^{32} \cdot 19^{16} \cdot 19^4 \cdot 19^2 \cdot 19 \equiv 1 \cdot -10 \cdot 9 \cdot 9 \cdot -3 \cdot 19 \equiv 1 \cdot 9 \cdot -3 \cdot 19$
$\equiv -27 \cdot 19 \equiv 33 \pmod{91}$

88 a. $17x - 8 \equiv 10x + 10 \pmod{45}$
$7x \equiv 18 \pmod{45}$
Vermenigvuldigen met 13 (want $7 \cdot 13 = 91 \equiv 1 \pmod{45}$) geeft:
$x \equiv 234 \equiv 9 \pmod{45}$.

b. $6x + 14 \equiv 2x + 23 \pmod{31}$
$4x \equiv 9 \pmod{31}$
Vermenigvuldigen met 8 (want $4 \cdot 8 = 32 \equiv 1 \pmod{31}$) geeft:
$x \equiv 72 \equiv 10 \pmod{31}$

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

$-20x \equiv -29 \pmod{51}$

$20x \equiv 29 \pmod{51}$

Vermenigvuldigen met 23 (want $20 \cdot 23 = 460 \equiv 1 \pmod{51}$) geeft:

$x \equiv 667 \equiv 4 \pmod{51}$

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

$7x \equiv 56 \pmod{5}$

Nu is $7 \cdot 8 = 56$, dus $x \equiv 8 \equiv 3 \pmod{5}$

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

$57x \equiv -52 \pmod{95}$

$57x \equiv 43 \pmod{95}$

Deze vergelijking is niet oplosbaar, want 43 is geen veelvoud van 19 = ggd(57,95).

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

$-3x \equiv -42 \pmod{117}$

$3x \equiv 42 \pmod{117}$

$x \equiv 14 \pmod{39}$

89 a. $m = 5 \cdot 7 \cdot 11 = 385$.

Om nu verder te kunnen gaan moeten we eerst de vergelijkingen omschrijven naar de vorm $x \equiv a \pmod{m}$. Daartoe vermenigvuldig je de eerste met 4, de tweede met 3 en de derde met 2. (Bedenk dat $4 \cdot 4 = 16 \equiv 1 \pmod{5}$, $3 \cdot 5 = 15 \equiv 1 \pmod{7}$ en $2 \cdot 6 = 12 \equiv 1 \pmod{11}$)

Dit geeft het volgende stelsel:

$$x \equiv 3 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

dus $x \equiv 3 \pmod{385}$

b. $m = 2 \cdot 11 \cdot 19 = 418$

Vermenigvuldig de tweede vergelijking met 6, de derde met 13 en

bedenk dat $7 \equiv 1 \pmod{2}$.

We krijgen dan het volgende stelsel vergelijkingen:

$$x \equiv 0 \pmod 2$$
$$x \equiv 6 \pmod{11}$$
$$x \equiv 6 \pmod{19}$$

Omdat $6 \equiv 0 \pmod 2$, zie je meteen dat $x \equiv 6 \pmod{418}$ de oplossing is.

c. Als je de eerste vergelijking door 2 deelt en de tweede door 7, dan krijg je het volgende stelsel:

$$2x \equiv 1 \pmod 3$$
$$3x \equiv 0 \pmod 5$$
$$8x \equiv 6 \pmod{17}$$

Vermenigvuldig de vergelijkingen nu respectievelijk met 2, 2 en 15. Dit geeft het volgende stelsel:

