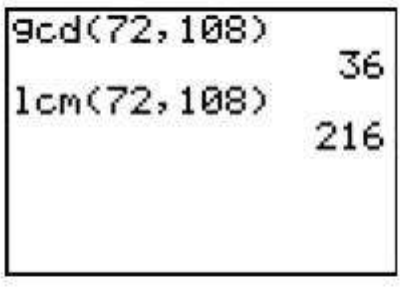
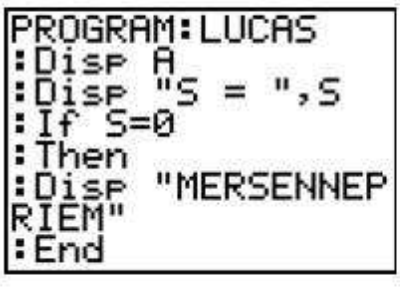
T³ VLAANDEREN

Getalmysteries met de TI-84

16de T³ Symposium

Philip Bogaert





Texas Instruments

Getalmysteries

1. Modulorekenen

1.1. Deelbaarheid

definitie

Als $a,n \in \mathbb{Z}$ dan noteren we de equivalente uitspraken “n is een deler van a”, “a is deelbaar door n” en “n is een veelvoud van a” als $n \mid a$.

$$n \mid a \;\Leftrightarrow\; \exists q \in \mathbb{Z} : a = qn$$

q wordt het quotiënt genoemd van de gehele deling van a door n.

gevolgen

- Als $n \mid a$ dan ook $-n \mid a$ en $n \mid -a$.
- Als n een deler is van a dan is het quotiënt q van de gehele deling van a door n eveneens een deler van a.
- ± 1 en $\pm a$ zijn delers van a.

praktische methode voor het opsporen van alle delers van een geheel getal

Als we alle delers van een geheel getal a willen bepalen dan gaan we na welke natuurlijke getallen tussen 1 en m, met m het grootste natuurlijk getal waarvoor $m \leq \sqrt{|a|}$, deler zijn. Is een natuurlijk getal k tussen 1 en m deler, dan is –k ook een deler en zijn $\pm$q, met q het quotiënt bij deling van a door k, eveneens delers.

De verzameling van de delers van een geheel getal a stellen we voor door $\mathrm{del}\, a$:

$$\mathrm{del}\, a = \{n \,;\, n \in \mathbb{Z} \wedge n \mid a\}$$

De verzameling van de gehele veelvouden van een geheel getal a stellen we voor door $a\mathbb{Z}$:

$$a\mathbb{Z} = \{n \,;\, n \in \mathbb{Z} \wedge a \mid n\}$$

eigenschappen/stellingen i.v.m. deelbaarheid

- transitiviteit: $a \mid b \ \wedge \ b \mid c \ \Rightarrow \ a \mid c$
- de absolute waarde van een deler van een van nul verschillend geheel getal is kleiner dan of gelijk aan de absolute waarde van dit getal: $a, n \in \mathbb{Z}_0 : \ n \mid a \ \Rightarrow \ |n| \leq |a|$
- een deler van een geheel getal is ook een deler van elk geheel veelvoud van dit getal: $n \mid a \ \Rightarrow \ n \mid ka \quad (k \in \mathbb{Z})$
- een deler van twee gehele getallen is ook een deler van hun som: $n \mid a \ \wedge \ n \mid b \ \Rightarrow \ n \mid a+b$
- een deler van twee gehele getallen is ook een deler van elke lineaire combinatie met gehele coëfficiënten van deze getallen: $n \mid a \ \wedge \ n \mid b \ \Rightarrow \ n \mid ka+lb \quad (k, l \in \mathbb{Z})$

1.2. Perfecte en bevriende getallen

Voor elk natuurlijk getal n groter dan nul definiëren we :

$d(n)$: het aantal delers van n
$s(n)$: de som van alle (natuurlijke) delers van n, behalve n
$\sigma(n)$: de som van alle delers van n, m.a.w. $\sigma(n) = s(n) + n$

n	delers	$d(n)$	$s(n)$	$\sigma(n)$
1	1	1	0	1
2	1,2	2	1	3
3	1,3	2	1	4
4	1,2,4	3	3	7
5	1,5	2	1	6
6	1,2,3,6	4	6	12
7	1,7	2	1	8
8	1,2,4,8	4	7	15
9	1,3,9	3	4	13
10	1,2,5,10	4	8	18
11	1,11	2	1	12
12	1,2,3,4,6,12	6	16	28

perfecte getallen

Een perfect getal of volmaakt getal is een natuurlijk getal dat gelijk is aan de som van zijn echte delers (dus buiten zichzelf, 1 wordt als echte deler meegerekend).

n is perfect $\Leftrightarrow$ $s(n)=n$ $\Leftrightarrow$ $\sigma(n)=2n$

bevriende getallen

Van twee natuurlijke getallen n en m wordt gezegd dat ze bevriend zijn als de som van de echte delers van n gelijk is aan m, terwijl de som van de echte delers van m samen het getal n opleveren.

n en m zijn bevriend $\Leftrightarrow$ $s(n)=m \ \wedge \ s(m)=n$

1.3. De Euclidische deling of delingsalgoritme

Als $a\in\mathbb{Z}$ en $n\in\mathbb{N}_0$ dan bestaat er een uniek stel van gehele getallen r en q zodat $a=qn+r$ met $0\le r<n$.

q wordt het quotiënt en r de rest genoemd van de deling van a door n in $\mathbb{Z}$. De rest r van a na gehele deling door n die aan het delingsalgoritme voldoet noemen we ook "*a modulo n*" en noteren we a mod n.

Als $n \mid a$ dan is de rest $r=a \bmod n=0$

Als $n \nmid a$ dan is de rest verschillend van nul en $r=a \bmod n\in\{1,2,...,n-1\}$

1.4. Grootste gemene deler

definitie

Het natuurlijk getal d is de grootste gemene deler van twee van nul verschillende natuurlijke getallen a en b als en slechts als d de grootste is van de gemeenschappelijke delers van a en b.

$$\begin{array}{c} \text{ggd}(a,b)=d \\ \Updownarrow \\ d\in \text{del}\,a\cap\text{del}\,b \ \wedge \ \forall c\in \text{del}\,a\cap\text{del}\,b: c\le d \end{array}$$

eigenschappen/stellingen i.v.m. ggd

- de gemeenschappelijke delers van twee van nul verschillende natuurlijke getallen a en b ($a \geq b$) zijn dezelfde als de gemeenschappelijke delers van b en de rest van de Euclidische deling van a door b.

  Als: $a, b \in \mathbb{N}_0 \qquad a \geq b$
  $a = bq + r \qquad 0 \leq r < b \qquad q \in \mathbb{N}$

  dan: $c \mid a \wedge c \mid b \;\Leftrightarrow\; c \mid b \wedge c \mid r$

- de grootste gemene deler van twee van nul verschillende natuurlijke getallen a en b is de kleinste en van nul verschillende lineaire combinatie van a en b met gehele coëfficiënten.

  Als: $a, b \in \mathbb{N}_0$
  $M = \{xa + yb;\ x, y \in \mathbb{Z} \wedge xa + by > 0\}$

  dan: $d = \text{ggd}(a,b) = \min(M)$

- gegeven twee gehele getallen a en b, dan bestaan er gehele getallen x en y zodat $ax + by = \text{ggd}(a,b)$. **(stelling van Bézout)**

- de vergelijking $ax + by = c$ heeft en oplossing (in $\mathbb{Z}$) als en slechts als $\text{ggd}(a,b) \mid c.$

- een gemeenschappelijke deler van twee getallen is ook een deler van hun grootste gemene deler en omgekeerd.

  Als: $a, b \in \mathbb{N}_0$
  $d = \text{ggd}(a,b)$ dan: $c \in \text{del}\, a \cap \text{del}\, b \;\Leftrightarrow\; c \mid d$

onderling ondeelbare getallen

Twee gehele getallen a en b zijn onderling ondeelbaar als en slechts als $\text{ggd}(a,b) = 1$.

Als men twee getallen door hun ggd deelt, dan zijn de quotiënten onderling ondeelbaar.

1.5. Ontbinding in priemfactoren

priemgetal

Een positief geheel getal p > 1 is een priemgetal als en slechts als 1 en p de enige positieve delers zijn van p.

eigenschappen/stellingen i.v.m. priemgetallen

- elk natuurlijk getal a > 1 is deelbaar door een priemgetal
- als een priemgetal een product van natuurlijke getallen deelt, dan is minstens één van de factoren deelbaar door dit priemgetal
- er bestaat geen grootste priemgetal, m.a.w. er zijn oneindig veel priemgetallen (stelling van Euclides)

hoofdstelling van de getaltheorie

Elk natuurlijk getal a $\geq$ 2 kan, op de volgorde van de factoren na, op een unieke wijze geschreven worden als een product van priemgetallen.

$\forall a \in \mathbb{N}: \; a = p_1^{n_1}.p_2^{n_2}...p_k^{n_k}$ met p_1 t.e.m. p_k priemgetallen en n_1 t.e.m. n_k natuurlijke exponenten groter dan of gelijk aan 1.

