IMO-selectietoets III

vrijdag 4 juni 2021

Uitwerkingen

Opgave 1. Laat m en n natuurlijke getallen zijn met mn even. Jetze gaat een $m \times n$-bord (dus bestaande uit m rijen en n kolommen) bedekken met dominostenen, zodat elke dominosteen precies twee vakjes bedekt, dominostenen niet uitsteken of overlappen, en alle vakjes bedekt worden door een dominosteen. Merlijn gaat vervolgens alle dominostenen op het bord rood of blauw kleuren. Bepaal het kleinste niet-negatieve gehele getal V (afhankelijk van m en n) zodat Merlijn er altijd voor kan zorgen dat in elke rij het aantal vakjes bedekt door een rode dominosteen en het aantal vakjes bedekt door een blauwe dominosteen ten hoogste V van elkaar verschillen, hoe Jetze het bord ook bedekt.

Oplossing I. Stel eerst dat n oneven is. Dan is het duidelijk dat $V \geq 1$; het verschil is immers altijd oneven. We laten zien dat $V = 1$ altijd mogelijk is. Kleur hiertoe de verticale dominostenen in oneven kolommen rood en de verticale dominostenen in even kolommen blauw. Omdat in elke rij elke horizontale dominosteen een vakje in een even en een vakje in een oneven kolom bedekt, is er nu in elke rij één vakje meer door een rode dominosteen dan door een blauwe dominosteen bedekt. Kleur de horizontale dominostenen in elke rij nu afwisselend blauw, rood, blauw, rood, ... Als het aantal horizontale domino's even is, is er uiteindelijk één rood vakje meer; is het aantal horizontale domino's oneven, dan is er uiteindelijk één blauw vakje meer. Het verschil is dus altijd 1.

Als $n \equiv 2 \mod 4$ geldt er dat $V \geq 2$ als Jetze elke dominosteen horizontaal legt; dan liggen er in elke rij immers een oneven aantal dominostenen. We laten nu zien dat $V = 2$ altijd mogelijk is. Gebruik daartoe dezelfde strategie als in het oneven geval. Na het kleuren van de verticale dominostenen zijn er in elke rij evenveel vakjes rood als blauw. Als we daarna weer de horizontale dominostenen per rij afwisselend rood en blauw kleuren, is in elke rij het verschil tussen het aantal rode en blauwe vakjes gelijk aan 0 of 2.

We bekijken ten slotte het geval waarin $n \equiv 0 \mod 4$. We laten daarin zien dat $V = 0$ altijd mogelijk is. Nummer de rijen van boven naar beneden van 1 tot en met m en zij b_i het aantal verticale dominostenen waarvan het bovenste vakje in rij i ligt. Met inductie naar i laten we eenvoudig zien dat b_i even is, waarbij we gebruiken dat een horizontale dominosteen altijd een even aantal vakjes in een rij bedekt. We kleuren de verticale dominostenen in rij i en rij $i + 1$ nu als volgt: als $b_i \equiv 0 \mod 4$ kleuren we de helft rood en

de helft blauw, en als $b_i \equiv 2 \mod 4$ kleuren we er twee meer rood dan blauw als i even is, en twee meer blauw dan rood als i oneven is. We laten nu zien dat we in elke rij k de horizontale dominostenen zo kunnen kleuren dat deze rij evenveel rode als blauwe vakjes heeft. Als $b_{k-1} \equiv b_k \equiv 0 \mod 4$ dan bedekken verticale dominostenen in rij k evenveel rode als blauwe vakjes. Bovendien is het aantal horizontale dominostenen in rij k nu even, dus we kleuren simpelweg de helft rood en de helft blauw. Als $b_{k-1} \equiv b_k \equiv 2 \mod 4$ geldt wederom dat de verticale dominostenen in rij k evenveel rode als blauwe vakjes bedekken, omdat er van $k-1$ en k één even en één oneven is. Verder is het aantal horizontale dominostenen in rij k weer even, dus kunnen we weer de helft rood en de helft blauw kleuren. Als $b_{k-1} \not\equiv b_k \mod 4$ is het verschil tussen rode en blauwe vakjes bedekt door verticale dominostenen gelijk aan 2. Het aantal horizontale dominostenen in rij k is nu oneven. We kunnen dus de horizontale dominostenen zo kleuren dat uiteindelijk evenveel vakjes rood als blauw zijn.

