Hoofdstuk 3

Gehele Getallen

Ring

Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:

Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:
1. $(R, +)$ is een **abelse** of **commutatieve** groep:

Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:

1. $(R, +)$ is een **abelse** of **commutatieve** groep:
   - De optelling is **associatief**
     $\forall a, b, c \in R : (a + b) + c = a + (b + c)$

Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:

1. $(R, +)$ is een **abelse** of **commutatieve** groep:
   - De optelling is **associatief**
     $\forall a, b, c \in R : (a + b) + c = a + (b + c)$
   - De optelling heeft een **neutraal element**
     $\exists n \in R : \forall a \in R : a + n = a = n + a$

Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:

1. $(R, +)$ is een **abelse** of **commutatieve** groep:
   - De optelling is **associatief**
     $\forall a, b, c \in R : (a + b) + c = a + (b + c)$
   - De optelling heeft een **neutraal element**
     $\exists n \in R : \forall a \in R : a + n = a = n + a$
   - Elk element a heeft een **invers** of **symmetrisch element** t.o.v. de optelling (dat we noteren als $-a$)
     $\forall a \in R : \exists b \in R : a + b = n = b + a$

Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:

1. $(R, +)$ is een **abelse** of **commutatieve** groep:
   - De optelling is **associatief**
     $\forall a, b, c \in R : (a + b) + c = a + (b + c)$
   - De optelling heeft een **neutraal element**
     $\exists n \in R : \forall a \in R : a + n = a = n + a$
   - Elk element a heeft een **invers** of **symmetrisch element** t.o.v. de optelling (dat we noteren als $-a$)
     $\forall a \in R : \exists b \in R : a + b = n = b + a$
   - De optelling is **commutatief**
     $\forall a, b \in R : a + b = b + a$

2. $(R, .)$ is een **monoide**:

2. $(R, .)$ is een **monoide**:
   - De vermenigvuldiging is associatief
     $\forall a, b, c \in R : (a.b).c = a.(b.c)$

2. $(R, .)$ is een **monoide**:
   - De vermenigvuldiging is associatief
     $\forall a, b, c \in R : (a.b).c = a.(b.c)$
   - De vermenigvuldiging heeft een neutraal element
     $\exists e \in R : \forall a \in R : a.e = a = e.a$

2. $(R, .)$ is een **monoide**:
   - De vermenigvuldiging is associatief
     $\forall a, b, c \in R : (a.b).c = a.(b.c)$
   - De vermenigvuldiging heeft een neutraal element
     $\exists e \in R : \forall a \in R : a.e = a = e.a$

3. De vermenigvuldiging is **distributief** t.o.v. de optelling

$$\forall a, b, c \in R : \quad \begin{aligned} a.(b+c) &= a.b + a.c \\ (a+b).c &= a.c + b.c \end{aligned}$$

2. $(R, .)$ is een **monoide**:
   - De vermenigvuldiging is associatief
     $\forall a, b, c \in R : (a.b).c = a.(b.c)$
   - De vermenigvuldiging heeft een neutraal element
     $\exists e \in R : \forall a \in R : a.e = a = e.a$

3. De vermenigvuldiging is **distributief** t.o.v. de optelling

$$\forall a, b, c \in R : \quad \begin{aligned} a.(b + c) &= a.b + a.c \\ (a + b).c &= a.c + b.c \end{aligned}$$

We zeggen dat $(R, +, .)$ een **ring met eenheid** is.
Wanneer ook de vermenigvuldiging commutatief is, spreken we van een **commutatieve ring met eenheid**.

Notatie. We schrijven $a - b$ voor $a + (-b)$.
$a - b$ is dus kort voor "a plus het symmetrisch element van b".

Notatie. We schrijven $a - b$ voor $a + (-b)$.
$a - b$ is dus kort voor "a plus het symmetrisch element van b".

Eigenschap.

De symmetrische en neutrale elementen zijn uniek.

Notatie. We schrijven $a - b$ voor $a + (-b)$.
$a - b$ is dus kort voor "a plus het symmetrisch element van b".

Eigenschap.

De symmetrische en neutrale elementen zijn uniek.

Bewijs. Oefening. $\square$

Notatie. We schrijven $a - b$ voor $a + (-b)$.
$a - b$ is dus kort voor "a plus het symmetrisch element van b".

Eigenschap.

De symmetrische en neutrale elementen zijn uniek.

Bewijs. Oefening. $\square$

Eigenschap.

$\forall m, n \in R : m - (-n) = m + n.$

Notatie. We schrijven $a - b$ voor $a + (-b)$.
$a - b$ is dus kort voor "a plus het symmetrisch element van b".

Eigenschap.

De symmetrische en neutrale elementen zijn uniek.

Bewijs. Oefening. $\square$

Eigenschap.

$\forall m, n \in R : m - (-n) = m + n.$

Bewijs. Als we bewijzen dat $-(-n) = n$ is het in orde, want $m - (-n) = m + (-(-n))$. Maar vermits symmetrische elementen uniek zijn is dit duidelijk want $n + (-n) = 0$. $\square$

Ring van gehele getallen

De verzameling van alle gehele getallen uitgerust met $+$ en $\cdot$ is een commutatieve ring met 0 als neutraal element voor de optelling en 1 als neutraal element voor de vermenigvuldiging die we noteren als $(\mathbb{Z}, +, \cdot)$.

Veeltermen

De verzameling van veeltermen met gehele coëfficiënten en onbekende X is

$$\mathbb{Z}[X] := \left\{ \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}, \forall i \in [0..n] : a_i \in \mathbb{Z} \right\}.$$

Veeltermen

De verzameling van veeltermen met gehele coëfficiënten en onbekende X is

$$\mathbb{Z}[X] := \left\{ \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}, \forall i \in [0..n] : a_i \in \mathbb{Z} \right\}.$$

Op deze verzameling definiëren we een optelling door

$$\left(\sum_{i=0}^{n} a_i X^i \right) + \left(\sum_{j=0}^{m} b_j X^j \right) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) X^k$$

waarbij we veronderstellen dat $a_k = 0$ voor $k > n$ en $b_k = 0$ voor $k > m$.

We definiëren ook een vermenigvuldiging door

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{m+n} c_k X^k$$

waarbij

$$c_k = \sum_{\substack{i \in [0..n] \\ j \in [0..m] \\ i+j=k}} a_i b_j.$$

De formule voor c_k drukt gewoon uit dat je de som neemt van alle producten van termen uit de eerste en de tweede veelterm die X^k opleveren.

We definiëren ook een vermenigvuldiging door

$$\left(\sum_{i=0}^{n} a_i X^i\right) . \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{m+n} c_k X^k$$

waarbij

$$c_k = \sum_{\substack{i \in [0..n] \\ j \in [0..m] \\ i+j=k}} a_i b_j .$$

De formule voor c_k drukt gewoon uit dat je de som neemt van alle producten van termen uit de eerste en de tweede veelterm die X^k opleveren.
Met deze definities is $(\mathbb{Z}[X], +, .)$ een ring.

We definiëren ook een vermenigvuldiging door

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{m+n} c_k X^k$$

waarbij

$$c_k = \sum_{\substack{i\in[0..n]\\ j\in[0..m]\\ i+j=k}} a_i b_j.$$

De formule voor c_k drukt gewoon uit dat je de som neemt van alle producten van termen uit de eerste en de tweede veelterm die X^k opleveren.
Met deze definities is $(\mathbb{Z}[X], +, .)$ een ring.
Analoog zijn ook $(\mathbb{Q}[X], +, .)$ en $(\mathbb{R}[X], +, .)$ ringen.

Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie $\leq$. Deze heeft ook enkele goed gekende eigenschappen:

Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie $\leq$. Deze heeft ook enkele goed gekende eigenschappen:

- $\leq$ is **reflexief**
  $\forall a \in \mathbb{Z} : a \leq a$

Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie $\leq$. Deze heeft ook enkele goed gekende eigenschappen:

- $\leq$ is **reflexief**
  $\forall a \in \mathbb{Z} : a \leq a$
- $\leq$ is **antisymmetrisch**
  $\forall a, b \in \mathbb{Z} : (a \leq b) \wedge (b \leq a) \Rightarrow (a = b)$

Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie $\leq$. Deze heeft ook enkele goed gekende eigenschappen:

- $\leq$ is **reflexief**
  $\forall a \in \mathbb{Z} : a \leq a$
- $\leq$ is **antisymmetrisch**
  $\forall a, b \in \mathbb{Z} : (a \leq b) \wedge (b \leq a) \Rightarrow (a = b)$
- $\leq$ is **transitief**
  $\forall a, b, c \in \mathbb{Z} : (a \leq b) \wedge (b \leq c) \Rightarrow (a \leq c)$

Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie $\leq$. Deze heeft ook enkele goed gekende eigenschappen:

- $\leq$ is **reflexief**
  $\forall a \in \mathbb{Z} : a \leq a$
- $\leq$ is **antisymmetrisch**
  $\forall a, b \in \mathbb{Z} : (a \leq b) \wedge (b \leq a) \Rightarrow (a = b)$
- $\leq$ is **transitief**
  $\forall a, b, c \in \mathbb{Z} : (a \leq b) \wedge (b \leq c) \Rightarrow (a \leq c)$
- Bovendien geldt:
  $\forall a, b, c \in \mathbb{Z} : a \leq b \Rightarrow a + c \leq b + c$
  en
  $\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N} : a \leq b \Rightarrow a.c \leq b.c$

Eigenschap.

Als $a \leq b$*, dan* $-b \leq -a$*.*

Eigenschap.

Als $a \leq b$, *dan* $-b \leq -a$.

Definitie.

Zij $S \subset \mathbb{Z}$. $x \in \mathbb{Z}$ *heet een* **ondergrens** *van* S *indien* $\forall s \in S : x \leq s$. *Het* **infimum** *van* S *is de grootste ondergrens van* S.

Eigenschap.
Als $a \leq b$*, dan* $-b \leq -a$*.*

Definitie.
Zij $S \subset \mathbb{Z}$*.* $x \in \mathbb{Z}$ *heet een* **ondergrens** *van* S *indien* $\forall s \in S : x \leq s$*. Het* **infimum** *van* S *is de grootste ondergrens van* S*.*

Voorbeeld. $S = \{-5, 3, 10, 20\}$ heeft vele ondergrenzen, bijvoorbeeld $-6, -200, -5, \ldots$. Het infimum is -5. Merk op dat in dit voorbeeld het infimum van S zelf tot S behoort.

Eigenschap.

Als $a \leq b$, dan $-b \leq -a$.

Definitie.

Zij $S \subset \mathbb{Z}$. $x \in \mathbb{Z}$ heet een **ondergrens** *van S indien $\forall s \in S$: $x \leq s$. Het* **infimum** *van S is de grootste ondergrens van S.*

Voorbeeld. $S = \{-5, 3, 10, 20\}$ heeft vele ondergrenzen, bijvoorbeeld $-6, -200, -5, \ldots$. Het infimum is -5. Merk op dat in dit voorbeeld het infimum van S zelf tot S behoort.

Definitie.

Indien het infimum van een verzameling S zelf tot S behoort, dan noemen we het een **minimum***.*

Eigenschap.

Als $a \leq b$, dan $-b \leq -a$.

Definitie.

Zij $S \subset \mathbb{Z}$. $x \in \mathbb{Z}$ heet een **ondergrens** *van S indien $\forall s \in S$: $x \leq s$. Het* **infimum** *van S is de grootste ondergrens van S.*

Voorbeeld. $S = \{-5, 3, 10, 20\}$ heeft vele ondergrenzen, bijvoorbeeld $-6, -200, -5, \ldots$. Het infimum is -5. Merk op dat in dit voorbeeld het infimum van S zelf tot S behoort.

Definitie.

Indien het infimum van een verzameling S zelf tot S behoort, dan noemen we het een **minimum***.*

De volgende bijzondere eigenschap van $\mathbb{Z}$ is in feite een axioma.

Principe van de Welgeordendheid.

Elke niet-lege deelverzameling van $\mathbb{Z}$ die een ondergrens heeft, heeft ook een minimum.

Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2.$$

Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2.$$

Dan gaan we ervan uit dat de eigenschap geldt voor $n = k$ en we bewijzen hieruit dat de eigenschap dan ook moet waar zijn voor $n = k + 1$.

Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2.$$

Dan gaan we ervan uit dat de eigenschap geldt voor $n = k$ en we bewijzen hieruit dat de eigenschap dan ook moet waar zijn voor $n = k + 1$. Dus nemen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ en dan tonen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$.

Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2.$$

Dan gaan we ervan uit dat de eigenschap geldt voor $n = k$ en we bewijzen hieruit dat de eigenschap dan ook moet waar zijn voor $n = k + 1$. Dus nemen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ en dan tonen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$. Gebruikmakend van de aanname, wordt het linkerlid $k^2 + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$.

Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2.$$

Dan gaan we ervan uit dat de eigenschap geldt voor $n = k$ en we bewijzen hieruit dat de eigenschap dan ook moet waar zijn voor $n = k + 1$. Dus nemen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ en dan tonen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$. Gebruikmakend van de aanname, wordt het linkerlid $k^2 + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$. Kunnen we uit deze algemene redenering afleiden dat de eigenschap geldt voor alle $n \in \mathbb{N}$?

Principe van Bewijs per Inductie.
Zij $P(n)$ *een eigenschap die we willen bewijzen voor alle* $n \in \mathbb{N}$.

Principe van Bewijs per Inductie.
Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*

Principe van Bewijs per Inductie.

Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*
2. *Onderstel dat de* **inductiehypothese** *geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k+1)$ dat ook (deze stap heet de* **inductiestap***).*

Principe van Bewijs per Inductie.

Zij $P(n)$ *een eigenschap die we willen bewijzen voor alle* $n \in \mathbb{N}$*.*

1. **Basis van de inductie.** *Zij* $P(0)$ *waar (of* $P(1)$ *of* $P(n_0)$*, met* n_0 *het kleinste natuurlijke getal waarvoor* P *zin heeft).*
2. *Onderstel dat de* **inductiehypothese** *geldt, i.e. wanneer* $P(k)$ *waar is voor een willekeurige* $k \in \mathbb{N}$*, dan is* $P(k+1)$ *dat ook (deze stap heet de* **inductiestap***).*

Dan is $P(n)$ *waar voor alle* $n \in \mathbb{N}$*.*

Principe van Bewijs per Inductie.
Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*
2. *Onderstel dat de* **inductiehypothese** *geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k+1)$ dat ook (deze stap heet de* **inductiestap***).*

Dan is $P(n)$ waar voor alle $n \in \mathbb{N}$.