1.6. Kleinste gemene veelvoud

Het van nul verschillend natuurlijk getal m is het kleinste gemene veelvoud van twee natuurlijke getallen a en b als en slechts als m het kleinste is van de strikt positieve gemeenschappelijke veelvouden van a en b.

$$\text{kgv}(a,b) = m$$
$$\Updownarrow$$
$$m \in a\mathbb{Z} \cap b\mathbb{Z} \;\wedge\; \forall c \in \mathbb{N}_0 \cap (a\mathbb{Z} \cap b\mathbb{Z}): m \leq c$$

praktische methode voor het berekenen van de ggd en het kgv van twee natuurlijke getallen

De grootste gemene deler van 2 natuurlijke getallen groter dan 1 kan als volgt worden gevonden:

- ontbind de 2 getallen in priemfactoren
- maak het product van de gemeenschappelijke factoren, ieder genomen met zijn kleinste exponent

Het kleinste gemene veelvoud van 2 natuurlijke getallen groter dan 1 kan als volgt worden gevonden:

- ontbind de 2 getallen in priemfactoren
- maak het product van alle factoren, ieder genomen met zijn grootste exponent

verband tussen a, b, ggd(a,b) en kgv(a,b)

- het product van 2 natuurlijke getalln is gelijk aan het product van hun grootste gemene deler en hun kleinste gemeen veelvoud

$$\forall a,b \in \mathbb{N}: \ \text{ggd}(a,b).\text{kgv}(a,b) = a.b$$

1.7. Congruentie modulo n

Stel $n \neq 0$ een natuurlijk getal en a en b twee gehele getallen, dan is a congruent aan b modulo n als en slechts als $n \mid (b-a)$.

a congruent aan b modulo n noteren we als $a \equiv b \pmod{n}$.

$$a \equiv b \pmod{n} \ \Leftrightarrow \ n \mid (b-a) \ \Leftrightarrow \ \exists q \in \mathbb{Z}: a = b + qn$$

eigenschappen/stellingen i.v.m. congruentie modulo n

Stel n een positief geheel getal. “Congruent modulo n” is een relatie met de volgende eigenschappen:

- Reflexiviteit: $a \equiv a \pmod{n}$
- Symmetrie: $a \equiv b \pmod{n} \ \Rightarrow \ b \equiv a \pmod{n}$
- Transitiviteit: $a \equiv b \pmod{n} \ \wedge \ b \equiv c \pmod{n} \ \Rightarrow \ a \equiv c \pmod{n}$

Deze eigenschappen toont eigenlijk aan dat de verzameling van de gehele getallen voor elke positieve $n \neq 0$ gepartitioneerd wordt in n verschillende congruentieklassen modulo n, ook wel restklassen genoemd. De restklasse van a modulo n noteren we als $\overline{a} \pmod{n}$ of kortweg $\overline{a}$.

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$$

De verzameling van alle restklassen modulo n noteren we als $\mathbb{Z}/n\mathbb{Z}$.

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$$

1.8. Bewerkingen modulo n

stelling

Stel dat $a_1 \equiv a_2 \pmod{n}$ en $b_1 \equiv b_2 \pmod{n}$ dan geldt:

- $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$
- $a_1 - b_1 \equiv a_2 - b_2 \pmod{n}$
- $a_1 b_1 \equiv a_2 b_2 \pmod{n}$

inverse

Een inverse van $a \pmod{n}$ is een getal x zodat $a.x \equiv 1 \pmod{n}$.

Met behulp van een vermenigvuldigingstabel kunnen we de restklassen opsporen die een symmetrisch element hebben voor de vermenigvuldiging. Als een restklasse een symmetrisch element heeft voor de vermenigvuldiging kunnen we in zo'n tabel ook aflezen welke restklasse dat symmetrisch element is.

Voorbeeld de vermenigvuldigingstabel voor $\mathbb{Z}/10\mathbb{Z}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{2}$	$\bar{5}$	$\bar{8}$	$\bar{1}$	$\bar{4}$	$\bar{7}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{8}$	$\bar{5}$	$\bar{2}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{9}$	$\bar{0}$	$\bar{9}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

In de vermenigvuldigingstabel voor $\mathbb{Z}/10\mathbb{Z}$ zien we dat de rijen (kolommen) met rijkoppen (kolomkoppen) $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ een $\bar{1}$ bevatten. Dit betekent dat deze 4 van de 10 restklassen een symmetrisch element voor de vermenigvuldiging hebben. Deze symmetrische elementen lezen we af op de corresponderende kolomkoppen (rijkoppen). We vinden voor $\mathbb{Z}/10\mathbb{Z}$:

$$\bar{1}^{-1} = \bar{1} \;;\; \bar{3}^{-1} = \bar{7} \;;\; \bar{7}^{-1} = \bar{3} \;;\; \bar{9}^{-1} = \bar{9}$$

stelling

Een inverse van $a \pmod{n}$ bestaat als en slechts als $\text{ggd}(a,n) = 1$.

1.9. Priemgetallen en modulorekenen

Voor een priemgetal p geldt:

- $(a+b)^p \equiv a^p + b^p \pmod{p}$
- $n^p \equiv n \pmod{p}$ (kleine stelling van Fermat)
- $(p-1)! \equiv -1 \pmod{p}$ (stelling van Wilson)

1.10. De stelling van Euler

definitie

De functie ϕ van Euler telt voor elk natuurlijk getal n hoeveel kleinere positieve getallen er zijn die geen factor met n gemeen hebben.

$\phi(n)$ = aantal getallen $1 \le i \le n$ met $ggd(i,n) = 1$

formule van Euler voor

Voor en getal $n = p^a q^b r^c s^d$ (p,q,r,s zijn priemfactoren en a,b,c,d zijn natuurlijke exponenten groter dan nul) geldt dat:

$$\phi(n) = p^{a-1} q^{b-1} r^{c-1} s^{d-1} . (p-1)(q-1)(r-1)(s-1)$$

stelling van Euler

Als a geen factor gemeen heeft met n dan geldt dat $a^{\phi(n)} \equiv 1 \pmod{n}$

1.11. De Chinese reststelling

Wanneer een Chinese boer zijn eieren 's morgens op de markt op rijtjes van 3 legt, heeft hij één ei over. Legt hij dezelfde eieren op rijtjes van 5 heeft hij er 2 over en legt hij ze op rijtjes van 7 heeft hij er 3 over. Hoeveel eieren heeft de boer minstens?

- Stel dat s en t twee natuurlijke getallen zijn met $\text{ggd}(s,t) = 1$. Als nu $x \equiv y \pmod{s}$ en ook $x \equiv y \pmod{t}$, dan geldt $x \equiv y \pmod{st}$.

- Stel dat $n = s \cdot t$ met $\text{ggd}(s,t) = 1$. Dan heeft het stelsel

$$\begin{cases} x \equiv a \pmod{s} \\ y \equiv b \pmod{t} \end{cases}$$

een unieke oplossing in $\mathbb{Z} / n\mathbb{Z}$.

De oplossing van het Chinese raadsel kunnen we nu herschrijven als volgt:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Uit $x \equiv 1 \pmod{3}$ volgt dat $x = 3y + 1$, invullen in de tweede vergelijking geeft:

$$3y + 1 \equiv 2 \pmod{5}$$

Van beide zijden 1 aftrekken en met 2 vermenigvuldigen geeft:

$$\begin{aligned} & 3y + 1 \equiv 2 \pmod{5} \\ \Leftrightarrow\ & 3y \equiv 1 \pmod{5} \\ \Leftrightarrow\ & 6y \equiv 2 \pmod{5} \\ \Leftrightarrow\ & y \equiv 2 \pmod{5} \end{aligned}$$

Zodat $y = 5z + 2$ en dus $x = 3y + 1 = 3(5z + 2) + 1 = 15z + 7$. Invullen in de derde vergelijking geeft:

$$15z + 7 \equiv 3 \pmod 7$$
$$\Leftrightarrow 15z \equiv 3 \pmod 7$$
$$\Leftrightarrow z \equiv 3 \pmod 7$$

M.a.w. $z = 7u + 3$ en dus $x = 15(7u + 3) + 7 = 105u + 52$. De kleinste gehele waarde die hier aan voldoet is 52 (eieren).

Hoeveel eieren had de boer minstens als blijkt dat als hij zijn eieren ook nog eens op rijtjes van 9 legt, hij 4 eieren over heeft?

2. Modulorekenen met de TI-84

2.1. Modulorekenen

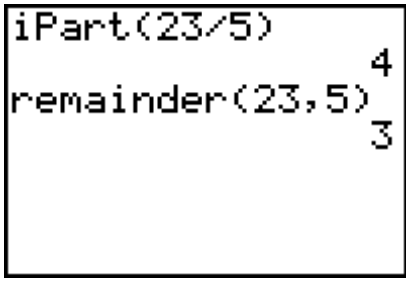
De rest en het quotiënt na deling van a door n in $\mathbb{N}$ worden bij de TI-84 respectievelijk gegeven via Math Num 0:remainder en Math Num 3:iPart.

M.a.w. a = q.n + b

Dan is q = iPart(a / n) en b = remainder(a , n)

Voorbeeld:

23 = 4.5 + 3



2.2. Rekenen met grote getallen

Modulorekenen wordt in het dagelijkse leven meer gebruikt dan we soms denken. De getallen waarmee gerekend wordt zijn echter cijferreeksen die soms meer dan 15 cijfers lang zijn.

