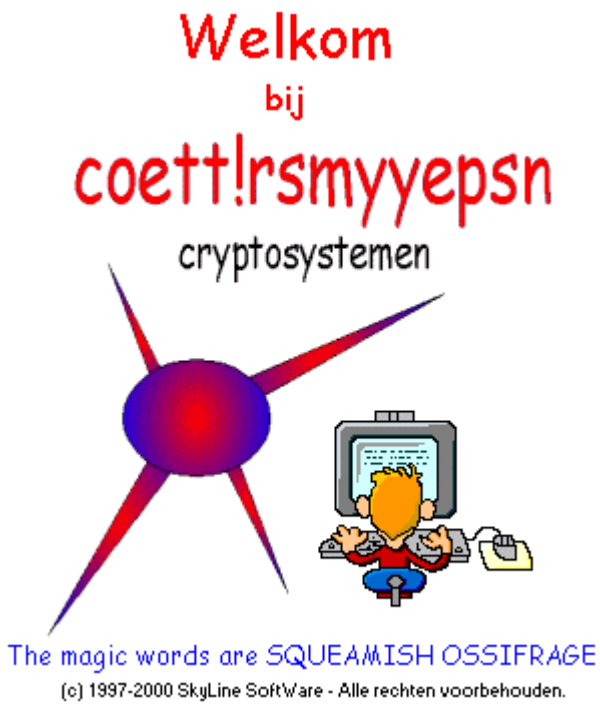

Docentenhandleiding

Inhoudsopgave

Priemfactoren

Hoe ontbind je een getal N in priemfactoren ?

Ga na of het getal N deelbaar is door de priemgetallen 2, 3, 5, 7, 11, 13, 17, ...
Vind je een priemfactor, dan deel je N door die priemfactor, en ga op dezelfde manier verder met wat je overhoudt.
Je kunt stoppen als een priemgetal bereikt waarvan het kwadraat groter is dan N.
Als je dan nog geen priemfactor gevonden hebt, dan is N zelf een priemgetal.

Deze methode is goed bruikbaar bij niet al te grote getallen.

Grote getallen

Bij grote getallen, zeg maar getallen van 30, 40 of meer cijfers, is de methode hierboven ongeschikt. De benodigde rekentijd neemt exponentieel toe met het aantal cijfers van N. Voor een getal van 10 cijfers zou je ongeveer 10.000 tests moeten uitvoeren. Grof gezegd: bij elke 2 cijfers meer wordt het aantal benodigde tests 10 keer zo groot.
Voor een getal van 20 cijfers heb je dus ongeveer 1.000.000.000 tests nodig. Als elke test één
miljoenste van een seconde zou duren, dan heb je ongeveer 17 minuten nodig. Voor een getal van 30 cijfers heb je ongeveer 1 · 1014 tests nodig. Dat zou dan ongeveer 3 jaar duren !
Een getal van 40 cijfers, 1 · 1019 tests, dat duurt ongeveer 316881 jaar !
En een getal van 100 cijfers ?

Geavanceerde methoden

In de getaltheorie zijn gelukkig methoden gevonden waarmee het allemaal wat sneller kan. Zo kun je met een gewone PC (Intel-486/33 MHz) een getal van 39 cijfers in ongeveer 1 minuut ontbinden in priemfactoren:

```
Input an integer =? 468608278103283944360822801872603992713
 468608278103283944360822801872603992713 =
 1937184826805989 * 241901687241645700028117
  0:01:10
```

(MPQS staat voor Multiple Polynomial Quadratic Sieve.) Dat duurde al met al 1 minuut en 10
seconden. Hier hadden we 'toevallig' te maken met een produkt van twee niet al te kleine
priemgetallen, meestal gaat het sneller.
Het ontbinden van
123128321321321873281738173817387138713871878787878787878787 duurt met MPQSHORS.UB maar 1 seconde:

```
 123128321321321873281738173817387138713871878787878787878787 =
 2971 * 19141 * 25013 * 865615252656838702443665816289164002008247409
  0:00:01
```

Primaliteit en factorisatie

Het probleem om een gegeven getal in priemfactoren te ontbinden wordt vaak in twee
deelproblemen gesplitst, die bekend staan onder de namen primaliteit en factorisatie.

