Uitwerking puzzel 92-1

Wanneer zijn veelvouden van proniks proniks?

Harm Bakker noemde het: **pro-niks ≠ voor-niks**

De puzzel was voor een groot deel afkomstig van Frits Göbel.

Een pronik is een getal dat we kunnen schrijven als p ($p + 1$), *met p een geheel positief getal.*

Alle gebruikte variabelen zijn gehele getallen en hoofdletters P, Q en R stellen steeds proniks voor, met $P = p$ $(p + 1)$, $Q = q\ (q + 1)$ en $R = r\ (r + 1)$. Natuurlijk is dan $q\ (q - 1)$ ook een pronik.
We onderzoeken voor welke factoren f, P en Q geldt: $f \cdot P = Q$ en dan blijkt al snel dat bij elke P wel een f is te vinden, maar niet bij elke f een P.
De eerste twee opgaven waren er om het een en ander te verkennen.
Opgave 1. Toon aan dat er een P en Q bestaan waarvoor geldt: $f \cdot P = Q$ als:

a) f is een driehoeksgetal = $d\ (d + 1) / 2$. Kies dan $P = 1 \cdot 2 = 2$, dus $Q = d\ (d + 1)$

b) $f = R \pm 1$: Kies $P = R$, dus $Q = R\ (R \pm 1)$

c) $f = R = r\ (r \pm 1)$. Kies dan $P = r(\mathrm{r} \mp 1)$ zodat $R = r\ (r \pm 1)\ r(r \mp 1) = r^{2}(r^2 - 1)$.

Opgave 2: Aan welke formule(s) moet f voldoen als $P = 2 \cdot 3 = 6$?
We zoeken dan $f \cdot P = q\ (q \pm 1)$ is een 6-voud. Merk op dat een pronik altijd even is, dus voldoende is als q deelbaar is door 3. Dus $f \cdot P = 3k\ (3k \pm 1)$ en $f = k\ (3k \pm 1) / 2$.
Leuker was de vraag die Frans van Hoeve stelde: $p = 6$, dus $P = 42$.
Dan zijn er 3 series oplossingen te bedenken:

$f = (3k + 1)(7k + 2) / 2$ met $Q = (21k + 7)(21k + 6)$

$f = (3k + 2)(7k + 5)/ 2$ met $Q = (21k + 14)(21k + 15)$

$f = k\ (21k \pm 1) / 2$ met $Q = 21k\ (21k \pm 1)$.

Opgave 3a : Bepaal de afstanden op de getallenlijn van een pronik $P = p\ (p + 1)$ tot de twee dichtstbijzijnde kwadraten en ook tot de twee dichtstbijzijnde proniks Q, uitgedrukt in p.
Als $P = p\ (p + 1) = p^2 + p$ dan zijn de dichtstbijzijnde proniks $(p - 1) \cdot p = p^2 - p$ en $(p + 1)(p + 2) = p^2 + 3\mathrm{p} + 2$.
De verschillen zijn respectievelijk $2p$ en $2p + 2$.

De dichtstbijzijnde kwadraten zijn p^2 en $(p + 1)^2 = p^2 + 2p + 1$.
Dan zijn de verschillen respectievelijk p en $p + 1$.

Opgave 3b : Bepaal de afstanden op de getallenlijn van een kwadraat k^2 tot de twee dichtstbijzijnde proniks , uitgedrukt in k.
De dichtstbijzijnde proniks zijn $(k - 1) \cdot k = k^2 - k$ en $k \cdot (k + 1) = k^2 + k$.
De verschillen met k^2 zijn aan weerszijde gelijk aan k.
Kwadraten liggen dus precies in het midden tussen 2 proniks.

Opgave 4a: Bewijs dat als $f = 9$ of $f = 25$, dan zijn er geen proniks P en Q zdd. $f \cdot P = Q$. Het zijn kwadraten van priemgetallen 3 en 5. We gaven de tip dat de resultaten van opgave 3 daarbij van nut zouden kunnen zijn.

Stel $9P = Q$, dus $9p\ (p + 1) = q\ (q + 1)$. Dan moet $9p^2 + 9p$ een pronik zijn. In elk geval is $3p\ (3p + 1) = 9p^2 + 3p$ een pronik, maar te klein. En het verschil met zijn grotere buur is volgens opgave 3a gelijk aan $6p + 2$, dus $9p^2 + 9p + 2$.