Bewijs. Onderstel van niet. Zij $S = \{n \in \mathbb{N} \mid \neg P(n) \text{ waar}\}$, dan is deze verzameling niet leeg.

Principe van Bewijs per Inductie.

Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*
2. *Onderstel dat de* **inductiehypothese** *geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k+1)$ dat ook (deze stap heet de* **inductiestap***).*

Dan is $P(n)$ waar voor alle $n \in \mathbb{N}$.

Bewijs. Onderstel van niet. Zij $S = \{n \in \mathbb{N} \mid \neg P(n) \text{ waar}\}$, dan is deze verzameling niet leeg. Vermits $S \subset \mathbb{N}$ heeft S een ondergrens (bijvoorbeeld -1). Door de welgeordendheid van de gehele getallen heeft S een minimum, m. Door de basis van de inductie weten we dat $0 \notin S$ en dus $m \geq 1$.

Principe van Bewijs per Inductie.

Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*
2. *Onderstel dat de* **inductiehypothese** *geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k+1)$ dat ook (deze stap heet de* **inductiestap***).*

Dan is $P(n)$ waar voor alle $n \in \mathbb{N}$.

Bewijs. Onderstel van niet. Zij $S = \{n \in \mathbb{N} \mid \neg P(n) \text{ waar}\}$, dan is deze verzameling niet leeg. Vermits $S \subset \mathbb{N}$ heeft S een ondergrens (bijvoorbeeld -1). Door de welgeordendheid van de gehele getallen heeft S een minimum, m. Door de basis van de inductie weten we dat $0 \notin S$ en dus $m \geq 1$. Omdat m een minimum is, hebben we zeker $(m-1) \notin S$ zodat $P(m-1)$ waar is,

Principe van Bewijs per Inductie.
Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*
2. *Onderstel dat de* **inductiehypothese** *geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k+1)$ dat ook (deze stap heet de* **inductiestap***).*

Dan is $P(n)$ waar voor alle $n \in \mathbb{N}$.

Bewijs. Onderstel van niet. Zij $S = \{n \in \mathbb{N} \mid \neg P(n) \text{ waar}\}$, dan is deze verzameling niet leeg. Vermits $S \subset \mathbb{N}$ heeft S een ondergrens (bijvoorbeeld -1). Door de welgeordendheid van de gehele getallen heeft S een minimum, m. Door de basis van de inductie weten we dat $0 \notin S$ en dus $m \geq 1$. Omdat m een minimum is, hebben we zeker $(m-1) \notin S$ zodat $P(m-1)$ waar is, maar de inductiestap verzekert dan dat $P(m)$ ook waar is, een tegenspraak. $\square$

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$.

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1 - b)a$ zodat $(1 - b)a \in R$, want $(1 - b)a \in \mathbb{N}$ omdat $1 - b \leq 0$ en $a < 0$.

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1 - b)a$ zodat $(1 - b)a \in R$, want $(1 - b)a \in \mathbb{N}$ omdat $1 - b \leq 0$ en $a < 0$. Uit het welordeningsprincipe kunnen we besluiten dat R een kleinste element r heeft. Dan geldt: $\exists y \in \mathbb{Z} : a = by + r$ zodat we $q := y$ kunnen nemen.

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1 - b)a$ zodat $(1 - b)a \in R$, want $(1 - b)a \in \mathbb{N}$ omdat $1 - b \leq 0$ en $a < 0$.
Uit het welordeningsprincipe kunnen we besluiten dat R een kleinste element r heeft. Dan geldt: $\exists y \in \mathbb{Z} : a = by + r$ zodat we $q := y$ kunnen nemen.
Er blijft te tonen dat $0 \leq r < b$.

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1 - b)a$ zodat $(1 - b)a \in R$, want $(1 - b)a \in \mathbb{N}$ omdat $1 - b \leq 0$ en $a < 0$.
Uit het welordeningsprincipe kunnen we besluiten dat R een kleinste element r heeft. Dan geldt: $\exists y \in \mathbb{Z} : a = by + r$ zodat we $q := y$ kunnen nemen.
Er blijft te tonen dat $0 \leq r < b$. Door de definitie van R is $0 \leq r$ in orde. Indien $r \geq b$, dan is $r - b \geq 0$ en uit $a = by + r \iff a = b(y + 1) + (r - b)$ volgt dan $r - b \in R$

Quotiënt en rest

Stelling.
Gegeven $a \in \mathbb{Z}$ *en* $b \in \mathbb{N}_0$*, dan* $\exists q, r \in \mathbb{Z}$*:* $a = bq + r$ *met* $0 \leq r < b$*.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1 - b)a$ zodat $(1 - b)a \in R$, want $(1 - b)a \in \mathbb{N}$ omdat $1 - b \leq 0$ en $a < 0$.
Uit het welordeningsprincipe kunnen we besluiten dat R een kleinste element r heeft. Dan geldt: $\exists y \in \mathbb{Z} : a = by + r$ zodat we $q := y$ kunnen nemen.
Er blijft te tonen dat $0 \leq r < b$. Door de definitie van R is $0 \leq r$ in orde. Indien $r \geq b$, dan is $r - b \geq 0$ en uit $a = by + r \iff a = b(y + 1) + (r - b)$ volgt dan $r - b \in R$ en dat is strijdig, want r was het kleinste element van R. $\square$

Stelling.
r en q in de vorige stelling zijn uniek.

Stelling.

r en q in de vorige stelling zijn uniek.

Bewijs. Bewijs uit het ongerijmde. Onderstel dat

$$\exists q \neq q' \in \mathbb{Z}, \exists r \neq r' \in [0..b-1] : bq + r = a = bq' + r'.$$

Stelling.

r en q in de vorige stelling zijn uniek.

Bewijs. Bewijs uit het ongerijmde. Onderstel dat

$$\exists q \neq q' \in \mathbb{Z}, \exists r \neq r' \in [0..b-1] : bq + r = a = bq' + r'.$$

Veronderstel dat $q' < q$, zodat $q - q' \geq 1$. Dan krijgen we:

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b \geq b.$$

Stelling.

r en q in de vorige stelling zijn uniek.

Bewijs. Bewijs uit het ongerijmde. Onderstel dat

$$\exists q \neq q' \in \mathbb{Z}, \exists r \neq r' \in [0..b-1] : bq + r = a = bq' + r'.$$

Veronderstel dat $q' < q$, zodat $q - q' \geq 1$. Dan krijgen we:

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b \geq b.$$

Strijdig. Bijgevolg is $q' < q$ niet waar. Analoog toon je dat $q' > q$ ook niet kan. Uiteindelijk moet dus $q' = q$ en dan ook $r = r'$. $\square$

Een belangrijke toepassing van de vorige stellingen is onze (decimale) schrijfwijze voor getallen. Gegeven een natuurlijk getal x en een 'basis' $t \geq 2$, dan kunnen we herhaaldelijk de stelling toepassen:

Een belangrijke toepassing van de vorige stellingen is onze (decimale) schrijfwijze voor getallen. Gegeven een natuurlijk getal x en een 'basis' $t \geq 2$, dan kunnen we herhaaldelijk de stelling toepassen:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\vdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n \end{aligned}$$

met elke $r_i \in [0..t-1]$ en $q_n = 0$.