780546 320783 111400 ≡ ?? (mod 97)

Dit probleem lossen we als volgt op:

$10000 \equiv 9 \pmod{97}$

En dus:

$10000^2 = 9^2$

$10000^3 = 9^3$

$10000^n = 9^n$

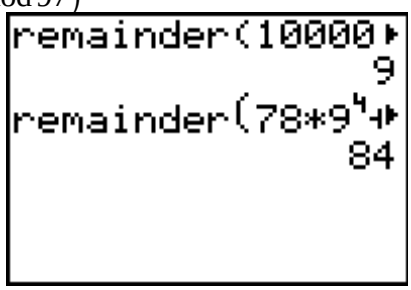
Zodat

78 0546 3207 8311 1400

$\equiv 78.9^4 + 0546.9^3 + 3207.9^2 + 8311.9 + 1400 \pmod{97}$

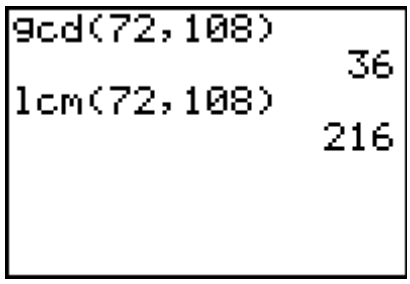
$\equiv 1245758 \pmod{97}$

$\equiv 84 \pmod{97}$



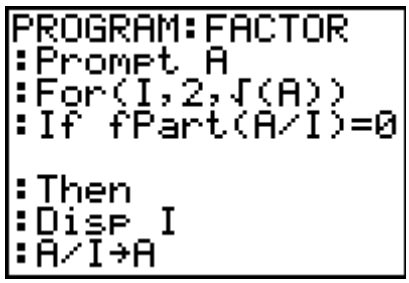
2.3. Grootste gemene deler – Kleinste gemene veelvoud

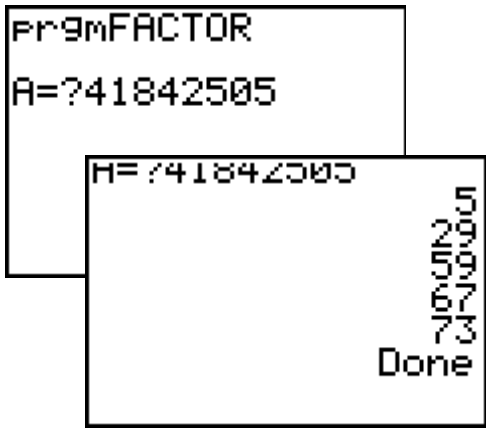
GGD vinden we bij Math Num 9:gcd
en KGV via Math Num 8:lcm



2.4. Ontbinden in priemfactoren

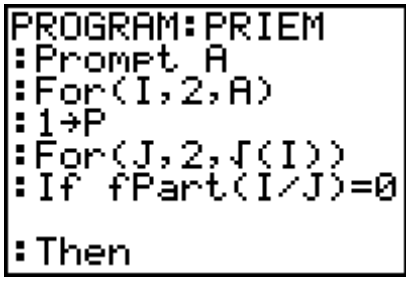
PROGRAM:FACTOR
:Prompt A
:For (I,2,$\sqrt{A}$)
:If fPart(A / I) = 0
:Then
:DISP I
:A / I → A
:I – 1 → I
:End
:If A = 1
:Then
:Stop
:End
:End
:If A <> 1
:Then
:Disp A
:End
:Stop

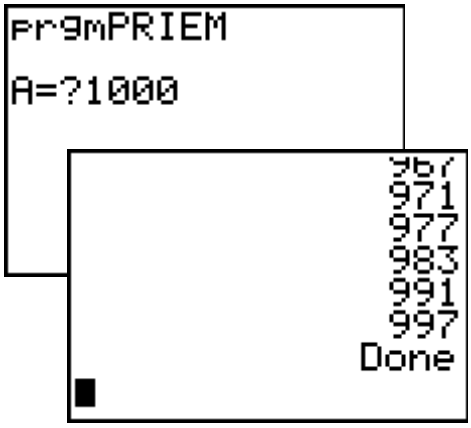




2.5. Priemgetallen van 2 tot A

PROGRAM:PRIEM
:Prompt A
:For (I,2,A)
:1→ P
:For (J,2,$\sqrt{I}$)
:If fPart(I / J) = 0
:Then
:0 → P
:End
:End
:If P = 1
:Then
:Disp I
:End
:End
:Stop





3. Toepassingen

3.1. rekeningnummers

Een Belgisch rekeningnummer (Belgian Bank Account Number of BBAN) bestaat uit 12 cijfers, verdeeld in drie groepen gescheiden door liggende streepjes: een groep van 3 cijfers, een groep van 7 cijfers en een groep van 2 cijfers. bvb. 780-5463207-83

- een eerste blok van drie cijfers, die informatie geven over de bank
- een blok van zeven cijfers, het eigenlijke rekeningnummer bij die bank
- een laatste blok met twee controlecijfers, deze twee cijfers zijn de rest (modulo) bij deling door 97 van het getal dat gevormd wordt door de 10 voorafgaande cijfers. (indien de rest 0 is, wordt 97 als controlegetal gebruikt)

Ga na dat: 7805463207 mod 97 = 83

IBAN-nummers

Een International Bank Account Number (IBAN) wordt gebruikt om internationale transacties tussen rekeningen en banken gelegen in verschillende landen vlotter te laten verlopen.

Het IBAN telt maximaal 34 alfanumerieke tekens en heeft een vaste lengte per land. Het IBAN bestaat uit een landcode (twee letters), een controlegetal (twee cijfers) en een nationaal rekeningnummer.

Zo wordt 780-5463207-83 → BE?? 7805 4632 0783

Het controlegetal wordt verkregen door het rekeningnummer te nemen

(1) 780546320783

er de landcode achter te plaatsen

(2) 780546320783BE

alle letters te vervangen door hun positie in het Romeinse alfabet, met als basispositie het begincijfer 9 (d.w.z. beginnen bij 10 met A=10, B=11...Z=35)

(3) 7805463207831114

twee nullen toe te voegen aan het einde

(4) 780546320783111400

dan de rest te nemen van de deling van het zo bekomen getal door 97

(5) 780546320783111400 mod 97 = 84

deze rest van 98 af te trekken om het controlegetal te krijgen

(6) 98 – 84 = 14

780-5463207-83 → BE14 7805 4632 0783

3.2. ISBN nummers

Een ISBN (International Standard Book Number) is een gecontroleerd identificatienummer van 10 of 13 cijfers dat uitgevers, bibliotheken en boekhandelaars toelaat boeken terug te vinden.

10-cijferig (oude nummers)

Bij de oude tiencijferige ISB-nummers is het laatste cijfer een controlecijfer. Van de bekende 9 cijfers van het ISBN wordt het eerste met 10 vermenigvuldigd, het tweede met 9, het derde met 8 en zo vervolgens, aflopend. Bij de som van de producten wordt dan een getal opgeteld, zodanig dat een veelvoud van 11 ontstaat. Dit toegevoegde getal wordt als controlecijfer genomen; het kan uiteraard 0 zijn, namelijk als de bedoelde productsom reeds een veelvoud van 11 is. Als het controlecijfer 10 is, wordt in plaats van een cijfer een X op de laatste positie gezet.

voorbeeld:

90-395-1394-?

9 x 10 + 0 x 9 + 3 x 8 + 9 x 7 + 5 x 6 + 1 x 5 + 3 x 4 + 9 x 3 + 4 x 2 = 259

259 mod 11 = 6 en 11 – 6 = 5

➔ 90-395-1394-5

13-cijferig (EAN systeem)

Bij de 13-cijferige ISB-nummers gaat de berekeningswijze van het controlegetal als volgt:

- ieder cijfer op een oneven positie wordt met 1 vermenigvuldigd
- ieder cijfer op een even positie wordt met 3 vermenigvuldigd
- deze producten worden bij elkaar opgeteld
- het controlecijfer is het cijfer nodig om van deze som een tienvoud te maken.

voorbeeld:

978-90-395-1394-?

(9 + 8 + 0 + 9 +1 + 9) + (7 + 9 + 3 + 5 + 3 + 4) x 3 = 129

129 + 1 = 130 dus controlegetal = 1

➔ 978-90-395-1394-1

3.3. barcodes

Een barcode bevat 13 cijfers en maakt deel uit van het EAN-systeem. M.a.w. het dertiende cijfer (controlecijfer) wordt op dezelfde manier berekend als bij de 13-cijferige ISBN nummers.

3.4. serienummers van bankbiljetten

In tegenstelling tot de euromunten hebben de bankbiljetten geen nationale zijde die de herkomst aangeeft. Deze informatie is wel vervat in de code op de achterkant van het biljet. De letter identificeert het land waar het biljet is uitgegeven. De Checksum wordt bepaald door alle getallen in het serienummer op te tellen. De cijfers in de uitkomst hiervan worden vervolgens ook opgeteld en eventueel wordt dit herhaald bij de uitkomst wat hieruit voorvloeit, teneinde een eencijferig cijfer over te houden. Dit cijfer wordt vervolgens vergeleken met het cijfer behorende bij het land om zo te bepalen of het biljet echt is. Als dat zo is dan is het biljet echt volgens het serienummer.