Maar $9p^2 + 9p$ ligt daartussenin, dus kan geen pronik zijn.

Stel $25P = Q$, dus $25p\,(p + 1) = q\,(q + 1)$. Dan moet $25p^2 + 25p$ een pronik zijn. Nu is $(5p + 1)(5p + 2) = 25p^2 + 15p + 2$ een te kleine pronik, en de eerstvolgende daarna is $(5p + 2)(5p + 3) = 25p^2 + 25p + 6$, te groot. En ook hier ligt $25p^2 + 25p$ ertussenin, dus kan nooit een pronik zijn. Opnieuw een tegenspraak.

Opgave 4b: Zelfde vraag voor $f = 4$.
Stel $4P = Q$ dus moet gelden $4p\,(p + 1)= 4p^2+4p=Q$. Maar $4p^2+4p+1=(2p+1)^2$, een kwadraat één groter dan Q. En dat verschil is te klein. Weer een tegenspraak.

Dus voor de factoren $f = 4$, 5 en 9, allemaal kwadraten van priemgetallen, zijn er geen waarden van P waarvoor $f \cdot P$ een pronik is.
Meer algemeen: Jan Guichelaar toont met die verschillen op analoge wijze aan dat het voor geen enkel kwadraat van een priemgetal lukt. Als $f = w^2$ is w dus altijd een samengesteld getal.
Zowel Frans van Hoeve als Harm Bakker kwam tot dezelfde conclusie zonder gebruik van die verschillen. Dat ging ongeveer als volgt:
Als $f = w^2$, met w priem, hebben we voor $Q = w^2P = wp\,(wp + w)$ en dat is groter dan de pronik $wp\,(wp + 1)$.
We kunnen dus stellen dat $q = wp + i$, waarbij $i > 0$. Dus $Q = (wp + i)(wp + i + 1)$
Invullen geeft
$w^2P = w^2p^2 + w^2p = (wp + i)(wp + i + 1)$.
En dat is te herleiden tot
$wp\,(w - 2i - 1) = i\,(i + 1)$. [1]
Dan moet $w - 2i - 1 > 0$, dus $w > 2i + 1$. En $i\,(i + 1)$ moet deelbaar zijn door w. Omdat i en $i + 1$ nooit een gemeenschappelijke deler hebben (ggd=1) is het priemgetal w een deler van i óf van $i + 1$. Maar $w > 2i + 1$ kan nooit een deler zijn van i of $i + 1$, tenzij $i = 0$. Dus hebben we een tegenspraak. **Q.E.D.**
We hebben zo in één klap de vragen 4a en 4b beantwoord.

Hiermee hebben we dus een hele groep kwadratische waarden van f waarvoor er geen oplossingen zijn. Maar zijn er nog meer? Daarvoor gaan we kijken naar andere kwadraten.
Frits Göbel maakte een tabel met waarden w, waarbij er weer proniks P en Q bestaan met $w^2 \cdot P = Q$. Bij elke waarde van p is er een rij mogelijke waarden van w.

p	**0**	**1**	**2**	**3**	**4**
1	1	6	35	204	1189
2	1	10	99	980	9701
3	1	14	195	2716	37829
4	1	18	323	5796	104005

Zo geldt voor $p = 3$ bijvoorbeeld: $(3 \cdot 4) \cdot 195^2 = 675 \cdot 676 = Q$.
De kwadraten van de getallen w in de eerste rij zijn driehoeksgetallen. Het is bekend dat de wortels w van alle kwadratische driehoeksgetallen o.a. te berekenen zijn met: $w_n = 6 \cdot w_{n-1} - w_{n-2}$ met $w_0 = 1$ en $w_1 = 6$. Dat levert dus de eerste rij van de tabel van Frits op.

Eerst even de tabel controleren:
Opgave 5a: Controleer het getal $w = 104005$ in de tabel voor $p = 4$ in kolom $n = 4$, door het getal q te bepalen waarvoor geldt: $Q = 4 \cdot 5 \cdot 104005^2 = q\,(q + 1)$.
q moet vlakbij de wortel uit $4 \cdot 5 \cdot 104005^2$ liggen, net iets eronder. Een grafiek tekenen van $y = x^2 + x$ met een standaard grafische rekenmachine valt helaas buiten het bereik, maar $\sqrt{Q} = \sqrt{(4 \cdot 5 \cdot 1045005^2)} = 2\cdot$

[1] Deze formule komt verderop in deze uitwerking, bij een bewijs gebaseerd op dat van Frans van Hoeve, nog eens terug als formule (F3).