$$x \equiv 2 \pmod 3$$
$$x \equiv 0 \pmod 5$$
$$x \equiv 5 \pmod{17}$$

$m = 3 \cdot 5 \cdot 17 = 255$
$\frac{m}{m_1} = \frac{255}{3} = 85$, $\frac{m}{m_2} = \frac{255}{5} = 51$ en $\frac{m}{m_3} = \frac{255}{17} = 15$.
$85b_1 \equiv 1 \pmod 3$ geeft $b_1 \equiv 1 \pmod 3$
$51b_2 \equiv 1 \pmod 5$ geeft $b_2 \equiv 1 \pmod 5$
$15b_3 \equiv 1 \pmod{17}$ geeft $b_3 \equiv 8 \pmod{17}$
$x = 85 \cdot 1 \cdot 2 + 51 \cdot 1 \cdot 0 + 15 \cdot 8 \cdot 5 = 770 \equiv 5 \pmod{255}$.
Alternatieve oplossing voor het laatste stelsel:
Uit $x \equiv 0 \pmod 5$ volgt $x = 5y$ voor een zekere y
Invullen in $x \equiv 2 \pmod 3$ geeft $5y \equiv 2 \pmod 3$, ofwel
$y \equiv 10y = 2 \cdot 5y \equiv 4 \equiv 1 \pmod 3$,
dus is er een z met $y = 1 + 3z$ en $x = 5y = 5(1 + 3z) = 5 + 15z$.
Substitutie hiervan in $x \equiv 5 \pmod{17}$ geeft $5 + 15z \equiv 5 \pmod{17}$, ofwel
$15z \equiv 0 \pmod{17}$, $z \equiv 120z = 8 \cdot 15z \equiv 0 \pmod{17}$ en
dus $z = 17k$ voor een zekere k en $x = 5 + 15z = 5 + 15 \cdot 17k = 5 + 255k$,
zodat ook nu volgt $x \equiv 5 \pmod{255}$

90 Als je de rest wilt weten bij deling van 2^{2003} door 7, dan wil je eigenlijk $2^{2003} \pmod 7$ weten.
$20 \equiv -1 \pmod 7$, dus $20^{2003} \equiv (-1)^{2003} \equiv -1 \equiv 6 \pmod 7$.
De rest is 6.

91 a. Om het laatste cijfer van $1! + 2! + \ldots + 100!$ te bepalen, bereken je

$1! + 2! + \ldots + 100! \pmod{10}$.

Nu is $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 \equiv 0 \pmod{10}$, $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720 \equiv 0 \pmod{10}$ en voor $n > 6$ geldt dat $n! = n \cdot (n-1) \cdot \ldots \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 0 \pmod{10}$ (het bevat minstens één factor 2 en minstens één factor 5, dus is het deelbaar door 10).

Dus $1! + 2! + \ldots + 100! \equiv 1! + 2! + 3! + 4! \equiv 1 + 2 + 6 + 24 \equiv 3 \pmod{10}$, het laatste cijfer is een 3.

b. Om de laatste twee cijfers van $1! + 2! + \ldots + 100!$ te bepalen, bereken je

$1! + 2! + \ldots + 100! \pmod{100}$.

Nu is $10! = 10 \cdot 9 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = 3628800 \equiv 0 \pmod{100}$ en voor $n > 10$ geldt dat $n! = n \cdot (n-1) \cdot \ldots \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 0 \pmod{100}$ (het bevat minstens twee factoren 2 en minstens twee factoren 5 (bijvoorbeeld uit de getallen 2, 5 en 10), dus is het deelbaar door $2^2 \cdot 5^2 = 100$).

$1! = 1$

$2! = 2 \cdot 1 = 2$

$3! = 3 \cdot 2 \cdot 1 = 3 \cdot 2! = 6$

$4! = 4 \cdot 3! = 24$

$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \equiv 20 \pmod{100}$

$6! = 6 \cdot 5! \equiv 6 \cdot 20 \equiv 20 \pmod{100}$

$7! = 7 \cdot 6! \equiv 7 \cdot 20 \equiv 40 \pmod{100}$

$8! = 8 \cdot 7! \equiv 8 \cdot 40 \equiv 20 \pmod{100}$

$9! = 9 \cdot 8! \equiv 9 \cdot 20 \equiv 80 \pmod{100}$

Dus $1! + 2! + \ldots + 100! \equiv 1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! + 9!$

$\equiv 1 + 2 + 6 + 24 + 20 + 20 + 40 + 20 + 80 \equiv 13 \pmod{100}$,

de laatste twee cijfers zijn 13.

c. Om de laatste drie cijfers van $1! + 2! + \ldots + 100!$ te bepalen, bereken je

$1! + 2! + \ldots + 100! \pmod{1000}$.

