

Dossier 3

PRIEMGETALLEN

atomen van de getallenleer



Dr. Luc Gheysens

Een *priemgetal* is een natuurlijk getal met twee verschillende delers, nl. 1 en het getal zelf. De priemgetallen zijn dus 2, 3, 5, 7, 11,

De naam priemgetal is afgeleid van het Latijnse woord 'primus', wat eerste of primair betekent.

Priemgetallen kan men immers de atomen van de getallenleer noemen omdat elk natuurlijk getal groter dan 1 ofwel zelf een priemgetal is, ofwel op een unieke manier te schrijven is als een product van priemgetallen.

Zo is bv. $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5$ en $2009 = 7 \cdot 7 \cdot 41 = 7^2 \cdot 41$. Men zegt dat 7 en 41 priemdelers zijn van 2009.

Om het belang van de priemgetallen beter te begrijpen, bestuderen we eerst bondig de deelbaarheid in de verzameling van de gehele getallen.

Deelbaarheid in $\mathbb{Z}$

Definitie 1.

Voor elke twee gehele getallen a en b geldt:

$$a \text{ is een veelvoud van } b \Leftrightarrow \exists z \in \mathbb{Z} : a = b \cdot z.$$

Wanneer a een veelvoud is van b , dan zegt men dat a deelbaar is door b . De verzameling van de veelvouden van het geheel getal b noteert men : $b\mathbb{Z}$.

Voorbeeld.

-35 is een veelvoud van 5 want voor het geheel getal $z = -7$ is $-35 = 5 \cdot (-7)$.

De verzameling van de veelvouden van 5 is $5\mathbb{Z} = \{ \dots, -10, -5, 0, 5, 10, \dots \}$.

Definitie 2.

Voor elke twee gehele getallen a en b geldt:

$$b \text{ is een deler van } a \Leftrightarrow \exists z \in \mathbb{Z} : a = b \cdot z.$$

Notatie: $b \mid a$.

De verzameling van de delers van a noteert men : $\text{del } a$.

Voorbeeld.

3 is een deler van -12 want voor het geheel getal $z = -4$ is $-12 = 3 \cdot (-4)$.

$\text{del } (-12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$.

Merk op. $\text{del } 0 = \mathbb{Z}$.

Opgave 1.

Bewijs de volgende twee eigenschappen van de relatie ‘is deler van’ in $\mathbb{Z}$.

Eigenschap 1. De relatie ‘is deler van’ in $\mathbb{Z}$ is reflexief.

Eigenschap 2. De relatie ‘is deler van’ in $\mathbb{Z}$ is transitief.

Is de relatie ‘is deler van’ in $\mathbb{Z}$ antisymmetrisch? Verklaar.

Opgave 2.

Bewijs de volgende twee stellingen. Schrijf telkens het gegeven en het te bewijzen op en bewijs hiermee de stelling.

Stelling 1. Een deler van twee gehele getallen is een deler van de som van die twee getallen.

Stelling 2. Een deler van een geheel getal is een deler van elk veelvoud van dit geheel getal.

Uit deze twee stellingen volgt:

$$\forall a, b, d \in \mathbb{Z}, \forall r, s \in \mathbb{Z} : d \mid a \text{ en } d \mid b \Rightarrow d \mid ra + sb.$$

Het getal $ra + sb$ noemt men een lineaire combinatie van a en b en de gehele getallen r en s zijn dan de coëfficiënten van de lineaire combinatie $ra + sb$. Dit gevolg kan men dus als volgt formuleren: elke deler van twee gehele getallen is een deler van elke lineaire combinatie van die twee getallen (*stelling van de lineaire combinatie*).

Voorbeeld.

$5 \mid -10$ en $5 \mid 15$, dan geldt: $5 \mid 2 \cdot (-10) + 3 \cdot 15$, m.a.w. $5 \mid 25$

$5 \mid -10$ en $5 \mid 15$, dan geldt: $5 \mid (-3) \cdot (-10) + 4 \cdot 15$, m.a.w. $5 \mid 90$

$5 \mid -10$ en $5 \mid 15$, dan geldt: $5 \mid 0 \cdot (-10) + 4 \cdot 15$, m.a.w. $5 \mid 60$

$5 \mid -10$ en $5 \mid 15$, dan geldt: $5 \mid 0 \cdot (-10) + 0 \cdot 15$, m.a.w. $5 \mid 0$.

Opgave 3.

Als a, b, m en n gehele getallen zijn dan geldt

(a) elke gemeenschappelijke deler van $a - b$ en $m + n$ is ook een deler van $am + bn$.

(b) elke gemeenschappelijke deler van $a + b$ en $m + n$ is ook een deler van $am - bn$.

Bewijs dit.

Opgave 4.

Toon aan dat er geen gehele getallen r en s bestaan zodat $4r - 2s = 1$.

Opgave 5.

