Hoofdstuk 3

Gehele Getallen

Notatie. Meestal groeperen we gelijke factoren in de priemontbinding van een getal $n \in \mathbb{N}$. In het algemeen noteren we dus een priemontbinding als

$$n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$$

met $p_1, p_2, \ldots, p_k$ verschillende priemgetallen en $l_1, l_2, \ldots, l_k \in \mathbb{N}_0$.

Toepassing. Zijn m, n niet-nulle natuurlijke getallen, dan geldt $m^2 \neq 2n^2$.

Bewijs. Als $m = 1$ of $n = 1$ is de stelling duidelijk. We nemen dus $m, n \geq 2$.
Bekijken we de ontbinding van m en n: $m = 2^x h$ en $n = 2^y k$ met $x, y \in \mathbb{N}$ en h, k oneven (het zijn de producten van de priemfactoren $\neq 2$).
Dan is $m^2 = 2^{2x} h^2$ en $2n^2 = 2^{2y+1} k^2$. Deze twee getallen kunnen nooit gelijk zijn omdat we anders twee priemontbindingen zouden hebben voor m^2, n met een even aantal factoren 2 n met een oneven aantal. □
Een gevolg is dat $\forall m, n \in \mathbb{N}_0 : \left(\frac{m}{n}\right)^2 \neq 2$, nog een bewijs dat $\sqrt{2} \notin \mathbb{Q}$.

Stelling.

Er zijn oneindig veel priemgetallen.

Bewijs. Veronderstel dat er maar $n \in \mathbb{N}$ priemgetallen $p_1, p_2, \ldots, p_n$ zijn. Beschouw het getal

$$m = p_1 p_2 \cdots p_n + 1.$$

Voor elk priemgetal p_i ($i \in [n]$) is $m - 1$ een veelvoud van p_i, dus $\forall i \in [n] : p_i \nmid m$. Maar m heeft een priemontbinding. Dus moeten er andere priemgetallen bestaan dan $p_1, p_2, \ldots, p_n$. $\square$

Definitie.
Voor twee niet-nulle natuurlijke getallen m en n definieren we het **kleinste gemeen veelvoud** *van m en n als het kleinste niet-nul natuurlijk getal dat een veelvoud is van zowel m als n. We noteren dit getal* $\text{kgv}(m, n)$*. We hebben dus dat elk gemeen veelvoud van m en n deelbaar is door* $\text{kgv}(m, n)$*.*

Lemma.
Zij m en n niet-nulle natuurlijke getallen en zij $P = \{p_1, p_2, \ldots, p_k\}$ de verzameling van alle priemgetallen die m of n delen. Dan hebben we

$$m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \qquad \text{en} \qquad n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

voor zekere natuurlijke getallen $m_1, m_2, \ldots, m_k$ en $n_1, n_2, \ldots, n_k$. Er geldt

$$\text{ggd}(m, n) = \prod_{i=1}^{k} p_i^{\min\{m_i, n_i\}}$$

en

$$\text{kgv}(m, n) = \prod_{i=1}^{k} p_i^{\max\{m_i, n_i\}}$$

Bewijs. Zij c een gemeenschappelijke deler van m en n. Dan moet elk priemgetal dat c deelt zeker behoren tot P. Dus geldt

$$c = \prod_{i=1}^{k} p_i^{c_i},$$

met voor elke $i \in [k]$, $c_i \leq m_i$ en $c_i \leq n_i$. Bovendien levert elke keuze van $c_i \in \mathbb{N}$ binnen deze beperkingen een gemeenschappelijke deler van m en n. Hieruit volgt nu gemakkelijk dat de grootste gemeenschappelijke deler moet gelijk zijn aan $\prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}}$. Het is ook duidelijk dat elk gemeenschappelijk veelvoud van m en n deelbaar moet zijn door $p_i^{\max\{m_i,n_i\}}$ voor elke $i \in [k]$. Het kleinste zulk veelvoud is juist $\prod_{i=1}^{k} p_i^{\max\{m_i,n_i\}}$. $\square$

Gevolg.
Voor niet-nulle natuurlijke getallen n en m geldt steeds

$$\text{ggd}(m,n)\cdot\text{kgv}(m,n) = mn.$$

Bewijs. Merk op dat $\min\{m_i,n_i\} = m_i$ impliceert dat $\max\{m_i,n_i\} = n_i$ en omgekeerd. Dus volgt uit vorig lemma dat

$$\text{ggd}(m,n)\cdot\text{kgv}(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}}\cdot\prod_{i=1}^{k} p_i^{\max\{m_i,n_i\}} = \prod_{i=1}^{k} p_i^{m_i+n_i} = m\cdot n.$$

□

Gevolg.

Voor niet-nulle natuurlijke getallen n en m zijn $\frac{m}{\text{ggd}(m,n)}$ en $\frac{n}{\text{ggd}(m,n)}$ steeds relatief priem.