104005 · √5 levert wel 465124,5, zodat q = 465124 zou moeten voldoen. En inderdaad is 20 · 104005^2 = 465124 · 465125. Controleren met pen en papier kan natuurlijk ook.

Opgave 5b: Bepaal formules om direct de getallen uit kolom 1 en 2 te berekenen als functie van p.
Voor kolom 1 geldt natuurlijk: $w = 4p + 2$.
Kolom 2 bestaat uit de kwadraten van kolom 1 min 1: $w = (4p + 2)^2 - 1$.

Opgave 5c: Bepaal formules die de hele tabel kunnen berekenen.
Voor de eerste rij hadden we al $w_n = 6w_{n-1} - w_{n-2}$, een lineaire recursie. We kunnen proberen of zoiets ook lukt voor de andere rijen.
Dan blijkt voor elke rij p:
$w_n = (4p + 2) \cdot w_{n-1} - w_{n-2}$.

Maar er zijn, net als voor de rij van Fibonacci ($u_n = u_{n-1} + u_{n-2}$) veel meer verbanden die we allemaal uit de bedoelde recursie kunnen afleiden. We geven er een paar:
Recursief: met $w_0 = 1$, $w_1 = 4p + 2$, $q_0 = p$.

$w_{n+2} = (4p + 2) \cdot w_{n+1} - w_n$
$w_n^2 - 1 = w_{n-1}w_{n+1}$
$w_{2n} = (w_n + w_{n-1})(w_n - w_{n-1})$ en $w_{2n+1} = w_n (w_{n+1} - w_{n-1})$
$w_n = 2q_{n-1} + 1 + (2p+1)\, w_{n-1}$ en $2q_n + 1 = (2p + 1)(2q_{n-1} + 1) + w_{n-1} \cdot 4P$
$2q_n = (2p + 1)w_n - 1 - w_{n-1}$
direct:
$w_n = (A^n - B^n) / (4\sqrt{P})$ en $2q_n + 1 = (A^n + B^n) / 2$,
met $A = 2p + 1 + 2\sqrt{P}$ en $B = 2p + 1 - 2\sqrt{P}$
$2q_n = (2p + 1 + 2\sqrt{P})^n - 1 - 2w_n\sqrt{P}$

En dan waren er nog een paar extra vragen:
a) Kun je bewijzen dat alle getallen die we volgens de beschreven recursie kunnen genereren allemaal voldoen aan de eis dat $P \cdot w^2$ een pronik is? En zijn dat alle mogelijkheden, of zijn er nog meer die niet in de voortgezette tabel voorkomen?
b) Zijn er niet-kwadratische getallen f waarvoor er geen P bestaat zodat $f \cdot P$ een pronik is?
Vraag a)
Dat alle getallen uit de voortgezette tabel voldoen aan de eis werd op verschillende manieren bewezen. We laten hieronder (na vraag b) twee verschillende bewijzen volgen.
Vraag b)
Hier hebben verschillende mensen wel over nagedacht, maar niet gevonden. Het lijkt erop dat ze niet bestaan, ook programmeren biedt voorlopig geen tegenvoorbeelden.

We beginnen met het bewijs van Harm Bakker die gebruikmaakte van de Pell-vergelijking. Kort door de bocht: De eis dat $Pw^2 = Q$ werd omgezet in een Pell-vergelijking en de oplossing daarvan werd vertaald naar de bedoelde recursie. Van de Pell-vergelijking is al lang geleden bewezen dat je daarmee precies alle oplossingen kan genereren[2], dus dat geldt dan ook in ons geval.