Als a, b en c gehele getallen zijn en als a deelbaar is door bc , dan is a deelbaar door b en door c . Bewijs dit. Is het omgekeerde ook waar?

Opgave 6.

Voor elk getal c , niet gelijk aan 0 geldt: a is deelbaar door b als en slechts als ac deelbaar is door bc . Bewijs dit.

De euclidische deling in $\mathbb{Z}$

We vertrekken van een merkwaardige vaststelling die we niet kunnen bewijzen met vroeger aangenomen axioma's, eigenschappen of stellingen. Daarom nemen we die eigenschap aan als een axioma:

Axioma van Archimedes

Voor een willekeurig geheel getal a en een willekeurig strikt positief geheel getal b , bestaat er precies één geheel getal z zodat $z \cdot b \leq a < (z + 1) \cdot b$.
Hierbij zijn $z \cdot b$ en $(z + 1) \cdot b$ dus twee opeenvolgende veelvouden van b .

In symbolen: $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}_0^+, \exists! z \in \mathbb{Z} : z \cdot b \leq a < (z + 1) \cdot b$.

Voorbeelden.

Tussen welke twee opeenvolgende veelvouden van 3 ligt -25?

Welnu: $(-9) \cdot 3 \leq -25 < (-8) \cdot 3$.

Tussen welke twee opeenvolgende veelvouden van 4 ligt -12?

Welnu: $(-3) \cdot 4 \leq -12 < (-2) \cdot 4$.

Wanneer we een geheel getal D (deeltal) delen door een strikt positief getal d (deler), dan zoeken we in feite naar het grootste veelvoud van d dat kleiner is dan of gelijk aan D . Hieruit volgt dat de rest geen negatief getal kan zijn.

Voorbeelden.

$(-38) : 7$ geeft als quotiënt -6 omdat $(-6) \cdot 7 = -42$ het grootste veelvoud is van -6 dat kleiner is dan of gelijk aan -38. De rest r is gelijk aan 4.

$(-130) : 12$ geeft als quotiënt -11 en als rest 2.

$(-123) : 12$ geeft als quotiënt -11 en rest 11.

$(-132) : 12$ geeft als quotiënt -11 en rest 0.

Algemene formule voor de euclidische deling in $\mathbb{Z}$:

$$D = d \cdot q + r \text{ met } 0 \leq r < d.$$

Hierbij is D = het deeltal, d = de deler (een strikt positief geheel getal), q = het quotiënt en r = de rest.

De rest is bijgevolg gelijk aan één van de volgende getallen : 0, 1, 2, ..., $d-1$.

Opgave 7.

- (a) Bepaal de gehele getallen die bij deling door 6 als quotiënt -16 hebben.
- (b) De deler van een deling is 18 en het quotiënt is -15. Bepaal het deeltal als de rest zo groot mogelijk moet zijn.
- (c) De deler van een deling is 18 en het quotiënt is -15. Bepaal het grootst mogelijke deeltal.

Stelling 1. Uniciteitsstelling

Als een geheel getal D gedeeld wordt door een strikt positief geheel getal d , dan bestaat er bij de euclidische deling juist één quotiënt q en één rest r .

Gegeven : $D, d \in \mathbb{Z}$
 $d > 0$

Te bewijzen : $\exists! q, r \in \mathbb{Z} : D = d \cdot q + r$ met $0 \leq r < d$.

Bewijs

Wegens het axioma van Archimedes weten we dat er juist één geheel getal q bestaat zodat $q \cdot d \leq D < (q + 1) \cdot d$. Bijgevolg is $0 \leq D - q \cdot d < d$, waarbij $D - q \cdot d$ een geheel getal is. Stellen we $D - q \cdot d$ gelijk aan r , dan geldt $D = d \cdot q + r$ met $0 \leq r < d$. Hierbij is q uniek en bijgevolg is ook r uniek bepaald.

Stelling 2.

Als een geheel getal deeltal en deler deelt, dan deelt dat getal ook de rest.

Opmerking. Met behulp van verzamelingen kunnen we dit resultaat ook als volgt uitdrukken:
 $(\text{del } D \cap \text{del } d) \subset \text{del } r$.

Stelling 3.

Als een geheel getal deler en rest deelt, dan deelt dat getal ook het deeltal.

Opmerking. Met behulp van verzamelingen kunnen we dit resultaat ook als volgt uitdrukken:
 $(\text{del } d \cap \text{del } r) \subset \text{del } D$.

Opgave 8.

Bewijs stelling 2 en stelling 3. Maak telkens gebruik van de stelling van de lineaire combinatie (zie opgave 2).

GROOTSTE GEMEENSCHAPPELIJKE DELER

Er bestaat een eenvoudig rekenschema om de *grootste gemeenschappelijke deler* van twee getallen te bepalen, het zogenaamd **algoritme van Euclides**.