We concluderen dat de minimale waarden zijn: $V = 1$ als n oneven is, $V = 2$ als $n \equiv 2 \mod 4$ en $V = 0$ als $n \equiv 0 \mod 4$. □

Oplossing II. Nummer de rijen van boven naar beneden van 1 tot en met m en zij b_i $(1 \leq i \leq m-1)$ het aantal verticale dominostenen waarvan het bovenste vakje in rij i ligt en het onderste vakje in rij $i+1$. Definieer $b_0 = 0$ en $b_m = 0$.

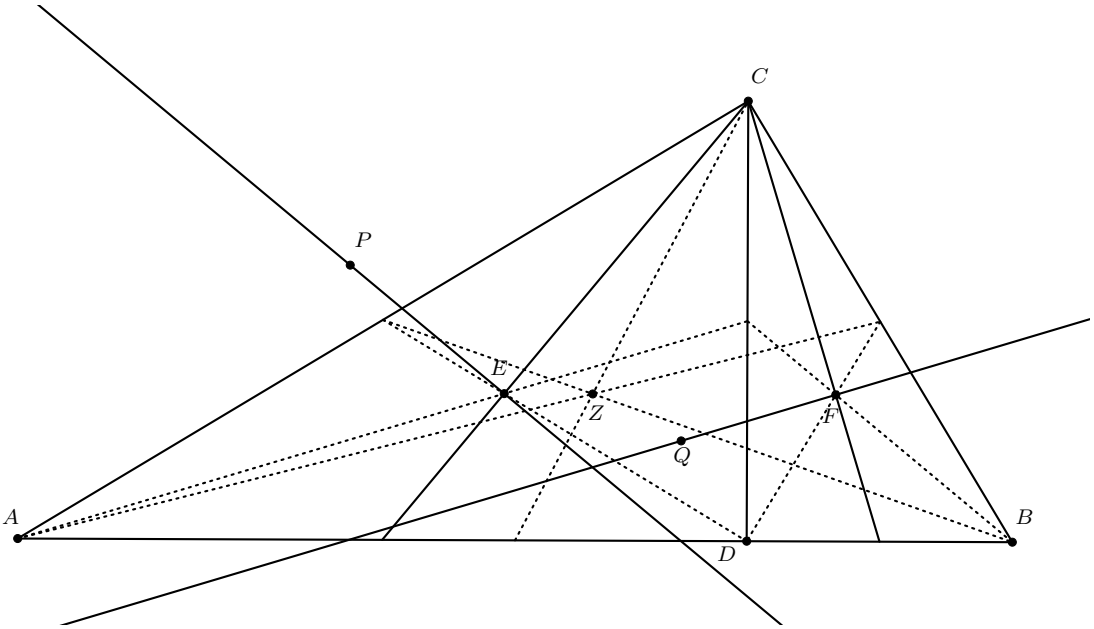
Stel eerst dat n oneven is. Schrijf $n = \frac{1}{2}(n-1) + \frac{1}{2}(n+1)$; precies een van deze twee termen is even en de ander is oneven; schrijf n_e voor de even term en n_o voor de oneven term. We hebben nu dus $n = n_\mathrm{e} + n_\mathrm{o}$ terwijl n_e en n_o precies 1 verschillen. Het is allereerst duidelijk dat $V \geq 1$; het verschil is immers altijd oneven. We laten zien dat $V = 1$ altijd mogelijk is. Met inductie naar i laten we eenvoudig zien dat b_i oneven is voor oneven i en even voor even i, waarbij we gebruiken dat een horizontale dominosteen altijd een even aantal vakjes in een rij bedekt. Voor oneven i hebben we in rij i te maken met een oneven aantal b_i verticale stenen die naar beneden uitsteken, een aantal horizontale dominostenen die een even aantal vakjes bedekken, en een even aantal b_{i-1} die naar boven uitsteken. Kleur nu de vakjes in rij i als volgt: van deze dominostenen, in de volgorde zoals zojuist opgesomd, kleur je de eerste n_o vakjes rood en juist de laatste n_e vakjes blauw. Voor even i hebben we in rij i te maken met een oneven aantal b_{i-1} verticale stenen die naar boven uitsteken, een aantal horizontale dominostenen die een even aantal vakjes bedekken, en een even aantal b_i die naar beneden uitsteken. Kleur nu de vakjes in rij i als volgt: van deze dominostenen, in de volgorde zoals zojuist opgesomd, kleur je de eerste n_o vakjes rood en juist de laatste n_e vakjes blauw. Op deze manier is in elke rij in ieder geval elke horizontale dobbelsteen monochroom (de twee vakjes hebben dezelfde kleur), terwijl we voor twee opeenvolgende rijen de vakjes op de verticale dominostenen in beide rijen ook dezelfde kleur hebben gegeven. De kleuring is dus correct en voldoet aan $V = 1$.