Code	Land	Uitkomst Checksum
Z	België	9
Y	Griekenland	1
X	Duitsland	2
(W)	*Denemarken*	(3)
V	Spanje	4
U	Frankrijk	5
T	Ierland	6
S	Italië	7
R	Luxemburg	8
P	Nederland	1

Code	Land	Uitkomst Checksum
N	Oostenrijk	3
M	Portugal	4
L	Finland	5
(K)	*Zweden*	(6)
(J)	*GB*	(7)
H	Slovenië	9
G	Cyprus	1
F	Malta	2
E	Slowakije	3
D	Estland	4

Afgesproken is dat ieder land zijn eigen euro's heeft, herkenbaar aan de landcode. Als een land uit de euro treedt dan zijn de biljetten met de code van dat land geen geldige euro's meer in de andere landen. Tegelijkertijd kunnen de biljetten van het uittredende land bijvoorbeeld gestempeld worden voor extra zichtbaarheid en dan dienen als lokale bankbiljetten zodat er niet gelijk of geen nieuwe lokale bankbiljetten gemaakt hoeven te worden. Weinig mensen blijken hiervan op de hoogte te zijn.

voorbeeld:

biljetnummer H55805151312 is afkomstig uit Slovenië en heeft als checksum dus 9;

$$5 + 5 + 8 + 0 + 5 + 1 + 5 + 1 + 3 + 1 + 2 = 36 \;>\; 3 + 6 = 9$$

3.5. Rijkregisternummer

Het Rijksregisternummer is een uniek identificatienummer toegekend aan natuurlijke personen ingeschreven in België. Het wordt toegekend na het invoeren van de basisgegevens door de dienst Bevolking in het Rijksregister. Men vindt het terug op de SIS-kaart of de (elektronische) identiteitskaart of men kan het persoonlijk opvragen aan het loket van de dienst Bevolking.

Het identificatienummer bevat 11 cijfers:

- Een eerste groep van zes cijfers, gevormd door de geboortedatum in de volgorde: jaar, maand, dag. Maand en/of dag kunnen nul zijn indien de exacte geboortedatum niet gekend is.
- Een tweede groep van drie cijfers dient als herkenning van de personen die op dezelfde dag geboren zijn. Dit reeksnummer is even voor een vrouw en oneven voor een man. Het is de dagteller van de geboortes. Voor een man van 001 tot 997 en voor een vrouw van 002 tot 998.

- Een derde groep van twee cijfers is een controlegetal op basis van de 9 voorafgaande cijfers. Dat wordt berekend door het getal van negen cijfers, dat gevormd wordt door de aaneenschakeling van de geboortedatum en het reeksnummer, te delen door 97. De rest van deze deling ("modulo") wordt van 97 afgetrokken. Het aldus bekomen verschil is het controlenummer. Voor personen geboren na 2000, moet men een 2 voor het getal van negen cijfers plaatsen (+ 2000000000) alvorens te delen door 97.

3.6. CAS-nummers

Een CAS-nummer is een unieke numerieke identifier voor chemische elementen, componenten, polymeren, en legeringen. CAS staat voor Chemical Abstracts Service, een divisie van de American Chemical Society gevestigd in Columbus, Ohio, USA.

De CAS Registry is een van de grootste databases in de wereld met informatie over meer dan 50 miljoen chemische verbindingen. De 50-miljoenste verbinding, CAS-nummer 1181081-51-5, werd op 7 september 2009 geregistreerd. Er worden dagelijks ongeveer 4000 nieuwe verbindingen toegevoegd. Aan het gebruik van de CAS-Registry-database waarnaar met behulp van een CAS-nummer verwezen wordt, zijn kosten verbonden.

Elke verbinding heeft een uniek nummer, het CAS Registry nummer. Dit nummer bestond aanvankelijk uit maximaal 9 cijfers, verdeeld in 3 groepjes die gescheiden zijn met een streepje. Het linker groepje bestond tot 2007 uit 3 tot maximaal 6 cijfers; het volgende uit 2 cijfers en rechts staat een controlecijfer. In september 2007 kondigde de CAS aan, dat ze vanaf januari 2008 CAS-nummers met tien cijfers zou gaan toekennen, vanwege de gestage groei van het aantal nieuw geregistreerde stoffen. Het tiende cijfer komt op de meest linkse plaats, dus het eerste groepje krijgt dan 7 cijfers. De CAS-nummers worden met een checksum gecodeerd en zijn daardoor snel te verifiëren op typefouten.

voorbeelden:

- cafeïne : 58-08-2
- polypropeen : 9003-07-0

berekenen van het controlecijfer:

$N_8N_7N_6N_5N_4N_3N_2N_1$-R

$R = (N_1 \times 1 + N_2 \times 2 + N_3 \times 3 + \ldots + N_8 \times 8) \bmod 10$

3.7. gestructureerde mededeling

Een gestructureerde mededeling of OGM is een combinatie van drie groepen van drie, vier en vijf cijfers gescheiden door een schuine streep, zoals:
+++090/9337/55493+++

Deze mededeling wordt in België vaak gebruikt om overschrijvingen automatisch te kunnen laten verwerken. Zo weet het computersysteem van de ontvanger onmiddellijk welke factuur betaald wordt. Op deze manier is er geen personeel nodig om te gaan kijken welke rekeningen vereffend werden.

De eerste tien cijfers zijn bijvoorbeeld een klantennummer of een factuurnummer. De laatste twee cijfers vormen het controlegetal dat bekomen wordt door van de voorgaande tien cijfers de rest bij deling door 97 te berekenen (modulo 97). Voor en achter de cijfers worden drie plussen (+++) of sterretjes (***) gezet.

Uitzondering: Indien de rest 0 bedraagt, dan wordt als controlegetal 97 gebruikt.

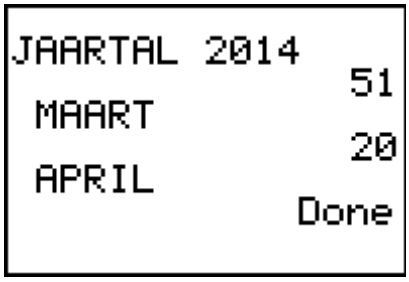
Als het controlegetal niet overeenstemt met de 10 eerste cijfers, dan wordt de betaling geweigerd. Zo wordt voorkomen dat er willekeurige fouten optreden bij het manueel inleiden van betalingsopdrachten.

3.8. Paasdag

Wanneer valt Pasen in 20xx. De berekening, volgens Gauss, gaat als volgt:

Voor de 20ste en 21ste eeuw is K = 24 en L = 5

- a = jaartal (mod 19)
- b = jaartal (mod 4)
- c = jaartal (mod 7)
- d = 19a + K (mod 30)
- e = 2b + 4c + 6d + L (mod 7)
- paasdag = (22 + d + e) maart of (d + e – 9) april




```
PROGRAM:PASEN
:Input "JAARTAL
",J
:remainder(J,19)
→A
:remainder(J,4)→
B
:remainder(J,7)→
```

```
PROGRAM:PASEN
:remainder(J,7)→
C
:remainder(19A+2
4,30)→D
:remainder(2B+4C
+6D+5,7)→E
:22+D+E→X
```

```
PROGRAM:PASEN
:22+D+E→X
:D+E-9→Y
:Disp X," MAART"
:Disp Y," APRIL"
:Stop
```

4. 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		151						157			
		163				167						173						179	
181										191		193				197		199	
										211									
		223				227		229				233						239	
241										251						257			
		263						269		271						277			
281		283										293							
						307				311		313				317			
										331						337			
						347		349				353						359	
						367						373						379	
		383						389								397			

Priemgetalhiaat

Een priemgetalhiaat is het verschil tussen twee opeenvolgende priemgetallen. Het n^{de} priemgetalhiaat, aangeduid door g_n, is het verschil tussen het (n+1)^{de} en het n^{de} priemgetal, dat wil zeggen $g_n = p_{n+1} - p_n$.

De eerste 30 priemgetalhiaten zijn:
1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4, 2, 4, 14

Priemtweelingen

Priemtweelingen zijn priemgetallen die voorkomen in de vorm p en $p+2$, waarbij zowel p als $p+2$ een priemgetal zijn.

Voorbeelden:
3 en 5 ; 5 en 7 ; 11 en 13 ; 17 en 19 ; 29 en 31 ; 41 en 43 ; 59 en 61 ; 71 en 73 ; 101 en 103 ; 107 en 109 ; …

Priemgetaltest

Een priemgetaltest is een algoritme dat bepaalt of een gegeven getal al dan niet priem is. Een dergelijke test wordt onder andere gebruikt in de cryptografie. Het verschil tussen een priemgetaltest en ontbinding in priemfactoren is dat een priemgetaltest niet noodzakelijk priemfactoren geeft, maar alleen zegt of het gegeven getal wel of niet priem is.