Een deel uit de inzending van Harm Bakker met de vergelijking van Pell: $x^2 - \alpha \cdot y^2 = 1$

Het ombouwen van de eis $w^2 \cdot P = Q$ tot een Pell-vergelijking:

[2] Zie b.v. http://www-bcf.usc.edu/~lototsky/PiMuEp/Pell-IMO.pdf

$w^2 \cdot P = Q = q(q+1) = q^2 + q$

$\Leftrightarrow$

$4w^2 \cdot P + 1 = 4q^2 + 4q + 1 = (2q+1)^2$

$\Leftrightarrow$

$(2q+1)^2 - 4 \cdot P \cdot w^2 = 1$

{*introduceer* $m = 2q + 1$ *en* $\alpha = 4 \cdot P$ }

$\Leftrightarrow$

$m^2 - \alpha \cdot w^2 = 1$

De kleinste oplossing is triviaal: $m_0 = 1$, ($q = 0$) en $w_0 = 0$.
De kleinste niet-triviale oplossing correspondeert met de triviale oplossing van het oorspronkelijke probleem: $w = 1$ en $q = p$:
$m_1 = 2 \cdot p + 1$ en $w_1 = 1$

Uit de theorie m.b.t. de vergelijking van Pell is bekend:

Stelling 1
Laat $(x,y)=(m_1,w_1)$ *de kleinste niet-triviale oplossing zijn van* $x^2-\alpha\cdot y^2 = 1$.
Dan is er bij elke oplossing (x,y) *die voldoet aan* $x^2 - \alpha \cdot y^2 = 1$ *een* $n \geq 0$ *zodanig dat*
$x + y\sqrt{\alpha} = (m_1 + w_1 \cdot\sqrt{\alpha})^n$

Neem aan dat je zo'n oplossing $x_n + y_n \cdot\sqrt{\alpha}$ hebt. Uit
$(m_1 + w_1\cdot\sqrt{\alpha}) \cdot (x_n + y_n\cdot\sqrt{\alpha}) = (m_1\cdot x_n + w_1\cdot\alpha\cdot y_n) + (w_1\cdot x_n + m_1\cdot y_n) \cdot \sqrt{\alpha}$
vinden we
$x_{n+1} = m_1 \cdot x_n + w_1 \cdot \alpha \cdot y_n$ en $y_{n+1} = w_1 \cdot x_n + m_1 \cdot y_n$

In termen van p: (bedenk dat in ons geval $w_1 = 1$, $m_1 = 2p + 1$, $x = m$ en $y = w$)
$m_n+1 = (2 \cdot p + 1) \cdot m_n + \alpha \cdot w_n$ en $w_{n+1} = m_n + (2 \cdot p + 1) \cdot w_n$

Hiermee zijn betrekkelijk eenvoudig de realisaties te bepalen.
Wat voorbeelden uitwerken suggereert dat we op deze manier dezelfde lijsten beschrijven als met de recurrente betrekking $w_{n+2}=(4p+2)\cdot w_{n+1}- w_n$ die in opdracht 5c is beschreven. Maar dat moeten we toch nog maar even echt vaststellen.
We generaliseren dat voor willekeurige p.
En $m_1 = 2p + 1$; $\alpha = 4 \cdot P = 4p(p + 1)$

$(m_1 + \sqrt{\alpha})^2$
$= (2p + 1 + \sqrt{(4P)})^2$
$= 4p^2 + 4p + 1 + 4p(p + 1) + 2 \cdot (2p + 1) \cdot \sqrt{(4P)}$
$= 8p^2 + 8p + 1 + (4p + 2) \cdot \sqrt{(4P)}=$
$= (4p + 2) \cdot (2p + 1) - 1 + (4p + 2) \cdot \sqrt{(4P)}$
$= (4p + 2)(2p + 1 + \sqrt{(4P)}) - 1$
$= (4p + 2)(m_1 + \sqrt{\alpha}) - 1$

Door beide leden van $(m_1 + \sqrt{\alpha})^2 = (4p + 2)(m_1 + \sqrt{\alpha}) - 1$
te vermenigvuldigen met $(m_1 + \sqrt{\alpha})^n$ krijgen we

$(m_1 + \sqrt{\alpha})^{n+2} = (4p + 2)(m_1 + \sqrt{\alpha})^{n+1} - (m_1 + \sqrt{\alpha})^n$

$\Leftrightarrow$

$m_{n+2} + w_{n+2}\sqrt{\alpha} = (4p + 2)(m_{n+1} + w_{n+1}\sqrt{\alpha}) - (m_n + w_n\sqrt{\alpha})$

$\Leftrightarrow$

$w_{n+2} = (4p + 2) \cdot w_{n+1} - w_n$

Waaruit we zien dat we het inderdaad over dezelfde rijen hebben en hebben we daarmee dus ook alle waarden w waarvoor er een P bestaat met $P \cdot w^2 = Q$. **Q.E.D.**

Dat het ook zonder Pell-vergelijkingen kan liet Frans van Hoeve zien.
Hij gaf een compact bewijs dat voor alle getallen w uit de (voortgezette) tabel inderdaad geldt: $P \cdot w^2$ is een pronik, en ook dat alle getallen waarvoor $P \cdot w^2$ een pronik is in de tabel voorkomen.