Als $n \equiv 2 \mod 4$ is $\frac{1}{2}n$ oneven en schrijven we $\frac{1}{2}n = n_\mathrm{e} + n_\mathrm{o}$ met n_e en n_o even en oneven

getallen die precies 1 verschillen. Er geldt dat $V \geq 2$ als Jetze elke dominosteen horizontaal legt; dan liggen er in elke rij immers een oneven aantal dominostenen. We laten nu zien dat $V = 2$ altijd mogelijk is. Gebruik daartoe dezelfde strategie als in het oneven geval. Met inductie naar i laten we eenvoudig zien dat b_i even is voor alle i. Voor oneven i hebben we in rij i te maken met een even aantal b_i verticale stenen die naar beneden uitsteken, een aantal horizontale dominostenen die een even aantal vakjes bedekken, en een even aantal b_{i-1} die naar boven uitsteken. Kleur nu de vakjes in rij i als volgt: van deze dominostenen, in de volgorde zoals zojuist opgesomd, kleur je de eerste $2n_{\mathrm{o}}$ vakjes rood en juist de laatste $2n_{\mathrm{e}}$ vakjes blauw. Voor even i hebben we in rij i te maken met een even aantal b_{i-1} verticale stenen die naar boven uitsteken, een aantal horizontale dominostenen die een even aantal vakjes bedekken, en een even aantal b_i die naar beneden uitsteken. Kleur nu de vakjes in rij i als volgt: van deze dominostenen, in de volgorde zoals zojuist opgesomd, kleur je de eerste $2n_{\mathrm{o}}$ vakjes rood en juist de laatste $2n_{\mathrm{e}}$ vakjes blauw. Op deze manier is in elke rij in ieder geval elke horizontale dobbelsteen monochroom (de twee vakjes hebben dezelfde kleur), terwijl we voor twee opeenvolgende rijen de vakjes op de verticale dominostenen in beide rijen ook dezelfde kleur hebben gegeven. De kleuring is dus correct en voldoet aan $V = 2$.

Als $n \equiv 0 \mod 4$ is $\frac{1}{2}n$ even en schrijven we $\frac{1}{2}n = 2n_0$. We laten nu zien dat $V = 0$ altijd mogelijk is. Gebruik daartoe dezelfde strategie als in het vorige geval. Met inductie naar i laten we eenvoudig zien dat b_i even is voor alle i. Voor oneven i hebben we in rij i te maken met een even aantal b_i verticale stenen die naar beneden uitsteken, een aantal horizontale dominostenen die een even aantal vakjes bedekken, en een even aantal b_{i-1} die naar boven uitsteken. Kleur nu de vakjes in rij i als volgt: van deze dominostenen, in de volgorde zoals zojuist opgesomd, kleur je de eerste $2n_0$ vakjes rood en juist de laatste $2n_0$ vakjes blauw. Voor even i hebben we in rij i te maken met een even aantal b_{i-1} verticale stenen die naar boven uitsteken, een aantal horizontale dominostenen die een even aantal vakjes bedekken, en een even aantal b_i die naar beneden uitsteken. Kleur nu de vakjes in rij i als volgt: van deze dominostenen, in de volgorde zoals zojuist opgesomd, kleur je de eerste $2n_0$ vakjes rood en juist de laatste $2n_0$ vakjes blauw. Op deze manier is in elke rij in ieder geval elke horizontale dobbelsteen monochroom (de twee vakjes hebben dezelfde kleur), terwijl we voor twee opeenvolgende rijen de vakjes op de verticale dominostenen in beide rijen ook dezelfde kleur hebben gegeven. De kleuring is dus correct en voldoet aan $V = 0$. $\square$

Opgave 2. Zij ABC een rechthoekige driehoek met $\angle C = 90^\circ$ en zij D het voetpunt van de hoogtelijn uit C. Zij E het zwaartepunt van driehoek ACD en zij F het zwaartepunt van driehoek BCD. Het punt P voldoet aan $\angle CEP = 90^\circ$ en $|CP| = |AP|$, terwijl het punt Q voldoet aan $\angle CFQ = 90^\circ$ en $|CQ| = |BQ|$.
Toon aan dat PQ door het zwaartepunt van driehoek ABC gaat.



