# Getaltheorie

Wiskunde

LJ2P1

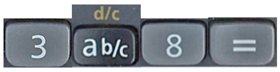
# Hoofdstuk 1 - Drie manieren om een getal te schrijven

## *§ 1.1 Beginnen met een breuk*

Je kunt een breuk schrijven als decimaal getal en ook als percentage, kijk maar:

$\frac{1}{2} = 0{,}5 = 50\%$ $\frac{3}{4} = 0{,}75 = 75\%$ $\frac{2}{5} = 0{,}4 = 40\%$

Hoe vind je het kommagetal dat bij een breuk hoort? Met je rekenmachine! De abc-knop kan heen en weer switchen tussen een breuk en een kommagetal.

Voer $\frac{3}{8}$ in met de abc-knop: 


Druk nu nóg een keer op de abc-knop en je ziet 0,375 verschijnen. Druk tenslotte nóg een keer op de abc-knop en je bent weer terug bij de breuk.

Het percentage vind je door het decimale getal te vermenigvuldigen met 100.

## *§ 1.2 Beginnen met een decimaal getal*

Je rekenmachine kan je ook helpen met het omzetten van een decimaal getal naar een breuk. Voer maar eens 0,45 in en druk daarna op de abc-knop. Die maakt er keurig $\frac{9}{20}$ van.

Dit had je trouwens ook zelf gekund. Decimale getallen met twee decimalen zijn namelijk honderdsten. 0,45 is dus hetzelfde als 45-honderdste. Dat kun je zo als breuk schrijven: $\frac{45}{100}$. Als je deze breuk vervolgens vereenvoudigt (teller en noemer door 5 delen), staat er ook $\frac{9}{20}$

Zo zijn decimale getallen met één decimaal tienden, met twee decimalen honderdsten, met drie decimalen duizendsten etc.

Op deze manier kun je zelfs breuken maken van decimale getallen waar je rekenmachine niets mee doet. Probeer maar eens 0,123 om te zetten. Dat wordt $\frac{123}{1000}$ en dat klopt, want het getal heeft drie decimalen. En 0,1234? Inderdaad: $\frac{1234}{10000}$. Maar 0,1234567 kan je rekenmachine niet meer omzetten en jij wel: $\frac{1234567}{10000000}$ . Gewoon alle decimalen boven de breukstreep zetten en een 1 met net zoveel nullen eronder.

Niet alle decimale getallen kun je als breuk schrijven. Als er een oneindige reeks cijfers achter de komma staat, waar ook geen patroon in te ontdekken valt, dan kun je dat getal niet schrijven als breuk. Bijvoorbeeld het getal π. Dat begint met 3,1415926… maar er komt geen einde aan. Ook het getal $\sqrt{2}$ kun je niet als breuk schrijven. De benadering is 1,414213562… maar ook hier is het aantal decimalen oneindig groot.

## § 1.3 Decimalen die zich herhalen

Je kent de breuk $\frac{1}{3}$. Met je rekenmachine vind je 0,333333333… Maar hoeveel decimalen heeft dit getal eigenlijk? Oneindig veel. Dat is moeilijk voor te stellen, maar het is wel duidelijk dat alleen 0,3 of 0,33 niet hetzelfde is als $\frac{1}{3}$. Probeer maar met je rekenmachine.

Maar hoe kun je nou aan je rekenmachine duidelijk maken dat je oneindig veel decimalen bedoelt? Dat doe je door minimaal 13 decimalen in te voeren.

Test maar: Voer 0,333333333333 (12 drieën) in en druk op de abc-knop. Dat is geen $\frac{1}{3}$.

Voer nu 0,33333333333333 (14 drieën) in en druk op de abc-knop. Daar maakt de rekenmachine wél $\frac{1}{3}$ van. Kennelijk heeft de CASIO een trucje ingebouwd waardoor hij 'snapt' dat 14 decimalen 'oneindig' betekent.

In werkelijkheid klopt dat natuurlijk niet, want:

$$0{,}333333333333 = \frac{333333333333}{1000000000000} \quad en \quad 0{,}33333333333333 = \frac{33333333333333}{100000000000000}$$

## § 1.4 Het begrip repetent

Een decimaal die zich oneindig vaak herhaalt, noemen we repetent. We schrijven dat met een streepje boven de decimaal die zich herhaalt:

$$0{,}\overline{3} = 0{,}3333333333333333... \quad \text{'}\textit{nul komma drie repetent}\text{'}$$
$$0{,}\overline{4} = 0{,}4444444444444444... \quad \text{'}\textit{nul komma vier repetent}\text{'}$$
$$0{,}1\overline{8} = 0{,}1888888888888888... \quad \text{'}\textit{nul komma één acht repetent}\text{'}$$
$$0{,}\overline{18} = 0{,}181818181818181818... \quad \text{'}\textit{nul komma achttien repetent}\text{'}$$