Nu is $15! = 15 \cdot 14 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = 1307674368000 \equiv 0 \pmod{1000}$ en voor $n > 15$ geldt dat $n! = n \cdot (n-1) \cdot \ldots \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 0 \pmod{1000}$ (het bevat minstens drie factoren 2 en drie factoren 5 (bijvoorbeeld uit de getallen 2, 5, 10, 12 en 15), dus is het deelbaar door $2^3 \cdot 5^3 = 1000$.)

$1! = 1$

$2! = 2 \cdot 1 = 2$

$3! = 3 \cdot 2 \cdot 1 = 3 \cdot 2! = 6$

$4! = 4 \cdot 3! = 24$

$5! = 5 \cdot 4! = 5 \cdot 24 = 120$

$6! = 6 \cdot 5! = 6 \cdot 120 = 720$

$7! = 7 \cdot 6! = 7 \cdot 720 = 5040 \equiv 40 \pmod{1000}$

$8! = 8 \cdot 7! \equiv 8 \cdot 40 \equiv 320 \pmod{1000}$

$9! = 9 \cdot 8! \equiv 9 \cdot 320 \equiv 2880 \equiv 880 \pmod{1000}$

$10! = 10 \cdot 9! \equiv 10 \cdot 880 \equiv 8800 \equiv 800 \pmod{1000}$

$11! = 11 \cdot 10! \equiv 11 \cdot 800 \equiv 8800 \equiv 800 \pmod{1000}$

$12! = 12 \cdot 11! \equiv 12 \cdot 800 \equiv 9600 \equiv 600 \pmod{1000}$

$13! = 13 \cdot 12! \equiv 13 \cdot 600 \equiv 7800 \equiv 800 \pmod{1000}$

$14! = 14 \cdot 13! \equiv 14 \cdot 800 \equiv 11200 \equiv 200 \pmod{1000}$

Dus $1! + 2! + \ldots + 100! \equiv 1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! + 9! + 10! + 11! + 12! + 13! + 14!$
$\equiv 1+2+6+24+120+720+40+320+880+800+800+600+800+200 \equiv 313 \pmod{100}$,
de laatste drie cijfers zijn 313.

92 a. $53 \equiv 1 \pmod{13}$, dus $53^{103} \equiv 1^{103} \equiv 1 \pmod{13}$
$103 \equiv -1 \pmod{13}$, dus $103^{53} \equiv (-1)^{53} \equiv -1 \pmod{13}$
Hieruit volgt $53^{103} + 103^{53} \equiv 1 + (-1) \equiv 0 \pmod{13}$,
dus $53^{103} + 103^{53}$ is deelbaar door 13.

b. $143 \equiv 3 \pmod{7}$
Volgens de kleine stelling van Fermat is $3^6 \equiv 1 \pmod{7}$, dus
$143^{32} \equiv 3^{32} \equiv (3^6)^5 \cdot 3^2 \equiv 1 \cdot 9 \equiv 2 \pmod{7}$ en
$143^{23} \equiv 3^{23} \equiv (3^6)^3 \cdot 3^2 \cdot 3^2 \cdot 3 \equiv 1 \cdot 9 \cdot 9 \cdot 3 \equiv 2 \cdot 2 \cdot 3 \equiv 5 \pmod{7}$, zodat
$143^{32} + 143^{23} \equiv 2 + 5 \equiv 0 \pmod{7}$, dus kun je $143^{32} + 143^{23}$ delen door 7.

c. 13 is een priemgetal, dus $9^{12} \equiv 1 \pmod{13}$ en $4^{12} \equiv 1 \pmod{13}$
$9^{240} = (9^{12})^{20} \equiv 1^{20} \equiv 1 \pmod{13}$
$9^2 = 81 \equiv 3 \pmod{13}$
$9^4 \equiv 3^2 \equiv 9 \pmod{13}$
$9^{244} = 9^{240} \cdot 9^4 \equiv 1 \cdot 9 \equiv 9 \pmod{13}$

