WELRIEKENDE WISKUNDE TUSSEN DE WOLKENKRABBERS

Reinier Schmiermann

Van 9 tot 16 juli vond in Hongkong de Internationale Wiskunde Olympiade (IMO) plaats. Het Nederlandse team behaalde hier drie bronzen medailles en drie eervolle vermeldingen. Deelnemer Reinier Schmiermann (15), die twee jaar aan de olympiadetraining heeft meegedaan en inmiddels Technische Wiskunde en Software Science studeert aan de Technische Universiteit Eindhoven (TU/e), bespreekt in dit artikel opgave 4, de eerste opgave van wedstrijddag 2.

Onvergetelijke ervaring

Hongkong is een plaats waar verschillende culturen elkaar ontmoeten. Ook tijdens de laatste IMO gebeurde dit. Deelnemers van over de hele wereld kwamen samen om zich te buigen over zes pittige wiskundeopgaven, verdeeld over twee dagen. Ook Nederland had weer een team gezonden en ik mocht hier deel van uitmaken. Na een trainingsweek in een luxehotel in Hongkong vertrokken we naar de campus van de Hong Kong University of Science and Technology, waar de wedstrijd plaatsvond. Hier hebben we deelnemers van vele andere landen ontmoet en tijdens de excursies hebben we de Hongkongse cultuur leren kennen. Dit alles was een onvergetelijke ervaring.

Opgave

De wedstrijd was verdeeld over twee dagen. Op elke dag kregen we 4,5 uur voor drie opgaven. De eerste opgave van wedstrijddag 2 luidde als volgt:
Een verzameling positieve gehele getallen noemen we welriekend *als die uit minstens twee elementen bestaat en elk van de elementen een priemdeler gemeen heeft met een van de andere elementen. Definieer $P(n) = n^2 + n + 1$. Wat is het kleinst mogelijke gehele getal $b \geq 1$ zodanig dat er een geheel getal $a \geq 0$ bestaat waarvoor de verzameling $\{P(a+1), P(a+2), \dots, P(a+b)\}$ welriekend is?*
Wat is hier nu eigenlijk de bedoeling? We gaan opeenvolgende gehele waarden in de polynoom P stoppen en bekijken de uitkomsten hiervan. Zo'n verzameling uitkomsten is welriekend als elke uitkomst een priemfactor gemeen heeft met een andere uitkomst; dus als bijvoorbeeld 15 erbij zit, dan moet er nog een andere uitkomst bij zitten die deelbaar is door 3 of 5. We moeten uiteindelijk de kleinste welriekende verzameling vinden die op deze manier (met de polynoom) is te maken. De grootte van die verzameling is het getal b waar de opgave naar vraagt.

Verkenning

Laten we eerst een aantal kleine waarden van P uitrekenen. We vinden zo de volgende waarden:

n	$P(n)$
1	3
2	7
3	13
4	$21 = 3 \cdot 7$
5	31
6	43
7	$57 = 3 \cdot 19$
8	73
9	$91 = 7 \cdot 13$
10	$111 = 3 \cdot 37$
11	$133 = 7 \cdot 19$
12	157

Ten eerste zien we dat al deze getallen oneven zijn. Dit geldt in het algemeen, aangezien $P(n) = n^2 + n + 1 = n(n+1) + 1$ en $n(n+1)$ altijd even is (omdat n of $n+1$ even moet zijn). Dus $P(n)$ is altijd oneven. Aan deze gevallen valt ook op dat $P(n)$ deelbaar lijkt te zijn door 3 als n congruent is aan 1 modulo 3. We kunnen dit vrij makkelijk controleren: als n congruent is aan 1 modulo 3, dan is $P(n) \equiv 1^2 + 1 + 1 = 3 \equiv 0 \bmod 3$, dus dit vermoeden klopt inderdaad. Er geldt verder dat als n congruent is aan 1 modulo 3, $n + 3$ dit natuurlijk ook is. Hieruit volgt dat in dat geval $P(n)$ en $P(n+3)$ een gemeenschappelijke factor 3 hebben. Wat gebeurt er als n een andere waarde aanneemt modulo 3: kan $P(n)$ dan ook deelbaar zijn door 3? Als $n \equiv 2 \bmod 3$, dan is $P(n) \equiv 2^2 + 2 + 1 = 7 \equiv 1 \bmod 3$ en als $n \equiv 0 \bmod 3$, dan is $P(n) \equiv 0^2 + 0 + 1 = 1 \equiv 1 \bmod 3$, dus $P(n)$ is alleen deelbaar door 3 als $n \equiv 1 \bmod 3$. Misschien hebben we hier later nog wat aan.