Een belangrijke toepassing van de vorige stellingen is onze (decimale) schrijfwijze voor getallen. Gegeven een natuurlijk getal x en een 'basis' $t \geq 2$, dan kunnen we herhaaldelijk de stelling toepassen:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\vdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n \end{aligned}$$

met elke $r_i \in [0..t-1]$ en $q_n = 0$.
Substitutie van de laatste vergelijking in de voorlaatste enz. geeft

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0$$

zodat de schrijfwijze voor x in basis t gelijk is aan

$$r_n r_{n-1} \ldots r_1 r_0.$$

Een belangrijke toepassing van de vorige stellingen is onze (decimale) schrijfwijze voor getallen. Gegeven een natuurlijk getal x en een 'basis' $t \geq 2$, dan kunnen we herhaaldelijk de stelling toepassen:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\vdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n \end{aligned}$$

met elke $r_i \in [0..t-1]$ en $q_n = 0$.
Substitutie van de laatste vergelijking in de voorlaatste enz. geeft

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0$$

zodat de schrijfwijze voor x in basis t gelijk is aan

$$r_n r_{n-1} \ldots r_1 r_0.$$

Notatie. We noteren de schrijfwijze van x in basis t als $(x)_t$.

Voorbeeld. In de informatica werkt men dikwijls in basis 2. Hoe berekenen we $(386)_2$?

Voorbeeld. In de informatica werkt men dikwijls in basis 2. Hoe berekenen we $(386)_2$?

$$\begin{array}{rcrcl}
386 & = & 193 \cdot 2 & + & \boxed{0} \\
193 & = & 96 \cdot 2 & + & 1 \\
96 & = & 48 \cdot 2 & + & 0 \\
48 & = & 24 \cdot 2 & + & 0 \\
24 & = & 12 \cdot 2 & + & 0 \\
12 & = & 6 \cdot 2 & + & 0 \\
6 & = & 3 \cdot 2 & + & 0 \\
3 & = & 1 \cdot 2 & + & 1 \\
1 & = & 0 \cdot 2 & + & 1
\end{array}$$

Voorbeeld. In de informatica werkt men dikwijls in basis 2. Hoe berekenen we $(386)_2$?

$$\begin{array}{rcrcc|c|} \cline{6-6} 386 & = & 193 \cdot 2 & + & & 0 \\ 193 & = & 96 \cdot 2 & + & & 1 \\ 96 & = & 48 \cdot 2 & + & & 0 \\ 48 & = & 24 \cdot 2 & + & & 0 \\ 24 & = & 12 \cdot 2 & + & & 0 \\ 12 & = & 6 \cdot 2 & + & & 0 \\ 6 & = & 3 \cdot 2 & + & & 0 \\ 3 & = & 1 \cdot 2 & + & & 1 \\ 1 & = & 0 \cdot 2 & + & & 1 \\ \cline{6-6} \end{array}$$

Dus $(386)_2 = 110000010$.

Definitie.
We zeggen dat een geheel getal b een **veelvoud** *is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$.*

Definitie.
We zeggen dat een geheel getal b een **veelvoud** *is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$. We zeggen in dat geval ook dat a het getal b* **deelt** *en schrijven $a \mid b$. Ook zeggen we dat a een* **factor** *of een* **deler** *is van b of dat b* **deelbaar** *is door a.*

Definitie.
We zeggen dat een geheel getal b een **veelvoud** *is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$. We zeggen in dat geval ook dat a het getal b* **deelt** *en schrijven $a \mid b$. Ook zeggen we dat a een* **factor** *of een* **deler** *is van b of dat b* **deelbaar** *is door a. Als $a \neq 0$, noteren we het getal $k \in \mathbb{Z}$ waarvoor $b = ka$ met $\frac{b}{a}$.*

Definitie.
We zeggen dat een geheel getal b een **veelvoud** *is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$. We zeggen in dat geval ook dat a het getal b* **deelt** *en schrijven $a \mid b$. Ook zeggen we dat a een* **factor** *of een* **deler** *is van b of dat b* **deelbaar** *is door a. Als $a \neq 0$, noteren we het getal $k \in \mathbb{Z}$ waarvoor $b = ka$ met $\frac{b}{a}$. Natuurlijk bestaat $\frac{b}{a}$ voor elke keuze $b \in \mathbb{Z}, a \in \mathbb{Z}_0$ maar in het algemeen behoort $\frac{b}{a}$ tot $\mathbb{Q}$ en niet tot $\mathbb{Z}$. Enkel als $a \mid b$ hebben we $\frac{b}{a} \in \mathbb{Z}$.*

Definitie.
We zeggen dat een geheel getal b een **veelvoud** *is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$. We zeggen in dat geval ook dat a het getal b* **deelt** *en schrijven $a \mid b$. Ook zeggen we dat a een* **factor** *of een* **deler** *is van b of dat b* **deelbaar** *is door a. Als $a \neq 0$, noteren we het getal $k \in \mathbb{Z}$ waarvoor $b = ka$ met $\frac{b}{a}$. Natuurlijk bestaat $\frac{b}{a}$ voor elke keuze $b \in \mathbb{Z}, a \in \mathbb{Z}_0$ maar in het algemeen behoort $\frac{b}{a}$ tot $\mathbb{Q}$ en niet tot $\mathbb{Z}$. Enkel als $a \mid b$ hebben we $\frac{b}{a} \in \mathbb{Z}$.*

Eigenschap.
Zij $n, d, c \in \mathbb{Z}$ met $c \neq 0 \neq d$. Er geldt

$$d \mid n \wedge c \mid \frac{n}{d} \Rightarrow c \mid n \wedge d \mid \frac{n}{c}$$

Definitie.
We zeggen dat een geheel getal b een **veelvoud** *is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$. We zeggen in dat geval ook dat a het getal b* **deelt** *en schrijven $a \mid b$. Ook zeggen we dat a een* **factor** *of een* **deler** *is van b of dat b* **deelbaar** *is door a. Als $a \neq 0$, noteren we het getal $k \in \mathbb{Z}$ waarvoor $b = ka$ met $\frac{b}{a}$. Natuurlijk bestaat $\frac{b}{a}$ voor elke keuze $b \in \mathbb{Z}, a \in \mathbb{Z}_0$ maar in het algemeen behoort $\frac{b}{a}$ tot $\mathbb{Q}$ en niet tot $\mathbb{Z}$. Enkel als $a \mid b$ hebben we $\frac{b}{a} \in \mathbb{Z}$.*

Eigenschap.
Zij $n, d, c \in \mathbb{Z}$ met $c \neq 0 \neq d$. Er geldt

$$d \mid n \wedge c \mid \frac{n}{d} \Rightarrow c \mid n \wedge d \mid \frac{n}{c}$$

Bewijs. $d \mid n \iff \exists k \in \mathbb{Z} : n = kd$ en
$c \mid \frac{n}{d} \iff c \mid k \iff \exists l \in \mathbb{Z} : k = lc$.

Definitie.

We zeggen dat een geheel getal b een **veelvoud** *is van* $a \in \mathbb{Z}$ *indien* $\exists k \in \mathbb{Z} : b = ka$. *We zeggen in dat geval ook dat a het getal b* **deelt** *en schrijven* $a \mid b$. *Ook zeggen we dat a een* **factor** *of een* **deler** *is van b of dat b* **deelbaar** *is door a. Als* $a \neq 0$, *noteren we het getal* $k \in \mathbb{Z}$ *waarvoor* $b = ka$ *met* $\frac{b}{a}$. *Natuurlijk bestaat* $\frac{b}{a}$ *voor elke keuze* $b \in \mathbb{Z}, a \in \mathbb{Z}_0$ *maar in het algemeen behoort* $\frac{b}{a}$ *tot* $\mathbb{Q}$ *en niet tot* $\mathbb{Z}$. *Enkel als* $a \mid b$ *hebben we* $\frac{b}{a} \in \mathbb{Z}$.