We beperken ons vanaf hier tot de verzameling van de natuurlijke getallen en noteren de grootste gemeenschappelijke deler van twee natuurlijke getallen a en b met $\text{ggd}(a, b)$.



Euclides van Alexandrië (ca. 300 v. Chr.)

Stelling.

De grootste gemeenschappelijke deler van het deeltal D en de deler d van een euclidische deling is dezelfde als de grootste gemeenschappelijke deler van de deler d en de rest r .

Gegeven: $D = d \cdot q + r$ met $0 \leq r < d$

Te bewijzen: $\text{ggd}(D, d) = \text{ggd}(d, r)$.

Bewijs

$$\begin{array}{lcl}
 (\text{del } D \cap \text{del } d) \subset \text{del } r & & (\text{del } d \cap \text{del } r) \subset \text{del } D \\
 \Downarrow & & \Downarrow \\
 (\text{del } D \cap \text{del } d \cap \text{del } d) \subset (\text{del } r \cap \text{del } d) & | & (\text{del } d \cap \text{del } r \cap \text{del } d) \subset (\text{del } D \cap \text{del } d) \\
 \Downarrow & & \Downarrow \\
 (\text{del } D \cap \text{del } d) \subset (\text{del } r \cap \text{del } d) \quad (1) & | & (\text{del } d \cap \text{del } r) \subset (\text{del } D \cap \text{del } d) \quad (2)
 \end{array}$$

Uit (1) en (2) volgt dat $(\text{del } d \cap \text{del } r) = (\text{del } D \cap \text{del } d)$ zodat $\text{ggd}(D, d) = \text{ggd}(d, r)$.

Het volstaat dus van twee natuurlijke getallen het quotiënt en de rest te bepalen via een euclidische deling en op die twee getallen weer dezelfde procedure toe te passen tot men uiteindelijk een rest gelijk aan nul bekommt. De laatst bekomen deler is dan de gezochte grootste gemeenschappelijke deler van de twee oorspronkelijke getallen. We kunnen dit in een overzichtelijk rekenschema uitwerken, via het zogenaamde algoritme van Euclides.

Voorbeeld 1.

Bepaal $\text{ggd}(84, 76)$ met het algoritme van Euclides.

	1	9	2	
84	76	8	4	← quotiënten
76	72	8		← delers
8	4	0		← resten

Besluit: $\text{ggd}(84, 76) = 4$.

Voorbeeld 2.

Bepaal $\text{ggd}(296, 136)$ met het algoritme van Euclides.

	2	5	1	2	
296	136	24	16	8	← quotiënten
272	120	16	16		← delers
24	16	8	0		← resten

Besluit: $\text{ggd}(296, 136) = 8$.

Hieruit volgt direct een merkwaardig resultaat uit de getaltheorie.

Stelling van Bachet-Bézout.

De grootste gemeenschappelijke deler van twee natuurlijke getallen a en b , niet allebei gelijk aan 0, is een lineaire combinatie van a en b , m.a.w.

$$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}_0, \exists r, s \in \mathbb{Z} : \text{ggd}(a, b) = ra + sb.$$

Dit illustreren we aan de hand van de twee bovenstaande voorbeelden.

Voorbeeld 1.

$$84 = 1 \cdot 76 + 8 \Rightarrow 8 = 84 - 1 \cdot 76$$

$$76 = 9 \cdot 8 + 4 \Rightarrow 4 = 76 - 9 \cdot 8 = 76 - 9 \cdot (84 - 1 \cdot 76) = 10 \cdot 76 - 9 \cdot 84.$$

Bijgevolg is $4 = 10 \cdot 76 - 9 \cdot 84$.

Voorbeeld 2..

$$296 = 2 \cdot 136 + 24 \Rightarrow 24 = 296 - 2 \cdot 136$$

$$136 = 5 \cdot 24 + 16 \Rightarrow 16 = 136 - 5 \cdot 24 = 136 - 5 \cdot (296 - 2 \cdot 136) = 11 \cdot 136 - 5 \cdot 296$$

$$24 = 1 \cdot 16 + 8 \Rightarrow 8 = 24 - 1 \cdot 16 = (296 - 2 \cdot 136) - 1 \cdot (11 \cdot 136 - 5 \cdot 296)$$

Bijgevolg is $8 = 6 \cdot 296 - 13 \cdot 136$.

Gevolg.

Als twee natuurlijke getallen a en b onderling ondeelbaar zijn (d.w.z. dat hun grootste gemeenschappelijke deler gelijk is aan 1), dan bestaat er een lineaire combinatie van a en b die gelijk is aan 1.