Bewijs. Rekening houdend met $\text{ggd}(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}}$, zien we dat

$$\frac{m}{\text{ggd}(m,n)} = \prod_{i=1}^{k} p_i^{m_i - \min\{m_i,n_i\}}, \quad \frac{n}{\text{ggd}(m,n)} = \prod_{i=1}^{k} p_i^{n_i - \min\{m_i,n_i\}}$$

Bovendien is voor elke $i \in [k]$ het minimum van $\{m_i, n_i\}$ gelijk is aan m_i of n_i zodat voor elke $i \in [k]$ minstens één van de exponenten $m_i - \min\{m_i, n_i\}$ of $n_i - \min\{m_i, n_i\}$ moet gelijk zijn aan nul. Dit betekent dat de priemfactor p_i niet voorkomt in de ontbinding van respectievelijk $\frac{m}{\text{ggd}(m,n)}$ of $\frac{n}{\text{ggd}(m,n)}$. Hierdoor hebben deze twee getallen geen enkele priemfactor gemeenschappelijk. $\square$

De φ-functie van Euler

Definitie.
Voor een $n \in \mathbb{N}_0$ definiëren we $\varphi(n)$ als het aantal getallen in $[n]$ die relatief priem zijn met n.

Laten we een kleine tabel maken voor de eerste 8 positieve natuurlijke getallen.

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1	1	2	2	4	2	6	4

We merken op: voor p priem is $\varphi(p) = p - 1$.
Laten we $\varphi(12)$ berekenen. We krijgen $\varphi(12) = 4$.
Als we de som nemen van $\varphi(d)$ voor alle delers d van 12 krijgen we

$$\begin{array}{ccccccccccccc} \varphi(1) & + & \varphi(2) & + & \varphi(3) & + & \varphi(4) & + & \varphi(6) & + & \varphi(12) & = & \\ 1 & + & 1 & + & 2 & + & 2 & + & 2 & + & 4 & = & 12 \end{array}$$

Algemeen hebben we

Stelling.
$\forall n \in \mathbb{N}_0 : \sum_{d|n} \varphi(d) = n.$

Bewijs. Stel

$$S := \{(d, f) \mid d \mid n, f \in [d], \text{ggd}(d, f) = 1\}.$$

Dan geldt

$$\begin{aligned} |S| &= \sum_{d|n} |\{f \mid (d, f) \in S\}| \\ &= \sum_{d|n} \varphi(d). \end{aligned}$$

We bewijzen nu $|S| = n$ door een bijectie $\beta : S \longrightarrow [n]$ te construeren. Stel

$$\beta(d, f) := f \times \frac{n}{d},$$

wat altijd een getal uit $[n]$ is (zie definitie van S).

Nu is β injectief omdat

$$\begin{array}{rcl} \beta(d,f) & = & \beta(d',f') \\ & \Updownarrow & \\ f \times \dfrac{n}{d} & = & f' \times \dfrac{n}{d'} \\ & \Updownarrow & \\ \dfrac{f}{d} & = & \dfrac{f'}{d'} \end{array}$$

met $\text{ggd}(f,d) = \text{ggd}(f',d') = 1$. Uit Eigenschap 12 volgt dan $f' = f$ en $d' = d$.

β is ook surjectief. Zij immers $x \in [n]$ en stel

$$d_x = \frac{n}{\text{ggd}(n,x)} \in \mathbb{N} \quad \text{en} \quad f_x = \frac{x}{\text{ggd}(n,x)} \in \mathbb{N}.$$

Dan is $f_x \leq d_x$ (omdat $x \leq n$) en $\text{ggd}(d_x, f_x) = 1$ (wegens Gevolg 2). Nu geldt ook

$$\beta(d_x, f_x) = f_x \times \frac{n}{d_x} = \frac{x}{\text{ggd}(x,n)} \times n \times \frac{\text{ggd}(x,n)}{n} = x.$$

$\square$

We kunnen ook een expliciete formule bekomen voor $\varphi(n)$, indien we de priemontbinding van n kennen. Laat ons bijvoorbeeld $\varphi(60)$ berekenen. We weten dat $60 = 2^2 \times 3 \times 5$. We zoeken de getallen $f \in [60]$ met $\text{ggd}(f, 60) = 1$. Dit zijn juist alle getallen in [60] die geen (priem)factor gemeenschappelijk hebben met 60. De getallen die wegvallen zijn dus alle veelvouden van 2, van 3 en van 5 tussen 1 en 60. Maar er zijn natuurlijk getallen die tegelijk een veelvoud zijn van 2 en van 3. We hebben hier een typisch probleem van inclusie en exclusie.

Noteer $A_d := \{x \in [60] \mid d \mid x\}$. Dan is

$$\begin{aligned}
\varphi(60) &= 60 - |A_2 \cup A_3 \cup A_5| \\
&= 60 - (|A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}|) \\
&= 60 - (30 + 20 + 12 - 10 - 6 - 4 + 2) \\
&= 16.
\end{aligned}$$

Algemeen bewijzen we:

Stelling.