Eigenschap.

Zij $n, d, c \in \mathbb{Z}$ *met* $c \neq 0 \neq d$. *Er geldt*

$$d \mid n \wedge c \mid \frac{n}{d} \Rightarrow c \mid n \wedge d \mid \frac{n}{c}$$

Bewijs. $d \mid n \iff \exists k \in \mathbb{Z} : n = kd$ en $c \mid \frac{n}{d} \iff c \mid k \iff \exists l \in \mathbb{Z} : k = lc$. Bijgevolg is $n = lcd$ en dus volgt $c \mid n$ en aangezien $\frac{n}{c} = ld$ volgt ook $d \mid \frac{n}{c}$. $\square$

Grootste gemene deler

Definitie.
Stel $a, b \in \mathbb{Z}$. *Een geheel getal* d *heet een* **grootste gemene deler (ggd)** *van* a *en* b *indien* $d \mid a$ *en* $d \mid b$ *(gemene deler) èn* $\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d$ *(grootste).*

Grootste gemene deler

Definitie.
Stel $a, b \in \mathbb{Z}$. Een geheel getal d heet een **grootste gemene deler (ggd)** *van a en b indien $d \mid a$ en $d \mid b$ (gemene deler) èn $\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d$ (grootste).*

Voorbeeld. $6 \mid 60$ en $6 \mid 84$ maar toch is 6 geen ggd van 60 en 84, want $12 \mid 60$ en $12 \mid 84$ maar $12 \nmid 6$.

Grootste gemene deler

Definitie.
Stel $a, b \in \mathbb{Z}$. Een geheel getal d heet een **grootste gemene deler (ggd)** *van a en b indien $d \mid a$ en $d \mid b$ (gemene deler) èn $\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d$ (grootste).*

Voorbeeld. $6 \mid 60$ en $6 \mid 84$ maar toch is 6 geen ggd van 60 en 84, want $12 \mid 60$ en $12 \mid 84$ maar $12 \nmid 6$.

Opmerking. Als d een ggd is, is ook $-d$ een ggd. We hebben:

Eigenschap.
Zijn $d \neq d'$ grootste gemene delers van a en b. Dan geldt $d = -d'$.

Bewijs.

Grootste gemene deler

Definitie.
Stel $a, b \in \mathbb{Z}$. Een geheel getal d heet een **grootste gemene deler (ggd)** *van a en b indien $d \mid a$ en $d \mid b$ (gemene deler) èn $\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d$ (grootste).*

Voorbeeld. $6 \mid 60$ en $6 \mid 84$ maar toch is 6 geen ggd van 60 en 84, want $12 \mid 60$ en $12 \mid 84$ maar $12 \nmid 6$.

Opmerking. Als d een ggd is, is ook $-d$ een ggd. We hebben:

Eigenschap.
Zijn $d \neq d'$ grootste gemene delers van a en b. Dan geldt $d = -d'$.

Bewijs. Dit volgt uit $d \mid d'$ en $d' \mid d$. $\square$

Grootste gemene deler

Definitie.
Stel $a, b \in \mathbb{Z}$. Een geheel getal d heet een **grootste gemene deler (ggd)** *van a en b indien $d \mid a$ en $d \mid b$ (gemene deler) èn $\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d$ (grootste).*

Voorbeeld. $6 \mid 60$ en $6 \mid 84$ maar toch is 6 geen ggd van 60 en 84, want $12 \mid 60$ en $12 \mid 84$ maar $12 \nmid 6$.

Opmerking. Als d een ggd is, is ook $-d$ een ggd. We hebben:

Eigenschap.
Zijn $d \neq d'$ grootste gemene delers van a en b. Dan geldt $d = -d'$.

Bewijs. Dit volgt uit $d \mid d'$ en $d' \mid d$. □

Definitie.
De *grootste gemene deler van a en b is de unieke positieve grootste gemene deler van a en b. We noteren hem* $\mathrm{ggd}(a, b)$*.*

Hoe berekenen we nu $\text{ggd}(a, b)$?

Hoe berekenen we nu $\mathrm{ggd}(a, b)$?

Eigenschap.
Stel $a = bq + r$. *Dan is* $\mathrm{ggd}(a, b) = \mathrm{ggd}(b, r)$.

Hoe berekenen we nu $\operatorname{ggd}(a, b)$?

Eigenschap.

Stel $a = bq + r$. *Dan is* $\operatorname{ggd}(a, b) = \operatorname{ggd}(b, r)$.

Bewijs. Stel $d \mid a$ en $d \mid b$. Dan zal ook $d \mid (a - bq)$

Hoe berekenen we nu $\text{ggd}(a, b)$?

Eigenschap.

Stel $a = bq + r$. *Dan is* $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Bewijs. Stel $d \mid a$ en $d \mid b$. Dan zal ook $d \mid (a - bq)$zodat $d \mid b$ en $d \mid r$.

Hoe berekenen we nu $\text{ggd}(a, b)$?

Eigenschap.

Stel $a = bq + r$. *Dan is* $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Bewijs. Stel $d \mid a$ en $d \mid b$. Dan zal ook $d \mid (a - bq)$zodat $d \mid b$ en $d \mid r$. Omgekeerd: als $d \mid b$ en $d \mid r$ dan volgt $d \mid (bq + r)$ zodat $d \mid \text{ggd}(a, b)$. $\square$

Hoe berekenen we nu $\mathrm{ggd}(a, b)$?

Eigenschap.

Stel $a = bq + r$. *Dan is* $\mathrm{ggd}(a, b) = \mathrm{ggd}(b, r)$.

Bewijs. Stel $d \mid a$ en $d \mid b$. Dan zal ook $d \mid (a - bq)$zodat $d \mid b$ en $d \mid r$. Omgekeerd: als $d \mid b$ en $d \mid r$ dan volgt $d \mid (bq + r)$ zodat $d \mid \mathrm{ggd}(a, b)$. $\square$

Voorbeeld. We bepalen $\mathrm{ggd}(2406, 654)$. We passen hiervoor de voorgaande eigenschap herhaaldelijk toe:

$$\begin{array}{rcllcl}
2406 & = & 654.3 + 444 & \Rightarrow & \mathrm{ggd}(2406, 654) & = \mathrm{ggd}(654, 444) \\
654 & = & 444.1 + 210 & \Rightarrow & & = \mathrm{ggd}(444, 210) \\
444 & = & 210.2 + 24 & \Rightarrow & & = \mathrm{ggd}(210, 24) \\
210 & = & 24.8 + 18 & \Rightarrow & & = \mathrm{ggd}(24, 18) \\
24 & = & 18.1 + 6 & \Rightarrow & & = \mathrm{ggd}(18, 6) \\
18 & = & 6.3 + 0 & \Rightarrow & & = 6
\end{array}$$