Wij geven hier een iets andere meer uitgebreide versie van die bewijzen.
In het volgende is i geheel en ≥ 0, x en y ($\epsilon\ \mathbb{R}$) en alle andere letters geheel en >0.

Bewijs gebaseerd op het bewijs van Frans van Hoeve

Frans gebruikt de volgende formules:

(F1) **De recursie** $\boldsymbol{w_{n+1} = s \cdot w_n - w_{n-1}}$ **met startgetallen** $\boldsymbol{w_0 = 1}$ **en** $\boldsymbol{w_1 = s}$
(F2) $\boldsymbol{w_n^2 - s \cdot w_n w_{n-1} + w_{n-1}^2 = 1}$
(F3) $\boldsymbol{wp\,(w - 2i - 1) = i\,(i + 1)}$

Verder gebruiken we een definitie van de (voortgezette) tabel van Frits:
De tabel van Frits is een tabel die bestaat uit rijen met rijnummer p, waarbij de rijen worden gevormd door de recursie (F1) met $s = 4p + 2$ [3]).

We geven de lemma's eerst zonder bewijs. De bewijzen volgen na stelling 2.

Stelling 1:
Voor alle getallen w uit de tabel van Frits is $P \cdot w^2 = p\,(p + 1) \cdot w^2$ een pronik

Lemma A: (F1)⟹(F2):
Tussen elk tweetal opvolgende termen in rijen die uit de recursie (F1) ontstaan geldt tussen w_{n-1} en w_n de kwadratische betrekking (F2)

Lemma B: Als $s = 4p + 2$ dan (F2)⟹(F3):
Als $w^2 - (4p + 2) \cdot wv + v^2 = 1$ met $w > v$ dan is er een $i \geq 0$ met $w \cdot p\,(w - 2i - 1) = i\,(i + 1)$

Lemma C: (F3)⟹: $P \cdot w^2$ is een pronik:
Als er voor een zekere p en w een $i \geq 0$ bestaat met $w \cdot p\,(w - 2i - 1) = i\,(i + 1)$ dan is $P \cdot w^2$ een pronik

Bewijs van stelling 1:
Omdat de getallen uit de tabel voortkomen uit de recursie (F1) met $s = 4p + 2$ volgt uit lemma A:
In elke rij van de tabel geldt voor elke $n > 0$: $w_n^2 - (4p + 2) \cdot w_n w_{n-1} + w_{n-1}^2 = 1$

We constateren dat de recursie ons garandeert dat geldt: $w_n > w_{n-1}$, zodat we lemma B kunnen toepassen met $w = w_n$ en $v = w_{n-1}$. Dat levert op: in rij p van de tabel is er voor elke w_n een $i \geq 0$ te vinden zodat $w_n\, p\,(w_n - 2i - 1) = i\,(i + 1)$ **(**strikt genomen: behalve voor $w_0 = 1$)

[3] Frits stelde zijn tabel op door eerst een groot aantal oplossingen van $P \cdot w^2 = Q$ te verzamelen, en vervolgens te constateren dat die allemaal aan deze recursie voldoen.

Daarop kunnen we dan Lemma C toepassen, zodat voor elke waarde w uit rij p van de tabel $P \cdot w^2$ een pronik is (voor $w_0 = 1$ is dat triviaal). **Q.E.D.**

Stelling 2:

De tabel van Frits is volledig, d.w.z. als $P \cdot u^2$ is een pronik dan komt u voor in rij p van de tabel.

Lemma C': $P \cdot w^2$ is een pronik⇒(F3):
Als $P \cdot w^2 = p\,(p + 1) \cdot w^2$ een pronik is dan is er een $i \geq 0$ met $wp\,(w - 2i - 1) = i\,(i + 1)$.
C' is dus het omgekeerde van C.