Zij $n \geq 2$ met als ontbinding in priemfactoren $n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$, dan geldt

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Bewijs. We stellen weer voor $d \mid n$:
$A_d := \{x \in [n] \mid d \mid x\} = \{kd \mid k \in [\frac{n}{d}]\}$ zodat $|A_d| = \frac{n}{d}$.Dan

$$\begin{aligned} \varphi(n) &= n - |A_{p_1} \cup A_{p_2} \cup \cdots \cup A_{p_k}| \\ &= n - (\alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{k-1}\alpha_k) \end{aligned}$$

met

$$\alpha_i = \sum_{\substack{\{j_1, j_2, \ldots, j_i\} \\ \in \binom{[k]}{i}}} |A_{p_{j_1}} \cap A_{p_{j_2}} \cap \cdots \cap A_{p_{j_i}}|,$$

de som van de cardinaliteiten van alle doorsnedes van i van de k verzamelingen.

Dit kunnen we nog schrijven als

$$\begin{aligned}
\alpha_i &= \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} \left| A_{p_{j_1} p_{j_2} \cdots p_{j_i}} \right| \\
&= \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} \frac{n}{p_{j_1} p_{j_2} \cdots p_{j_i}} \\
&= n \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} \frac{1}{p_{j_1} p_{j_2} \cdots p_{j_i}}.
\end{aligned}$$

Dus

$$\begin{aligned}
\varphi(n) &= n - \Big(n(\tfrac{1}{p_1} + \tfrac{1}{p_2} + \cdots + \tfrac{1}{p_k}) \\
&\quad - n(\tfrac{1}{p_1 p_2} + \tfrac{1}{p_1 p_3} + \cdots) \\
&\quad + \cdots \\
&\quad + (-1)^{k-1} n(\tfrac{1}{p_1 p_2 \cdots p_k}) \Big) \\
&= n \left(1 - \tfrac{1}{p_1}\right) \left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_k}\right).
\end{aligned}$$

□

Definitie.
Een relatie $\mathcal{R} \subset X \times X$ *is een* **equivalentierelatie** *als ze*

1. *reflexief is:*
$$\forall x \in X : x\mathcal{R}x$$
2. **symmetrisch** *is:*
$$\forall x, y \in X : x\mathcal{R}y \iff y\mathcal{R}x$$
3. *transitief is:*
$$\forall x, y, z \in X : x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

Definitie.
Gegeven een verzameling V, definiëren we een **partitie** *van V als een verzameling $\mathcal{A}$ van deelverzamelingen van V die voldoen aan volgende twee voorwaarden:*

(P1) $\forall A \neq B \in \mathcal{A}\colon A \cap B = \emptyset$

(P2) $\bigcup \mathcal{A} = V$

Stelling.

Een equivalentierelatie geeft steeds aanleiding tot een partitie.

Bewijs. Stel voor $x \in X$:

$$E_x := \{y \in X \mid y\mathcal{R}x\}.$$

E_x heet de **equivalentieklasse** van x en x zelf heet **representant**. Dan is $\mathcal{E} = \{E_x \mid x \in X\}$ een partitie. Inderdaad,

- (P2) is voldaan omdat $\forall x \in X : E_x \subset X$, zodat $\mathcal{E} \subset X$ maar bovendien geeft de reflexiviteit van $\mathcal{R}$ dat $\forall x \in X : x \in E_x$, zodat $X \subset \mathcal{E}$.
- (P1) is ook voldaan. We bewijzen dat $E_x \cap E_y \neq \emptyset \Rightarrow E_x = E_y$. Zij namelijk $z \in E_x \cap E_y$. Dan $x\mathcal{R}z$ en $y\mathcal{R}z$ en bijgevolg $x\mathcal{R}y$ zodat $x \in E_y$. De transitiviteit toont aan dat $E_x \subset E_y$. Ook $y \in E_x$ zodat $E_y \subset E_x$.

□

Stelling.

Ook omgekeerd geeft elke partitie van een verzameling X aanleiding tot een equivalentierelatie.

Bewijs. Zij $\mathcal{A}$ een partitie van X. Definieer, voor $x, y \in X$:

$$x \mathcal{R} y \iff \exists A \in \mathcal{A} : x, y \in A.$$

Ga zelf als oefening na dat dit een equivalentierelatie is. $\square$

Definitie.
Zij $x_1, x_2 \in \mathbb{Z}, m \in \mathbb{N}_0$. x_1 *en* x_2 *heten* **congruent modulo** m *indien* $m \mid x_2 - x_1$. *Het natuurlijk getal* m *heet de* **modulus**. *We schrijven* $x_1 \equiv_m x_2$ *of* $x_1 \equiv x_2 \pmod{m}$.

Eigenschap.
$\equiv_m$ *is een equivalentierelatie.*

Bewijs. $\equiv_m$ is

- reflexief: $x \equiv_m x$ want $x - x = 0$ is een veelvoud van m;
- symmetrisch:
  $x \equiv_m y \Rightarrow y - x = km \Rightarrow x - y = (-k)m \Rightarrow y \equiv_m x$;
- transitief: $x \equiv_m y$ en $y \equiv_m z \Rightarrow y - x = km$ en $z - y = lm$
  $\Rightarrow z - x = (z - y) + (y - x) = (k + l)m$.