$4^{120} = (4^{12})^{10} \equiv 1^{10} \equiv 1 \pmod{13}$

$4^2 = 16 \equiv 3 \pmod{13}$

$4^4 \equiv 3^2 \equiv 9 \pmod{13}$

$4^{124} = 4^{120} \cdot 4^4 \equiv 1 \cdot 9 \equiv 9 \pmod{13}$

$9^{244} - 4^{124} \equiv 9 - 9 \equiv 0 \pmod{13}$, dus is $9^{244} - 4^{124}$ deelbaar door 13.

93 a. $10 \equiv 1 \pmod{3}$, $10^2 \equiv 1^2 \equiv 1 \pmod{3}$ en $10^3 \equiv 1^3 \equiv 1 \pmod{3}$

b. $10^k \equiv 1^k \equiv 1 \pmod{3}$

c. $34567 = 3{\cdot}10^4{+}4{\cdot}10^3{+}5{\cdot}10^2{+}6{\cdot}10{+}7 \equiv 3{\cdot}1{+}4{\cdot}1{+}5{\cdot}1{+}6{\cdot}1{+}7 \equiv 3{+}4{+}5{+}6{+}7 \pmod{3}$

d. Elke macht van 10 is gelijk aan 1 modulo 3, dus modulo 3 is de som van de cijfers gelijk aan het getal zelf. Als de som van de cijfers deelbaar is door 3, dan is deze gelijk aan 0 modulo 3, dus het getal zelf is gelijk aan 0 modulo 3, ofwel het getal zelf is ook deelbaar door 3. Deze redenering kun je ook omgekeerd houden, dus is het getal deelbaar door 3 precies dan als de som van de cijfers dat ook is.

e. Ook $10 \equiv 1 \pmod{9}$, dus $10^k \equiv 1 \pmod{9}$. De redenering hierboven gaat dus ook op voor modulo 9 in plaats van modulo 3: een getal is deelbaar door 9 precies dan als de som van de cijfers deelbaar is door 9.

f. $10 \equiv -1 \pmod{11}$, dus voor oneven k is $10^k \equiv -1 \pmod{11}$, terwijl voor even k geldt $10^k \equiv 1 \pmod{11}$. Hieruit volgt bijvoorbeeld $34567 = 3{\cdot}10^4{+}4{\cdot}10^3{+}5{\cdot}10^2{+}6{\cdot}10{+}7 \equiv 3 \cdot 1 + 4 \cdot -1 + 5 \cdot 1 + 6 \cdot -1 + 7 \equiv 3 - 4 + 5 - 6 + 7 \pmod{11}$. Ofwel, algemeen: een getal is modulo 11 gelijk aan het eerste cijfer-het tweede cijfer+het derde cijfer-het vierde cijfer $+ \ldots$. Dus is een getal deelbaar door 11 precies dan als eerste cijfer-het tweede cijfer+het derde cijfer-het vierde cijfer $+ \ldots$ het ook is.

94 a. $9+0+8+3+1+8+8+6+1 = 44$ is niet deelbaar door 3 of 9, dus 908318861 is niet deelbaar door 3 of 9.

$9-0+8-3+1-8+8-6+1 = 10$ is niet deelbaar door 11, dus 908318861 is niet deelbaar door 11.

b. $1+4+6+6+8+7+8+3+0 = 43$ is niet deelbaar door 3 of 9, dus 146687830 is niet deelbaar door 3 of 9.

$1-4+6-6+8-7+8-3+0 = 3$ is niet deelbaar door 11, dus 146687830 is niet deelbaar door 11.

c. $5+1+4+7+0+1+9+5+1 = 33$ is deelbaar door 3, maar niet door 9, dus 514701951 is deelbaar door 3, maar niet door 9.