Lemma B': Als $s = 4p + 2$ dan (F3)⇒(F2):
Als $w \cdot p\,(w - 2i - 1) = i\,(i + 1)$ met $i \geq 0$ en $w > 1$ dan is er een v met $v < w$ met $w^2 - (4p + 2) \cdot w \cdot v + v^2 = 1$
B' is dus in zekere zin het omgekeerde van B, als we $w = w_n$ en $v = w_{n-1}$ invullen in (F2)

Lemma A': (F1)⇔(F2):
$(x,y) = (u,v)$ met u en v geheel is een oplossing van de vergelijking $x^2 - s \cdot x \cdot y + y^2 = 1$ met $s > 2$ ⇔ u en v zijn opvolgende termen uit de rij die ontstaat uit de recursie (F1).

A' is dus niet alleen het omgekeerde van A, maar omvat ook A zelf. Lemma A en het bewijs ervan zijn daardoor in feite overbodig. We geven ze toch omdat het bewijs van A' een stuk langer is dan dat van A.

Bewijs van stelling 2:

Stel $P \cdot u^2$ is een pronik.
Als $u = 1$ is u de eerste waarde in de rij. Dan is de stelling bewezen. We mogen dus aannemen dat $u > 1$.
Volgens Lemma C' is er een $i \geq 0$ zdd $u \cdot p\,(u - 2i - 1) = i\,(i + 1)$.
Hieruit, in combinatie met $u > 1$ is er dan volgens lemma B' een v met $v < u$ met $u^2 - (4p + 2) \cdot u \cdot v + v^2 = 1$
$(x,y) = (u,v)$ is dan een geheeltallige oplossing met $x > y$ van de vergelijking $x^2 - (4p + 2) \cdot x \cdot y + y^2 = 1$
en volgens Lemma A' komen dan u en v voor in rij die ontstaat uit de recursie (F1) met $s = 4p + 2$, en dus in rij p van de tabel. **Q.E.D.**

Bewijs van de lemma's:

Lemma A:
Tussen elk tweetal opvolgende termen w_{n-1} en w_n in rijen die uit de recursie (F1) ontstaan geldt tussen w_{n-1} en w_n de kwadratische betrekking (F2).
Bewijs door volledige inductie: het klopt voor $n = 1$: vul w_0 en w_1 in.
Stel het klopt voor een zekere n, dus ${w_n}^2 - s \cdot w_n w_{n-1} + {w_{n-1}}^2 = 1$
Dan is ${w_{n+1}}^2 - s \cdot w_{n+1} w_n + {w_n}^2 = (s \cdot w_n - w_{n-1})^2 - s\,(s \cdot w_n - w_{n-1})\,w_n + {w_n}^2 =$
$s^2 {w_n}^2 - 2s\, w_n w_{n-1} + {w_{n-1}}^2 - s^2 {w_n}^2 + s \cdot w_n w_{n-1} + {w_n}^2 =$
${w_n}^2 - s \cdot w_n w_{n-1} + {w_{n-1}}^2 = 1$ Het klopt dan dus ook voor $n + 1$. **Q.E.D.**

Lemma B:
Als $w^2 - (4p + 2) \cdot wv + v^2 = 1$ met $w > v$ dan is er een $i \geq 0$ met $w \cdot p\,(w - 2i - 1) = i(i+1)$
Bewijs:
Laat $w^2 - (4p + 2) \cdot w \cdot v + v^2 = 1$ met $w > v$. Dat kunnen we schrijven als:
$w^2 - 2w \cdot v + v^2 - 4P \cdot w \cdot v = (w - v)^2 - 4P \cdot w \cdot v = 1$
Uit $(w - v)^2 - 4P \cdot w \cdot v = 1$ blijkt: $w - v$ is oneven. Kies nu $i = (w - v - 1) / 2$. i is dan een heel getal ≥ 0, en $v = w - 2i - 1$ en $w - v = 2i + 1$
Vullen we dat in in $(w - v)^2 - 4P \cdot w \cdot v = 1$ dan krijgen we:
$(2i + 1)^2 - 4p \cdot w\,(w - 2i - 1) - 1 = 0$ en dat resulteert in
$w \cdot p\,(w - 2i - 1) = i\,(i + 1)$, **Q.E.D.**