### *Oefeningen*

1. Vul de ontbrekende getallen in de tabel in:

| | breuk | decimaal getal | percentage |
|---|---|---|---|
| 1 | | 0,375 | |
| 2 | $\frac{36}{900}$ | | |
| 3 | | $0{,}1\overline{6}$ | |
| 4 | $1\frac{1}{5}$ | | |
| 5 | | | 45% |
| 6 | | 0,52 | |
| 7 | $\frac{1}{17}$ | | |
| 8 | | 0,2345 | |
| 9 | $\frac{3}{45}$ | | |
| 10 | | | 82% |
| 11 | $\frac{2}{9}$ | | |
| 12 | | $1{,}\overline{5}$ | |
| 13 | $\frac{5}{32}$ | | |
| 14 | | | 105% |
| 15 | | 0,06 | |
| 16 | | 2,0014 | |
| 17 | $3\frac{4}{8}$ | | |
| 18 | | $0{,}\overline{9}$ | |

2. Het getal π kun je niet schrijven als breuk, maar het getal 3,1415926 wel. Leg uit waarom en schrijf dit getal als breuk.
3. Schrijf de breuken hieronder allemaal als decimaal getal. Maak gebruik van de repetent-schrijfwijze indien nodig.

   $\frac{1}{2}$ $\frac{1}{3}$ $\frac{1}{4}$ $\frac{1}{5}$ $\frac{1}{6}$ $\frac{1}{7}$ $\frac{1}{8}$ $\frac{1}{9}$

4. Schrijf de decimale getallen hieronder allemaal handmatig als breuk (zonder rekenmachine). Vergeet niet om zoveel mogelijk te vereenvoudigen.

   2,3456789 1,141414 0,4444444 0,123123

# 2. Cryptografie

## § 2.1 *Het eerste geheimschrift*

Misschien heb je zelf wel eens een paar woorden in geheimschrift geschreven. Bijvoorbeeld met de codering: a=1 b=2 c=3 d=4 etc. Als je dan "wiskunde is saai" wou schrijven, dan stond er: 23-9-19-11-21-14-4-5 9-19 19-1-1-9. Niet zo moeilijk om te kraken; de meeste mensen zullen begrijpen dat er voor ieder cijfer een letter moet komen en zij zullen waarschijnlijk eerst proberen of a=1 b=2 etc. de codering is.

Het gebruik van geheimschrift is al heel oud. Julius Caesar, een Romeins politicus en generaal, leefde in de laatste eeuw voor Christus. Ook hij gebruikte geheimschrift om instructies door te geven aan zijn veldheren. Hij bedacht het volgende systeem: In plaats van de letter A schrijf je de letter die 3 plaatsen verder staat, dus de D. In plaats van de letter B schrijf je dan E, in plaats van C schrijf je F en zo verder.

A B C D E F G H I J K …

A B C D E F G H I J K …

Julius Caesar varieerde natuurlijk met het aantal plaatsen. De ene keer 3 plaatsen, de andere keer 7 of 15. De methode staat daarom bekend als 'Caesarcijfer'. Bij iedere gecodeerde instructie moest het Caesarcijfer meegegeven worden; dat was dan het aantal plaatsen dat je moest opschuiven om het bericht te ontcijferen.

## § 2.2 *Frequentieanalyse*

Kijk eens naar de laatste alinea van §2.1 hierboven en tel hoe vaak de letter e voorkomt in dit stukje (*"Julius Caesar varieerde t/m ontcijferen"*). Als het goed is kom je op 53 uit. De letter e is de meest voorkomende letter in Nederlandse teksten. Daarna komen de letters a en n. Bij het ontcijferen van een gecodeerde tekst, waarbij iedere letter vervangen is door een andere, kun je daar gebruik van maken.

We nemen dit voorbeeld: VM LAVMKQMMMK BMMJU MMA ULKSMVL GGA DLLKV.

De codering is onbekend, maar we zien wel dat de letter M heel vaak voorkomt. We nemen aan dat de meest voorkomende letter een e moet zijn en vullen dat in:

V**E** LAV**E**KQ**EEE**K B**EE**JU **EE**A ULKS**E**VL GGA DLLKV.

Het eerste en vierde woord kun je nu raden, namelijk DE en EEN. Er zijn natuurlijk wel andere woorden mogelijk, maar deze woorden komen veel voor en liggen dus het meest voor de hand. Dat betekent dat V = **D** en A = **N**.