Voorbeeld.

$$\text{ggd}(5, 13) = 1.$$

$$13 = 2 \cdot 5 + 3 \Rightarrow 3 = 13 - 2 \cdot 5$$

$$5 = 1 \cdot 3 + 2 \Rightarrow 2 = 5 - 1 \cdot 3 = 5 - 1 \cdot (13 - 2 \cdot 5) = 3 \cdot 5 - 1 \cdot 13$$

$$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 1 \cdot 2 = (13 - 2 \cdot 5) - 1 \cdot (3 \cdot 5 - 1 \cdot 13) = 2 \cdot 13 - 5 \cdot 5$$

$$\text{Dus is } 2 \cdot 13 - 5 \cdot 5 = 1.$$

Opgave 9.

Bepaal telkens de gevraagde grootste gemeenschappelijke deler en schrijf die als een lineaire combinatie van de twee gegeven getallen.

- 1) $\text{ggd}(360, 128)$
- 2) $\text{ggd}(105, 85)$
- 3) $\text{ggd}(5250, 1925)$.

Opgave 10.

Bepaal een koppel gehele getallen (r, s) zodat

- 1) $7r + 11s = 1$
- 2) $9r + 23s = 1$.

Opmerking.

Als men de grootste gemeenschappelijke deler wil bepalen van drie natuurlijke getallen a , b en c , niet alle drie gelijk aan 0, dan volstaat het de eerste twee getallen te vervangen door hun grootste gemeenschappelijke deler d en dan de grootste gemeenschappelijke deler van c en d te bepalen:

$$\text{ggd}(a, b, c) = \text{ggd}(\text{ggd}(a, b), c).$$

Opgave 11.

Bepaal $\text{ggd}(144, 240, 204)$.

KLEINSTE GEMEENSCHAPPELIJK VEELVOUD

Om het kleinste gemeenschappelijk veelvoud van twee natuurlijke getallen a en b te bepalen, kunnen we op een handige manier gebruik maken van hun grootste gemeenschappelijke deler. We noteren het kleinste gemeenschappelijk veelvoud van a en b met $\text{kgv}(a, b)$.

Hulpstelling

Als men twee natuurlijke getallen deelt door hun grootste gemeenschappelijke deler, dan zijn de quotiënten onderling ondeelbaar.

Gegeven: $\text{ggd}(a, b) = d$

Te bewijzen: $\text{ggd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Bewijs uit het ongerijmde.

Stel dat $a = d \cdot q_1$ en $b = d \cdot q_2$ en dat de quotiënten q_1 en q_2 een gemeenschappelijke deler d' hebben die groter is dan 1.

Dan is

$$q_1 = d' \cdot q_3 \text{ en } q_2 = d' \cdot q_4$$

en bijgevolg is

$$a = d \cdot (d' \cdot q_3) = (d \cdot d') \cdot q_3 \text{ en } b = d \cdot (d' \cdot q_4) = (d \cdot d') \cdot q_4$$

waaruit blijkt dat a en b een gemeenschappelijke deler $d \cdot d'$ hebben die groter is dan d . Dit is een contradictie met het gegeven dat d de grootste gemeenschappelijke deler is van a en b .

Stelling.

Het kleinste gemeenschappelijk veelvoud van twee natuurlijke getallen a en b , niet gelijk aan 0, is gelijk aan

$$\text{kgv}(a, b) = \frac{a \cdot b}{\text{ggd}(a, b)}.$$

Gegeven: $a, b \in \mathbb{N}_0$
 $\text{ggd}(a, b) = d$

Te bewijzen: $\text{kgv}(a, b) = \frac{a \cdot b}{d}$

Bewijs

- Deel 1. We tonen aan dat $\frac{a \cdot b}{d}$ een gemeenschappelijke deler is van a en b .

Omdat d een gemeenschappelijke deler is van a en b zijn de getallen $\frac{a}{d}$ en $\frac{b}{d}$ allebei natuurlijke getallen.

Bijgevolg is $\frac{a \cdot b}{d} = a \cdot \frac{b}{d}$ een veelvoud van a en is $\frac{a \cdot b}{d} = b \cdot \frac{a}{d}$ ook een veelvoud van b .

- Deel 2. We tonen aan dat $\frac{a \cdot b}{d}$ een deler is van alle gemeenschappelijke veelvouden van a en b .

Stel dat v een gemeenschappelijk veelvoud is van a en b , dan is $v = a \cdot n_1$ en $v = b \cdot n_2$ met $n_1, n_2 \in \mathbb{N}$.

Omdat $\text{ggd}(a, b) = d$, is $a = d \cdot q_1$ en $b = d \cdot q_2$, waarbij q_1 en q_2 onderling ondeelbaar zijn (wegens de hulpstelling).