Euclidisch algoritme

Algemeen: als we hebben

$$
\begin{array}{rclcl}
a & = & bq_1 & + & r_1 \quad \text{met} \quad 0 \le r_1 < b \\
b & = & r_1 q_2 & + & r_2 \quad\quad\quad 0 \le r_2 < r_1 \\
r_1 & = & r_2 q_3 & + & r_3 \quad\quad\quad 0 \le r_3 < r_2 \\
 & \vdots & & & \vdots \\
r_{k-4} & = & r_{k-3} q_{k-2} & + & r_{k-2} \quad\quad 0 \le r_{k-2} < r_{k-3} \\
r_{k-3} & = & r_{k-2} q_{k-1} & + & \boxed{r_{k-1}} \quad 0 \le r_{k-1} < r_{k-2} \\
r_{k-2} & = & r_{k-1} q_k & + & 0
\end{array}
$$

Euclidisch algoritme

Algemeen: als we hebben

$$\begin{array}{rclcll}
a & = & bq_1 & + & r_1 & \text{met} \quad 0 \leq r_1 < b \\
b & = & r_1 q_2 & + & r_2 & \quad 0 \leq r_2 < r_1 \\
r_1 & = & r_2 q_3 & + & r_3 & \quad 0 \leq r_3 < r_2 \\
& \vdots & & & & \quad \vdots \\
r_{k-4} & = & r_{k-3} q_{k-2} & + & r_{k-2} & \quad 0 \leq r_{k-2} < r_{k-3} \\
r_{k-3} & = & r_{k-2} q_{k-1} & + & \boxed{r_{k-1}} & \quad 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} & = & r_{k-1} q_k & + & 0 &
\end{array}$$

dan is

$$\begin{aligned}
\operatorname{ggd}(a, b) &= \operatorname{ggd}(r_{k-2}, r_{k-1}) \\
&= r_{k-1} \\
&= \text{de laatste niet-nulle rest.}
\end{aligned}$$

Stelling. (Bézout)

Stel $a, b \in \mathbb{Z}, b \geq 0$ *met* $d = \mathrm{ggd}(a, b)$, *dan* $\exists m, n \in \mathbb{Z} : d = ma + nb$. *Ook is* d *het kleinste natuurlijk getal waarvoor dit kan.*

Stelling. (Bézout)

Stel $a, b \in \mathbb{Z}, b \geq 0$ *met* $d = \text{ggd}(a, b)$*, dan* $\exists m, n \in \mathbb{Z} : d = ma + nb$*. Ook is* d *het kleinste natuurlijk getal waarvoor dit kan.*

Bewijs.

Voor $b = 0$ is de stelling triviaal.

Stelling. (Bézout)

Stel $a, b \in \mathbb{Z}, b \geq 0$ *met* $d = \mathrm{ggd}(a, b)$*, dan* $\exists m, n \in \mathbb{Z} : d = ma + nb$*. Ook is* d *het kleinste natuurlijk getal waarvoor dit kan.*

Bewijs.
Voor $b = 0$ is de stelling triviaal.
Als $b \neq 0$, lezen we het resultaat van het euclidisch algoritme van achter naar voor:

$$d = r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}.$$

Dus $d = m'r_{k-2} + n'r_{k-3}$, met $m' = -q_{k-1}$ en $n' = 1$.

Stelling. (Bézout)

Stel $a, b \in \mathbb{Z}, b \geq 0$ *met* $d = \operatorname{ggd}(a, b)$, *dan* $\exists m, n \in \mathbb{Z} : d = ma + nb$. *Ook is* d *het kleinste natuurlijk getal waarvoor dit kan.*

Bewijs.
Voor $b = 0$ is de stelling triviaal.
Als $b \neq 0$, lezen we het resultaat van het euclidisch algoritme van achter naar voor:

$$d = r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}.$$

Dus $d = m'r_{k-2} + n'r_{k-3}$, met $m' = -q_{k-1}$ en $n' = 1$. Nu substitueren we $r_{k-2} = r_{k-4} - r_{k-3}q_{k-2}$ zodat

$$\begin{aligned} d &= m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3} \\ &= (-m'q_{k-2} + n')r_{k-3} + m'r_{k-4} \\ &= m''r_{k-3} + n''r_{k-4}. \end{aligned}$$

Daarin substitueren we $r_{k-3} = r_{k-5} - r_{k-4}q_{k-3}$ enz. Uiteindelijk vinden we

$$d = m^{(k-3)}r_2 + n^{(k-3)}r_1$$

Daarin substitueren we $r_{k-3} = r_{k-5} - r_{k-4}q_{k-3}$ enz. Uiteindelijk vinden we

$$d = m^{(k-3)}r_2 + n^{(k-3)}r_1$$

waaruit, via de substituties $r_2 = b - r_1q_2$ en $r_1 = a - bq_1$:

$$\begin{aligned} d &= m^{(k-3)}(b - r_1q_2) + n^{(k-3)}r_1 \\ &= (-m^{(k-3)}q_2 + n^{(k-3)})r_1 + m^{(k-3)}b \\ &= m^{(k-2)}r_1 + n^{(k-2)}b \\ &= m^{(k-2)}(a - bq_1) + n^{(k-2)}b \\ &= (-m^{(k-2)}q_1 + n^{(k-2)})b + m^{(k-2)}a \\ &= mb + na. \end{aligned}$$

Daarin substitueren we $r_{k-3} = r_{k-5} - r_{k-4}q_{k-3}$ enz. Uiteindelijk vinden we

$$d = m^{(k-3)}r_2 + n^{(k-3)}r_1$$

waaruit, via de substituties $r_2 = b - r_1q_2$ en $r_1 = a - bq_1$:

$$\begin{aligned}
d &= m^{(k-3)}(b - r_1q_2) + n^{(k-3)}r_1 \\
&= (-m^{(k-3)}q_2 + n^{(k-3)})r_1 + m^{(k-3)}b \\
&= m^{(k-2)}r_1 + n^{(k-2)}b \\
&= m^{(k-2)}(a - bq_1) + n^{(k-2)}b \\
&= (-m^{(k-2)}q_1 + n^{(k-2)})b + m^{(k-2)}a \\
&= mb + na.
\end{aligned}$$

Bewijs als oefening dat er geen kleiner getal $d' > 0$ bestaat waarvoor $\exists n', m' \in \mathbb{Z}$: $d' = m'a + n'b$. $\square$

Voorbeeld. We passen de stelling van Bézout toe op het vorige voorbeeld:

$$\begin{aligned}
6 &= 24-18 \\
&= 24-(210-8.24) &&= 9.24-210 \\
&= 9(444-2.210)-210 &&= 9.444-19.210 \\
&= 9.444-19(654-444) &&= 28.444-19.654 \\
&= 28(2406-3.654)-19.654 &&= 28.2406-103.654
\end{aligned}$$

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\mathrm{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\mathrm{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Gevolg.

Zij a en b gehele getallen. Enkel veelvouden van $\mathrm{ggd}(a, b)$ zijn te schrijven als $ma + nb$.

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\mathrm{ggd}(a,b)$ te schrijven zijn als $ma+nb$ voor zekere $m,n\in\mathbb{Z}$.

Gevolg.

Zij a en b gehele getallen. Enkel veelvouden van $\mathrm{ggd}(a,b)$ *zijn te schrijven als $ma+nb$.*

Bewijs. Schrijf $d=\mathrm{ggd}(a,b)=ma+nb$, uit vorige stelling, en veronderstel even dat een ander geheel getal x met $d\nmid x$ kan geschreven worden als $m'a+n'b$.