Lemma B':
Als $w \cdot p\ (w - 2i - 1) = i\ (i + 1)$ met $i \geq 0$ en $w > 1$ dan is er een v met $v < w$ met $w^2 - (4p + 2) \cdot w \cdot v + v^2 = 1$
Het bewijs loopt parallel aan het van achter naar voren geschreven bewijs van lemma B:
Laat $w \cdot p\ (w - 2i - 1) = i\ (i + 1)$ met $i \geq 0$ en $w > 1$
$i = 0$ voldoet hier niet, want dan zou $w \cdot p\ (w - 1) = 0$, en dat kan niet, want $w > 1$
Dus $w \cdot p\ (w - 2i - 1) > 0$ en dus $w - 2i - 1 > 0$.
Kies $v = w - 2i - 1$, en dus $v < w$
dan $i = (w - v - 1) / 2$. Deze i en v vullen we in in $w \cdot p\ (w - 2i - 1) = i\ (i + 1)$:
$p \cdot w \cdot v = (w - v - 1)(w - v + 1) / 4$
$4p \cdot w \cdot v = (w - v)^2 - 1 = w^2 - 2w \cdot v + v^2 - 1$
$w^2 - (4p + 2) \cdot w \cdot v + v^2 = 1$. **Q.E.D.**

Lemma C:
Er bestaat een $i \geq 0$ met $w \cdot p\ (w - 2i - 1) = i\ (i + 1) \Longrightarrow P \cdot w^2$ is een pronik
Bewijs:
Stel: $w \cdot p\ (w - 2i - 1) = i\ (i + 1)$ met $i \geq 0$.
$w \cdot p\ (w - 2i - 1) = i\ (i + 1) \Longleftrightarrow$
$w^2 p = 2w \cdot p \cdot i + w \cdot p + i^2 + i \Longleftrightarrow$
$w^2 p^2 + w^2 p = w^2 p^2 + 2w \cdot p \cdot i + w \cdot p + i^2 + i \Longleftrightarrow$
$p\ (p + 1) \cdot w^2 = (w \cdot p + i)^2 + w \cdot p + i = (w \cdot p + i)(w \cdot p + i + 1) \Longrightarrow$
$P \cdot w^2$ is een pronik. **Q.E.D.**

Lemma C':
$P \cdot w^2$ is een pronik $\Longrightarrow$ Er bestaat een $i \geq 0$ met $w \cdot p\ (w - 2i - 1) = i\ (i + 1)$
Bewijs:
Stel $P \cdot w^2$ is een pronik, dus $p\ (p + 1) \cdot w^2 = q\ (q + 1)$
$p\ (p + 1) \cdot w^2 = w \cdot p\ (w \cdot p + w) = q\ (q + 1)$ dus $q \geq w \cdot p$. Kies $i \geq 0$ zdd $q = w \cdot p + i$ zodat:
$p\ (p + 1) \cdot w^2 = w \cdot p\ (w \cdot p + w) = (w \cdot p + i)(w \cdot p + i + 1)$
Dan geldt de voorlaatste regel uit het bewijs van Lemma C, dus ook de 3 regels daarvoor, en dus geldt
$w \cdot p\ (w - 2i - 1) = i\ (i + 1)$. **Q.E.D.**

Lemma A':
$(x,y) = (u,v)$ met u en v geheel is een oplossing van de vergelijking $x^2 - s \cdot x \cdot y + y^2 = 1$ met $s > 2 \Longleftrightarrow$
u en v zijn opvolgende termen uit de rij die ontstaat uit de recursie (F1).
Bewijs:
We bekijken de vergelijking $x^2 - s \cdot x \cdot y + y^2 = 1$ op het XY vlak met $(x,y) \in \mathbb{R}^2$.

Het zal duidelijk zijn dat we te maken hebben met een kegelsnede. Het is gemakkelijk na te gaan dat de figuur een hyperbool is voor $s > 2$. Verder is uit de vergelijking direct te zien dat als (x,y) een oplossing is, dat ook (y,x) en $(-x, -y)$ oplossingen zijn. De figuur die we krijgen is dus symmetrisch in de lijnen $x = y$ en $x = -y$. En de punten $(\pm1,0)$ en $(0,\pm1)$ voldoen aan de vergelijking.
In de figuur (volgende bladzijde) is een voorbeeld geschetst: de gestippelde lijnen zijn de asymptoten, de blauwe de hyperbool.[4] De snijpunten met de x- en de y-as liggen bij ±1. We gaan dus op zoek naar roosterpunten die op de grafiek liggen.