4.1. Mersennegetallen

Een Mersennegetal is een (positief geheel) getal dat precies één kleiner is dan een macht van twee.

$$M_n = 2^n - 1$$

Een Mersennepriemgetal is een Mersennegetal dat een priemgetal is.

n	$2^n - 1$	faktorisatie
2	3	3
3	7	7
4	15	3 x 5
5	31	31
6	63	3 x 3 x 7
7	127	127
8	255	3 x 5 x 17
9	511	7 x 73
10	1023	3 x 11 x 31
11	2047	23 x 89
12	4095	3 x 3 x 5 x 7 x 13
13	8191	8191

Januari 2013 zijn er 48 Mersennepriemgetallen bekend. Het grootst bekende priemgetal is een Mersennepriemgetal:

$$M_{57885161} = 2^{57885161} - 1$$

Een basisstelling over Mersennegetallen stelt dat M_n alleen een Mersennepriemgetal is, als de exponent n zelf ook een priemgetal is. Dit sluit getallen, zoals M_4 = 24−1 = 15 uit, aangezien de exponent 4(=2×2) samengesteld is. De stelling voorspelt dat 15 ook samengesteld is, wat inderdaad klopt, want 15 = 3×5. De drie kleinste Mersennepriemgetallen zijn M_2 = 3, M_3 = 7, M_5 = 31.

Hoewel het waar is dat alleen Mersennegetallen M_p priem kunnen zijn, als p ook een priemgetal is, kan het niettemin het geval zijn dat M_p geen priemgetal is, terwijl p dat wel is. Het kleinste tegenvoorbeeld is het Mersennegetal M_{11} = 211−1 = 2047 = 23×89 .

Het ontbreken van een duidelijke regel om te bepalen of een gegeven Mersennegetal een priemgetal is maakt de zoektocht naar Mersennepriemgetallen een interessante taak, die aangezien Mersennegetallen zeer snel groeien, heel snel zeer moeilijk wordt.

Lucas-Lehmertest voor Mersennegetallen

De Lucas-Lehmertest voor Mersennegetallen is een algoritme om te bepalen of het Mersennegetal $M_p = 2^p - 1$ (p een priemgetal) een Mersennepriemgetal is. De test is ontwikkeld door Edouard Lucas en later verbeterd door Derrick Henry Lehmer.

Gegeven een Mersennegetal $M_p = 2^p - 1$ met p een priemgetal. Definieer nu de rij s_i als volgt:

$$s_i = \begin{cases} 4 & als\ i = 0 \\ s_{i-1}^2 - 2 & als\ i > 0 \end{cases}$$

de eerste termen van deze rij zijn 4, 14, 194, 37634, 1416317954, …

Nu geldt dat M_p een priemgetal is dan en slechts dan als $s_{p-2} \equiv 0 \pmod{M_p}$.

Voorbeeld:

$M_5 = 2^5 - 1 = 31$

$s_0 \equiv 4 \pmod{31}$
$s_1 \equiv 4^2 - 2 \equiv 14 \pmod{31}$
$s_2 \equiv 14^2 - 2 \equiv 8 \pmod{31}$
$s_3 \equiv 8^2 - 2 \equiv 0 \pmod{31}$

$s_3 = 0$ dus 31 is een priemgetal.

```
PROGRAM:LUCAS
:Prompt P
:2^P-1→A
:4→S
:For(I,1,P-2)
:remainder(S²-2,
A)→S
:End
```

```
PROGRAM:LUCAS
:Disp A
:Disp "S = ",S
:If S=0
:Then
:Disp "MERSENNEP
RIEM"
:End
```

```
P=?19
              524287
S =
                   0
MERSENNEPRIEM
              Done
```

Perfecte getallen en Mersennepriemgetallen

Er is een verband tussen Mersennepriemgetallen en perfecte getallen.

Als $2^n - 1$ een priemgetal is, dan is $2^{n-1}.\left(2^n - 1\right)$ een perfect getal.

Omgekeerd kan ieder perfect getal geschreven worden als $2^{n-1}.\left(2^n - 1\right)$ waarbij n een priemgetal is en $2^n - 1$ een Mersennepriemgetal.

4.2. De Priemgetalstelling

Definieer de priemgetal-telfunctie $\pi(x)$ die voor elke positieve x het aantal gevonden priemgetallen kleiner of gelijk aan x geeft.

vb. $\pi(10) = 4$ omdat er precies vier priemgetallen (2, 3, 5 en 7) kleiner of gelijk aan 10 zijn.

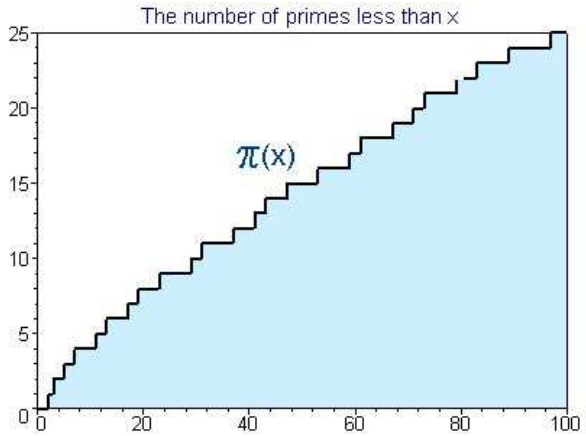
De priemgetalstelling stelt dat de limiet van het quotiënt van de functies $\pi(x)$ en $\frac{x}{\ln(x)}$ gelijk wordt aan één als x tot oneindig nadert.

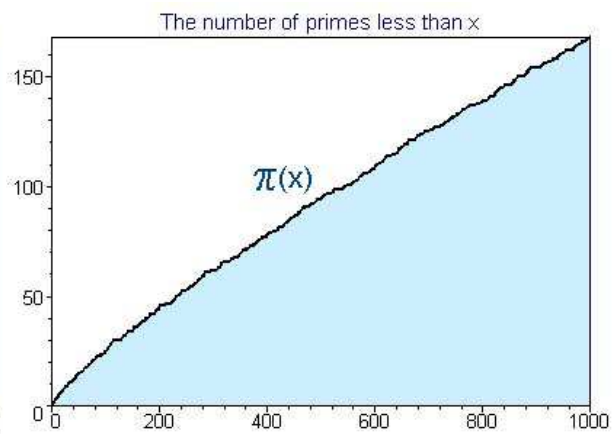
$$\lim_{x \to \infty} \frac{\pi(x)}{x / \ln(x)} = 1$$

Deze formule staat bekend als de asymptotische verdelingswet van de priemgetallen.

vb. stel x = 1 000 000

$\pi(x) = 78498$ en $\frac{x}{\ln(x)} \approx 72382$





4.3. De Riemann hypothese

In het jaar 2000 stelde het Clay Institute in Cambridge in Massachusetts een lijst van zeven belangrijke onopgeloste vraagstukken in de wiskunde op en loofde voor de oplossing van een probleem een prijs van een miljoen Amerikaanse dollar. Tot nu toe is uit deze lijst van millenniumprijsproblemen alleen “het Vermoeden van Poincaré” opgelost door Grigori Perelman in 2002.

De Riemann-hypothese is één van de onopgeloste problemen van de wiskunde. Wie een sluitend bewijs levert, wordt wereldberoemd en verdient bovendien een prijs van een miljoen dollar.

De Riemann-hypothese kan worden gezien als een verfijning van de priemgetalstelling. De priemgetalstelling geeft een nauwkeurige schatting voor het aantal priemgetallen en de Riemann-hypothese vertelt ons hoever de priemgetalstelling ernaast zit.

De zèta functie

Als u_1 , u_2 , u_3 , ... de termen zijn van een willekeurige rij u , definiëren we

- $S_1 = u_1$
- $S_2 = u_1 + u_2$
- $S_3 = u_1 + u_2 + u_3$
- …

Dan geldt dat S_1 , S_2 , S_3 , ... de termen (functiewaarden) zijn van bijbehorende reeks (functie) S

Een reeks is eigenlijk een oneindige som:

$$S = \sum u_k = \sum_{k=1}^{\infty} u_k = u_1 + u_2 + u_3 + ...$$

Hyperharmonische reeksen

De harmonische reeks wordt gegeven door:

$$\sum \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ...$$

De hyperharmonische reeks wordt gegeven door:

$$\sum \frac{1}{k^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$$

zo voor

$$s = 2: \ \sum \frac{1}{k^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots$$

$$s = \frac{1}{2}: \sum \frac{1}{\sqrt{k}} = 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{4}} + \ldots$$

men kan bewijzen dat:

- voor $s \leq 1$ deze oneindige som naar ∞ gaat, men zegt dat de reeks divergeert,
- voor $s > 1$ deze oneindige som eindig is, men zegt dat de reeks convergeert.

Euler bewees dat:

$$\sum \frac{1}{k^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \frac{\pi^2}{6}$$

$$\sum \frac{1}{k^4} = \frac{\pi^4}{90} \ , \ \sum \frac{1}{k^6} = \frac{\pi^6}{945} \ , \ \sum \frac{1}{k^8} = \frac{\pi^8}{9450} \ , \ \sum \frac{1}{k^{10}} = \frac{\pi^{10}}{93555}$$

De zèta functie

Men definieert de zèta functie $\zeta(s)$ als volgt:

$\zeta(x) = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \ldots$ met x een complex getal waarbij Re(x) > 1

Euler bewees dat deze functie kan herschreven worden als:

$$\zeta(x) = \frac{2^x}{2^x - 1} \times \frac{3^x}{3^x - 1} \times \frac{5^x}{5^x - 1} \times \frac{7^x}{7^x - 1} \times \frac{11^x}{11^x - 1} \times \ldots$$

m.a.w. als een oneindig product van factoren van de vorm $\frac{p^x}{p^x - 1}$, waarbij je voor p achtereenvolgens alle priemgetallen moet nemen.

