LIMO 2020

ANTWOORDEN BOEKJE

transtrend

Utrecht University

Dit uitwerkingenboekje is een uitgave van de LIMO-commissie 2020:
Ludo Dekker, Lizanne van der Laan, Jorke de Vlas, Jasper Oostlander, Stein Meereboer, Rinske Oskamp en Mieke Wessel
e-mail: `limo2020@a-eskwadraat.nl`
website: `limo2020.a-eskwadraat.nl`
Opgaven: T. Verhoeff, H. de Boer, J. de Vlas, M. Daas, M. Wessel, M. Staps, H. Smit, M. Caspers en S. Cambie

Inhoudsopgave

1. Sommen met kwadraten

dr. T. (Tom) Verhoeff
Technische Universiteit Eindhoven

Op maandag 10 februari jl. vestigde rekenwonder Willem Bouman (1939) aan de TU Eindhoven een nieuw wereldrecord. Daarvoor moest hij elk van tien 5-cijferige getallen (willekeurig door de jury gekozen) schrijven als som van vier kwadraten. Hij mocht alleen naar de getallen kijken en dan zijn antwoord opschrijven (en daarna niet meer controleren of verbeteren). Alles moest uit het hoofd. Dat lukte (en zelfs binnen vijf minuten).

Het is goed om te weten dat volgens de *vier-kwadratenstelling* van Lagrange uit 1770 elk natuurlijk getal te schrijven is als som van vier kwadraten. Willem kon er dus niet 'ingeluisd' worden. Ook is het goed te weten dat niet elk natuurlijk getal te schrijven is als som van drie kwadraten (bijv. 7). De *drie-kwadratenstelling* van Legendre uit 1798 maakt dit precies: een getal n is *niet* te schrijven als som van drie kwadraten dan en slechts dan als

$$\underset{k,m\in\mathbb{Z}_{\geq 0}}{\exists} \quad n = 4^k(8m+7)$$

We weten niet precies hoe Willem te werk gaat. Er zijn meestal veel oplossingen mogelijk, en hij hoeft er slechts één te vinden. Het volgende kan hem helpen.

Laat $n, r \in \mathbb{N}$ waarbij $r^2 \leq n < (r+1)^2$.

a) **(6 punten)** Bewijs dat, als n niet deelbaar is door 8, er $n_1, n_2, n_3 \in \mathbb{N}$ bestaan met

$$n = n_1^2 + n_2^2 + n_3^2 + n_4^2$$

waarbij $n_4 = r$ of $n_4 = r - 1$.

b) **(4 punten)** Geef twee $n \in \mathbb{N}$ waarvoor $n - r^2$ en $n - (r-1)^2$ beide niet te schrijven zijn als som van drie kwadraten. Schrijf deze n bovendien als som van vier kwadraten.

Uitwerking.

a) Zij $n, r \in \mathbb{N}$ waarbij n niet deelbaar is door 8 en $r^2 \leq n < (r+1)^2$. We laten zien dat $n - n_4^2$ te schrijven is als som van drie kwadraten, waarbij $n_4 = r$ of $n_4 = r - 1$.

Volgens de drie-kwadratenstelling van Legendre volstaat het om te laten zien dat $n - n_4^2$ niet van de vorm $4^k(8m+7)$ is. Daarom is het goed om modulo 8 te rekenen.

Merk op dat van r en $r-1$ er precies één even en de ander oneven is. We weten daarom dat n_4^2 mod 8 alleen de waarden 0, 1 of 4 kan aannemen: 0 of 4 wanneer n_4 even is en 1 wanneer n_4 oneven is.[1]

We weten verder dat $n \not\equiv 0 \pmod 8$ en derhalve $n \bmod 8 \in \{1, 2, 3, 4, 5, 6, 7\}$.

De volgende tabel toont n_4^2 (verticaal), n (horizontaal) en $n - n_4^2$ (allemaal modulo 8):

$n - n_4^2$	$n =$	1	2	3	4	5	6	7
$n_4^2 = 0$		1	2	3	$\boxed{4}$	5	6	$\boxed{7}$
4		5	6	$\boxed{7}$	$\boxed{0}$	1	2	3
1		$\boxed{0}$	1	2	3	$\boxed{4}$	5	6

[1]Voor de volledigheid: $(2a)^2 = 4a^2 \equiv 0 \pmod 4$ en $(2a+1)^2 = 4a(a+1)+1 \equiv 1 \pmod 8$ omdat van a en $a+1$ er een even is.