Oplossing I. Noem M, N, R en S de middens van respectievelijk zijden BC, CA, BD en AD. Zij Z het zwaartepunt van $\triangle ABC$. Vierhoek $QFMC$ is een koordenveriehoek wegens rechte hoeken $\angle QFC = 90^\circ = \angle QMC$. Merk op dat CQ dus de middellijn van de omgeschreven cirkel is. Analoog zien we dat $PNEC$ een koordenvierhoek is, met CP de middellijn van de omgeschreven cirkel.

We bewijzen nu dat Z ook op deze koordenvierhoeken ligt. Driehoek CZM gaat onder de gelijkvormigheid $\triangle BCA \sim \triangle BDC$ over in driehoek DFR, want C gaat naar D, het zwaartepunt Z gaat naar het zwaartepunt F, en het midden M van BC gaat naar het midden van BD en dat is R. Dus $\triangle CZM \sim \triangle DFR$, waaruit in het bijzonder volgt dat $\angle CZM = \angle DFR = \angle CFM$ wegens overstaande hoeken. Dus Z ligt op koordenvierhoek $QFMC$. Analoog volgt dat $\angle CZN = \angle DES = \angle CEN$, waaruit volgt dat Z op koordenvierhoek $PNEC$ ligt.

We kunnen nu bewijzen dat Z op PQ ligt. Omdat CQ de middellijn is van de cirkel door Q, F, M, C, Z, geldt $\angle QZC = 90^\circ$. Omdat CP de middellijn is van de cirkel door P, N, E, Z, C, geldt ook $\angle CZP = 90^\circ$. Samen kunnen we hieruit concluderen dat P, Z en Q op een lijn liggen. $\square$

Oplossing II. Noem M, N, K en L de middens van respectievelijk zijden BC, CA, AB en CD. Zij Z het zwaartepunt van $\triangle ABC$. Omdat ML een middenparallel in driehoek BCD is, geldt $ML \parallel BD$ en dus $ML \parallel AB$. Zo is ook $NL \parallel AB$, dus M, N en L liggen op een lijn ℓ evenwijdig aan AB. Verder geldt vanwege $ML \parallel BD$ dat $\triangle BDF \sim \triangle LMF$, waarbij de vermenigvuldigingsfactor tussen deze twee driehoeken gelijk aan 2 is. Dus de afstand van F tot ℓ (wat de lijn ML is) is twee keer zo klein als de afstand van F tot AB (wat de lijn BD is). Net zo is de afstand van E tot ℓ twee keer zo klein als de afstand van E tot AB, en hetzelfde geldt voor Z. Dus E, F en Z liggen allemaal op een lijn evenwijdig aan AB die twee keer zo ver van AB af ligt als van ℓ.

(Een andere manier om dit in te zien, is door gebruik te maken van het feit dat zwaartepunten altijd op $\frac{1}{3}$ hoogte van een zwaartelijn liggen. De punten E, F en Z liggen allemaal op $\frac{1}{3}$ hoogte van de corresponderende zwaartelijnen uit C, waaruit het gestelde volgt.)

Hieruit volgt in het bijzonder dat $\angle CZE = \angle CKA$ (F-hoeken). We gaan dit gebruiken om aan te tonen dat de punten Z, E, N en C samen op een cirkel liggen. Bekijk hiervoor eerst de gelijkvormige driehoeken $\triangle ABC$ en $\triangle ACD$. Er geldt nu $\frac{|AK|}{|AN|} = \frac{|AB|}{|AC|} = \frac{|AC|}{|AD|}$, dus $\triangle AKC \sim \triangle AND$ (zhz). Hieruit volgt $\angle CKA = \angle DNA$. Al met al vinden we nu

$$\angle CZE = \angle CKA = \angle DNA = 180^\circ - \angle DNC = 180^\circ - \angle ENC,$$

dus $CZEN$ is een koordenvierhoek.