Kleine waarden van b

We willen uiteindelijk de kleinst mogelijke waarde van b vinden die voldoet, dus laten we alvast van wat kleine waarden van b gaan vaststellen of deze kunnen voldoen. Als we van een b kunnen bewijzen dat hij niet voldoet, dan geeft dit misschien een idee hoe we van andere b kunnen bewijzen dat ze ook niet voldoen. Bovendien hebben we de opgave opgelost als we een b vinden die wel voldoet en van alle kleinere b hebben bewezen dat deze niet voldoen. In de opgave is gegeven dat een welriekende verzameling uit minstens twee elementen moet bestaan, hieruit volgt dat b minstens 2 moet zijn. Laten we dus eens kijken wat er gebeurt als $b = 2$. De vraag is nu of er een a bestaat zodat de verzameling $\{P(a + 1), P(a + 2)\}$ welriekend is. Deze verzameling is alleen welriekend als $P(a + 1)$ en $P(a + 2)$ een gemeenschappelijke priemdeler hebben. Nu kan $a + 1$ elk positief geheel getal zijn, dus het is nu de vraag of er een positieve gehele n is zodat $P(n)$ en $P(n + 1)$ een gemeenschappelijke priemfactor hebben. Twee getallen hebben een gemeenschappelijke priemdeler dan en slechts dan als hun *grootste gemene deler* (ggd) groter is dan 1. We gaan daarom de ggd van $P(n)$ en $P(n + 1)$ berekenen. Er geldt dat $P(n) = n^2 + n + 1$ en $P(n + 1) = (n + 1)^2 + (n + 1) + 1 = n^2 + 3n + 3$. Het gaat hier dus om $\text{ggd}(n^2 + n + 1, n^2 + 3n + 3)$. Nu is er een rekenregel die zegt dat je voor het berekenen van de ggd van twee getallen net zo goed bij een van die getallen een veelvoud van het andere getal kunt optellen. Hiermee vinden we dat de ggd van $P(n)$ en $P(n + 1)$ gelijk is aan $\text{ggd}(n^2 + n + 1, n^2 + 3n + 3 - (n^2 + n + 1)) = \text{ggd}(n^2 + n + 1, 2n + 2)$. Omdat we weten dat $n^2 + n + 1$ oneven is, mogen we de tweede term door 2 delen, dus $\text{ggd}(n^2 + n + 1, 2n + 2) = \text{ggd}(n^2 + n + 1, n + 1)$. (Immers $n^2 + n + 1$ is niet deelbaar door 2, dus zijn beide ggd's dit ook niet, zodat de factor 2 in de andere term niets uitmaakt. Ook deze eigenschap zullen we nog een aantal keer tegenkomen. Door nogmaals de rekenregel toe te passen, vinden we dat deze laatste ggd weer gelijk is aan $\text{ggd}(n^2 + n + 1 - n(n + 1), n + 1) = \text{ggd}(1, n + 1) = 1$. We vinden dus dat $\text{ggd}(P(n), P(n + 1)) = 1$. Hieruit volgt dat $P(n)$ en $P(n + 1)$ nooit een gemeenschappelijke priemfactor kunnen hebben. Er geldt dus dat $b = 2$ niet voldoet. Stel nu dat $b = 3$. We willen nu weten of de verzameling $\{P(a + 1), P(a + 2), P(a + 3)\}$ welriekend kan zijn. Als dit het geval zou zijn, dan weten we dat $P(a + 2)$ een priemfactor gemeenschappelijk heeft met $P(a + 1)$ of $P(a + 3)$. We hebben echter net al bewezen dat de P van twee opeenvolgende getallen nooit een gemeenschappelijke priemfactor kan hebben, dus dit kan niet. We zien nu dus ook dat $b = 3$ ook niet kan, er moet dus gelden dat $b \geq 4$.

figuur 1 Van links naar rechts: Gabriel Visser, Pim Spelier, Reinier Schmiermann, Levi van de Pol, Wietze Koops en Erik van Cappellen tijdens de openingsceremonie.