We kunnen de omkaderde uitkomsten vermijden door geschikte keuze van $n_4 = r$ of $n_4 = r - 1$, omdat een even is en de ander oneven. In de niet-omkaderde gevallen kan $n - n_4^2$ niet van de vorm $4^k(8m + 7)$ zijn, en is derhalve te schrijven als $n_1^2 + n_2^2 + n_3^2$.

b) We zoeken $n \in \mathbb{N}$ met $8 \mid n$ (vanwege het eerste onderdeel) en beide $n - r^2$ en $n-(r-1)^2 = n-r^2+2r-1$ zijn van de vorm $4^k(8m+7)$, zodat deze niet te schrijven zijn als som van drie kwadraten. Gezien één van de twee oneven moet zijn, moet die wel van de vorm $8m_1+7$ zijn. De ander moet even zijn en dus van de vorm $4^k(8m_2+7)$ met $k \geq 1$.

Neem eerst aan dat r oneven is en dus $n - r^2 = 8m_1 + 7$ en $n - (r - 1)^2 = 4^k(8m_2 + 7)$. Gezien $n < (r+1)^2$ vinden we dat $n - r^2 < 2r+1$. Dus we vinden dat $8m_1 + 7 < 2r+1$ en $4^k(8m_2 + 7) < 4r$. Uit de tweede ongelijkheid volgt dat voor $k = 1$ en $m_2 = 0$ geldt dat $r \geq 9$. Als we nu een paar oneven r proberen vinden we:
$r = 9$ verplicht $k = 1, m_2 = 0$ en $m_1 \leq 1$. Dus $n - 64 = 28$ en $n = 92$. Maar 92 is niet deelbaar door 8.
$r = 11$ verplicht $k = 1, m_2 = 0$ en $m_1 \leq 1$. Dus $n - 100 = 28$. Dit geeft $n = 128$ en $128 - 121 = 7 = 8 \cdot 0 + 7$. Dus $n = 128$ voldoet inderdaad.

Natuurlijk kunnen we ook kijken naar even r en dus $n-r^2 = 4^k(8m_2+7)$ en $n-(r-1)^2 = 8m_1 + 7$. Dit geeft de ongelijkheden $4^k(8m_2 + 7) < 2r + 1$ en $8m_1 + 7 < 4r$. De eerste ongelijkheid geeft direct al dat $r \geq 14$. De eerste waarde voor r invullen geeft dan:
$r = 14$ verplicht $k = 1, m_2 = 0$ en $m_1 \leq 6$. Dus $n - 196 = 28$ en dat geeft $n = 224$ en $n - 169 = 55 = 6 \cdot 8 + 7$. Dus $n = 224$ voldoet ook.

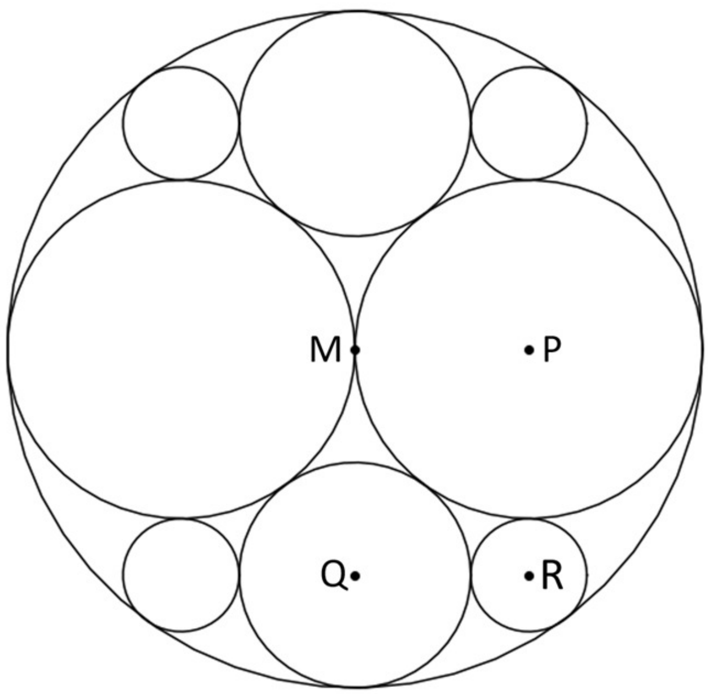
We kunnen 128 schrijven als $64 + 64 + 0 + 0$ en 224 als $144 + 64 + 16 + 0$.

2. Cirkelbedekking

Ir. H. (Harold) de Boer
Transtrend BV

In het plaatje zie je een cirkel met middelpunt M. Binnen deze cirkel liggen 8 kleinere cirkels die allemaal de grote cirkel raken. De beide grootste raken elkaar in M. Het middelpunt van de rechter van deze cirkels noemen we P. Boven en onder deze 2 cirkels liggen 2 zo groot mogelijke cirkels, zodanig dat ze de beide andere cirkels niet overlappen. Het middelpunt van de onderste van deze cirkels noemen we Q. De 4 overige cirkels zijn de grootst mogelijke cirkels binnen de grote cirkel die de eerder gedefinieerde 4 cirkels niet overlappen. Het middelpunt van de cirkel rechtsonder noemen we R.