Omdat $|CP| = |AP|$ ligt P op de middelloodlijn van AC. Er geldt dus $\angle CNP = 90^\circ = \angle CEP$, wat betekent dat C, E, N en P op een cirkel liggen. We hebben zojuist gezien dat Z ook op deze cirkel ligt. Dus geldt $\angle CZP = \angle CEP = 90^\circ$. Analoog volgt $\angle CZQ = 90^\circ$. Samen kunnen we hieruit concluderen dat P, Z en Q op een lijn liggen. $\square$

Opgave 3. Vind alle functies $f\colon \mathbb{R} \to \mathbb{R}$ met

$$f\big(x + yf(x+y)\big) = y^2 + f(x)f(y)$$

voor alle $x, y \in \mathbb{R}$.

Oplossing I. Merk op dat de functie $f(x) = 0$ voor alle x niet voldoet. Er is dus een a met $f(a) \neq 0$. Vul $x = a$ en $y = 0$ in, dat geeft $f(a) = f(a)f(0)$, dus $f(0) = 1$. Vul nu $x = 1$ en $y = -1$ in, dat geeft $f(1 - f(0)) = 1 + f(1)f(-1)$. Omdat $f(0) = 1$, staat hier $1 = 1 + f(1)f(-1)$, dus $f(1) = 0$ of $f(-1) = 0$. We onderscheiden deze twee gevallen.

Stel eerst dat $f(1) = 0$. Vul $x = t$ en $y = 1 - t$ in, en vervolgens $x = 1 - t$ en $y = t$, dan krijgen we de twee vergelijkingen

$$\begin{aligned} f(t) &= (1-t)^2 + f(t)f(1-t), \\ f(1-t) &= t^2 + f(t)f(1-t). \end{aligned}$$

Deze van elkaar afhalen geeft $f(t) - f(1-t) = (1-t)^2 - t^2 = 1 - 2t$, dus $f(1-t) = f(t) + 2t - 1$. Dit invullen in de eerste van bovenstaande twee vergelijkingen geeft

$$f(t) = (1-t)^2 + f(t)^2 + (2t-1)f(t),$$

wat we kunnen herschrijven tot

$$f(t)^2 + (2t-2)f(t) + (1-t)^2 = 0,$$

oftewel $\big(f(t) - (1-t)\big)^2 = 0$. We concluderen dat $f(t) = 1 - t$. Controleren van deze functie in de oorspronkelijke functievergelijking geeft links $1 - (x + y(1-x-y)) = 1 - (x + y - xy - y^2) = 1 - x - y + xy + y^2$ en rechts $y^2 + (1-x)(1-y) = y^2 + 1 - x - y + xy$ en dat is hetzelfde, dus de functie voldoet.

Stel nu $f(-1) = 0$. Vul $x = t$ en $y = -1 - t$ in, en vervolgens $x = -1 - t$ en $y = t$, dan krijgen we de twee vergelijkingen

$$\begin{aligned} f(t) &= (-1-t)^2 + f(t)f(-1-t), \\ f(-1-t) &= t^2 + f(t)f(-1-t). \end{aligned}$$

Deze van elkaar afhalen geeft $f(t) - f(-1-t) = (-1-t)^2 - t^2 = 1 + 2t$, dus $f(-1-t) = f(t) - 2t - 1$. Dit invullen in de eerste van bovenstaande twee vergelijkingen geeft

$$f(t) = (-1-t)^2 + f(t)^2 + (-2t-1)f(t),$$

wat we kunnen herschrijven tot

$$f(t)^2 - (2t+2)f(t) + (t+1)^2 = 0,$$

oftewel $\big(f(t)-(t+1)\big)^2 = 0$. We concluderen dat $f(t) = t+1$. Controleren van deze functie in de oorspronkelijke functievergelijking geeft links $x+y(x+y+1)+1 = x+xy+y^2+y+1$ en rechts $y^2+(x+1)(y+1) = y^2+xy+x+y+1$ en dat is hetzelfde, dus de functie voldoet.

We concluderen dat er precies twee oplossingen zijn: $f(x) = 1-x$ voor alle x en $f(x) = x+1$ voor alle x. □

Oplossing II. Net als in de eerste oplossing leiden we af dat $f(0) = 1$ en dat $f(1) = 0$ of $f(-1) = 0$.