□

Stelling.
$\equiv_m$ is 'compatibel' met '$+$' en '$.$' in $\mathbb{Z}$, i.e.: $\forall x_1, x_2, y_1, y_2 \in \mathbb{Z}$ met $x_1 \equiv_m x_2$ en $y_1 \equiv_m y_2$:

$$x_1 + y_1 \equiv_m x_2 + y_2$$

en

$$x_1 y_1 \equiv_m x_2 y_2.$$

Bewijs. Stel $x_2 - x_1 = km$ en $y_2 - y_1 = lm$. Dan geldt

$$(x_2 + y_2) - (x_1 + y_1) = (x_2 - x_1) + (y_2 - y_1) = km + lm = (k + l)m$$

en

$$\begin{aligned} x_2 y_2 - x_1 y_1 &= x_2 y_2 - x_1 y_2 + x_1 y_2 - x_1 y_1 \\ &= (x_2 - x_1) y_2 + (y_2 - y_1) x_1 \\ &= km y_2 + lm x_1 \\ &= (k y_2 + l x_1) m \end{aligned}$$

□

Toepassing.(De 9-proef) Als een getal in basis 10 geschreven wordt als $x_n x_{n-1} \cdots x_0$ dan hebben we

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod 9.$$

Bewijs.

$$\begin{aligned} x - (x_0 + x_1 + \cdots + x_n) &= x_0 + x_1 \times 10 + \cdots + x_n \times 10^n \\ &\quad -x_0 - x_1 - \cdots - x_n \\ &= 9x_1 + 99x_2 + 999x_3 + \cdots + (10^n - 1)x_n. \end{aligned}$$

Maar er geldt duidelijk dat $9 \mid 10^i - 1 = \underbrace{99 \cdots 99}_{i \text{ keer}}$. Als we dan $\rho(x)$ schrijven voor $x_0 + x_1 + \cdots + x_n$, dan hebben we aangetoond:

$$\forall x \in \mathbb{Z} : x \equiv \rho(x) \pmod 9.$$

□

Dit wordt in de lagere school gebruikt om berekeningen na te kijken. Inderdaad, we weten dat $x \equiv \rho(x) \pmod 9$ en $y \equiv \rho(y) \pmod 9$. Als $xy = z$ moet dus

$$\rho(z) \equiv z \equiv xy \equiv \rho(x)\rho(y) \pmod 9.$$

Opgelet: het omgekeerde geldt niet noodzakelijk. Als de 9-proef klopt ben je dus nog niet zeker van je resultaat.

Voorbeeld. $54321 \times 98765 = 5363013565$ kan onmogelijk juist zijn, want $\rho(54321) = 15$, $\rho(98765)=35$ en $\rho(5363013565) = 37$. Wil de berekening kloppen, dan moet dus ook $15 \times 35 \equiv 37 \pmod 9$. Maar we mogen elk van deze getallen nog reduceren mod 9 om de berekeningen te vereenvoudigen. Dus

$$\begin{aligned} & 15 \times 35 \equiv 37 \pmod 9 \\ \iff \quad & 6 \times 8 \equiv 1 \pmod 9 \\ \iff \quad & 48 \equiv 1 \pmod 9 \\ \iff \quad & 3 \equiv 1 \pmod 9 \end{aligned}$$

wat dus fout is.

Vermits congruentie modulo m een equivalentierelatie is, kunnen we kijken naar de partitie die ontstaat. Bijvoorbeeld:

$$
\begin{aligned}
E_0 &= \{0, m, 2m, -5m, \ldots\} \\
&= \{km \mid k \in \mathbb{Z}\} \\
&= \{\text{veelvouden van } m\} \\
E_1 &= \{1, m+1, -3m+1, \ldots\} \\
&= \{km+1 \mid k \in \mathbb{Z}\} \\
&= \{\text{gehele getallen met rest bij deling door } m \text{ gelijk is aan } 1\} \\
E_2 &= \{km+2 \mid k \in \mathbb{Z}\} \\
&\vdots \\
E_{m-1} &= \{km+(m-1) \mid k \in \mathbb{Z}\} \\
E_m &= E_0.
\end{aligned}
$$

We hebben m congruentieklassen. Ze vormen een partitie van $\mathbb{Z}$. De bewerkingen van $\mathbb{Z}$ induceren bewerkingen op deze m congruentieklassen:

$$E_k + E_l := E_{k+l}, \qquad E_k \times E_l := E_{k \times l}.$$

Natuurlijk moeten we nagaan dat deze bewerkingen niet afhangen van de keuze van de representanten in E_k en E_l.
Zij $E_k = E_{k'}$ en $E_l = E_{l'}$. We moeten bewijzen dat $E_{k+l} = E_{k'+l'}$. Maar dat is gewoon een gevolg van Stelling 6 omdat $k \equiv_m k'$ en $l \equiv_m l'$ en dus $k + l \equiv_m k' + l'$. Voor de vermenigvuldiging werken we volledig analoog.
Notatie. De verzameling $\{E_0, E_1, \ldots, E_{m-1}\}$ noteren we $\mathbb{Z}_m$.