Is de vierhoek $MPRQ$ een rechthoek? Bewijs je antwoord.



Uitwerking.
Ja, de vierhoek $MPRQ$ is een rechthoek. Om dit uit te werken gebruiken we een coördinatenstelsel. Laat $M = (0,0)$ en noem de straal van de grote cirkel r. Omdat de eerste twee cirkels elkaar en de grote cirkel raken is hun straal $\frac{1}{2}r$. Verder kunnen we de cirkel zo draaien dat P op de x-as ligt en dus heeft het punt P coördinaten $(\frac{1}{2}r, 0)$.
Voor het punt Q kunnen we vanwege symmetrie direct zien dat het op de y-as moet liggen. Om de x-coördinaat te bepalen willen we de straal, r_Q, van de cirkel met middelpunt Q bepalen. De x-coördinaat is dan gelijk aan $-r + r_Q$. Bekijk nu de driehoek MPQ. Gezien P op de x-as ligt, Q op de y-as en M de oorsprong is, is de hoek QMP recht. Uit Pythagoras volgt dus dat $|MP|^2 + |MQ|^2 = |PQ|^2$. Deze drie zijdes zijn allemaal uit te drukken in r en r_Q. $|MP| = \frac{1}{2}r$, $|MQ| = r - r_Q$ en $|PQ| = \frac{1}{2}r + r_Q$. Dit geeft de vergelijking:

$$\frac{1}{4}r^2 + r^2 - 2rr_Q + r_Q^2 = \frac{1}{4}r^2 + rr_Q + r_Q^2.$$

Oftewel, $r_Q = \frac{1}{3}r$ en $Q = (0, -\frac{2}{3}r)$.

Nu resteert slechts om de coördinaten van R te bepalen. Schrijf nu dat $R = (x, y)$ en laat r_R de straal zijn van de cirkel rondom het punt R. Er geldt nu dat $|MR| = r - r_R$, $|PR| = \frac{1}{2}r + r_R$ en $|QR| = \frac{1}{3}r + r_R$. We kunnen deze afstanden ook allemaal aan de hand van de coördinaten uitrekenen en zien dan:

$$\begin{aligned} x^2 + y^2 &= |MR|^2 = (r - r_R)^2 \\ \left(x - \frac{1}{2}r\right)^2 + y^2 &= |PR|^2 = \left(\frac{1}{2}r + r_R\right)^2 \\ x^2 + \left(y + \frac{2}{3}r\right)^2 &= |QR|^2 = \left(\frac{1}{3}r + r_R\right)^2 \end{aligned}$$

We kunnen nu de eerste vergelijking van de tweede afhalen om $r - 3r_R = x$ te vinden en door de eerste vergelijking van de derde af te halen vinden we $y = 2r_R - r$. Nu kunnen we die uitdrukkingen weer in de eerste vergelijking zetten en vinden we:

$$0 = x^2 + y^2 - (r - r_R)^2 = 12r_R^2 - 8rr_R + r^2 = (2r_R - r)(6r_R - r)$$

Dit houdt ons twee mogelijkheden over, echter als $r_R = \frac{1}{2}r$ dan volgt er dat $R = (-\frac{1}{2}r, 0)$ wat duidelijk niet kan. Dus dan zien we dat $r_R = \frac{1}{6}r$ en dat $R = (\frac{1}{2}r, -\frac{2}{3}r)$ en daarmee zien we dat $MPRQ$ een rechthoek is.

Alternatieve uitwerking.
We kunnen ook de formule van Descartes gebruiken. Zij k de kromming van de grote cirkel, en verder k_P, k_Q en k_R de krommingen van de cirkels met die respectievelijke middelpunten. Dan kunnen we zonder verlies van algemeenheid aannemen dat $k = -1$ (waarbij deze negatief is omdat alle cirkels inwendig aan de grote cirkel raken), dan zien we omdat de cirkel rondom P de helft van de straal van de grote cirkel heeft dat $k_P = 2$. Dan zien we met de formule van Descartes dat

$$k_Q = k + 2k_P \pm 2\sqrt{2kk_P + k_P^2} = 3 \pm \sqrt{0} = 3.$$

Verder zien we dan ook dat

$$k_R = k + k_P + k_Q \pm 2\sqrt{kk_P + kk_Q + k_Pk_Q} = 4 \pm 2.$$

Omdat deze cirkel kleiner is dan de andere cirkels zien we dat $k_R = 6$. Nu we de stralen van alle cirkels weten kunnen we simpel de zijdelengtes in vierhoek $MPRQ$ uitrekenen om te zien dat dit een parallellogram is, en ten slotte zien we wegens symmetrie dat $\angle PMQ = 90°$, dus $MPRQ$ is een rechthoek.