Bijgevolg geldt:

$$\begin{aligned} a \cdot n_1 &= b \cdot n_2 \\ \Downarrow \\ (d \cdot q_1) \cdot n_1 &= (d \cdot q_2) \cdot n_2 \\ \Downarrow \\ d \cdot (q_1 \cdot n_1) &= d \cdot (q_2 \cdot n_2) \\ \Downarrow \\ q_1 \cdot n_1 &= q_2 \cdot n_2 \\ \Downarrow \\ q_1 \mid q_2 \cdot n_2 & \quad (q_1 \text{ en } q_2 \text{ zijn onderling ondeelbaar}) \\ \Downarrow \\ q_1 \mid n_2 & \\ \Downarrow \\ n_2 &= q_1 \cdot n \quad \text{met } n \in \mathbb{N}. \end{aligned}$$

Dus is

$$\begin{aligned} v &= b \cdot n_2 \\ \Downarrow \\ v &= b \cdot (q_1 \cdot n) \\ \Downarrow \\ v &= b \cdot \left(\frac{a}{d} \cdot n\right) \\ \Downarrow \\ v &= \frac{a \cdot b}{d} \cdot n \\ \Downarrow \\ \frac{a \cdot b}{d} &\mid n. \end{aligned}$$

Voorbeeld.

$$\text{kgv}(12, 15) = \frac{12 \cdot 15}{\text{ggd}(12, 15)} = \frac{180}{3} = 60.$$

Opgave 12.

Bepaal

- 1) $\text{kgv}(75, 100)$
- 2) $\text{kgv}(84, 220)$

Opmerking.

Als men het kleinste gemeenschappelijk veelvoud wil bepalen van drie natuurlijke getallen a , b en c , dan volstaat het de eerste twee getallen te vervangen door hun kleinste gemeenschappelijk veelvoud v en dan het kleinste gemeenschappelijk veelvoud van c en v te bepalen:

$$\text{kgv}(a, b, c) = \text{kgv}(\text{kgv}(a, b), c).$$

Opgave 13.

- (a) Bepaal $\text{kgv}(36, 210, 330)$
- (b) Een lucifersdoosje heeft de volgende afmetingen:
lengte = 54 mm, breedte = 36 mm en hoogte = 12 mm.
Bepaal het kleinste aantal doosjes dat men nodig heeft om ze als een kubus te stapelen.

PRIEMGETALLEN

Zoals we eerder al opmerkten beperken we ons hier tot de studie van deelbaarheid in de verzameling van de natuurlijke getallen.

Een natuurlijk getal is een *priemgetal* als het precies twee delers heeft, nl. 1 en het getal zelf.

De priemgetallen kleiner dan 100 zijn:

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

Op <http://www.kennislink.nl/publicaties/priemgetallen> vind je een leerrijke tekst over priemgetallen, met o.a. een verwijzing naar de zeef van Eratosthenes, Mersenne-priemgetallen, het belang van priemgetallen in de cryptografie en onopgeloste problemen i.v.m. priemgetallen (zoals het vermoeden van Goldbach, het probleem van het aantal priemtweelingen ...).

De delers 1 en n van een natuurlijk getal n ($n \neq 0$), noemt men de **onechte delers** van n . Alle andere delers van n noemt men **echte delers** van n .

Een natuurlijk getal n verschillend van 0 en 1 en dat geen priemgetal is, noemt men **een deelbaar getal**.

Voorbeeld.

De echte delers van 12 zijn 2, 3, 4, en 6.

Stelling.

De kleinste echte deler van een deelbaar getal is een priemgetal en zijn kwadraat is niet groter dan het gegeven getal.

Gegeven: n is een deelbaar getal

d is de kleinste echte deler van n .

Te bewijzen: 1. d is een priemgetal

2. $d^2 \leq n$.

Bewijs

1. Om te bewijzen dat d een priemgetal is maken we gebruik van een bewijs uit het ongerijmde.

Veronderstel dat d geen priemgetal is.

Dan geldt :

$$\begin{aligned} \exists d_1 \in \mathbb{N} : d_1 \mid d \text{ en } d_1 \notin \{1, d\} \\ \Downarrow \\ 0 < d_1 < d. \quad (1) \end{aligned}$$

Bovendien is $d_1 \mid d$ en $d \mid n \Rightarrow d_1 \mid n$. (2)

Uit (1) en (2) besluiten we dat d niet de kleinste echte deler is van n . Dit is in tegenstrijd met het gegeven en bijgevolg is d een priemgetal.

2. We bewijzen dat $d^2 \leq n$.

d is de kleinste echte deler van n

$\Downarrow$

$n = d \cdot n_1$ met $n_1 \in \mathbb{N}$ en $d \leq n_1$

$\Downarrow$

$d \cdot d \leq n$.

Gevolg. Elk deelbaar getal is deelbaar door een priemgetal.

Om te onderzoeken of een natuurlijk getal n een priemgetal is of niet, controleer je of het getal deelbaar is door één van de priemgetallen 2, 3, 5, 7, 11, ... en je eindigt jouw onderzoek van zodra je een priemgetal gebruikt waarvan het kwadraat groter is dan n .

Voorbeeld.