Stelling.

$(\mathbb{Z}_m, +, .)$ *is een commutatieve ring met eenheid.*

Bewijs. De bewerkingen zijn inwendig: $E_k + E_l \in \mathbb{Z}_m$ en $E_k \times E_l \in \mathbb{Z}_m$. De commutativiteit komt neer op $E_k + E_l = E_l + E_k$ en $E_k \times E_l = E_l \times E_k$, wat klopt door de overeenkomstige eigenschappen van $+$ en $\times$ in $\mathbb{Z}$. Verder moeten we nog aantonen dat

$$
\begin{aligned}
&(E_k + E_l) + E_n = E_k + (E_l + E_n)\\
&(E_k \times E_l) \times E_n = E_k \times (E_l \times E_n)\\
&E_k + E_0 = E_k = E_0 + E_k\\
&E_k \times E_1 = E_k = E_1 \times E_k\\
&E_k \times (E_l + E_n) = E_k \times E_l + E_k \times E_n\\
&(E_k + E_l) \times E_n = E_k \times E_n + E_l \times E_n\\
&\forall E_k \in \mathbb{Z}_m : \exists\ -E_k = E_{-k} \in \mathbb{Z}_m : E_k + (-E_k) = E_0 = (-E_k) + E_k
\end{aligned}
$$

We laten de bewijzen als oefening. $\square$

Vereenvoudiging van notatie

Vermits de rekenregels in $(\mathbb{Z}_m, +, \times)$ dezelfde zijn als in $(\mathbb{Z}, +, \times)$, kunnen we zonder gevaar k noteren in plaats van E_k voor de restklasse van k modulo m. De context moet dan uitwijzen of we modulo m tellen of gewoon in $\mathbb{Z}$. $5 + 3$ zal dus een verkorte notatie zijn voor $E_5 + E_3$ in $\mathbb{Z}_6$ bijvoorbeeld. We zullen dan ook hebben $5 + 3 = 2$.

Toch even wijzen op een belangrijk verschil tussen $\mathbb{Z}$ en $\mathbb{Z}_m$. In $\mathbb{Z}$ geldt voor elke $a \neq 0$ dat $ab = ac \Rightarrow b = c$. Dit is niet langer waar in $\mathbb{Z}_m$. In $\mathbb{Z}_6$ bijvoorbeeld hebben we $3 \times 1 = 3 \times 5$, maar $1 \neq 5$.

Inverteerbare elementen in $\mathbb{Z}_m$

We hebben gezien dat $(\mathbb{Z}_m, +, \times)$ een commutatieve ring is met eenheid. Het verschil met veelgebruikte ringen zoals $(\mathbb{Q}, +, \times)$ of $(\mathbb{R}, +, \times)$ is dat sommige elementen niet inverteerbaar zijn.

Definitie.
$x \in \mathbb{Z}_m$ heet **inverteerbaar** *indien er een $y \in \mathbb{Z}_m$ bestaat met $x \times y = 1$ (dus $x \times y \equiv_m 1$).*

Voorbeeld. In $\mathbb{Z}_6$ is 1 inverteerbaar, want $1 \times 1 = 1$. 2 is *niet* inverteerbaar want $2 \times 0 = 0$, $2 \times 1 = 2$, $2 \times 2 = 4$, $2 \times 3 = 0$, $2 \times 4 = 2$, $2 \times 5 = 4$. Dus $\nexists y \in \mathbb{Z}_6 : 2 \times y = 1$.

Lemma.
Zij $x \in \mathbb{Z}_m$ inverteerbaar. Dan is het invers van x uniek.

Bewijs. Veronderstel dat y en z twee inversen zijn. Dus $xy = xz = 1$. Dan $y = y \times 1 = y(xz) = (yx)z = 1 \times z = z$. $\square$

Bijgevolg kunnen we een notatie invoeren voor het uniek invers van $x \in \mathbb{Z}_m$, namelijk x^{-1}. Noteer ook
$\mathcal{U}_m = \{x \in \mathbb{Z}_m \mid x \text{ inverteerbaar}\}$.

Stelling.

$$\forall x \in \mathbb{Z}_m : x \in \mathcal{U}_m \iff \text{ggd}(x, m) = 1.$$

Bewijs.

$\boxed{\Rightarrow}$

$$\begin{aligned} x \in \mathcal{U}_m &\iff \exists\, y \in \mathbb{Z}_m : xy = 1 \\ &\iff \exists y \in \mathbb{Z}, \exists\, k \in \mathbb{Z} : xy - 1 = km \\ &\iff \exists y \in \mathbb{Z}, \exists\, k \in \mathbb{Z} : xy - km = 1 \end{aligned}$$

Een gemene deler van x en m is ook een deler van $xy - km$. Bijgevolg is $\text{ggd}(x, m) = 1$.