3. Flowrelatie

J. (Jorke) de Vlas, BSc.
Universiteit Utrecht

Een *ongerichte graaf* G bestaat uit een eindige verzameling V (de *knopen*) en een eindige verzameling E bestaande uit paren knopen (de *kanten*). Twee knopen kunnen door meerdere kanten verbonden zijn, en een kant kan twee dezelfde knopen verbinden.
Voor twee knopen $v, w \in V$ definiëren we een *pad van* v *naar* w als een rij verschillende kanten $\{e_1, e_2, \dots, e_\ell\}$ en een rij knopen $\{v_0, v_1, \dots, v_\ell\}$ waarbij geldt dat $v_0 = v$, $v_\ell = w$ en dat voor elke $i \leq \ell$ de kant e_i de knopen v_{i-1} en v_i verbindt. Twee paden zijn *kant-disjunct* als de verzameling kanten disjunct is.
Merk op dat het lege pad, bestaande uit een enkele knoop en een lege verzameling kanten, kant-disjunct met zichzelf is. Merk ook op dat de verzameling knopen niet per se verschillend hoeft te zijn.

Laat nu een ongerichte graaf $G = (V, E)$ en een natuurlijk getal k gegeven zijn. We definiëren op V een relatie R_k waarbij $vR_kw \in R_k$ als er minstens k paarsgewijs kant-disjuncte paden van v naar w bestaan. Laat zien dat R_k voor elke $k \in \mathbb{N}$ een equivalentierelatie is.

Een relatie R op een verzameling V heet een equivalentierelatie als aan de volgende drie eisen wordt voldaan:

(i) voor elke $v \in V$ geldt dat $vRv \in R$

(ii) voor elke $v, w \in V$ geldt dat $vRw \in R$ dan en slechts dan als $wRv \in R$

(iii) voor elke $v, w, x \in V$ geldt dat $vRw \in R$ en $wRx \in R$ impliceert dat $vRx \in R$

Uitwerking.
We laten zien dat R_k aan de drie eigenschappen voldoet.
(i) Aangezien het lege pad bestaande uit de knoop v kant-disjunct is met zichzelf geldt dat k kopieën van dit pad paarsgewijs kant-disjunct zijn. Hieruit volgt dat $vR_kv \in R_k$.
(ii) Stel dat $vR_kw \in R_k$. Dan bestaan er per definitie k paarsgewijs kant-disjuncte paden van v naar w. We kunnen elk pad omdraaien tot een pad van w naar v door de rij knopen en de rij kanten van het pad om te draaien. Omdat de verzameling kanten niet veranderd is, zijn de paden nog steeds kant-disjunct. Er bestaan dan dus minstens k kant-disjuncte paden van w naar v dus $wR_kv \in R_k$. De inverse implicatie volgt op analoge wijze dus $vR_kw \in R_k$ dan en slechts dan als $wR_kv \in R_k$.
(iii) Gegeven is dat $vR_kw \in R_k$ en $wR_kx \in R_k$. Hieruit volgt dat er minstens k paden van v naar w bestaan. Noem deze verzameling paden P. Er bestaan ook k paden van w naar x. Noem deze verzameling paden Q.

We bekijken nu de verzameling S van multisets knopen A die aan de volgende eisen voldoen:

1. Elke knoop $a \in A$ ligt op een pad in $p_a \in P$, en geen tweetal knopen ligt op hetzelfde pad. Het deelpad van v naar a (langs dit pad) noemen we p'_a.

2. Elke knoop $a \in A$ ligt op een pad in $q_a \in Q$, en geen tweetal knopen ligt op hetzelfde pad. Het deelpad van a naar x (langs dit pad) noemen we q'_a.

3. Voor elk paar $a, b \in A$ geldt dat p'_a en q'_b kant-disjunct zijn.

4. Elke $p \in P$ ongelijk aan p_a (voor elke $a \in A$) is kant-disjunct met elke q'_b.

Merk op dat elke A maximaal k elementen bevat omdat elke p_a een uniek element van P is en $|P| = k$.

Voor elke $A \in S$ definiëren we P_A als $P \setminus \{p_a \mid a \in A\}$ en Q_A als $Q \setminus \{q_a \mid a \in A\}$, de paden die *niet* gelijk zijn aan een p_a of q_a voor elke a. Ook definiëren we voor elke $A \in S$ als variant de geordende tuple $(|A|, -\Sigma(A))$ waarbij $\Sigma(A)$ de som is van de lengte van p'_a voor alle $a \in A$. Omdat S eindig (het is een deelverzameling van V^k) en niet leeg ($A = \emptyset$ voldoet aan de eisen) bestaat er een element $M \in S$ waarvoor deze variant maximaal is. We hebben al bewezen dat $|M| \leq k$. We gaan nu uit het ongerijmde bewijzen dat $|M| = k$.