$5-1+4-7+0-1+9-5+1 = 5$ is niet deelbaar door 11, dus 514701951 is ook niet deelbaar door 11.

d. $4+0+5+8+0+9+6+4+2=38$ is niet deelbaar door 3 of 9, dus 514701951 is ook niet deelbaar door 3 of 9.

$5-1+4-7+0-1+9-5+1=5$ is niet deelbaar door 11, dus 514701951 is niet deelbaar door 11.

e. $7+3+3+8+1+2+3+1+2=30$ is deelbaar door 3, maar niet door 9, dus 733812312 is deelbaar door 3, maar niet door 9.

$7-3+3-8+1-2+3-1+2=2$ is niet deelbaar door 11, dus 733812312 is niet deelbaar door 11.

f. $4+3+9+9+1+9+8+1=44$ is niet deelbaar door 3 of 9, dus 43991981 is niet deelbaar door 3 of 9.

$4-3+9-9+1-9+8-1=0$ is deelbaar door 11, dus 43991981 is deelbaar door 11.

g. $3+3+9+3+6+2+5+8+6=45$ is deelbaar door 3 en door 9, dus 339362586 is deelbaar door 3 en door 9.

$3-3+9-3+6-2+5-8+6=13$ is niet deelbaar door 11, dus 339362586 is niet deelbaar door 11.

h. $9+9+5+4+6+6+3+4+0=46$ is niet deelbaar door 3 of 9, dus 995466340 is niet deelbaar door 3 of 9.

$9-9+5-4+6-6+3-4+0=0$ is deelbaar door 11, dus 995466340 is deelbaar door 11.

95 a. Modulo 12 krijgen we $0^2=0, 1^2=1, 2^2=4, 3^2=9, 4^2=16\equiv 4, 5^2=25\equiv 1$,
$6^2=36\equiv 0, 7^2=49\equiv 1, 8^2=64\equiv 4, 9^2=81\equiv 9, 10^2=100\equiv 4$ en $11^2=121\equiv 1$.

Dus de mogelijke uitkomsten zijn 0, 1, 4 en 9.

b. De uitkomsten van $5x^2$ modulo 12 zijn dan $5\cdot 0=0, 5\cdot 1=5, 5\cdot 4=20\equiv 8$ en
$5\cdot 9=45\equiv 9$, dus 0, 5, 8 en 9.

c. $8\cdot 0=0, 8\cdot 1=8, 8\cdot 2=16\equiv 4, 8\cdot 3=24\equiv 0, 8\cdot 4=32\equiv 8, 8\cdot 5=40\equiv 4$,
$8\cdot 6=48\equiv 0, 8\cdot 7=56\equiv 8, 8\cdot 8=64\equiv 4, 8\cdot 9=72\equiv 0, 8\cdot 10=80\equiv 8, 8\cdot 11=88\equiv 4$, allemaal mod 12.

Dus de mogelijke uitkomsten zijn 0, 4 en 8.

d. Zie de volgende opteltabel modulo 12: de mogelijke uitkomsten zijn 0, 1, 4, 5, 8 en 9.

	0	5	8	9
0	0	5	8	9
4	4	9	0	1
8	8	1	4	5

e. $23 \equiv 11 \pmod{12}$, maar 11 komt niet voor in de bij d. genoemde uitkomsten. Dus is er geen x te vinden met $5x^2 + 8x \equiv 23 \pmod{12}$, maar dan is er ook geen geheel getal x te vinden met $5x^2 + 8x = 23$.

96 a. Modulo 3 is $3x^2 + 14 \equiv 0 + 2 \equiv 2$.

Modulo 3 is $y \equiv 0$, $y \equiv 1$ of $y \equiv 2$.

Maar dan is $y^2 \equiv 0^2 \equiv 0$, $y^2 \equiv 1^2 \equiv 1$ of $y^2 \equiv 2^2 \equiv 4 \equiv 1$ (alles mod 3), dus nooit gelijk aan 2 modulo 3.

Dus zijn er geen x en y zodanig dat $3x^2 + 14 \equiv y^2 \pmod{3}$, dus heeft $3x^2 + 14 = y^2$ geen gehele oplossingen.

b. Modulo 7 is $7x^3 + 5 \equiv 5$.