Om te controleren of 149 een priemgetal is kijken we of 149 deelbaar is door 2, 3, 5, 7 of 11. Dit blijkt niet het geval te zijn en bijgevolg is 149 een priemgetal.

Elk natuurlijk getal kan men schrijven als een product van priemfactoren (als het zelf een priemgetal is, kan je dit beschouwen als een ‘product’ met slechts één factor). Men noemt dit ‘een getal ontbinden in priemfactoren’. Het volstaat het getal telkens te delen door een zo klein mogelijk priemgetal.

Voorbeelden.

180		2	9 625		5
90		2	1 925		5
45		3	385		5
15		3	77		7
5		5	11		11
1			1		

$$180 = 2^2 \cdot 3^2 \cdot 5$$

$$9\,625 = 5^3 \cdot 7 \cdot 11$$

We tonen nu aan dat deze ontbinding in priemfactoren uniek is. Hiervoor bewijzen we eerst een hulpstelling (lemma).

Lemma van Euclides

Als het product van twee natuurlijke getallen deelbaar is door een priemgetal, dan is tenminste één van die getallen deelbaar door dat priemgetal.

Gegeven: een priemgetal p
 a en b zijn natuurlijke getallen
 p deelt het product ab

Te bewijzen: p deelt a of b

Bewijs:

Stel dat p het getal a niet deelt. Dan is $\text{ggd}(p, a) = 1$. Wegens de stelling van Bachet-Bézout bestaan er dan gehele getallen r en s zodat $rp + sa = 1$. We vermenigvuldigen beide leden met b en bekomen zo dat $rpb + sab = b$. We stellen vast dat p een deler is van rpb (evident) en van sab (gegeven). Bijgevolg is p een deler van de som van deze beide getallen en dus ook van b .

Gevolg.

Als een product van meerdere natuurlijke getallen deelbaar is door een priemgetal, dan is minstens één van de factoren deelbaar door dit priemgetal.

Voor het bewijs hiervan volstaat het het lemma van Euclides herhaald toe te passen.

Hoofdstelling van de rekenkunde

Ieder natuurlijk getal groter dan 1 is op de volgorde van de factoren na eenduidig te schrijven als product van priemgetallen.

Bewijs uit het ongerijmde.

Veronderstel dat het natuurlijk getal n op twee verschillende manieren te schrijven is als een product van priemfactoren: $n = p_1 p_2 \dots p_r$ en $n = q_1 q_2 \dots q_s$ met $r \leq s$.

Wegens de definitie van ‘deler’ is p_1 een deler van $q_1 q_2 \dots q_s$. Wegens het gevolg van het lemma van Euclides zal p_1 één van de getallen $q_1, q_2, \dots, q_s$ delen, laten we zeggen q_i . Maar omdat p_1 en q_i allebei priemgetallen zijn, volgt dat $p_1 = q_i$. We verwisselen nu de factoren q van plaats zodat q_i op de eerste plaats komt in het product $q_1 q_2 \dots q_s$. We delen beide priemfactorontbindingen van n dan door p_1 en bekomen dat $p_2 \dots p_r = q_2 \dots q_s$. We herhalen nu dit procédé en vinden zo dat elke factor p ook moet voorkomen bij de factoren q .

Wanneer we in beide ontbindingen alle factoren p hebben geschrapt, zijn er twee mogelijkheden:

- ofwel is $r = s$ en dan is de stelling bewezen:
- ofwel is $r < s$. Maar dan verkrijgen we na het schrappen van $p_1, p_2, \dots$ en p_r dat $1 = q_{r+1} q_{r+2} \dots q_s$. Dit is echter onmogelijk: een product van een aantal priemgetallen kan niet gelijk zijn aan 1.

Bijgevolg is $r = s$.

Een **algemene formule voor priemgetallen** is niet gekend. De Zwitserse wiskundige Leonhard Euler ontdekte wel dat $n^2 + n + 41$ een priemgetal oplevert voor $n = 0, 1, 2, \dots$ tot en met $n = 39$.

Zo is voor $n = 40$ de uitdrukking $n^2 + n + 41$ gelijk aan

$$40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \cdot 41 + 41 = 41^2$$

en dus duidelijk geen priemgetal.



Leonhard Euler (1707 – 1783)

Euclides bewees dat de rij van de priemgetallen onbegrensd is.

Stelling.

Er bestaat geen grootste priemgetal.

Gegeven : p is een priemgetal.

Te bewijzen: er bestaat een priemgetal groter dan p .

Bewijs.

Bepaal het product van alle priemgetallen kleiner dan of gelijk aan p en vermeerder dit product met 1. Het bekomen getal noemen we n :

$$n = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p + 1.$$

- Als n een priemgetal is, dan is de stelling bewezen want n is groter dan p .
- Als n geen priemgetal is, dan bestaat er een priemgetal d , groter dan 1, dat een deler is van n . Deze deler d kan niet gelijk zijn aan één van de factoren 2, 3, 5, ..., p omdat de rest bij deling van n door elk van die priemgetallen steeds gelijk is aan 1. Bijgevolg is d een priemgetal groter dan p .