Stel dat $|M| < k$. Omdat $|Q| = |P| = k > |M|$ zijn P_M en Q_M niet leeg. Er bestaan dus paden $p \in P_M$ en $q \in Q_M$. Als q kant-disjunct is met alle p'_a voor $a \in M$ en alle $p' \in P_M$, geldt dat de verzameling $M \cup \{w\}$ in S zit (waarbij $p_w = p$ en $q_w = q$) omdat aan alle eisen voldaan wordt. Dit is in tegenspraak met de maximaliteit van M, dus er bestaat een p'_a of een $p' \in P_M$ niet kant-disjunct is met q en dus ook een *laatste* kant in het pad q die ook op zo een p'_a of p' ligt. Noem deze kant e. We onderscheiden twee gevallen.

In het eerste geval bestaat er een $a \in M$ zodat e op p'_a ligt. Definieer b als het een eindpunt van de kant e ongelijk aan a en bekijk de verzameling $B := (M \setminus \{a\}) \cup \{b\}$, waarbij p'_b gelijk is aan het pad p'_a maar dan slechts tot aan knoop b en waarbij q'_b gelijk is aan het pad van b over q naar x. Omdat e de laatste kant op q is die op een p'_a of p' ligt, is q'_b kant-disjunct met elke p'_a en elke $p' \in P_B$. Het restant van de derde en vierde eis en de andere eisen zijn triviaal, dus er geldt dat $B \in S$. Omdat b op het pad p_a ligt en ongelijk is aan a, geldt dat de lengte van p_b kleiner is dan de lengte van p_a. De verzameling B heeft dus een grotere variant dan M. Dit is in tegenspraak met de maximaliteit van M.

In het tweede geval bestaat er een $p' \in P_M$ zodat e op p' ligt. Nu definiëren we b als een willekeurig eindpunt van e en bekijken we de verzameling $B := M \cup \{b\}$, waarbij p'_b gelijk is aan het pad p' tot aan het punt b en waarbij q'_b gelijk is aan het pad van b over q naar x. Omdat e de laatste kant op q is die op een p'_a of p' ligt, is q'_b kant-disjunct met elke p'_a en elke $p' \in P_B$. Ook hier geldt nu dat aan alle eisen voldaan wordt en dus dat $B \in S$, wat in tegenspraak is met de maximaliteit van M. We concluderen dat alle gevallen leiden tot tegenspraak en dus dat $|M| = k$.

We kunnen nu aan de hand van elke $a \in M$ een pad van v naar x construeren door de paden p'_a en q'_a te combineren. Omdat alle p'_a en q'_a kant-disjunct zijn, zijn al deze paden paarsgewijs kant-disjunct. We concluderen dat er k paarsgewijs kant-disjuncte paden van v naar x bestaan en dus dat $vR_kx \in R_k$.

4. Ongelijkheid met twee parameters

M. (Mike) Daas, BSc.
Universiteit van Amsterdam

Vind alle paren reële getallen (a, b) waarvoor de ongelijkheid

$$xy(x+y) + ab \geq bxy + a(x+y)$$

geldt voor alle reële $x, y \geq 1$.

Uitwerking.
Merk op dat we de uitdrukking kunnen ontbinden, zodat het altijd zou moeten gelden dat

$$(xy - a)(x + y - b) \geq 0.$$

Invullen $x = y = 1$ levert dat $(1 - a)(2 - b) \geq 0$. Als $a < 1$, dan volgt dat $b \leq 2$. Voor deze keuzes van a en b zijn beide factoren altijd niet-negatief, dus deze (a, b) werken zeker. Net zo, als $b < 2$ dan $a \leq 1$ en opnieuw zullen deze paren altijd werken. We nemen daarom vanaf nu aan dat $a \geq 1$ en dat $b \geq 2$.
Zij nu $\alpha > a$. Invullen $x = y = \sqrt{\alpha} > 1$ en opmerken dat de eerste factor positief is, geeft dan dat $2\sqrt{\alpha} > b$. Omdat dit moet gelden voor alle $\alpha > a$, vinden we dat $2\sqrt{a} \geq b$. Zij nu $\beta > b$. Dan levert invullen $x = 1$ en $y = \beta - 1 > 1$ na opmerken dat de tweede factor altijd positief is, dat $\beta - 1 > a$. Opnieuw, omdat dit geldt voor alle $\beta > b$, concluderen we dat $b - 1 \geq a$. Wanneer we deze twee resultaten combineren vinden we dat $2\sqrt{a} \geq b \geq a + 1$. Kwadrateren geeft $4a \geq (a+1)^2$ en dus $0 \geq (a-1)^2$. We zien dat $a = 1$ en omdat $2 \geq b \geq 2$ volgt direct dat $b = 2$. Inderdaad, als $(a, b) = (1, 2)$, dan wordt altijd aan de ongelijkheid voldaan.
Alles samennemend vinden we dat (a, b) voldoet precies als $a \leq 1$ en $b \leq 2$. $\square$