**DE** L**NDE**KQ**EEE**K B**EE**JU **EEN** ULKS**ED**L GG**N** DLLK**D**.

Ook het zesde woord is nu te kraken, want de G moet een klinker zijn en is geen e. De enige klinker die dan een woord oplevert is a. Dus: G = **A**

**DE** L**NDE**KQ**EEE**K B**EE**JU **EEN** ULKS**ED**L **AAN** DLLK**D**.

Nu kijken we naar het vijfde woord: ULKS**ED**L. Met wat kennis van de Nederlandse taal weet je dat dit woord na de letters ED niet veel mogelijkheden heeft. De laatste letter zou een E, A, O of T kunnen zijn. De E en A hebben we al, dus blijft over O of T. Het is niet de letter T, want dan zou het tweede woord beginnen met TNDE. Dus blijft over de letter O.

**DE ONDE**KQ**EEEE**K B**EE**JU **EEN** U**O**KS**EDO AAN** D**OO**K**D**.

Herken je het tweede woord? En als je bedenkt dat dit een militaire tekst is uit de Tweede Wereldoorlog? Je kunt altijd nog de beide K's in het woord één voor één vervangen door de letters die je nog niet hebt gebruikt. Zeker weten dat je uiteindelijk op onderzeeër uitkomt. En dan weet je ook dat K = **R** en Q = **Z**.

**DE ONDERZEEER** B**EE**JU **EEN** U**OR**S**EDO AAN** D**OORD**.

En zo komen we uiteindelijk aan de juiste tekst: DE ONDERZEEËR HEEFT EEN TORPEDO AAN BOORD. Deze methode heet 'frequentieanalyse' en kan in principe alle codes kraken waarbij iedere letter door één andere letter vervangen wordt.

Rond de middeleeuwen ging men daarom op zoek naar een ander codesysteem.

### *Oefeningen*

1. Julius Caesar gebruikte een codering voor de instructies aan zijn veldheren (zie § 2.1).
    a) Ontcijfer het woord QRRUGHUSRRUW aan de hand van Caesarcijfer 3.
    b) Hoeveel verschillende varianten kun je maken met het coderingssysteem van Julius Caesar?
    c) Maak een Excelblad met in de eerste kolom het alfabet van boven naar beneden en in de eerste rij de getallen 1 t/m 26 (zie afbeelding). Typ nu in het vakje B2 de volgende formule: =VERSCHUIVING($A2;B$1;0;1;1) en kopieer deze formule naar alle andere vakjes. Je hebt nu een soort decoderingstabel gemaakt voor alle Caesarcijfers.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 2 | a | | | | | | | | | | | | | |
| 3 | b | | | | | | | | | | | | | |
| 4 | c | | | | | | | | | | | | | |
| 5 | d | | | | | | | | | | | | | |
| 6 | e | | | | | | | | | | | | | |
| 7 | f | | | | | | | | | | | | | |
| 8 | g | | | | | | | | | | | | | |
| 9 | h | | | | | | | | | | | | | |
| 10 | i | | | | | | | | | | | | | |
| 11 | j | | | | | | | | | | | | | |
| 12 | k | | | | | | | | | | | | | |
| 13 | l | | | | | | | | | | | | | |
| 14 | m | | | | | | | | | | | | | |
| 15 | n | | | | | | | | | | | | | |
| 16 | o | | | | | | | | | | | | | |
| 17 | p | | | | | | | | | | | | | |

    d) Verklaar waarom er zoveel nullen in de tabel staan.
    e) Zet nog een tweede alfabet onder het eerste alfabet in de cellen A28 t/m A56
    f) Decodeer de tekst "Kpa pz llu tvvpl gpu." met Caesarcijfer 7.
    g) Decodeer het woord "fgnqfxnanny" met Caesarcijfer 13.

2. Zoek met behulp van frequentieanalyse uit wat hier staat:
    a) PG UGGV XWU PCUWQP YH GGU GGUP.
    b) MMX RMMK PWX RM HMXRM SWR CMMX CMKR.

# 3. Priemgetallen

## *A. Wat is een priemgetal?*

1. Een priemgetal is een geheel getal, groter dan 1, dat alléén deelbaar is door zichzelf en door 1.

   Voorbeelden:
   Het getal 7 is alléén deelbaar door zichzelf en door 1, dus 7 is een priemgetal
   Het getal 13 is alléén deelbaar door zichzelf en door 1, dus 13 is een priemgetal
   Het getal 8 is deelbaar door 1, 2, 4 en zichzelf, dus 8 is géén priemgetal
   Het getal 12 is deelbaar door 1, 2, 3, 4, 6 en zichzelf, dus 12 is géén priemgetal

   a) Ga met behulp van deze definitie na of de volgende getallen priemgetallen zijn:
      3 - 9 - 11 - 14 - 19 - 20 - 21
   b) Bestaan er eigenlijk wel *even* priemgetallen?