$b = 4$

Laten we dus verder gaan met het geval $b = 4$. Is er een a zodat de verzameling $\{P(a + 1), P(a + 2), P(a + 3), P(a + 4)\}$ welriekend is? Als dit het geval is, dan moet $P(a + 2)$ een priemdeler gemeenschappelijk hebben met $P(a + 4)$ (want met $P(a + 1)$ of $P(a + 3)$ is weer geen optie). Op een vergelijkbare manier volgt dat $P(a + 3)$ een priemdeler gemeenschappelijk moet hebben met $P(a + 1)$. Nu is het dus de vraag of dit kan. Daarvoor kijken we naar de ggd van $P(n)$ en $P(n + 2)$.
Er geldt dat $P(n) = n^2 + n + 1$ en $P(n + 2) = (n + 2)^2 + (n + 2) + 1 = n^2 + 5n + 7$, dus $\text{ggd}(P(n), P(n + 2)) = \text{ggd}(n^2 + n + 1, n^2 + 5n + 7)$. Als we nu weer de rekenregel voor ggd's toepassen, dan vinden we dat deze ggd gelijk is aan $\text{ggd}(n^2 + n + 1, n^2 + 5n + 7 - (n^2 + n + 1)) = \text{ggd}(n^2 + n + 1, 4n + 6)$. Omdat $n^2 + n + 1$ oneven is, kunnen we de tweede term delen door 2 en dus is deze ggd gelijk aan $\text{ggd}(n^2 + n + 1, 2n + 3)$. Nu geldt dat $2n + 3$ oneven is, dus mogen we de eerste term wel met een factor 2 vermenigvuldigen. Dus $\text{ggd}(n^2 + n + 1, 2n + 3) = \text{ggd}(2n^2 + 2n + 2, 2n + 3)$. Dit is fijn, want deze rechter ggd kunnen we met de rekenregel weer herschrijven tot $\text{ggd}(2n^2 + 2n + 2 - n(2n + 3), 2n + 3) = \text{ggd}(-n + 2, 2n + 3)$. En als we nu nogmaals de rekenregel toepassen, dan vinden we dat deze ggd weer gelijk is aan $\text{ggd}(-n + 2, 2n + 3 + 2(-n + 2)) = \text{ggd}(-n + 2, 7)$. Deze ggd is altijd 1 of 7, en hij is precies 7 als $-n + 2$ deelbaar is door 7, dus als $n \equiv 2 \bmod 7$. Dit is dus het enige geval dat $P(n)$ en $P(n + 2)$ een gemeenschappelijke priemfactor hebben. In het geval $b = 4$ moest er gelden dat $P(a + 1)$ en $P(a + 3)$ een gemeenschappelijke priemfactor hebben en dat $P(a + 2)$ en $P(a + 4)$ een gemeenschappelijke priemfactor hebben. Dit betekent dus dat zowel $a + 1 \equiv 2 \bmod 7$ als $a + 2 \equiv 2 \bmod 7$, maar dat kan nooit tegelijkertijd waar zijn. Ook het geval $b = 4$ voldoet dus niet.

$b = 5$

Omdat we nog steeds geen b hebben gevonden die voldoet, gaan we gewoon de volgende b proberen. Stel dus dat $b = 5$. We willen nu weten of de verzameling $\{P(a+1), P(a+2), P(a+3), P(a+4), P(a+5)\}$ welriekend kan zijn. Stel dat deze verzameling welriekend is, dan moet er dus ook gelden dat $P(a+3)$ een priemfactor gemeenschappelijk heeft met een van de andere getallen in deze verzameling, en dat moet dan om $P(a+1)$ of $P(a+5)$ gaan. Met wat we net hebben bewezen, geeft dit dat $a+1 \equiv 2 \bmod 7$ of $a+3 \equiv 2 \bmod 7$. Uit de welriekendheid van de verzameling volgt ook dat $P(a+2)$ een gemeenschappelijke priemfactor moet hebben met een ander element. Nu weten we weer dat $P(a+1)$ en $P(a+3)$ niet dit andere element kunnen zijn. Ook kan er niet gelden dat $a+2 \equiv 2 \bmod 7$, want $a+1 \equiv 2 \bmod 7$ of $a+3 \equiv 2 \bmod 7$, dus heeft $P(a+2)$ ook geen gemeenschappelijke priemfactor met $P(a+4)$. Er moet dus wel gelden dat $P(a+2)$ een gemeenschappelijke priemfactor heeft met $P(a+5)$. Er is zo ook te bewijzen dat $P(a+4)$ een gemeenschappelijke priemfactor heeft met $P(a+1)$. Om erachter te komen of dit mogelijk is, gaan we weer kijken wanneer $P(n)$ en $P(n+3)$ een gemeenschappelijke priemfactor hebben. Aan het begin hebben we al gezien dat als $n \equiv 1 \bmod 3$ deze getallen een gemeenschappelijke factor 3 hebben (en anders niet). Is er misschien nog een andere situatie waarin $P(n)$ en $P(n+3)$ een gemeenschappelijke priemdeler hebben? Om hier achter te komen, kijken we nu weer naar de ggd van $P(n)$ en $P(n+3)$. We kunnen op een vergelijkbare manier als bij de vorige ggd-berekeningen laten zien dat deze ggd gelijk is aan 1 als $P(n)$ niet deelbaar is door 3. De getallen $P(n)$ en $P(n+3)$ hebben in dit geval dus geen gemeenschappelijke priemfactor, zodat we zien dat $P(n)$ en $P(n+3)$ alleen een gemeenschappelijke priemfactor hebben als $n \equiv 1 \bmod 3$. Het is dus onmogelijk dat $P(a+1)$ en $P(a+4)$ een gemeenschappelijke priemfactor hebben en dat $P(a+2)$ en $P(a+5)$ ook een gemeenschappelijke priemfactor hebben, want dan zouden zowel $a+1$ als $a+2$ congruent moeten zijn aan 1 modulo 3. Ook $b = 5$ voldoet dus niet.