Het primaliteitsprobleem bestaat eruit te beslissen of een gegeven getal een priemgetal is of niet. Hiervoor heeft men in de wiskunde verschillende methoden gevonden. Het nadeel is dat in het geval je niet te maken hebt met een priemgetal je nog niets weet over de ontbinding van het getal. Het voordeel van deze methoden is dat ze snel zijn.

Ook voor het factorisatieprobleem zijn verschillende methoden gevonden. Maar op dit moment is het zo dat de beste priemtests veel grotere getallen aankunnen dan de beste factorisatiemethoden. Het uitzoeken of een getal van 300 cijfers een priemgetal is of niet kost niet meer dan een paar minuten, maar het factoriseren van zulke grote getallen is, zelfs met de allersnelste methoden op de allerkrachtigste supercomputers volstrekt ondoenlijk.

Grof gezegd kunnen we dat samenvatten als:

Priemtesten gaat 'snel'
Factoriseren gaat 'langzaam'

Dit gegeven heeft belangrijke cryptografische toepassingen mogelijk gemaakt. Een voorbeeld daarvan is het RSA-systeem, dat in 1978 door Rivest, Shamir en Adleman bedacht is en nog steeds gebruikt wordt.

Literatuur

- Het ontbinden van grote getallen in priemfactoren, H.W.Lenstra, Jr, Nieuwe Wiskrant, september 1995.
- Pasjes en Pincodes, J. v.d. Craats, ...
- Basismethoden cryptografie, J.A.C. van der Lubbe, Delfse Univeristaire Pers, Delft, 1994.
- Cursus discrete wiskunde, deel 3: Getaltheorie, E.M. van der Vrie e.a., Open Universiteit, Heerlen, 1989
- The lore of large numbers, P.J. Davis, Mathematical Association of America, Yale University, 1961.
- Nieuwe Wiskunde, E.J. Wijdeveld, Dutch Efficiency Bureau, Pijnacker, 1969.
- Number Theory in Science and Communication, M.R.Schroeder, ...

Software

Bij het lespakketje kunnen de volgende programma's worden gebruikt:

UBasic

UBasic is een variant van BASIC. Met het programma kan je heel handig met grote getallen rekenen. Vooral wat getaltheorie betreft zijn er zeer veel interessante mogelijkheden. De bijgeleverde programma's (priemtests en factorisatie) maken gebruik van moderne methoden. Het programma is 'freeware', dus gratis en mag worden verspreid.

Numbers

Numbers is een (gratis) engelstalig programma waarmee je allerlei dingen op het gebied van getaltheorie kan doen. Van GGD tot PRIEMTESTS, van FIBONACCIGETALLEN tot RSA.

Derive

Het ontbinden in priemfactoren gaat met Derive natuurlijk erg makkelijk.

Internet

Docent en leerlingen kunnen ondersteuning krijgen via Internet.
Neem eens een kijkje op http://skyline.www.cistron.nl/crypto
Voor meer informatie kunt u emailen naar skyline@cistron.nl

Op de internetpagina en de CD-rom kunt u verwijzingen vinden naar andere pagina's over cryptografie. De software staat op de CD-rom. De programma’s kunnen vanaf de CD-rom worden uitgevoerd.

Achtergronden RSA-systeem

Bij het RSA-systeem, zoals dat in het lespakket ter sprake komt, spelen de variabelen n, e en d een belangrijke rol.
Iedere persoon heeft drie sleutels, twee openbare sleutels (n en e) en één geheime sleutel (d).
Deze sleutels leveren de exponenten en de modulus voor de twee functies waarmee cijferteksten versleuteld en ontsleuteld kunnen worden.

openbare sleutel: $f(x) = x^e \pmod n$
geheime sleutel: $g(x) = x^d \pmod n$

Hierbij is x de cijfertekst die versleuteld of ontsleuteld moet worden.