Stel eerst dat $f(1) = 0$. Invullen van $x = t-1$ en $y = 1$ geeft $f(t-1+f(t)) = 1$. Anderzijds geldt ook $f(0) = 1$. We laten nu zien dat $f(z) = 1$ impliceert dat $z = 0$. Stel $f(z) = 1$. Invullen van $x = 1$ en $y = z-1$ geeft $f(1+(z-1)f(z)) = (z-1)^2$, dus $f(z) = (z-1)^2$, oftewel $1 = (z-1)^2$. Dus $z = 0$ of $z = 2$. Stel $z = 2$, dan geeft invullen van $x = 0$ en $y = 2$ dat $f(2f(2)) = 4+f(0)f(2)$, wat met $f(2) = f(z) = 1$ leidt tot $f(2) = 5$, in tegenspraak met $f(2) = 1$. Dus $z = 0$. In het bijzonder volgt uit $f(t-1+f(t)) = 1$ dus dat $t-1+f(t) = 0$, dus $f(t) = 1-t$. Deze functie voldoet (zie eerste oplossing).

Stel nu dat $f(-1) = 0$. Invullen van $x = t+1$ en $y = -1$ geeft $f(t+1-f(t)) = 1$. Anderzijds geldt ook $f(0) = 1$. We laten nu wederom zien dat $f(z) = 1$ impliceert dat $z = 0$. Stel $f(z) = 1$. Invullen van $x = -1$ en $y = z+1$ geeft $f(-1+(z+1)f(z)) = (z+1)^2$, dus $f(z) = (z+1)^2$, oftewel $1 = (z+1)^2$. Dus $z = 0$ of $z = -2$. Stel $z = -2$, dan geeft invullen van $x = 0$ en $y = -2$ dat $f(-2f(-2)) = 4+f(0)f(-2)$, wat met $f(-2) = f(z) = 1$ leidt tot $f(-2) = 5$, in tegenspraak met $f(-2) = 1$. Dus $z = 0$. In het bijzonder volgt uit $f(t+1-f(t)) = 1$ dus dat $t+1-f(t) = 0$, dus $f(t) = t+1$. Deze functie voldoet ook (zie eerste oplossing). □

Opgave 4. Zij $p > 10$ een priemgetal. Bewijs dat er positieve gehele getallen m en n met $m + n < p$ bestaan waarvoor p een deler is van $5^m 7^n - 1$.

Oplossing I. Wegens de kleine stelling van Fermat geldt $a^{p-1} \equiv 1 \mod p$ voor alle a met $p \nmid a$. Omdat $p > 10$ is p oneven, dus $p - 1$ is even. Er geldt

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) = a^{p-1} - 1 \equiv 0 \mod p.$$

Dus $p \mid (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, dus p is een deler van minstens één van beide factoren. Dus $a^{\frac{p-1}{2}}$ is modulo p congruent aan 1 of -1.

We passen dit toe op $a = 5$ en $a = 7$. Merk op dat $p > 10$ dus $p \neq 5, 7$. Als $5^{\frac{p-1}{2}} \equiv 1 \mod p$ en $7^{\frac{p-1}{2}} \equiv 1 \mod p$, dan nemen we $m = n = \frac{p-1}{2}$ en dat voldoet. Hetzelfde geldt als ze beide $-1 \mod p$ zijn. Blijft over het geval dat één van beide 1 en de ander -1 is. Neem aan dat $5^{\frac{p-1}{2}} \equiv 1 \mod p$ en $7^{\frac{p-1}{2}} \equiv -1 \mod p$. Het geval waarin het andersom is, gaat precies analoog.

Als er een n is met $0 < n < \frac{p-1}{2}$ en $7^n \equiv 1 \mod p$, dan kiezen we deze n en verder $m = \frac{p-1}{2}$. Dat voldoet. Zo niet, dan kan er ook geen n zijn met $\frac{p-1}{2} < n < p - 1$ en $7^n \equiv 1 \mod p$, want dan zou $7^{p-1-n} \equiv 7^{p-1} \cdot (7^n)^{-1} \equiv 1 \mod p$, terwijl $0 < p - 1 - n < \frac{p-1}{2}$, tegenspraak. Verder kunnen er nu geen i en j zijn met $1 \leq i < j \leq p - 1$ zodat $7^i \equiv 7^j \mod p$, want als die wel zouden bestaan, dan is $7^{j-i} \equiv 1 \mod p$ met $1 \leq j - i < p - 1$. We concluderen dat 7^i met $1 \leq i \leq p - 1$ allemaal verschillende waarden aanneemt modulo p, en daar zit waarde 0 niet bij, dus het zijn precies alle waarden van 1 tot en met $p - 1$.