Modulo 7 is $y \equiv 0$, $y \equiv 1$, $y \equiv 2$, $y \equiv 3$, $y \equiv 4$, $y \equiv 5$ of $y \equiv 6$.

Maar dan is $y^3 \equiv 0^3 \equiv 0$, $y^3 \equiv 1^3 \equiv 1$, $y^3 \equiv 2^3 \equiv 8 \equiv 1$, $y^3 \equiv 3^3 \equiv 27 \equiv 6$, $y^3 \equiv 4^3 \equiv 64 \equiv 1$, $y^3 \equiv 5^3 \equiv 125 \equiv 6$ of $y^3 \equiv 6^3 \equiv 216 \equiv 6$, dus nooit gelijk aan 5 modulo 7.

Dus zijn er geen x en y zodanig dat $7x^3 + 5 \equiv y^3 \pmod{7}$, dus heeft $7x^3 + 5 = y^3$ geen gehele oplossingen.

c. Modulo 4 is $x \equiv 0$, $x \equiv 1$, $x \equiv 2$ of $x \equiv 3$.

Maar dan is $x^2 \equiv 0^2 \equiv 0$, $x^2 \equiv 1^2 \equiv 1$, $x^2 \equiv 2^2 \equiv 4 \equiv 0$ of $x^2 \equiv 3^2 \equiv 9 \equiv 1$ (alles mod 4).

Dus is modulo 4 $x^2 \equiv 0$ of $x^2 \equiv 1$. Evenzo is natuurlijk modulo 4 $y^2 \equiv 0$ of $y^2 \equiv 1$.

Hieruit volgt dat modulo 4 $x^2 + y^2$ gelijk is aan 0, 1 of 2, dus nooit aan 3.

Er zijn derhalve geen x en y zodanig dat $x^2 + y^2 \equiv 3 \equiv n \pmod{4}$, dus heeft $x^2 + y^2 = n$ geen gehele oplossingen als $n \equiv 3 \pmod{4}$.

97 Modulo 4 is $x \equiv 0$, $x \equiv 1$, $x \equiv 2$ of $x \equiv 3$.

Maar dan is $x^2 \equiv 0^2 \equiv 0$, $x^2 \equiv 1^2 \equiv 1$, $x^2 \equiv 2^2 \equiv 4 \equiv 0$ of $x^2 \equiv 3^2 \equiv 9 \equiv 1$ (alles mod 4).

Dus is modulo 4 $x^2 \equiv 0$ of $x^2 \equiv 1$. Evenzo is natuurlijk modulo 4 $y^2 \equiv 0$ of $y^2 \equiv 1$.

Hieruit volgt dat modulo 4 $x^2 + y^2$ gelijk is aan 0 $(0+0)$, 1 $(1+0$ of $0+1)$ of 2 $(1+1)$.

Als z even is, dan is $z \equiv 0 \pmod{4}$ of $z \equiv 2 \pmod{4}$.

Maar dan is $z^2 \equiv 0^2 \equiv 0 \pmod{4}$ of $z^2 \equiv 2^2 \equiv 4 \equiv 0 \pmod{4}$, dus $z^2 \equiv 0 \pmod{4}$.

Dus $x^2 + y^2 \equiv z^2 \pmod{4}$ is alleen mogelijk als $x^2 \equiv 0 \pmod{4}$, dus als $x \equiv 0 \pmod{4}$ of als $x \equiv 2 \pmod{4}$, ofwel als x even is. Hetzelfde moet voor de y gelden, maar dan is ggd(x,y) minstens 2.

Dus $x^2 + y^2 = z^2$ heeft geen gehele oplossingen met even z en ggd(x,y)=1.

3 Moderne cryptografische systemen

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

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

c. Bob moet $\ln 7$ noemen.

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

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

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

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

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

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

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

c. Eva moet nu dus G_A en G_B kennen.