$\boxed{\Leftarrow}$ $\text{ggd}(x, m) = 1 \Rightarrow \exists\, y, k \in \mathbb{Z} : xy + km = 1$ of $xy - 1 = -km$ of nog $m \mid xy - 1$ zodat $xy = 1$ in $\mathbb{Z}_m$.

□

Gevolg.
$|\mathcal{U}_m| = \varphi(m)$.

Definitie.
Een ring met eenheid waarin elk niet-nul element inverteerbaar is, heet een **lichaam**. *Indien de vermenigvuldiging bovendien commutatief is, spreekt men van een* **veld**.

Gevolg.
Voor p priem is elk van nul verschillend element in $\mathbb{Z}_p$ inverteerbaar. $(\mathbb{Z}_p, +, \times)$ is dus een veld.

Lemma.
Als $x, y \in \mathcal{U}_m$*, dan* $xy \in \mathcal{U}_m$ *en* $(xy)^{-1} = y^{-1}x^{-1}$*.*

Bewijs. $xy \times y^{-1}x^{-1} = xx^{-1} = 1$ en inversen zijn uniek. □

Stelling.

$$\forall y \in \mathcal{U}_m : y\mathcal{U}_m = \mathcal{U}_m.$$

Bewijs. Uit Lemma 3 volgt $y\mathcal{U}_m \subset \mathcal{U}_m$. Stel nu $x \in \mathcal{U}_m$. Dan is $x = y(y^{-1}x)$ en $y^{-1} \in \mathcal{U}_m$, want $y^{-1}y = 1$, zodat $y^{-1}x \in \mathcal{U}_m$. □

Stelling.

Zij $y \in \mathcal{U}_m$. Dan geldt: $y^{\varphi(m)} = 1$ in $\mathbb{Z}_m$.

Bewijs. Nummer de elementen van $\mathcal{U}_m$. Dus $\mathcal{U}_m = \{u_1, u_2, \ldots, u_{\varphi(m)}\}$. Stel $u := u_1 u_2 \cdots u_{\varphi(m)}$. Dan is u een element van $\mathcal{U}_m$, want het is een product van elementen van $\mathcal{U}_m$. Vermits $y\mathcal{U}_m = \mathcal{U}_m$ zijn de elementen $yu_1, yu_2, \ldots, yu_{\varphi(m)}$ niets anders dan $u_1, u_2, \ldots, u_{\varphi(m)}$, eventueel in een andere volgorde geschreven. Bijgevolg geldt ook:

$$yu_1 \times yu_2 \times \cdots \times yu_{\varphi(m)} = u$$

of nog

$$y^{\varphi(m)} u_1 u_2 \cdots u_{\varphi(m)} = u$$

of

$$\begin{aligned} & y^{\varphi(m)} u = u \\ \iff \quad & y^{\varphi(m)} u u^{-1} = u u^{-1} \\ \iff \quad & y^{\varphi(m)} = 1. \end{aligned}$$

□

Andere formuleringen van dezelfde stelling:

$$\forall y \in \mathbb{Z}, \forall m \in \mathbb{N}_0 : \text{ggd}(y, m) = 1 \Rightarrow y^{\varphi(m)} \equiv_m 1.$$

Dit resultaat heet de *Stelling van Euler*. Een speciaal geval is de *Kleine stelling van Fermat*:

Stelling.

Voor p priem hebben we

$$\forall n \in \mathbb{N} : n^p \equiv_p n.$$

Bewijs. Als $p \nmid n$ is n inverteerbaar modulo p zodat $n^{\varphi(p)} \equiv_p 1$, of nog $n^{p-1} \equiv_p 1$, zodat $n^p \equiv_p n$.
Als $p \mid n$ is het duidelijk dat $n^p \equiv_p 0 \equiv_p n$. □

De Chinese reststelling

In de eerste eeuw stelde de Chinese wiskundige Sun-Tsu het volgende vraagstuk: "Van een getal weet men dat de rest bij deling door 3 gelijk is aan 2; wanneer men deelt door 5, vindt men als rest 3 en bij deling door 7 bedraagt de rest 2. Over welk getal gaat het?"
Het gaat hier eigenlijk om een *stelsel* van verschillende vergelijkingen waaraan het onbekende getal x moet voldoen:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Stelling. (Chinese reststelling)

Zij $m_1, m_2, \ldots, m_n$ paarsgewijs relatief prieme natuurlijke getallen en $a_1, a_2, \ldots, a_n$ willekeurige gehele getallen. Dan heeft het stelsel

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

een oplossing die uniek is modulo $m = m_1 m_2 \cdots m_n$. D.w.z. een unieke oplossing x met $0 \leqslant x < m$ en alle andere oplossingen congruent modulo m met deze x.