De zèta functie voldoet aan de volgende functionaalvergelijkingen:

$$\zeta(x) = 2^x \pi^{x-1} \sin\left(\frac{\pi x}{2}\right) \Gamma(1-x)\, \zeta(1-x)$$

$$\zeta(-x) = -2 \frac{1}{(2\pi)^{x+1}} \sin\left(\frac{\pi x}{2}\right) \Gamma(1+x)\, \zeta(x+1) \qquad \forall x \in \mathbb{C} \setminus \{0,1\}$$

hierbij stelt Γ de gammafunctie voor. $\forall n \in \mathbb{N} : \Gamma(1+n) = n!$

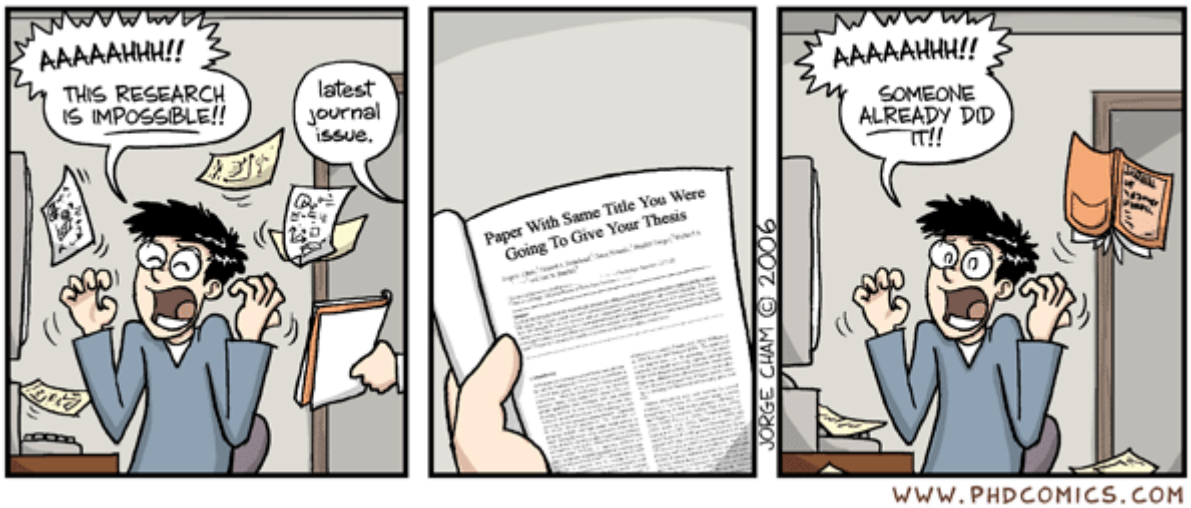
De Riemann hypothese

De zèta-functie is nul voor alle complexe getallen z = x + yi die liggen in het halfvlak x > 1.

De Riemann-zèta-functie heeft nulpunten in de negatieve even gehele getallen. Deze nulpunten zijn eenvoudig te vinden vertrekkende van de functionaalvergelijking en ze worden dan ook triviale nulpunten genoemd.

De zèta-functie heeft echter nog meer nulpunten en deze liggen noodzakelijkerwijze in de zogenaamde kritieke strook, de verzameling van alle complexe getallen met reële gedeelte strikt tussen nul en een.
De beroemde Riemann-hypothese zegt dan dat alle niet-triviale nulpunten precies 1/2 als reële gedeelte hebben. Deze hypothese is nog niet bewezen en ze wordt zelfs als een van de belangrijkste (of in ieder geval een van de meest bekende) problemen in de wiskunde beschouwd.

Toch is er redelijk wat geweten over de structuur van de verzameling van alle niet-triviale nulpunten. Zo zijn er bijvoorbeeld oneindig veel niet-triviale nulpunten en ze zijn symmetrisch gelegen ten opzichte van de reële as (de complexe getallen met imaginaire gedeelte gelijk aan nul) en de as van de complexe getallen met reële gedeelte gelijk aan 1/2.



4.4. Het vermoeden van Goldbach

Elk even getal groter dan 2 is te schrijven als de som van twee priemgetallen.

Men heeft dit vermoeden met de computer gecontroleerd tot aan 10^{18}, dus het ziet er “zeer waarschijnlijk” uit dat dit vermoeden wel waar is. Bewezen is dit echter nog niet.

Stelling van Vinogradov – Bombieri

Elk oneven getal groter dan 5 is te schrijven als de som van drie priemgetallen.

Deze stelling wordt ook wel het “zwakke” vermoeden van Goldbach genoemd.

4.5. Problemen van Landau

Het vermoeden van Legendre

Er ligt minstens één priemgetal tussen n^2 *en* $(n+1)^2$*.*

Problemen van Landau

Op het internationale congres van wiskundigen in 1912 besprak Edmund Landau vier basisproblemen met betrekking tot de priemgetallen. Landau karakteriseerde deze vier problemen in zijn toespraak als "niet aanvalbaar bij de huidige stand van de wetenschap". Zij staan nu bekend als de problemen van Landau.

- Het vermoeden van Goldbach
- Het vermoeden van Legendre
- Het priemtweelingvermoeden: *zijn er oneindig veel priemgetallen* p *zodanig dat* $p+2$ *ook een priemgetal is?*
- Zijn er oneindig veel priemgetallen p zodanig dat $p-1$ een kwadraat is? Met andere woorden: *bestaan er oneindig veel priemgetallen van de vorm* n^2+1*?*

Anno 2012 (100 jaar later) zijn deze vier problemen nog niet opgelost.

Het vermoeden van Brocard

Er liggen minstens vier priemgetallen tussen $(p_n)^2$ *en* $(p_{n+1})^2$ *waarbij* p_n *het* n^{de} *priemgetal is.*

Het vermoeden van Polignac

Voor elk natuurlijk getal k bestaan er oneindig veel priemgetalhiaten van grootte 2k.

In het geval van k = 1 is het vermoeden van Polignac gelijkwaardig aan het priemtweelingvermoeden

5. RSA

RSA is een asymmetrisch encryptiealgoritme, dat veel gebruikt wordt voor elektronische betalingen en handel (beveiliging van transacties). Het formele algoritme werd in 1977 ontworpen door Ron Rivest, Adi Shamir en Len Adleman (vandaar de afkorting RSA).

De veiligheid van RSA steunt op het probleem van de ontbinding in factoren bij heel grote getallen. Op dit moment is het bijna onmogelijk de twee oorspronkelijke priemgetallen p en q te achterhalen als alleen p*q bekend is en p en q groot genoeg zijn; het zou te veel tijd in beslag nemen. Nieuwe ontwikkelingen op dit gebied zouden RSA onbruikbaar kunnen maken.

Hoe werkt nu RSA?

Stel dat je de zin “JEROEN SPEELT GITAAR” wilt coderen.

- Eerst maak je van elk teken een getal door het om te zetten in de bijbehorende ASCII-code.

DEC	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240
0			space	0	@	P	`	p	€	□	nbsp	°	À	Ð	à	ð
1			!	1	A	Q	a	q	□	‘	¡	±	Á	Ñ	á	ñ
2			"	2	B	R	b	r	‚	’	¢	²	Â	Ò	â	ò
3			#	3	C	S	c	s	ƒ	“	£	³	Ã	Ó	ã	ó
4			$	4	D	T	d	t	„	”	¤	´	Ä	Ô	ä	ô
5			%	5	E	U	e	u	…	•	¥	µ	Å	Õ	å	õ
6			&	6	F	V	f	v	†	–	¦	¶	Æ	Ö	æ	ö
7			'	7	G	W	g	w	‡	—	§	·	Ç	×	ç	÷
8			(	8	H	X	h	x	ˆ	˜	¨	¸	È	Ø	è	ø
9	TAB		)	9	I	Y	i	y	‰	™	©	¹	É	Ù	é	ù
10	LF		*	:	J	Z	j	z	Š	š	ª	º	Ê	Ú	ê	ú
11			+	;	K	[	k	{	‹	›	«	»	Ë	Û	ë	û
12			,	<	L	\	l	|	Œ	œ	¬	¼	Ì	Ü	ì	ü
13	CR		-	=	M	]	m	}	□	□		½	Í	Ý	í	ý
14			.	>	N	^	n	~	Ž	ž	®	¾	Î	Þ	î	þ
15			/	?	O	_	o	□	□	Ÿ	¯	¿	Ï	ß	ï	ÿ

Om het rekenwerk te beperken gebruiken we in ons voorbeeld een eenvoudigere omzettingstabel:

0	1	2	3	4	5	6	7	8	9		A	B	C	D	E	F	G	H
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	

JEROEN SPEELT GITAAR

→ 20 15 28 25 15 24 10 29 26 15 15 22 30 10 17 19 30 11 11 28

- Kies twee priemgetallen p en q. Normaal gesproken worden daarvoor gigantisch grote getallen gekozen. Neem p = 37 en q = 29.