figuur 2

Oplossing

Laten we dus onderzoeken of $b = 6$ wel kan voldoen. We willen dat de verzameling $\{P(a+1), P(a+2), P(a+3), P(a+4), P(a+5), P(a+6)\}$ welriekend is. Met alles wat we al hebben bewezen, weten we dat bij de getallen $a+1$ tot en met $a+6$ er hoogstens één paar is met verschil 2 zodat de P's van deze getallen een gemeenschappelijke priemfactor hebben en er is hoogstens één paar getallen met verschil 3 zodat de P's van deze getallen een gemeenschappelijke priemfactor hebben. Ook zouden er twee getallen kunnen zijn met verschil 4 zodat de P daarvan een gemeenschappelijke priemfactor hebben. Bij de kleine waarden van P zien we dat $P(7)$ en $P(11)$ een gemeenschappelijke factor 19 hebben. Met modulorekenen volgt dan direct dat $P(n)$ en $P(n+4)$ priemdeler 19 gemeen hebben als $n \equiv 7 \bmod 19$. (Door naar de ggd van $P(n)$ en $P(n+4)$ te kijken, kunnen we inzien dat dit ook echt de enige mogelijkheid is, maar dat blijken we niet nodig te hebben). Het is nu de vraag of we door deze paren slim te kiezen kunnen zorgen dat elk getal in de verzameling een gemeenschappelijke priemfactor heeft met een ander element. Na wat gepuzzel blijkt dat dit bijvoorbeeld het geval is als $P(a+1)$ een gemeenschappelijke priemfactor heeft met $P(a+5)$, $P(a+2)$ een gemeenschappelijke priemfactor heeft met $P(a+4)$ en $P(a+3)$ een gemeenschappelijke priemfactor heeft met $P(a+6)$. De vraag is nu of er een niet-negatief geheel getal a is zodat $a+1 \equiv 7 \bmod 19$, $a+2 \equiv 2 \bmod 7$ en $a+3 \equiv 1 \bmod 3$. Volgens de Chinese reststelling, een stelling die we bij de olympiadetraining hebben geleerd, heeft dit stelsel een oplossing, omdat 19, 7 en 3 verschillende priemgetallen zijn. Als we dit stelsel zouden oplossen (wat niet nodig is voor het bewijs), dan vinden we dat dit geldt als $a \equiv 196 \bmod 399$. De verzameling $\{P(197), P(198), \ldots, P(202)\}$ is dus welriekend. Er volgt dus dat $b = 6$ inderdaad voldoet. We hebben ook al laten zien dat alle b kleiner dan 6 niet voldoen, dus dit is de kleinste b die voldoet. Het antwoord op de vraag is dus 6.

Bij deze opgave brengt het controleren van kleine waarden van b ons tot een oplossing. Vaak is het een goed idee om bij dit soort opgaven kleine waarden in te vullen, maar dit maakt deze opgave nog niet makkelijk. Het is namelijk erg verleidelijk om iets in het algemeen te proberen, bijvoorbeeld om voor alle gehele m en n de ggd van $P(n)$ en $P(n+m)$ te berekenen, maar dit is niet makkelijk te doen. Ook is een rekenfout snel gemaakt. Desondanks wist ik deze opgave wel volledig op te lossen, wat me een eervolle vermelding heeft opgeleverd. Het belangrijkste van alles is echter dat ik erg van de IMO heb genoten en er met veel plezier op terug kan kijken.

Over de auteur

Reinier Schmiermann nam als vwo-scholier van het Stedelijk Gymnasium 's-Hertogenbosch twee jaar lang deel aan het trainingsprogramma van de Wiskunde Olympiade. In 2016 maakte hij deel uit van het Nederlandse team. Nu studeert hij Technische Wiskunde en Software Science aan de Technische Universiteit Eindhoven (TU/e).
E-mailadres: *rf.schmiermann@home.nl*