Nu is het, in het algemeen, niet mogelijk om de geheime functie g af te leiden uit de functie f. Deze functie g is in feite de inverse van f.

Voorbeeld:
$f(x) = x^5 \pmod{4198350484237446659}$
Wat is de inverse van f ?

Dit lijkt een eenvoudig probleem, maar dat is het niet. Voor het vinden van de inverse van f heb je in ieder geval een priemontbinding nodig van de modulus. Als men nu deze modulus groot genoeg kiest, is het vinden van de inverse van f niet te doen, omdat het vinden van de priemontbinding voor hele grote getallen niet te doen is.

In het geval men wel de priemontbinding van de modulus vindt:
$n = 4198350484237446659 = 133990427 \cdot 31333212217$
$p = 133990427$
$q = 31333212217$
$(p - 1)(q - 1) = 133990426 \cdot 31333212216 = 4198350452770244016$

Nu geldt dat
$d = \text{MODINV}(5, 4198350452770244016) = 3358680362216195213$

Waarmee de inverse van f gelijk is aan

$g(x) = x^{3358680362216195213} \pmod{4198350484237446659}$

Nu hebben we hier te maken met een modulus van slechts 20 cijfers. In dat geval in het vinden van de priemontbinding van *n* nog wel te doen.

Antwoorden en uitwerkingen van de opdrachten

1.
a. ♏
b. ■

2.
a. Rechtsonderbeginnend en dan zigzaggend naar linksboven toe.
b. sen more money
c. de sleutel zelf....

3.
a. 3x5 of 5x3 dus 5! + 3! = 126
b. ik ga niet meer mee
c. zie b.

4. de kat zit in de boom
5. ibm
6. r bestaat geen getal *c* zodat 24 = 0 · *c*

7.
a. 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180 en 360.
b. 1, 7, 11, 13, 77, 91, 143 en 1001
c. 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 en 1024
d. 1 en 17

8. 1001 = 7 · 11 · 13 6378 = 2 · 3 · 1063

9.
a. i. n = 5 ii. n = 4 iii. n = 1
c. de grootste gemeenschappelijke deler

10.
a. $\frac{5}{8}$
b. 12
c. deel teller en noemer door 12 (= g.g.d.)

11.

a	**b**	**rel.priem**
40	78	ee
256	243	ja
100	45	nee
6	21	nee
1	1	ja
44	11.111	nee

12. 10 + (-3) + 14 + 2 =23

13.
a. nee
b. nee
c. nee
d. nee

14.
a. 2
b. 6
c. zie achterin
d. 3
e. kan niet
f. dat e. niet kan. 4 en 6 zijn niet relatief priem

15. 554
16. klopt
17. 9

18.
a. i. x = 23 ii. x = 1008
b. nee, 100 is geen priemgetal

19. 5 , 13 en 25
20. ik zou het niet weten
21. je kunt de versleutelse tekst niet terug vertalen

22.
a. 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 en 25
b. 11
c. 26
d. $11 \cdot 26 = 286$

23. $(15 \cdot (x - 10) \bmod 26 = (15 \cdot x - 150) \bmod 26 = (15 \cdot x + 6) \bmod 26$

24.
a. **g** en **x** komen het meeste voor. x = e en g is de spatie (xx komt ook voor!)
b. $f(x) = 19 \cdot x + 15$
$f^{-1}(x) = 26 \cdot x + 15$
c. wie dit leest is gek

25.
a. voor elke mogelijke ‘verbinding’ heb je een andere sleutel nodig
b. 15, 105, 499500, $\frac{1}{2} \cdot n \cdot (n-1)$
c. 1999