- Bereken het product: N = p • q = 37 • 29 = 1073

  Om echt veilig te zijn, zijn p en q priemgetallen van minstens 80 cijfers en telt hun product N minstens 200 cijfers.

- Bereken M = (p – 1) • (q – 1) = 36 • 28 = 1008, vernietig nu p en q, je hebt ze niet meer nodig.

- Kies een getal K kleiner dan M zodat ggd(K,M) = 1.
  Bijvoorbeeld K = 25 voldoet aan de voorwaarden.

- Nu kun je aan het coderen met behulp van de getallen K = 25 en N = 1073.

- Omdat N niet groot is (normaal gezien is dit een getal met enorm veel cijfers), verdelen we onze te coderen zin in blokjes van 3 cijfers. Een blokje B moet immers kleiner zijn dan N. (B < N).

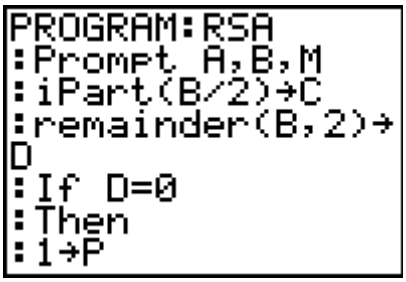
  201 528 251 524 102 926 151 522 301 017 193 011 112 810

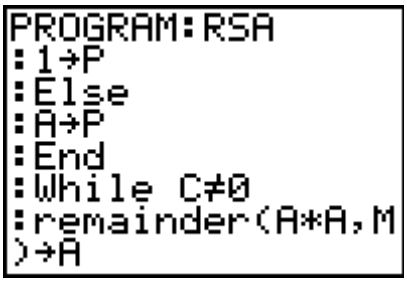
- Doe elk blokje tot de macht 25. Vervolgens trek je er zo vaak mogelijk 1073 van af. (Je berekent dus B^{25} (mod.1073) waarin B het blokje voorstelt.)
  Zet alles achter elkaar en je hebt je geheimschrift.

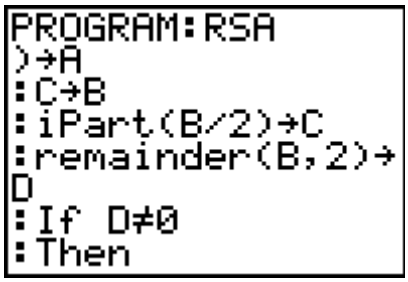
$$\begin{aligned}
201^{25} \pmod{1073} &= 201.\left[201^2\right]^{12} \pmod{1073} = 201.[700]^{12} \pmod{1073} \\
&= 201.\left[700^2\right]^{6} \pmod{1073} = 201.[712]^{12} \pmod{1073} \\
&= 201.\left[712^2\right]^{3} \pmod{1073} = 201.[488]^{3} \pmod{1073} \\
&= 201.488.\left[488^2\right] \pmod{1073} = 201.488.1011 \pmod{1073} \\
&= 308
\end{aligned}$$

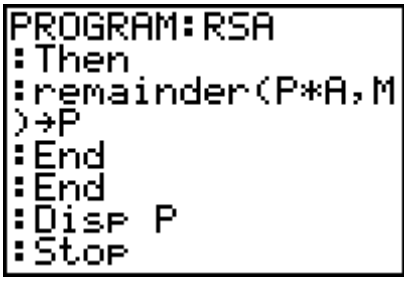
…

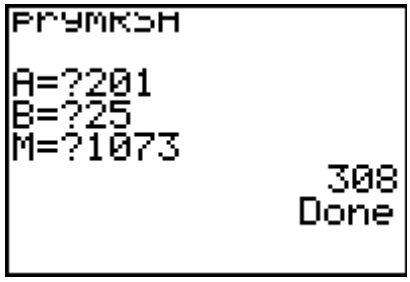
$$\begin{aligned}
810^{25} \pmod{1073} &= 810.\left[810^2\right]^{12} \pmod{1073} = 810.[497]^{12} \pmod{1073} \\
&= 810.\left[497^2\right]^{6} \pmod{1073} = 810.[219]^{12} \pmod{1073} \\
&= 810.\left[219^2\right]^{3} \pmod{1073} = 810.[749]^{3} \pmod{1073} \\
&= 810.749.\left[749^2\right] \pmod{1073} = 810.749.895 \pmod{1073} \\
&= 192
\end{aligned}$$











308 676 843 968 095 482 966 696 019 133 785 048 778 192

- De getallen K en N vormen de publieke sleutel. Die mag iedereen weten, iedereen kan dus een bericht versleutelen.

- Om het gecodeerde woord weer te decoderen heb je de decodeersleutel L nodig.

  Die decodeersleutel moet voldoen aan K • L = 1 (mod.M),

  In ons voorbeeld moet dus 25 • L = 1 (mod.1008).

  L (hier 121) is de geheime sleutel die alleen bekend is aan degene die moet decoderen.

- Je decodeert door de afzonderlijke cijfers van het geheimschrift tot de macht L te doen en er veelvouden van 1073 (= N) van af te trekken. (Je berekent dus C^{121} (mod.1073) waarin C een gecodeerd blokje voorstelt.)

$$\begin{aligned}
308^{121}\ (\mathrm{mod}1073) &= 308.\left[308^2\right]^{60}\ (\mathrm{mod}1073) = 308.[440]^{60}\ (\mathrm{mod}1073) \\
&= 308.\left[440^2\right]^{30}\ (\mathrm{mod}1073) = 308.[460]^{30}\ (\mathrm{mod}1073) \\
&= 308.\left[460^2\right]^{15}\ (\mathrm{mod}1073) = 308.[219]^{15}\ (\mathrm{mod}1073) \\
&= 308.219.\left[219^2\right]^{7}\ (\mathrm{mod}1073) = 926.[749]^{7}\ (\mathrm{mod}1073) \\
&= 926.749.\left[749^2\right]^{3}\ (\mathrm{mod}1073) = 416.[895]^{3}\ (\mathrm{mod}1073) \\
&= 416.895.\left[895^2\right]\ (\mathrm{mod}1073) = 1062.567\ (\mathrm{mod}1073) \\
&= 201
\end{aligned}$$

201 528 251 524 102 926 151 522 301 017 193 011 112 810

➔ 20 15 28 25 15 24 10 29 26 15 15 22 30 10 17 19 30 11 11 28

➔ JEROEN SPEELT GITAAR

Samengevat

p en q twee “grote” priemgetallen

N = p • q

M = (p – 1) • (q – 1)

K < M én ggd(K,M) = 1

L < M en K • L = 1 (mod.M)

K en N zijn publiek, iedereen (ook de “vijand”) kent deze sleutels

Tekst
➔ omzetten in cijfervorm
➔ verdelen in blokjes B
➔ coderen: $B^K \pmod N = C$
➔ code

L is de geheime sleutel die enkel de “ontvanger van de boodschap” kent

Code
➔ decoderen: $C^L \pmod N = B$
➔ cijfervorm
➔ omzetten in tekst

6. Oefeningen

6.1. Reeks 1

(1) Ontbind volgende getallen in priemfactoren

(a) 1 080 432 = ……

(b) 20 073 277 = ……

(c) 118 459 = ……

(d) 5 504 701 = ……

(e) 62 656 243 = ……

(f) 12 689 123 = ……

(g) 15 581 523 = ……

(h) 249 001 = ……

(i) 41 842 505 = ……

(j) 121 330 189= ……

(k) 8 587 340 257 = ……

(l) 11 161 = ……

(2) Bewijs volgende eigenschappen

(a) $17 \mid 10a + b \;\Rightarrow\; 17 \mid a - 5b$

(b) $13 \mid 5a + 7b \;\Rightarrow\; 13 \mid -3a + 27b$

(c) $19 \mid 8a + 3b \;\Rightarrow\; 19 \mid 37a + 2b$

(d) Als men een getal van 4 cijfers tweemaal naast elkaar schrijft, dan bekomt men een getal van 8 cijfers dat steeds deelbaar is door 137.