2. Hieronder staat de vermenigvuldigingstabel van de tafels van 1 t/m 10.

| | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* |
|---|---|---|---|---|---|---|---|---|---|---|
| *1* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* |
| *2* | *2* | *4* | *6* | *8* | *10* | *12* | *14* | *16* | *18* | *20* |
| *3* | *3* | *6* | *9* | *12* | *15* | *18* | *21* | *24* | *27* | *30* |
| *4* | *4* | *8* | *12* | *16* | *20* | *24* | *28* | *32* | *36* | *40* |
| *5* | *5* | *10* | *15* | *20* | *25* | *30* | *35* | *40* | *45* | *50* |
| *6* | *6* | *12* | *18* | *24* | *30* | *36* | *42* | *48* | *54* | *60* |
| *7* | *7* | *14* | *21* | *28* | *35* | *42* | *49* | *56* | *63* | *70* |
| *8* | *8* | *16* | *24* | *32* | *40* | *48* | *56* | *64* | *72* | *80* |
| *9* | *9* | *18* | *27* | *36* | *45* | *54* | *63* | *72* | *81* | *90* |
| *10* | *10* | *20* | *30* | *40* | *50* | *60* | *70* | *80* | *90* | *100* |

   a) Getallen die alléén deelbaar zijn door zichzelf en door 1 kunnen NIET voorkomen binnen het vak met de dikke zwarte rand. Leg uit waarom niet.
   b) Schrijf nu met behulp van deze tabel alle priemgetallen tussen 4 en 100 op.

3. Er is een simpele, maar tijdrovende methode om er achter te komen of een getal een priemgetal is:
   - probeer te delen door 2 (lukt dat? dan is het geen priemgetal)
   - probeer te delen door 3 (lukt dat? dan is het geen priemgetal)
   - probeer te delen door 5 (lukt dat? dan is het geen priemgetal)
   - enz.

   a) Leg uit waarom je ‘delen door 4’ kunt overslaan.
   b) Hoe lang moet je eigenlijk doorgaan met proberen?
   c) Test deze methode voor het getal 91

## *B. Priemfactoren*

4. Een priemfactor is een priemgetal dat je met een ander priemgetal vermenigvuldigt.
   Je kunt ieder (geheel) getal schrijven als een product (keersom) van priemfactoren. Dat kan ook maar op één manier.

   Voorbeelden:
   Het getal 8 kun je schrijven als $2 \times 2 \times 2$ (of $2^3$)
   Het getal 10 kun je schrijven als $2 \times 5$
   Het getal 12 kun je schrijven als $2 \times 2 \times 3$ (of $2^2 \times 3$)
   Het getal 63 kun je schrijven als $3 \times 3 \times 7$ (of $3^2 \times 7$)

   Methode:
   Deel het getal net zo lang door het kleinste priemgetal (2), totdat het niet meer kan.
   Deel daarna het overgebleven getal net zo lang door het volgende priemgetal (3), totdat het niet meer kan. Ga zo verder, net zo lang totdat je bent uitgekomen bij… een priemgetal.

   Voorbeeld:
   Stel je wilt 588 schrijven als een product van priemfactoren:

| | |
|---|---|
| 588 | 2 |
| 294 | 2 |
| 147 | 3 |
| 49 | 7 |
| 7 | 7 |

   $\Rightarrow$ $588 = 2 \times 2 \times 3 \times 7 \times 7$ (of $2^2 \times 3 \times 7^2$)

   a) Schrijf de volgende getallen als een product van priemfactoren:
      9 - 16 - 22 - 30 - 231 - 273
   b) Je merkt dat dit een behoorlijke klus is, vooral als de getallen groter worden. Google eens op *Online Prime Factorization Calculator* en test verschillende grote getallen. Kun je je voorstellen dat een getal van bijvoorbeeld 100 cijfers zelfs voor een computer lastig is?

## *C. RSA*

5. RSA is een manier om berichten te versleutelen, genoemd naar de drie ontwerpers:
   Ron **R**ivest, Adi **S**hamir en Len **A**dleman (1977). RSA wordt nu nog steeds door banken gebruikt om betalingsverkeer te versleutelen.

   Bij RSA worden twee getallen berekend, een codeergetal en een decodeergetal. Deze berekening vindt plaats aan de hand van twee priemfactoren, die met elkaar worden vermenigvuldigd. Het decodeergetal moet naar de ontvanger gestuurd worden, maar moet verder geheim blijven. Theoretisch is het mogelijk om de twee priemfactoren te achterhalen, als je de boodschap en het codeergetal hebt onderschept. En dan zou je ook het decodeergetal kunnen berekenen. Maar als je de twee priemfactoren maar groot genoeg maakt, kost het een computer een paar miljoen jaar om de berekening te maken. We hebben het dan bijvoorbeeld over priemfactoren van ieder 100 cijfers, die met elkaar vermenigvuldigd worden. Wil je meer weten? Kijk dan eens op:
   https://www.nemokennislink.nl/publicaties/hoe-werkt-rsa/