Bewijs. We geven een *constructief* bewijs. We gaan dus een algoritme geven om de oplossing werkelijk te construeren.
Voor $k \in [n]$ stellen we eerst $M_k := m/m_k$. Dit is het product van alle moduli, behalve m_k. Vermits alle moduli relatief priem zijn, hebben we zeker $\text{ggd}(m_k, M_k) = 1$. Stelling 8 zorgt dan voor een getal y_k met

$$M_k y_k \equiv 1 \pmod{m_k}$$

Stel nu

$$x := a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \in \mathbb{Z}.$$

We tonen nu dat deze x een oplossing is van het stelsel. Merk eerst op dat $M_j \equiv 0 \pmod{m_i}$ van zodra $i \neq j$. Als we dus x reduceren modulo m_k, blijft er alleen maar

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$$

over.
Onderstel nu dat y een andere oplossing is van het stelsel. Dan geldt voor elke $k \in [n]$ dat $m_k \mid x - y$. Vermits alle m_k relatief priem zijn, volgt hieruit $m \mid x - y$. $\square$

Voorbeeld. We kunnen nu de vraag van Sun-Tsu oplossen.
We berekenen $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$ en $M_3 = m/7 = 15$. De inversen van M_k modulo m_k berekenen is ook niet moeilijk. We vinden $y_1 = 2$, $y_2 = 1$ en $y_3 = 1$. Hieruit vinden we

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \mod 105.$$

Public key cryptography

Als je geheime berichten wil versturen moet je een techniek afspreken om te *coderen*. Deze techniek noemen we een **cryptosysteem**.
Een bekend eenvoudig cryptosysteem bestaat erin om de letters te "verschuiven" in het alfabet. Als je bijvoorbeeld het bericht "`IK HEB EEN KOEKJE`" wil versturen, kan je elke letter drie plaatsen opschuiven in het alfabet. Je stuurt dus "`LN KHE HHQ NRHNMH`". Indien je als antwoord "`LN ZLO HHQ VWXN`" krijgt, kan je door de inverse operatie het bericht ontcijferen. Je krijgt "`IK WIL EEN STUK`".

Zulk eenvoudig systeem is doeltreffend indien men er zeker van is dat het bericht nooit zal onderschept worden door iemand die iets weet over de frequentie waarmee letters voorkomen in de Nederlandse taal. In onze berichten zie je bijvoorbeeld twee keer "HHQ". Er is veel kans dat dit "EEN" voorstelt.
Een ander nadeel van dit systeem is dat de twee personen die willen communiceren, op voorhand moeten afspreken hoeveel plaatsen zij elke letter opschuiven. Dit is wat men de *sleutel* van het cryptosysteem noemt. Deze sleutel moet geheim blijven. De sleutel uitwisselen tussen de twee personen die willen communiceren is dus een probleem bij dit soort cryptosysteem. Voor betalingen over internet moeten vele gebruikers communiceren met één bedrijf. Het is onbegonnen werk om voor elke gebruiker een sleutel mee te delen zonder dat hij kan onderschept worden. Gelukkig werd er in de jaren '70 door Rivest, Shamir en Adleman een systeem bedacht waarbij de sleutels niet meer geheim hoeven te zijn. Men spreekt van *Public Key Cryptography*.

Het systeem is gebaseerd op priemgetallen en modulair rekenen. Persoon A wil een geheim bericht naar persoon B sturen. Hiervoor gaat hij eerst zijn bericht (dat in letters geschreven is) vertalen naar getallen zodat er kan gerekend worden. Dit gebeurt via een standaard tabel die niet geheim hoeft te zijn. We kunnen bijvoorbeeld afspreken dat "A" wordt voorgesteld door het getal 1, "B" door 2, enz. De spatie is 0. Het bericht "`LUISTER GOED`" wordt dan bijvoorbeeld "`12 21 09 19 20 05 18 00 07 15 05 04`".
We gaan nu elke letter coderen door het te verheffen tot een vaste macht en dan het resultaat te reduceren modulo 33 (omdat er bijvoorbeeld 33 tekens zijn in ons eenvoudig systeem: letters plus wat leestekens). Laat ons bijvoorbeeld telkens de derde macht nemen. Dan is het gecodeerd bericht "`12 21 3 28 14 26 24 0 13 9 26 31`".

Dit was een voorbeeld met kleine getallen om te illustreren wat er gebeurt. In de praktijk gaan we te werk met veel grotere getallen. We moeten ook nog zien hoe deze machtsverheffing kan geïnverteerd worden om te decoderen.
Eén van de voornaamste eigenschappen waarop de veiligheid van het RSA cryptosysteem steunt, is de moeilijkheid om een willekeurig getal te ontbinden in priemfactoren. Het is bijvoorbeeld zeer gemakkelijk om de twee priemgetallen 71 en 59 met elkaar te vermenigvuldigen. We krijgen 4189. Probeer nu het omgekeerde: neem een vergelijkbaar getal, 4161, en probeer dat eens te ontbinden in priemfactoren.