5. Recursieve priemgetallen

M. (Mieke) Wessel, BSc.
Universiteit Utrecht

Laat m, n en p_0 drie getallen in $\mathbb{N}$ en zij $(p_i)_{i\in\mathbb{N}}$ een rijtje dat wordt gedefinieerd door de recursieve formule $p_{i+1} = mp_i - n$.

a) **(2 punten)** Stel $m = 2$ en $n = 3$. Vind twee priemgetallen als waardes voor p_0, eentje zodat $(p_i)_{i\in\mathbb{N}}$ uit alleen maar priemgetallen bestaat en eentje zodat dit niet zo is.

b) **(8 punten)** Stel p_0 is bekend. Voor welke tweetallen (m, n) bevat het rijtje $(p_i)_{i\in\mathbb{N}}$ alleen maar priemgetallen? Bewijs ook dat het niet goed gaat voor andere tweetallen (m, n).

Hierbij is $\mathbb{N}$ gedefineerd als de positieve getallen *zonder* 0.

Uitwerking.

a) De waarde $p_0 = 3$ is de enige mogelijkheid zodat $(p_i)_{i\in\mathbb{N}}$ volledig uit priemgetallen bestaat. Dit geeft namelijk het rijtje $(3, 3, 3, \ldots)$.
De kleinste waarde voor p_0 zodat p_1 niet priem is, is $p_0 = 19$. Dan geldt $p_1 = 35$. Maar elk ander priemgetal ongelijk aan 3 leidt ook tot een niet volledig priem rijtje, alhoewel dit dan natuurlijk wel aangetoond moet worden.

b) Alleen de tweetallen van de vorm $(m, (m-1)p_0)$ voldoen mits p_0 priem is. Als p_0 niet priem is voldoet geen enkel tweetal.
Stel eerst dat p_0 wel priem is en $n = (m-1)p_0$. Dan geldt dat $p_{i+1} = mp_i - (m-1)p_0$. Uit inductie volgt dan dat $p_i = p_0$ voor alle $i \in \mathbb{N}$ en dus bestaat er een rijtje met alleen maar priemgetallen.
Stel nu dat $n \neq (m-1)p_0$. Ten eerste geldt dan dat het rijtje niet constant zal blijven en zelfs ofwel volledig stijgend ofwel volledig dalend is. Stijgend als $mp_0 > n + p_0$ en dalend als $mp_0 < n + p_0$. Dit is gemakkelijk aan te tonen met inductie. Nu bekijken we de recursieve formule modulo p_0 en zullen we aantonen dat er een $k \in \mathbb{N}$ bestaat met $p_k \equiv 0 \mod p_0$. Als $p_0 \not| m$ geldt dat voor elke $a \in \{0, \ldots, p_0 - 1\}$ er een unieke modulo klasse b bestaat zodat $mb - n \equiv a \mod p_0$, omdat $\text{ggd}(m, p_0) = 1$. Gezien er maar een eindig aantal mogelijkheden zijn voor $p_i \mod p_0$ zijn er $l, k \in \mathbb{N}$ zodat $p_{l+k} \equiv p_l \mod p_0$. Maar dan geldt dus ook dat $p_k \equiv p_0 \equiv 0 \mod p_0$. Omdat we al eerder hadden gezien dat het rijtje stijgend of dalend moet zijn geldt nu dat $p_k \neq p_0$ en dus kan p_k niet priem zijn.
Als wel geldt dat p_0 een deler is van m kunnen we hetzelfde argument gebruiken voor een p_j die geen deler is van m. Zo een j moet bestaan omdat m eindig is en het rijtje niet twee keer dezelfde waarde aanneemt. Verder kunnen we aannemen dat p_j dan ook priem is omdat er anders geen argument meer nodig is.
Als p_0 niet priem is moet p_1 nog steeds wel priem zijn. Uit de argumentatie hierboven volgt dan dat $n = (m-1)p_1$. Maar als we daaruit p_0 uitrekenen vinden we $p_0 = p_1$ wat in tegenspraak is met het feit dat p_1 priem moet zijn.

6. Correlatieconsternatie

H. J. (Harry) Smit, MSc. en M. (Merlijn) Staps, MSc.
Universiteit Utrecht & Princeton University

Bekijk de volgende bewering: “Voor iedere toevalsvariabele X met positieve variantie bestaan er toevalsvariabelen Y en Z, zodat Y en Z allebei dezelfde verdeling hebben als X, en zodat de correlatie tussen Y en Z gelijk is aan ρ.”

a) **(5 punten)** Is deze bewering waar voor $\rho = \frac{1}{2}$?

b) **(5 punten)** Is deze bewering waar voor $\rho = -\frac{1}{2}$?