Merk op.

$2 + 1 = 3$ is een priemgetal

$2 \cdot 3 + 1 = 7$ is een priemgetal

$2 \cdot 3 \cdot 5 + 1 = 31$ is een priemgetal

$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ is een priemgetal

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ is een priemgetal

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ en is dus geen priemgetal.

Toepassing 1.

De grootste gemeenschappelijke deler van twee natuurlijke getallen die in priemfactoren zijn ontbonden, is het product van de gemeenschappelijke priemfactoren, elk met de kleinste exponent die hierin voorkomt.

Voorbeelden.

Als $a = 135 = 3^3 \cdot 5$ en $b = 1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$, dan is $\text{ggd}(a, b) = 3^2 \cdot 5 = 45$.

Als $a = 2800 = 2^4 \cdot 5^2 \cdot 7$ en $b = 3000 = 2^3 \cdot 3 \cdot 5^3$, dan is $\text{ggd}(a, b) = 2^3 \cdot 5^2 = 200$.

Toepassing 2.

Het kleinste gemeenschappelijk veelvoud van twee natuurlijke getallen die in priemfactoren zijn ontbonden, is het product van alle verschillende priemfactoren, elk met de grootste exponent die hierin voorkomt.

Voorbeelden.

Als $a = 135 = 3^3 \cdot 5$ en $b = 1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$, dan is $\text{kgv}(a, b) = 2^2 \cdot 3^3 \cdot 5 \cdot 7 = 3780$.

Als $a = 2800 = 2^4 \cdot 5^2 \cdot 7$ en $b = 3000 = 2^3 \cdot 3 \cdot 5^3$, dan is $\text{kgv}(a, b) = 2^4 \cdot 3 \cdot 5^3 \cdot 7 = 42000$.

Je kan hiermee direct controleren dat $a \cdot b = \text{kgv}(a, b) \cdot \text{ggd}(a, b)$.

Opgave 15.

Ontbind telkens de gegeven getallen in priemfactoren en bepaal hiermee hun ggd en kgv.

1. $a = 84$ en $b = 126$.
2. $a = 400$ en $b = 5\,500$.
3. $a = 4\,200$, $b = 500$ en $c = 324$.

Opgave 16.

1. Bepaal twee natuurlijke getallen a en b zodat $a^2 - b^2 = 17$.
2. Is elk oneven getal gelijk aan het verschil van de kwadraten van twee natuurlijke getallen? Verklaar.

Opgave 17.

1. Bepaal a en b als $\text{kgv}(a, b) = 336$ en $\text{ggd}(a, b) = 14$.
2. Bepaal a en b als $\text{kgv}(a, b) = 540$ en $a \cdot b = 6480$.

Opgave 18.

1. Pas het principe van de zeef van Eratosthenes toe om in het onderstaande schema alle priemgetallen kleiner dan of gelijk aan 100 te bepalen.

	2	3	4	5	6
6	8	9	10	11	12
12	14	15	16	17	18
18	20	21	22	23	24
24	26	27	28	29	30
30	32	33	34	35	36
36	38	39	40	41	42
42	44	45	46	47	48
48	50	51	52	53	54
54	56	57	58	59	60
60	62	63	64	65	66
66	68	69	70	71	72
72	74	75	76	77	78
78	80	81	82	83	84
84	86	87	88	89	90
90	92	93	94	95	96
96	98	99	100		

2. Verklaar waarom alle priemgetallen groter dan 3 zich in de eerste en de vijfde kolom bevinden.
3. Kies een willekeurig priemgetal tussen 10 en 100. Kwadrateer dit getal en tel er 5 bij op. Waarom is het bekomen resultaat steeds deelbaar door 3?

Opgave 19.

Twee kerkklokken worden gelijktijdig op het juiste uur gezet. Het eerste klok loopt per dag 6 minuten voor en de tweede klok loopt per dag 4 minuten achter. Na hoeveel dagen zullen beide klokken weer voor het eerst tegelijk het juiste uur aanwijzen?

Opgave 20.

De omtrek van de voorwielen van een tractor is 172 cm en de omtrek van de achterwielen is 396 cm. Welke is de kortste afstand die de tractor moet afleggen zodat de voor- en de achterwielen tegelijk een geheel aantal omwentelingen hebben gemaakt? Hoeveel omwentelingen hebben de voorwielen dan gemaakt?