(3) Bepaal de natuurlijke delers van volgende getallen en ga na dat deze getallen perfect zijn:

(a) $6 = 2^1\left(2^2 - 1\right)$

$d(n)$: ……

$s(n)$: ……

(b) $28 = 2^2\left(2^3 - 1\right)$

$d(n)$: ……

$s(n)$: ……

(c) $496 = 2^4\left(2^5 - 1\right)$

$d(n)$: ……

$s(n)$: ……

(d) $8128 = 2^6\left(2^7 - 1\right)$

$d(n)$: ……

$s(n)$: ……

(4) Bepaal de “vriend” van volgende getallen:

(a) 1184

$d(n) = d(1184)$: ……

$m = s(n) = s(1184)$: ……

$d(m) = d(.....)$: ……

$1184 = s(m)$: ……

(b) 2924

$d(n) = d(2924)$: ……

$m = s(n) = s(2924)$: ……

$d(m) = d(.....)$: ……

$2924 = s(m)$: ……

(c) 5020

$d(n) = d(5020)$: ……

$m = s(n) = s(5020)$: ……

$d(m) = d(.....)$: ……

$5020 = s(m)$: ……

(5) Bereken ggd(a,b) en kgv(a,b)

(a) a = 130 801 ggd(a,b) = ……

b = 279 312 kgv(a,b) = ……

(b) a = 1 227 744 ggd(a,b) = ……

b = 666 792 kgv(a,b) = ……

(c) a = 121 125 ggd(a,b) = ……

b = 18 135 kgv(a,b) = ……

(d) a = 49 786 511 ggd(a,b) = ……

b = 50 874 269 kgv(a,b) = ……

(e) a = 126 619 ggd(a,b) = ……

b = 12 890 623 kgv(a,b) = ……

(6) Bepaal, indien mogelijk, een oplossing van … (toepassing op de st. v. Bézout)

(a) $37x + 73y = 1$ x = …… y = ……

(b) $54x + 24y = 12$ x = …… y = ……

(c) $101x + 11y = 1$ x = …… y = ……

(d) $89x + 67y = 1$ x = …… y = ……

(e) $19x + 29y = 3$ x = …… y = ……

(f) $129x + 123y = 6$ x = …… y = ……

(7) Bereken

(a) modulo 11: $12 + 7 \times 8 - 9 =$ ……

(b) modulo 7: $3 \times (7 + 4 \times (8 + 9) - 5) =$ ……

(c) modulo 19: $4 \times 12 + 13 \times 28 - 7 \times 6 =$ ……

(d) modulo 14: $3 \times (4 - 6) + 8 \times (12 + 25) + 16^2 =$ ……

(e) modulo 23: $[44 \times (57 - 13)^2 + 5^2 \times (8 + 11)]^2 =$ ……

(f) modulo 67: $99999999 - 12345678 =$ ……

(8) Stel de vermenigvuldigingstabel op voor $\mathbb{Z}/7\mathbb{Z}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$							
$\bar{1}$							
$\bar{2}$							
$\bar{3}$							
$\bar{4}$							
$\bar{5}$							
$\bar{6}$							

Welke restklassen hebben een symmetrisch element?

……

(9) Bepaal het kleinste natuurlijk getal x dat voldoet aan:

(a) $4x + 5 = 4 \pmod 7$ x = ……

(b) $5x + 7 = 3 \pmod{11}$ x = ……

(c) $6x + 1 = 7 \pmod 9$ x = ……

(d) $3x + 8 = 7 \pmod 7$ x = ……

(e) $7x + 5 = 2 \pmod{11}$ x = ……

(10) Bepaal het kleinste natuurlijk getal x dat voldoet aan (Chinese reststelling):

(a) $\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 8 \pmod{12} \end{cases}$ x = ……

(b) $\begin{cases} x \equiv 3 \pmod 6 \\ x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod 8 \end{cases}$ x = ……

(c) $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 0 \pmod 9 \\ x \equiv 6 \pmod{11} \end{cases}$ x = ……

(d) $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 5 \pmod 6 \\ x \equiv 8 \pmod 9 \end{cases}$ x = ……

(e) $\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 9 \\ x \equiv 5 \pmod{12} \\ x \equiv 7 \pmod{14} \end{cases}$ x = ……

6.2. Reeks 2

(1) Vervolledig volgende rekeningnummers

(a) 860 – 0112905 - ……

(b) 833 – 4819287 - ……

(c) 780 – 54632 …… - 83

(d) 001 – 42820 …… - 92

(e) BE … … - 8602 - 7 … 48 - … 667

(f) BE … … - 7994 - … 43 … - 7436

(2) Vervolledig volgende ISBN-nummers

(a) 978 – 90 – 351 – 3801 – …

(b) 978 – 90 – 5764 – 993 – …

(c) 978 – 90 – 314 – 30…7 – 0

(d) 978 – 90 – 314 – 3…07 – 3

(3) Vervolledig volgende serienummers

(a) Z 6648 … 386393

(b) U 27 … 60155785

(c) M 334846 … 7205

(4) Vervolledig volgende gestructureerde mededelingen

(a) +++ 568 / 2469 / 654 … … +++

(b) +++ 478 / 8 … … 5 / 25733 +++

(c) +++ 9 … 8 / 721 … / 95735 +++

(d) +++ 201 / 8 … 25 / 787 … 0 +++

(5) In volgende rekeningnummers zit één fout (eerste drie en laatste twee zijn sowieso juist). Kan je het juiste nummer terugvinden?

(a) 001 – 1246129 – 42 → 001 - …… - 42

(b) 680 – 4200678 – 02 → 680 - …… - 02

(c) 000 – 5544233 – 07 → 000 - …… - 07

(d) 850 – 4710482 – 77 → 850 - …… - 77

(6) Vervolledig volgende CAS nummers

(a) 2-butenal ; C_4H_6O ; CAS : 123 – 73 – …

(b) waterstofcyanide ; HCN ; CAS : 74 – 90 – …

(c) diethylsulfaat ; $C_4H_{10}O_4S$; CAS : 64 – …7 – 5

(d) DDT ; $C_{14}H_9Cl_5$; CAS : 7…9 – 02 – 6

(e) isoproturon ; $C_{12}H_{18}N_2O$; CAS : 34123 – …9 – 6

(7) Bepaal alle natuurlijke getallen $x \in [40,60]$ waarvoor geldt:

$\left[x \pmod{19}\right] \pmod{11} = 2$ antwoord : ……

(8) Bepaal alle natuurlijke getallen x kleiner dan 100 die voldoen aan:

$\left[x \pmod 8\right].\left[x \pmod{11}\right] = 7$ antwoord : ……

(9) Bepaal alle natuurlijke getallen $x \in [0,50]$ waarvoor geldt:

$(2x-1) \pmod 7 = (3x+4) \pmod 8$ antwoord : ……

(10) Wanneer valt Paasdag de komende vijf jaar?

6.3. Reeks 3

(1) Geef alle priemtweelingen tussen 300 en 500:

……

……

(2) Toon aan dat het vermoeden van Goldbach klopt voor alle even getallen tussen 55 en 85:

56 = …… 72 = ……

58 = …… 74 = ……

60 = …… 76 = ……

62 = …… 78 = ……

64 = …… 80 = ……

66 = …… 82 = ……

68 = …… 84 = ……

70 = ……

(3) Ga m.b.v. de Lucas-Lehmertest na of volgende Mersennegetallen een priemgetal zijn of niet. Indien priem, bepaal dan het bijbehorende perfecte getal.

(a) $M_{17} = 2^{17} - 1 = 131071$

priem : ja / neen → zo ja, perfecte getal : ……

(b) $M_{19} = 2^{19} - 1 = 524287$

priem : ja / neen → zo ja, perfecte getal : ……

(c) $M_{23} = 2^{23} - 1 = 8388607$

priem : ja / neen → zo ja, perfecte getal : ……

(d) $M_{31} = 2^{31} - 1 = 2147483647$

priem : ja / neen → zo ja, perfecte getal : ……

(4) Bereken m.b.v. de functionaalvergelijking:

(a) $\zeta(2) =$

(b) $\zeta(-1) =$

(c) $\zeta(-2) =$

(d) $\zeta(-3) =$

(e) $\zeta(-5) =$

(f) $\zeta(-7) =$

(5) Gamma-functie:

(a) Stel in de eerste functionaalvergelijking x = ½ en bereken zo $\Gamma\left(\frac{1}{2}\right)$.

$\Gamma\left(\frac{1}{2}\right) =$

(b) Als je weet dat $\Gamma(x+1) = x.\Gamma(x)$ bereken dan:

$\Gamma\left(-\frac{1}{2}\right) =$

$\Gamma\left(\frac{3}{2}\right) =$

$\Gamma\left(\frac{5}{2}\right) =$

6.4. Reeks 4

(1) Decodeer volgende zin. K = 41 , N = 1043 , L = 65

926 690 464 644 786 127 557 422 927 353 159 901 464 038 584 521

... ...

Antwoord : ……..

(2) Codeer volgende zin. K = 31 , N = 1027 , L = 151

JENS DROOMT NOOIT

J E N S D R O O M T N O O I T

… … … … … … … … … … … … … … … … …

groeperen per 3 cijfers

… … … … … … … … … … … …

coderen

… … … … … … … … … … … …

(3) Bepaal L als p = 11, q = 101, K = 21.

N =

M =

L =

(4) Decodeer volgende zin. K = 619 , N = 1769 , M = 1680 , L = …….

1651	486	512	1114	401	1108	336	929	512	1114
…	…	…	…	…	…	…	…	…	…

Antwoord : ……..

(5) Kies p en q priem zodat $19 \leq p, q \leq 83$.

p =

q =

Bereken N en M

N =

M =

Kies een K < M zodat ggd(K,M) = 1

K =

Bepaal L < M zodat K • L = 1 (mod.M)

L =

Geef de publieke sleutels K en N door aan en andere groep en vraag naar een gecodeerd woord.

Probeer het gecodeerde woord te decoderen.

Bibliografie

- Frits Beukers, Getaltheorie voor Beginners, Epsilon Uitgaven, 2000
- Roland van der Veen en Jan van de Craats, De Riemannhypothese, Epsilon Uitgaven, 2011
- Jan De Beule, Tom De Medts en Jeroen Demeyer, Opgeloste en onopgeloste mysteries in de getaltheorie, Die Keure, 2013
- Aldine Aaten en Cor Kraaikamp, Verborgen boodschappen, Epsilon Uitgaven, 2013
- nl.wikipediia.org/wiki/