Toelichting: De *correlatie* $\operatorname{cor}(A, B)$ tussen twee toevalsvariabelen A en B met $\operatorname{Var}(A) > 0$ en $\operatorname{Var}(B) > 0$ is gedefinieerd als

$$\operatorname{cor}(A, B) = \frac{\operatorname{cov}(A, B)}{\sqrt{\operatorname{Var}(A)\operatorname{Var}(B)}} = \frac{\mathbb{E}[AB] - \mathbb{E}[A]\mathbb{E}[B]}{\sqrt{\operatorname{Var}(A)\operatorname{Var}(B)}}.$$

Je mag bij deze opgave eventueel voor het gemak aannemen dat $\mathbb{E}[X] = 0$ en $\operatorname{Var}(X) = 1$, zodat $\operatorname{cor}(Y, Z) = \mathbb{E}[YZ]$.

Uitwerking.

a) Het antwoord is **ja**. Neem zonder beperking der algemeenheid aan dat $\mathbb{E}[X] = 0$ en $\operatorname{Var}(X) = 1$. Neem $Y = X$ en neem

$$Z = \begin{cases} X & \text{met kans } \frac{1}{2}; \\ X' & \text{met kans } \frac{1}{2}, \end{cases}$$

waarbij X' een onafhankelijke kopie van X is. Merk op dat Z dezelfde verdeling heeft als X. Aangezien X en X' onafhankelijk zijn, geldt er bovendien dat

$$\operatorname{cor}(Y, Z) = \mathbb{E}[YZ] = \tfrac{1}{2} \cdot \mathbb{E}[X^2] + \tfrac{1}{2} \cdot \mathbb{E}[XX'] = \tfrac{1}{2} \cdot 1 + \tfrac{1}{2} \cdot 0 = \tfrac{1}{2},$$

zoals gewenst.

b) Het antwoord is **nee**. Een tegenvoorbeeld wordt gegeven door de verdeling X met $\mathbb{P}(X = 1) = \frac{3}{4}$ en $\mathbb{P}(X = -3) = \frac{1}{4}$. Voor deze verdeling geldt $\mathbb{E}[X] = 0$ en dus $\operatorname{Var}(X) = \mathbb{E}(X^2) = \frac{3}{4} \cdot 1 + \frac{1}{4} \cdot 9 = 3$. Voor Y en Z geldt

$$\mathbb{P}(YZ = 1) = \mathbb{P}(Y = Z = 1) \geq 1 - \mathbb{P}(Y \neq 1) - \mathbb{P}(Z \neq 1) = 1 - \tfrac{1}{4} - \tfrac{1}{4} = \tfrac{1}{2}.$$

Aangezien er altijd geldt dat $YZ \geq -3$, geldt er dus dat

$$\mathbb{E}[YZ] \geq \tfrac{1}{2} \cdot 1 + \tfrac{1}{2} \cdot -3 \geq -1,$$

zodat $\operatorname{cor}(Y, Z) = \mathbb{E}[YZ]/\sqrt{\operatorname{Var}(Y)\operatorname{Var}(Z)} \geq -\frac{1}{3} > -\frac{1}{2}$. We zien dat voor deze keuze van X de correlatie tussen Y en Z altijd groter dan $-\frac{1}{2}$ is. Dus $\rho = -\frac{1}{2}$ voldoet niet.

7. Periodieke punten op een cirkel

dr. M. (Martijn) Caspers
Technische Universiteit Delft

Zij $f : X \to X$ een functie op een verzameling X. Een punt $x \in X$ heet periodiek als er een $n \in \mathbb{N}_{\geq 1}$ bestaat zodanig dat $f^n(x) = x$ waar, $f^n(x) = f(f(\ldots f(x)\ldots))$ (de n-voudige samenstelling van f met zichzelf). De kleinste n met deze eigenschap heet de orde van x.

Zij S^1 de eenheidscirkel in $\mathbb{R}^2$ en zij $f : S^1 \to S^1$ een continue functie. Veronderstel dat f een periodiek punt heeft van orde 3, maar geen periodiek punt heeft van orde 2. Laat zien dat f surjectief is.

Uitwerking.
Veronderstel dat f niet surjectief is. We zullen een tegenspraak afleiden. Zij $p \in S^1$ een punt dat nooit als waarde van f wordt aangenomen. $S^1 \backslash \{p\}$ is homeomorf met het open interval $(0,1)$ en we beschouwen de restrictie $f : S^1\backslash\{p\} \to S^1\backslash\{p\}$ als continue functie $f : (0,1) \to (0,1)$ met periodiek punt van orde 3, maar zonder periodiek punt van orde 2.

Zij $q_0 \in (0,1)$ het periodieke punt van orde 3 en beschouw de andere twee punten $q_1 = f(q_0)$ and $q_2 = f^2(q_0)$. Veronderstel dat $q_0 < q_1 < q_2$ (alle andere gevallen kunnen op dezelfde manier worden behandeld). We hebben $f([q_0, q_1]) \supseteq [q_1, q_2]$ (want f is continu). Verder $f([q_1, q_2]) \subseteq [q_0, q_2]$.