6 De stelling van Euler zegt dat $x^{\phi(n)} \equiv 1 \pmod{n}$ mits ggd(x,n)=1.
Maar dan is ook $x^{k\phi(n)} = (x^{\phi(n)})^k \equiv 1^k \equiv 1 \pmod{n}$ voor elk geheel getal k
en $x^{k\phi(n)+1} = x^{k\phi(n)} \cdot x \equiv 1 \cdot x \equiv x \pmod{n}$.
Als we dus een d kunnen vinden met de eigenschap dat $de = k\phi(n) + 1$,
dan is $(x^e)^d = x^{de} = x^{k\phi(n)+1} \equiv x \pmod{n}$: we hebben x teruggevonden.
Dit werkt dus als $de = k\phi(n) + 1$, ofwel als $1 = de - k\phi(n)$,
met andere woorden als ggd(e,$\phi(n)$)=1.

7 $(x^e)^d = x^{de} = x^{k\phi(n)+1} = x^{k\phi(n)} \cdot x = (x^{\phi(n)})^k \cdot x \equiv 1^k \cdot x \equiv 1 \cdot x \equiv x \pmod{n}$
Met het berekenen van $(x^e)^d \pmod{n}$ kun je dus x vinden!

8 a. Als g=ggd(e,$\phi(n)$, dan deelt g ook ieder veelvoud van e en van $\phi(n)$.

In het bijzonder deelt g dan ook de en $k\phi(n)$, maar dan ook $1 = de - k\phi(n)$. Dus moet $g = 1$.

b. Met het algoritme van Euclides kun je de ggd van $\phi(n)$ en e (dus 1) schrijven als een lineaire combinatie van $\phi(n)$ en e: $1 = de - k\phi(n)$. Hieruit haal je d.

c. We weten dat $de = k\phi(n) + 1$, ofwel $de \equiv 1 \pmod{\phi(n)}$.

Omdat ggd(e,$\phi(n)$)=1 geldt $e^{\phi(\phi(n))} \equiv 1 \bmod \phi(n)$ (neem $a = e$ en $m = \phi(n)$),

zodat $e^{\phi(\phi(n))-1} \cdot e = e^{\phi(\phi(n))} \equiv 1 \bmod \phi(n)$, en we $d \equiv e^{\phi(\phi(n))-1} \pmod{\phi(n)}$ kunnen nemen.

9 Als $n = p_1^{k_1} \cdot_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ de priemfactorontbinding van n is,
dan is $\phi(n) = p_1^{k_1-1} \cdot (p_1 - 1) \cdot p_2^{k_2-1} \cdot (p_2 - 1) \cdot \ldots \cdot p_m^{k_m-1} \cdot (p_m - 1)$.

10 Eva kan een aantal dingen doen.

- Ze kan voor alle getallen $i < n$ nagaan of ggd(i,n)=1 en daarmee $\phi(n)$ vinden. Vervolgens proberen $\phi(\phi(n))$ uit te rekenen (door voor alle getallen $i < \phi(n)$ na te gaan of ggd(i,$\phi(n)$)=1, of door de priemfactorontbinding van $\phi(n)$ te vinden). Daarna berekent ze $d \equiv e^{\phi(\phi(n))-1} \pmod{\phi(n)}$. Maar dat kost heel veel tijd aangezien n 200 cijfers lang is.

- Ze kan voor d elk der getallen $1, 2, 3, \ldots$ proberen, daarmee $(x^e)^d$ te bereken in de hoop zo x te vinden. Maar dan moet Eva waarschijnlijk heel veel getallen proberen (d is dan ongeveer 100 cijfers lang), dus dat kost ook heel veel tijd.

- Of ze kan voor alle mogelijke x proberen $x^e \pmod{n}$ uitrekenen in de hoop als uitkomst het onderschepte bericht te krijgen. Maar x is een getal kleiner of gelijk aan n, dus mogelijk ook 200 cijfers lang. Dit kost dus ook al heel veel tijd.