[4] In de getekende figuur is weliswaar $s > 2$, maar niet geheel. In feite is s maar ietsje groter dan 2. Dat is zo gekozen om het mogelijk te maken meerdere waarden van A en B af te kunnen beelden, zonder dat de schaal van de figuur zo klein wordt dat niet meer te zien wat er zich vlak bij de oorsprong afspeelt. In het bewijs is s wel geheel.

We beginnen in het punt $A = (x,y)$ op de onderste 'tak' van de hyperbool met dus $x > y$. Omdat we meer punten A gaan genereren kiezen we $A_{n+1} = A$ en $(x_{n+1},y_{n+1}) = (x,y)$
Vanaf dat punt gaan we de rode lijn volgen. We gaan dan horizontaal naar links en vinden op de bovenste tak een oplossing in B_n. Het spiegelbeeld $A_n = (x_n,y_n)$ daarvan in de lijn $y = x$ ligt dan weer op de onderste tak.
We kunnen zo doorgaan naar B_{n-1} en dan naar A_{n-1} en zo verder. De symmetrie zorgt dan dat $x_i = y_{i+1}$, dus $A_i = (x_i,x_{i-1})$ en $B_i = (x_{i-1},x_i)$. B_i en A_{i-1} liggen dus recht boven elkaar.

Kijken we naar een horizontale lijn, b.v. $A_{n+1}B_n$ waarvoor geldt $y = y_{n+1} = x_n$, en naar de vierkantsvergelijking in x: $x^2 - s \cdot x_n x + x_n^2 = 1$. Het zal duidelijk zijn dat de x-coördinaten van A_{n+1} en B_n, dus x_{n+1} en x_{n-1} de 2 oplossingen zijn van de vierkantsvergelijking. We weten dat als p en q de oplossingen zijn van $x^2 - bx + c = 0$ geldt dat $p + q = b$, want $x^2 - bx + c$ kan dan ontbonden worden in $(x - p)(x - q)$. In ons geval hebben we dus $x_{n+1} + x_{n-1} = s \cdot x_n$ of
$\boldsymbol{x_{n+1} = s \cdot x_n - x_{n-1}}$. Dit is dezelfde recursieformule als (F1), maar zonder de startwaarden.

Als A_{n+1} een roosterpunt is zijn x_{n+1} en y_{n+1} geheel. Ook s is geheel, dus is ook B_n een roosterpunt, en het spiegelbeeld A_n ook.
Gevolg: Als A_{n+1} een roosterpunt is zijn alle andere A's en B's dat ook.
Kijken we nu naar het punt waarop onze rode lijn het 1^e kwadrant verlaat. Dat gebeurt zodra de laatste A onder het snijpunt van de bovenste tak met de y-as komt. Maar dat snijpunt is (0,1), dus zoals het in de figuur getekend is, is die laatste A geen roosterpunt, en dus is A_{n+1} geen roosterpunt.
De enige zigzaglijn waarop roosterpunten liggen is dus de groene lijn door de snijpunten van de grafiek met de x- en de y-as, en voor die lijn geldt dus: de **knikpunten van de groene zigzaglijn zijn precies de roosterpunten op de grafiek**.

Dat legt de startwaarden van de recursie vast:
Op deze zigzaglijn liggen de punten (0, −1) en (1,0). 0 en 1 zijn dus opvolgende x-waarden waarop we de recursie kunnen toepassen. Kiezen we $x_0 = 1$ dan is $x_1 = s \cdot x_0 - 0 = s$ waarmee de startwaarden voor gelijk zijn aan die voor (F1).
De x-coördinaten $x_n > 0$ van de knikpunten op de groene lijn zijn dus precies de getallen die voortkomen uit de recursie (F1), waarbij voor de coördinaten van knikpunt A_n geldt: $A_n = (x_n,x_{n-1})$ ligt op de grafiek. Dus:
$(x,y) = (u,v)$ met u en v geheel is een oplossing van de vergelijking $x^2 - s \cdot x \cdot y + y^2 = 1$ met $s > 2 \Leftrightarrow$
u en v zijn opvolgende termen uit de rij die ontstaat uit de recursie (F1). **Q.E.D.**