In het bijzonder is er een n zodat $7^n \equiv 5^{-1} \mod p$. Er geldt $n \leq p-2$, want $7^{p-1} \equiv 1 \not\equiv 5^{-1} \mod p$. We kiezen nu deze n en verder $m = 1$ en dan geldt $7^n \cdot 5^m \equiv 5^{-1} \cdot 5 \equiv 1 \mod p$.

We zien dat het in alle gevallen mogelijk is om m en n te vinden die aan de voorwaarden voldoen. □

Oplossing II. We bekijken alle getallen van de vorm $5^i 7^j$ voor $1 \leq i, j \leq p - 1$. Dit zijn $(p-1)^2$ getallen. Modulo p nemen deze getallen nooit de waarde 0 aan, want vanwege $p > 10$ geldt $p \neq 5, 7$. Dus modulo p worden er hooguit $p - 1$ verschillende waarden aangenomen. Vanwege het ladenprincipe is er nu een waarde k zodat minstens $\frac{(p-1)^2}{p-1} = p - 1$ van deze paren (i, j) voldoen aan $5^i 7^j \equiv k \mod p$. Noem deze paren *k-waardig*.

Neem zo'n k-waardig paar $(i, j) = (a, b)$. We gaan eerst laten zien dat niet alle k-waardige paren van de vorm (x, b) zijn. Bijvoorbeeld $(a + 1, b)$ (en net zo goed $(a - 1, b)$ als net toevallig $a = p - 1$) is niet k-waardig, want uit $5^{a+1} 7^b \equiv 5^a 7^b \mod p$ zou volgen dat $5 \equiv 1$

mod p, dus $p \mid 4$, tegenspraak. Omdat er minstens $p-1$ paren k-waardig zijn, volgt nu dat niet alle k-waardige paren van de vorm (x, b) kunnen zijn. Dus er is een k-waardig paar (c, d) met $d \neq b$. Net zo bestaat er een k-waardig paar (e, f) met $e \neq a$. Als nu $a \neq c$, dan zijn (a, b) en (c, d) twee paren met twee verschillende getallen in de eerste component en twee verschillende getallen in de tweede component. Als $b \neq f$, zijn (a, b) en (e, f) zulke paren. Als $a = c$ en $b = f$, dan zijn juist $(c, d) = (a, d)$ en $(e, f) = (e, b)$ zulke paren.

We kunnen dus altijd twee k-waardige paren (i_1, j_1) en (i_2, j_2) vinden met $i_1 \neq i_2$ en $j_1 \neq j_2$. Er geldt nu

$$5^{i_1-i_2}7^{j_1-j_2} \equiv 5^{i_1}(5^{i_2})^{-1} \cdot 7^{j_1}(7^{j_2})^{-1} \equiv k \cdot k^{-1} \equiv 1 \mod p.$$

Uit de kleine stelling van Fermat volgt $u^{p-1} \equiv 1 \mod p$ als $u \in \{5, 7\}$. Voor $t \in \mathbb{Z}$ geldt nu $u^{p-1+t} \equiv u^{p-1}u^t \equiv u^t \mod p$. Schrijf $m' = i_1 - i_2$ als $i_1 > i_2$ en $m' = p - 1 + i_1 - i_2$ als $i_1 < i_2$, dan geldt dus $5^{m'} \equiv 5^{i_1-i_2} \mod p$. Verder is $1 \leq m' \leq p-2$. Analoog definiëren we n' zodat $7^{n'} \equiv 7^{j_1-j_2} \mod p$ en $1 \leq n' \leq p-2$. We hebben nu $5^{m'}7^{n'} \equiv 1 \mod p$.

Als $n' + m' < p$, dan kiezen we $m = m'$ en $n = n'$ en zijn we klaar. Zo niet, dan kiezen we $m = p - 1 - m'$ en $n = p - 1 - n'$ en geldt $5^m 7^n \equiv 5^{p-1}(5^{m'})^{-1} \cdot 7^{p-1}(7^{n'})^{-1} \equiv 1 \cdot 1^{-1} \equiv 1$ mod p. Nu geldt $n+m = 2(p-2)-(n'+m') \leq 2p-4-p = p-4$, dus zijn we ook klaar. $\square$