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\operatorname{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Gevolg.

Zij a en b gehele getallen. Enkel veelvouden van $\operatorname{ggd}(a, b)$ *zijn te schrijven als* $ma + nb$*.*

Bewijs. Schrijf $d = \operatorname{ggd}(a, b) = ma + nb$, uit vorige stelling, en veronderstel even dat een ander geheel getal x met $d \nmid x$ kan geschreven worden als $m'a + n'b$. Vermits x geen veelvoud is van d, hebben we $x = kd + q$, met $0 < q < d$.

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\mathrm{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Gevolg.

Zij a en b gehele getallen. Enkel veelvouden van $\mathrm{ggd}(a, b)$ *zijn te schrijven als* $ma + nb$.

Bewijs. Schrijf $d = \mathrm{ggd}(a, b) = ma + nb$, uit vorige stelling, en veronderstel even dat een ander geheel getal x met $d \nmid x$ kan geschreven worden als $m'a + n'b$. Vermits x geen veelvoud is van d, hebben we $x = kd + q$, met $0 < q < d$. Maar dan is $q = x - kd = (m' - km)a + (n' - kn)b$ een getal kleiner dan d dat te schrijven is als $ra + sb$, tegenspraak. $\square$

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\text{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Gevolg.

Zij a en b gehele getallen. Enkel veelvouden van $\text{ggd}(a, b)$ zijn te schrijven als $ma + nb$.

Bewijs. Schrijf $d = \text{ggd}(a, b) = ma + nb$, uit vorige stelling, en veronderstel even dat een ander geheel getal x met $d \nmid x$ kan geschreven worden als $m'a + n'b$. Vermits x geen veelvoud is van d, hebben we $x = kd + q$, met $0 < q < d$. Maar dan is $q = x - kd = (m' - km)a + (n' - kn)b$ een getal kleiner dan d dat te schrijven is als $ra + sb$, tegenspraak. $\square$

Definitie.

$a, b \in \mathbb{Z}$ heten **relatief priem** *indien $\text{ggd}(a, b) = 1$.*

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\text{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Gevolg.

Zij a en b gehele getallen. Enkel veelvouden van $\text{ggd}(a, b)$ *zijn te schrijven als* $ma + nb$.

Bewijs. Schrijf $d = \text{ggd}(a, b) = ma + nb$, uit vorige stelling, en veronderstel even dat een ander geheel getal x met $d \nmid x$ kan geschreven worden als $m'a + n'b$. Vermits x geen veelvoud is van d, hebben we $x = kd + q$, met $0 < q < d$. Maar dan is $q = x - kd = (m' - km)a + (n' - kn)b$ een getal kleiner dan d dat te schrijven is als $ra + sb$, tegenspraak. $\square$

Definitie.

$a, b \in \mathbb{Z}$ *heten* **relatief priem** *indien* $\text{ggd}(a, b) = 1$.

Eigenschap.

$ggd(a, b) = 1 \Rightarrow \exists m, n \in \mathbb{Z} : ma + nb = 1.$

Gevolg.

Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.

Gevolg.

Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.

Bewijs. Vermits alle getallen veelvouden zijn van $1 = \mathrm{ggd}(a, b)$, volgt dit uit voorgaande eigenschap. $\square$

Gevolg.

Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.

Bewijs. Vermits alle getallen veelvouden zijn van $1 = \mathrm{ggd}(a, b)$, volgt dit uit voorgaande eigenschap. $\square$

Eigenschap.

Een positief rationaal getal heeft een unieke *schrijfwijze als $\frac{a}{b}$ met a en b relatief priem en positief.*

Gevolg.

Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.

Bewijs. Vermits alle getallen veelvouden zijn van $1 = \operatorname{ggd}(a, b)$, volgt dit uit voorgaande eigenschap. $\square$

Eigenschap.

Een positief rationaal getal heeft een unieke *schrijfwijze als $\frac{a}{b}$ met a en b relatief priem en positief.*

Bewijs. Stel $\dfrac{a}{b} = \dfrac{a'}{b'}$ met $\operatorname{ggd}(a, b) = 1 = \operatorname{ggd}(a', b')$. Dan is $ab' = a'b$.

Gevolg.

Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.

Bewijs. Vermits alle getallen veelvouden zijn van $1 = \text{ggd}(a, b)$, volgt dit uit voorgaande eigenschap. □

Eigenschap.

Een positief rationaal getal heeft een unieke *schrijfwijze als $\frac{a}{b}$ met a en b relatief priem en positief.*

Bewijs. Stel $\dfrac{a}{b} = \dfrac{a'}{b'}$ met $\text{ggd}(a, b) = 1 = \text{ggd}(a', b')$. Dan is $ab' = a'b$. Maar

$$\begin{aligned} b' &= 1.b' \\ &= (ma + nb)b' \\ &= mab' + nbb' \\ &= ma'b + nb'b \\ &= (ma' + nb')b. \end{aligned}$$

Dus $b \mid b'$. Analoog geldt $b' \mid b$ zodat $b = b'$ en $a = a'$. □

Een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Stelling.

Elk natuurlijk getal groter dan 1 *een ontbinding heeft in priemfactoren.*

Een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Stelling.

Elk natuurlijk getal groter dan 1 *een ontbinding heeft in priemfactoren.*

Bewijs. Veronderstel even dat er minstens één getal is zonder factorisatie in priemgetallen. Dan is de verzameling A van alle getallen zonder factorisatie een niet-leeg deel van $\mathbb{N}$.

Een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Stelling.

Elk natuurlijk getal groter dan 1 *een ontbinding heeft in priemfactoren.*

Bewijs. Veronderstel even dat er minstens één getal is zonder factorisatie in priemgetallen. Dan is de verzameling A van alle getallen zonder factorisatie een niet-leeg deel van $\mathbb{N}$. Bijgevolg heeft A een minimum m. Indien m een priemgetal is, heeft m een triviale priemontbinding. Dus moet $m = m_1 m_2$ met $m_1, m_2 \in [2..m-1]$.

Een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Stelling.

Elk natuurlijk getal groter dan 1 *een ontbinding heeft in priemfactoren.*

Bewijs. Veronderstel even dat er minstens één getal is zonder factorisatie in priemgetallen. Dan is de verzameling A van alle getallen zonder factorisatie een niet-leeg deel van $\mathbb{N}$. Bijgevolg heeft A een minimum m. Indien m een priemgetal is, heeft m een triviale priemontbinding. Dus moet $m = m_1 m_2$ met $m_1, m_2 \in [2..m-1]$. Maar vermits m het kleinste element is van A, zullen m_1 en m_2 niet tot A behoren. Bijgevolg zijn deze getallen ontbindbaar.

Een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Stelling.

Elk natuurlijk getal groter dan 1 *een ontbinding heeft in priemfactoren.*

Bewijs. Veronderstel even dat er minstens één getal is zonder factorisatie in priemgetallen. Dan is de verzameling A van alle getallen zonder factorisatie een niet-leeg deel van $\mathbb{N}$. Bijgevolg heeft A een minimum m. Indien m een priemgetal is, heeft m een triviale priemontbinding. Dus moet $m = m_1 m_2$ met $m_1, m_2 \in [2..m-1]$. Maar vermits m het kleinste element is van A, zullen m_1 en m_2 niet tot A behoren. Bijgevolg zijn deze getallen ontbindbaar. Maar als we deze twee ontbindingen naast elkaar schrijven, hebben we een priemontbinding van m. Dit is in tegenspraak met $m \in A$. $\square$

Stelling.

Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ deelt, moet p één van de factoren delen.

Stelling.

Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ *deelt, moet p één van de factoren delen.*

Bewijs.

Door inductie op het aantal factoren van $x_1 x_2 \cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

Stelling.

Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ *deelt, moet p één van de factoren delen.*

Bewijs.

Door inductie op het aantal factoren van $x_1 x_2 \cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $\boxed{n = 1}$ OK, triviaal

Stelling.

Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ *deelt, moet p één van de factoren delen.*

Bewijs.

Door inductie op het aantal factoren van $x_1 x_2 \cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $\boxed{n = 1}$ OK, triviaal
- $\boxed{n = k} \Rightarrow \boxed{n = k + 1}$

Stelling.

Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ *deelt, moet p één van de factoren delen.*

Bewijs.

Door inductie op het aantal factoren van $x_1 x_2 \cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $\boxed{n = 1}$ OK, triviaal
- $\boxed{n = k} \Rightarrow \boxed{n = k + 1}$
  Onderstel dat $p \mid x_1 x_2 \cdots x_k x_{k+1}$ en stel $x := x_1 x_2 \cdots x_k$. Dan hebben we $p \mid x.x_{k+1}$.

Stelling.

Zij p een priemgetal. Indien p een product $x_1x_2\cdots x_n$ *deelt, moet p één van de factoren delen.*

Bewijs.

Door inductie op het aantal factoren van $x_1x_2\cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $\boxed{n=1}$ OK, triviaal
- $\boxed{n=k}\Rightarrow\boxed{n=k+1}$
  Onderstel dat $p \mid x_1x_2\cdots x_kx_{k+1}$ en stel $x := x_1x_2\cdots x_k$. Dan hebben we $p \mid x.x_{k+1}$.
  Indien $p \mid x$, hebben we door de inductiehypothese dat $\exists i \in [k] : p \mid x_i$.

Stelling.

Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ *deelt, moet p één van de factoren delen.*

Bewijs.

Door inductie op het aantal factoren van $x_1 x_2 \cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $\boxed{n = 1}$ OK, triviaal
- $\boxed{n = k} \Rightarrow \boxed{n = k + 1}$

  Onderstel dat $p \mid x_1 x_2 \cdots x_k x_{k+1}$ en stel $x := x_1 x_2 \cdots x_k$. Dan hebben we $p \mid x.x_{k+1}$.

  Indien $p \mid x$, hebben we door de inductiehypothese dat $\exists i \in [k] : p \mid x_i$.

  Indien $p \nmid x$ weten we dat $\mathrm{ggd}(p, x) = 1$ omdat p priem is en dus maar twee delers heeft en p niet de ggd kan zijn.

De stelling van Bezout levert $m, n \in \mathbb{Z}$ zo dat $1 = mp + nx$.

De stelling van Bezout levert $m, n \in \mathbb{Z}$ zo dat $1 = mp + nx$. Dan geldt:

$$\begin{aligned} x_{k+1} &= 1.x_{k+1} \\ &= (mp + nx)x_{k+1} \\ &= mpx_{k+1} + nxx_{k+1} \end{aligned}$$

De stelling van Bezout levert $m, n \in \mathbb{Z}$ zo dat $1 = mp + nx$. Dan geldt:

$$\begin{aligned} x_{k+1} &= 1.x_{k+1} \\ &= (mp + nx)x_{k+1} \\ &= mpx_{k+1} + nxx_{k+1} \end{aligned}$$

Vermits $p \mid mpx_{k+1}$ en $p \mid nxx_{k+1}$ (omdat $p \mid xx_{k+1}$), moet $p \mid x_{k+1}$. $\square$

Stelling.

Een natuurlijk getal $n \geq 2$ *heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).*

Stelling.

Een natuurlijk getal $n \geq 2$ *heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).*

Bewijs. Als de stelling niet waar zou zijn, is er, door de welordeningseigenschap, een kleinste getal n met twee verschillende ontbindingen:

$$p_1 p_2 \cdots p_k = n = p'_1 p'_2 \cdots p'_l$$

met p_i en p'_j (niet noodzakelijk verschillende) priemgetallen voor $i \in [k]$ en $j \in [l]$.

Stelling.

Een natuurlijk getal $n \geq 2$ heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).

Bewijs. Als de stelling niet waar zou zijn, is er, door de welordeningseigenschap, een kleinste getal n met twee verschillende ontbindingen:

$$p_1 p_2 \cdots p_k = n = p'_1 p'_2 \cdots p'_l$$

met p_i en p'_j (niet noodzakelijk verschillende) priemgetallen voor $i \in [k]$ en $j \in [l]$.
Uit $n = p_1 p_2 \cdots p_k$ leiden we af dat $p_1 \mid n$ en dus $p_1 \mid p'_1 p'_2 \cdots p'_l$.
De vorige stelling zegt dan dat $\exists j \in [l] : p_1 \mid p'_j$.

Stelling.

Een natuurlijk getal $n \geq 2$ heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).

Bewijs. Als de stelling niet waar zou zijn, is er, door de welordeningseigenschap, een kleinste getal n met twee verschillende ontbindingen:

$$p_1 p_2 \cdots p_k = n = p'_1 p'_2 \cdots p'_l$$

met p_i en p'_j (niet noodzakelijk verschillende) priemgetallen voor $i \in [k]$ en $j \in [l]$.
Uit $n = p_1 p_2 \cdots p_k$ leiden we af dat $p_1 \mid n$ en dus $p_1 \mid p'_1 p'_2 \cdots p'_l$.
De vorige stelling zegt dan dat $\exists j \in [l] : p_1 \mid p'_j$. Maar vermits p_1 en p'_j beide priemgetallen zijn (en 1 geen priemgetal is) wil dit zeggen dat $p'_j = p_1$.
Voor de eenvoud hernummeren we de priemfactoren $p'_1, p'_2, \ldots, p'_l$ zodanig dat de nieuwe $p'_1 = p_1$.

Stelling.

Een natuurlijk getal $n \geq 2$ heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).

Bewijs. Als de stelling niet waar zou zijn, is er, door de welordeningseigenschap, een kleinste getal n met twee verschillende ontbindingen:

$$p_1 p_2 \cdots p_k = n = p_1' p_2' \cdots p_l'$$

met p_i en p_j' (niet noodzakelijk verschillende) priemgetallen voor $i \in [k]$ en $j \in [l]$.

Uit $n = p_1 p_2 \cdots p_k$ leiden we af dat $p_1 \mid n$ en dus $p_1 \mid p_1' p_2' \cdots p_l'$.

De vorige stelling zegt dan dat $\exists j \in [l] : p_1 \mid p_j'$. Maar vermits p_1 en p_j' beide priemgetallen zijn (en 1 geen priemgetal is) wil dit zeggen dat $p_j' = p_1$.

Voor de eenvoud hernummeren we de priemfactoren $p_1', p_2', \ldots, p_l'$ zodanig dat de nieuwe $p_1' = p_1$. Dan hebben we $p_2 \cdots p_k = p_2' \cdots p_l'$ hetgeen een tegenspraak is, want dan zou $p_2 \cdots p_k$ een getal kleiner dan n zijn met twee verschillende ontbindingen. $\square$