Laat ons de methode van de machtsverheffing nu eens proberen met grotere getallen: we verheffen tot de macht 101 en reduceren modulo 1189. Vermits resten modulo 1189 groter kunnen worden dan 27 hebben we de mogelijkheid om meer symbolen te gebruiken of meerdere letters ineens te coderen. In ons bericht "12 21 09 19 20 05 18 00 07 15 05 04" van hoger kunnen we de cijfers per drie groeperen zodat we "122 109 192 005 180 007 150 504" verkrijgen. Indien het aantal cijfers geen veelvoud is van drie, voegen we op het einde nullen toe om overal groepjes van drie cijfers te hebben.
We moeten nu dus 122^{101} berekenen. Dat is een ander paar mouwen... Zelfs met een rekenmachine zal dat niet lukken, tenzij we het slim aanpakken. We hebben hier immers te maken met een getal van 211 cijfers. Een eerste idee zou zijn om die macht stap voor stap te berekenen en steeds te reduceren modulo 1189. Op die manier krijgen we geen al te grote getallen.

Hier gaan we dan:

$$
\begin{aligned}
122^2 &= 122 \cdot 122 = 14884 \equiv 616 \pmod{1189} \\
122^3 &= 122^2 \cdot 122 \equiv 616 \cdot 122 = 75152 \equiv 245 \pmod{1189} \\
122^4 &= 122^3 \cdot 122 \equiv 245 \cdot 122 = 29890 \equiv 165 \pmod{1189} \\
&\vdots
\end{aligned}
$$

Maar dat is ook nogal veel werk. Veel slimmer is om steeds te kwadrateren.

$$
\begin{aligned}
122^2 &= \qquad = 14884 \equiv 616 \pmod{1189} \\
122^4 &\equiv 616^2 = 379456 \equiv 165 \pmod{1189} \\
122^8 &\equiv 165^2 = 27225 \equiv 1067 \pmod{1189} \\
122^{16} &\equiv 1067^2 = 1138489 \equiv 616 \pmod{1189} \\
122^{32} &\equiv 616^2 = 379456 \equiv 165 \pmod{1189} \\
122^{64} &\equiv 165^2 = 27225 \equiv 1067 \pmod{1189}
\end{aligned}
$$

Nu geldt $101 = 1 + 4 + 32 + 64$ zodat
$122^{101} = 122^1 \cdot 122^4 \cdot 122^{32} \cdot 122^{64} \equiv 122 \cdot 165 \cdot 165 \cdot 1067 =$
$3543987150 \equiv 245 \pmod{1189}$.
Dus met vijf kwadrateringen, een paar vermenigvuldigingen en reducties modulo 1189 hebben we het resultaat. Dit is veel efficiënter dan de honderd vermenigvuldigingen en reducties die we eerst gingen uitvoeren! Deze methode werkt steeds omdat we elke mogelijke exponent steeds kunnen schrijven als som van machten van 2. Dit komt er immers op neer dat we de exponent uitschrijven in basis 2.

We beschrijven nu het RSA algoritme in het algemeen. Persoon B die berichten wil ontvangen kiest twee (grote) priemgetallen p en q en berekent hun product $n := pq$. Hij bepaalt ook $b := (p-1)(q-1)$ en zoekt e met $\text{ggd}(e, b) = 1$. De informatie die publiek wordt gemaakt is n en e.
Indien persoon A een gecodeerd bericht wil sturen naar B zal hij eerst zijn bericht omzetten in getallen. Elk van die getallen m gaat hij dan coderen als volgt

$$c := m^e \pmod{n}$$

Het symbool c wordt dan verstuurd.

Wanneer B het bericht c ontvangt, moet hij dat decoderen. Hij maakt hiervoor gebruik van het feit dat $\text{ggd}(e, b) = 1$. Er is dus een invers d van e modulo b. Er bestaat dus een k met $ed = 1 + k(p-1)(q-1)$zodat

$$c^d \equiv (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} \pmod{n}$$

We veronderstellen nu even dat $\text{ggd}(m, p) = \text{ggd}(m, q) = 1$, wat geen grote beperking is. Dan kunnen we de uit de Stelling van Euler (Stelling 10) halen dat $m^{p-1} \equiv 1 \pmod{p}$ en $m^{q-1} \equiv 1 \pmod{q}$. Bijgevolg geldt

$$c^d \equiv m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1 \equiv m \pmod{p}$$

alsook

$$c^d \equiv m \cdot (m^{q-1})^{k(p-1)} \equiv m \cdot 1 \equiv m \pmod{q}.$$

Merk op dat indien m een veelvoud is van p of q, bovenstaande equivalenties geldig blijven. De onderstelling $\text{ggd}(m, p) = \text{ggd}(m, q) = 1$ was dus slechts tijdelijk nodig.
Uit de Chinese reststelling volgt nu dat

$$c^d \equiv m \pmod{pq}$$

Dus kan B decoderen door gewoon c^d te reduceren modulo n.

In de praktijk worden priemgetallen van ongeveer tweehonderd cijfers gebruikt. Dan heeft n ongeveer vierhonderd cijfers en duurt de ontbinding in priemfactoren, met de beste algoritmen die tot nu toe bekend zijn, nog duizenden jaren. Men mag dus zeggen dat RSA cryptosystemen voorlopig veilig zijn. Bovendien bieden zij het grote voordeel dat de sleutel die dient voor het coderen publiek mag gemaakt worden zonder het systeem in gevaar te brengen.