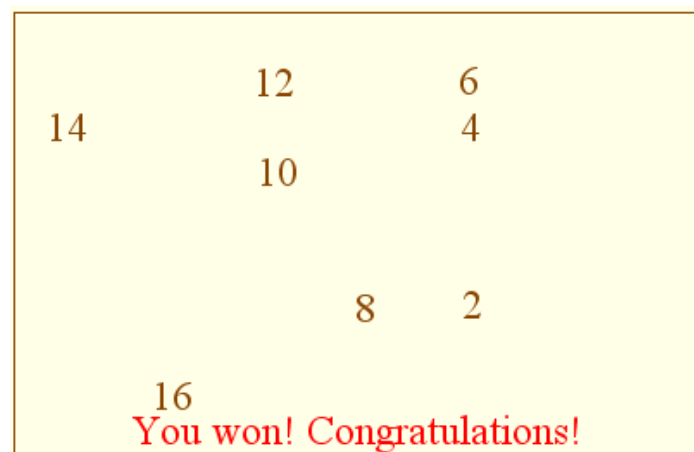
Het spel van Euclides

Op de Engelstalige website <http://www.cut-the-knot.org/blue/EuclidAlg.shtml> kan je een leuk spel spelen tegen de computer. Het spel steunt in feite op het algoritme van Euclides en wordt daarom **Euclid's game** genoemd.

De computer kiest twee natuurlijke getallen en plaatst die in een kader. Dan moeten jij en de computer om de beurt een natuurlijk getal geven dat het verschil is van twee getallen die reeds in het kader staan. De verliezer is de speler die geen nieuw getal meer kan geven.

Bij dit spel is het belangrijk wie begint en daarom kan jij onder het kader het vakje aanvinken met 'please start' waarmee je de computer verplicht de eerste 'zet' te doen. Die zet ligt natuurlijk vast, want bij de eerste zet kan je alleen het kleinste getal in het kader aftrekken van het grootste.

Bij het spel dat ik onlangs speelde waren de begingetallen 10 en 16. Ik liet de computer starten (met het getal 6). Hieronder zie je de eindsituatie.



Welke strategie moet je volgen om bij dit spel te winnen?

Bronvermelding.

F. Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven, Utrecht, 2000.

A. van den Essen, *Nieuwe getallenstelsels*, Veen Magazines, Diemen, 2010.

Priemgetallen – Luc Gheysens

Bijlage.

Een programma voor het grafisch rekentoestel om de grootste gemeenschappelijke deler en het kleinste gemeenschappelijk veelvoud van twee natuurlijke getallen te bepalen. Dit programma is gebaseerd op het algoritme van Euclides

PROGRAM:GGDKGV

```
:ClrHome
:Input "GROOTSTE GETAL",A
:Input "KLEINSTE GETAL",B
:A*B→P
:1→R
:While R≠0
:  int(A/B)→Q
:  A - B*Q→R
:  B→A
:  R→B
:End
:Disp "GGD="
:Output(5,6,A)
:Disp "KGV="
:Output(6,6,P/A)
```

Commentaar

wis het scherm

input: het grootste getal A

input: het kleinste getal B

P = het product van de getallen A en B

*aan R (de rest) kennen we de waarde 1 toe
zolang R≠0 is, blijven we verder delen*

Q : quotiënt van de deling van A door B

R : de rest van de deling van A door B

B wordt de nieuwe A-waarde

R wordt de nieuwe B-waarde

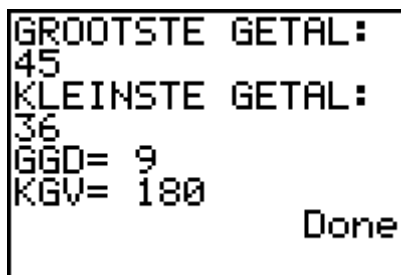
einde van het algoritme (als R = 0)

output: tekst

output A (= gcd) op lijn 5 positie 6

output: tekst

output P/A (=kgv) op lijn 6 positie 6

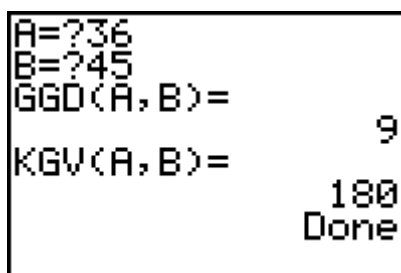


```
GROOTSTE GETAL:
45
KLEINSTE GETAL:
36
GGD= 9
KGV= 180
Done
```

Er bestaat natuurlijk een eenvoudiger versie van dit programma waarbij we gebruik maken van de ingebouwde functies gcd (greatest common divisor) en lcm(least common multiple) om de gcd en het kgv van twee natuurlijke getallen te bepalen.

PROGRAM:GGDKGV1

```
:ClrHome
:Prompt A,B
:Disp "GGD(A,B)="
:Disp gcd(A,B)
:Disp "KGV(A,B)="
:Disp lcm(A,B)
```



```
A=?36
B=?45
GGD(A,B)=
9
KGV(A,B)=
180
Done
```