We claimen dat $[q_1, q_2]$ een periodiek punt van orde 2 bevat. Neem een gesloten deelinterval $I_1 \subseteq [q_0, q_1]$ zodanig dat $f(I_1) = [q_1, q_2]$ en een gesloten deelinterval $I_0 \subseteq [q_1, q_2]$ zodanig dat $f(I_0) = I_1$. Dan geldt $f^2(I_0) \supseteq I_0$ en dat impliceert dat I_0 een vast punt q voor f^2 bevat (vanwege de tussenwaardestelling). q is geen vast punt voor f (d.w.z. niet van orde 1) want $f(q) \in I_1 \subseteq [q_0, q_1]$ en $q \in [q_1, q_2]$ (en q_1 heeft periode 3). Dus q heeft periode 2 en dat is een tegenspraak.

8. Meer, meest, metro

drs. S. (Stijn) Cambie
Radboud Universiteit Nijmegen

In een stad hebben we 60 metrostations $1, 2, \ldots, 60$, waarbij er rechtstreekse verbindingen $C_{i,j}$ zijn tussen bepaalde stations $i < j$. Op zo'n verbinding, rijden de metro's in beide richtingen. Een traject (rit tussen twee metrostations) kost één euro. Zij a_i het aantal stations naar waar men kan reizen vanaf station i voor exact één euro (station i dus niet inbegrepen). Voor elke verbinding $C_{i,j}$, zij $L_{i,j}$ het aantal stations dat (strikt) goedkoper te bereiken is vanaf station i dan vanaf station j. Merk op dat station i zelf zo een station is. Analoog noemen we voor elke verbinding $C_{i,j}$, $H_{i,j}$ het aantal stations waarvoor het (strikt) duurder is om deze te bereiken vanaf station i dan vanaf station j. Hier is station j een voorbeeld van.

Wat is de maximale waarde van

$$\sum_{C_{i,j} \in E} (a_i + a_j) \cdot L_{i,j} \cdot H_{i,j}$$

waar E de verzameling is van alle metroverbindingen?

Uitwerking.
We starten met de volgende cruciale observatie.

Lemma 1. *Voor elke verbinding $C_{i,j} \in E$ geldt dat $L_{i,j} \leq 60 - a_j$ en $H_{i,j} \leq 60 - a_i$.*

Bewijs. Merk op dat voor elk station k verschillend van j die rechtstreeks te bereiken is vanaf i, het niet strikt duurder kan zijn om k te bereiken vanaf i (exact 1 euro) dan vanaf j (minstens 1 euro). Er zijn $a_i - 1$ zo'n stations. Ook station i is niet meegeteld in $H_{i,j}$ en dus $H_{i,j} \leq 60 - a_i$. Analoog geldt $L_{i,j} \leq 60 - a_j$. $\square$

Via het principe van dubbeltellen, vinden we de volgende twee gelijkheden (de eerste is het zogenaamde hand shaking lemma).

Lemma 2. *We hebben dat*

$$\sum_i a_i = 2|E| \text{ en } \sum_i a_i^2 = \sum_{C_{i,j} \in E} a_i + a_j.$$

Als derde en laatste observatie, merken we op dat AM-GM zegt dat $x(60 - x) \leq 30^2$ voor elke x met gelijkheid dan en slecht dan $x = 30$. Bijgevolg geldt voor elke $0 \leq a_i, a_j \leq 60$ dat

$$(a_i + a_j)(60 - a_j)(60 - a_i) = a_i(60 - a_i) \cdot (60 - a_j) + a_j(60 - a_j) \cdot (60 - a_i) \leq 30^2(120 - a_i - a_j).$$

We combineren nu de 3 observaties, waardoor we concluderen dat

$$\begin{aligned}
\sum_{C_{i,j} \in E} (a_i + a_j) \cdot L_{i,j} \cdot H_{i,j} &\leq \sum_{C_{i,j} \in E} (a_i + a_j)(60 - a_j)(60 - a_i) \text{ (via lemma 1)} \\
&\leq 30^2 \sum_{C_{i,j} \in E} (120 - a_i - a_j) \text{ (derde observatie)} \\
&\leq 30^2 \sum_{i=1}^{60} (60 - a_i)a_i \text{ (via lemma 2)} \\
&\leq 2 \cdot 30^5.
\end{aligned}$$

Gelijkheid is slecht mogelijk indien voor elke verbinding $e = C_{i,j}$ geldt dat $L_{i,j} = H_{i,j} = a_i = a_j = 30$.
Dit is bijvoorbeeld mogelijk indien de verbindingen $C_{i,j}$ exact degene zijn waarbij $1 \leq i \leq 30$ en $31 \leq j \leq 60$.