11 a. In dat geval is n snel te ontbinden, dus $\phi(n)$ en daarmee ook d snel te vinden. In dat geval is een onderschept bericht snel te ontcijferen.

b. Nee, hiermee is niet direct het RSA-systeem onveilig. Je moet alleen de getallen p en q nog groter maken, bijvoorbeeld elk 150 cijfers.

12 $n = 221 = 13 \cdot 17$, dus $\phi(221) = 12 \cdot 16 = 192$ en $\phi(192) = \phi(2^6 \cdot 3) = 2^5 \cdot 1 \cdot 2 = 2^6 = 64$.
Nu is $d \equiv 175^{64-1} \equiv 175^{63} \pmod{192}$.
$175^2 = 30625 \equiv 97 \pmod{192}$
$175^4 \equiv 97^2 \equiv 9409 \equiv 1 \pmod{192}$
$175^8 \equiv 1^2 \equiv 1 \pmod{192}$
$175^{16} \equiv 1^2 \equiv 1 \pmod{192}$
$175^{32} \equiv 1^2 \equiv 1 \pmod{192}$

$175^{63} = 175^{32} \cdot 175^{16} \cdot 175^8 \cdot 175^4 \cdot 175^2 \cdot 175 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 97 \cdot 175 \equiv 79 \pmod{192}$
Tenslotte is $x \equiv 84^{79} \pmod{221}$.
$84^2 = 7056 \equiv 205 \pmod{221}$
$84^4 \equiv 205^2 \equiv 42025 \equiv 35 \pmod{221}$
$84^8 \equiv 35^2 \equiv 1225 \equiv 120 \pmod{221}$
$84^{16} \equiv 120^2 \equiv 14400 \equiv 35 \pmod{221}$
$84^{32} \equiv 35^2 \equiv 1225 \equiv 120 \pmod{221}$
$84^{64} \equiv 120^2 \equiv 14400 \equiv 35 \pmod{221}$
$84^{79} = 84^{64} \cdot 84^8 \cdot 84^4 \cdot 84^2 \cdot 84 \equiv 35 \cdot 120 \cdot 35 \cdot 205 \cdot 84 \equiv 1 \cdot 35 \cdot 205 \cdot 84 \equiv 103 \cdot 84 \equiv 33 \pmod{221}$
dus $x = 33$.

13 -

14 Elke A vervang je door het rangnummer 1, wat je daarna telkens op dezelfde manier vercijfert. Elke A wordt dus vercijferd tot steeds hetzelfde getal. Zoiets geldt ook voor elk der andere letters.

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

b. Kun je dit lezen?

16 De codes van een aantal letters aan elkaar plakken en dit als één getal vercijferen.

17 a. Door de cijfers van dit getal op te delen in blokken van 3. Als het aantal cijfers geen drievoud is, dan moet je vooraan een 0 bijschrijven.

b. Er is een maximaal aantal ASCII-codes dat je achter elkaar kunt zetten om er één getal van te maken. Het getal moet namelijk kleiner zijn dan de n van de sleutel die je wilt gebruiken (anders zou het mogelijk zijn dat twee rijtjes ASCII-codes modulo n hetzelfde zijn, waardoor je bij ontcijfering alleen het kleinste rijtje terug kunt vinden. Het aantal ASCII-codes maal 3 moet dus kleiner zijn dan het aantal cijfers van het getal n.

18 a. $n = 1013 \cdot 401 = 406213$, $\phi(406213) = 1012 \cdot 400 = 404800$,
$\phi(404800) = \phi(2^6 \cdot 5^2 \cdot 11 \cdot 23) = 2^5 \cdot 1 \cdot 5 \cdot 4 \cdot 10 \cdot 22 = 140800$,
$d \equiv 123^{140799} \equiv 115187 \pmod{404800}$.

b. $41835^{115187} \equiv 71111 \pmod{406213}$
$218629^{115187} \equiv 101100 \pmod{406213}$
$385915^{115187} \equiv 33 \pmod{406213}$
Dus de boodschap in ASCII-codes luidt 071 111 101 100 033, ofwel in gewone tekst: Goed!

19 -