26.
a. $f(x) = x - 2$

b. $f(x) = \frac{1}{2}x$

c. $f(x) = \frac{1}{2}x^2$

d. $f(x) = \sqrt{\frac{x}{2}} + 3$

27.
a. 11 en 17
b. 31 en 37
c. 97 en 167

28.
a. 6, 15, 3000 en 3n
b. 3 en 3

29. 565
30. 5376
31. 62

32.
a. 4451
b. 4151

33. als Piet een bericht naar Quintin stuurt moet ze $\mathbf{G_p}$ en $\mathbf{O_p}$ weglaten.
34 de cijfertekst voordat Quiten de openbare sleutel van Piet er op los laat.
of wel: $\mathbf{G_q(O_q(G_p(x)))}$
35

p	q	(p-1)(q-1)	d
1049	12347	12938608	1427
1237	8893	10990512	5965
2237	4447	9941256	3889
3347	3359	11235868	2791

36.
a. A = 01, B = 02, C = 03, enzovoort....
b. 10622057
c. nee, want Catja kent de geheime sleutel van Adrie niet.

37. kom ook
38. ga niet
39. ga fietsen

EINDE

Eindtoets

Opdracht 1

a. Bereken ggd(120,88).
b. Geef alle delers van 315.
c. Ontbind 27720 in priemfactoren.
d. Bereken $115 \cdot 89 \pmod 9$
e. Bereken $32^{54} \pmod{12}$

Opdracht 2

Beschouw onderstaande tekst:

“Mfof efple phu jnsmfu nbrfofe du ifflahsf efple.”

We vermoeden dat hier sprake is van de Julius Caesar methode. Dit betekent dat gebruik is gemaakt van de functie: **$f(x) = a \cdot x + b \pmod{26}$**
Op grond van analyses van groepen van letters bestaat het vermoeden dat:

‘e’ wordt afgebeeld op **‘f’**
‘t’ wordt afgebeeld op **‘e’**

a. Bepaal de waarden van **a** en **b.**
b. Ontcijfer bovenstaand bericht.

Opdracht 3

Aan het einde van deze toets staat “**Zknhz’**. Dit staat natuurlijk ‘**Einde’**.
Dit woord is versleuteld met een **substitutie-alfabet** met 29 letters.

a. Bepaal de sleutel die gebruikt is.
b. Schrijf je eigen voornaam in dit geheimschrift.

Opdracht 4

Hieronder staat een gedeelte uit het sleutelboek van een RSA-clubje:

	Sleutel 1	**Sleutel 2**
...		
Daniël	87415	17
Moniek	1005973	31
...		

Je gebruikt de volgende vercijfering:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

De getallen zij zo gekozen dat krake van deze sleutels goed te doen is.

a. Bepaal m.b.v. een tabel **p, q** en de **geheime sleutel** van Daniël en Moniek.
b. Moniek stuurt het bericht **'bel'** naar Daniëel. Vercijfer dit bericht en versleutel de cijfertekst zonder signeren.
c. Daniëel stuurt Moniek het gesigneerde bericht '**nee'** terug. Bepaal de versleutelde cijfertekst die Daniël verstuurt.
d. Een dag later ontvangt Daniël 762653. Welk bericht stuurt Moniek aan Daniël?
e. Hoe kom je er achter of het bericht dat je ontvangt gesigneerd is of niet?

Zknhz

Antwoorden eindtoets.

Opdracht 1

a. 8
b. 1, 3 ,5, 7, 9, 15, 21 ,35, 45, 63, 105 en 315
c. $2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
d. 2
e. 4

Opdracht 2

a. a = 11 en b = 1 of a = 19 en b = 7
b. deze tekst kan worden omgezet in leesbare tekst

Opdracht 3

a. a = 18 en b = 11 of a = 21 en b = 30
b. kan van alles zijn.....☺

Opdracht 4

a.

	p	**q**	**d**
Daniël	983	991	91.499
Moniek	997	1010	48.579

b. 884288
c. 670293
d. zak
e. pas eerst je eigen geheime sleutel toe. lijkt het nergens op, pas dan de openbare sleutel van de afzender toe.