Deze zomer bogen 565 getalenteerde scholieren uit 104 verschillende landen zich twee dagen over in totaal zes heel pittige wiskundeopgaven. De leerlingen en hun begeleiders waren voor anderhalve week naar Bremen gekomen voor de jubileumeditie van de Internationale Wiskunde Olympiade. Twee ochtenden hiervan waren gereserveerd voor de wed-

■ door Birgit van Dalen en Quintijn Puite

MODULOREKENEN BIJ DE IMO

Het Nederlandse team, v.l.n.r.: Wouter Berkelmans, Raymond van Bommel, Merlijn Staps, Maarten Roelofsma, Saskia Chambille, Harm Campmans, David Kok.

strijd; de rest van de tijd konden de scholieren kennismaken met leeftijdsgenoten van over de hele wereld. Ze leerden elkaar kaartspelletjes, vormden samen voetbalteams en gingen op excursie naar onder andere het prachtige waddeneiland Wangerooge.

Het Nederlandse team voor de vijftigste editie van de Internationale Wiskunde Olympiade (IMO) bestond uit Wouter Berkelmans, Raymond van Bommel, Harm Campmans, Saskia Chambille, David Kok en Maarten Roelofsma. Merlijn Staps ging mee als aanstormend talent. Direct voorafgaand aan de IMO heeft het team nog een trainingskamp gehad samen met het team van Nieuw-Zeeland. Het team is 47ste geworden in het officieuze landenklassement. In de afgelopen tien jaar heeft Nederland het slechts één keer beter gedaan. In dit artikel gaan we nader in op opgave 1 van deze IMO, die door het Nederlandse team erg goed is gemaakt.

MODULOREKENEN

Een van de mogelijke oplossingen van opgave 1 maakt gebruik van de techniek van het *modulorekenen*. Hoe gaat dat in zijn werk? Iedereen die kan klokkijken, gebruikt deze techniek ongemerkt dagelijks. Als het nu 22 uur is, hoe laat is het dan over 5 uur? Precies, 3 uur. We zeggen dat $22 + 5$ *congruent* is aan 3, althans, als je modulo 24 rekent. Notatie: $22 + 5 \equiv 3 \pmod{24}$. Zo geldt ook dat $4 - 10 \equiv 18 \pmod{24}$, want 10 uur vóór 4 uur was het 18 uur. Anders gezegd: $27 \equiv 3 \pmod{24}$ en $-6 \equiv 18 \pmod{24}$. Er hoeft niet per se maar één keer 24 verschil tussen de twee getallen links en rechts van het congruentieteken ($\equiv$) te zitten: er geldt ook dat $-23 \equiv 25 \pmod{24}$, want 23 uur voor middernacht is het even laat als 25 uur na middernacht. In het algemeen noemen we twee getallen congruent aan elkaar modulo 24 als ze op veelvouden van 24 na gelijk zijn. Dat wil zeggen: als het verschil een veelvoud is van 24, oftewel deelbaar is door 24 (met rest 0). Het hoeft niet zo te zijn dat een van die getallen altijd tussen de 0 en de 23 ligt. Dat doen we bij klokkijken meestal wel; daar rekenen we meestal alles terug naar uren tussen de 0 en de 23. Maar met modulorekenen hoeft dat niet, zoals het laatste voorbeeldje al liet zien.

We kunnen op dezelfde manier ook modulo andere getallen dan 24 rekenen. Zo geldt $28 \equiv 2 \pmod{13}$, want het verschil tussen 28 en 2 is deelbaar door 13. En $-12 \equiv 18 \pmod{10}$, want het verschil tussen -12 en 18 is deelbaar door 10. We kunnen nu een algemene definitie geven voor rekenen modulo n, waarbij n een positief geheel getal is.

Definitie. Voor gehele getallen a en b en een geheel getal $n \geq 1$ zeggen we dat *a congruent is aan b modulo n* als $b - a$ een n-voud is, dus als $b - a = k \cdot n$ voor zekere gehele k. We noteren dit als volgt: $a \equiv b \pmod{n}$. Hierbij noemen we n de *modulus*.

Stel nu eens dat twee getallen a en b gegeven zijn waarvan je weet dat $a \equiv 6 \pmod{24}$ (a is bijvoorbeeld 30) en dat $b \equiv 2 \pmod{24}$ (b is bijvoorbeeld 50). Wat weet je dan van $a \cdot b$ modulo 24? Als we het gewoon uitrekenen, komen we in dit voorbeeld uit op $a \cdot b = 30 \cdot 50 = 1500$. Als we dat delen-met-rest door 24, krijg je $1500 = 62 \cdot 24 + 12$, dus $a \cdot b \equiv 12 \pmod{24}$. Hadden we dit antwoord nou kunnen voorspellen? Die 12 is precies $6 \cdot 2$, dus het lijkt erop dat je de twee getallen in een product (hier a en b) mag vervangen door de getallen waar ze congruent aan zijn (hier respectievelijk 6 en 2) als je toch alleen maar geïnteresseerd bent in de waarde van dit product modulo 24.

Werkt dat echt? Stel $a = 99$ en $b = 102$. Wat is dan $a \cdot b$ als we modulo 10 gaan rekenen? Door eerst het product te berekenen, vinden we dat $a \cdot b = 10098$ en dat is congruent aan 8 als je het modulo 10 bekijkt. Anderzijds weten we dat $a \equiv 9 \pmod{10}$ en $b \equiv 2 \pmod{10}$, en inderdaad $9 \cdot 2 = 18 \equiv 8 \pmod{10}$. Of we bekijken het zelfs nog anders: $a \equiv -1 \pmod{10}$ en $b \equiv 2 \pmod{10}$, en inderdaad $-1 \cdot 2 = -2 \equiv 8 \pmod{10}$. Het maakt wederom niet uit of we eerst de waardes modulo 10 nemen en dan het product, of juist andersom!

Deze eigenschap is inderdaad algemeen geldig. Voor het nemen van de som of het verschil geldt bovendien net zoiets. We zetten deze rekenregels en de bewijzen ervan even op een rij:

REKENREGELS

- Als $a \equiv b \pmod{n}$ en $a' \equiv b' \pmod{n}$, dan is $a + a' \equiv b + b' \pmod{n}$.
- Als $a \equiv b \pmod{n}$ en $a' \equiv b' \pmod{n}$, dan is $a - a' \equiv b - b' \pmod{n}$.
- Als $a \equiv b \pmod{n}$ en $a' \equiv b' \pmod{n}$, dan is $a \cdot a' \equiv b \cdot b' \pmod{n}$.

Eerst geven we het bewijs van de eerste regel. Stel dat $a \equiv b \pmod{n}$ en $a' \equiv b' \pmod{n}$. Dat betekent dus dat $b - a$ en $b' - a'$ beide n-vouden zijn. Het is duidelijk dat de som $(b - a) + (b' - a')$ dan ook een n-voud is. Maar dat is niets anders dan $(b + b') - (a + a')$. Omdat dit een n-voud is, geldt nu volgens de definitie dat $a + a' \equiv b + b' \pmod{n}$. En dat is precies wat we moesten bewijzen.

Voor de tweede rekenregel geldt net zo'n argument, maar dan met het verschil in plaats van de som. Voordat we naar de derde rekenregel gaan, bewijzen we eerst dit bijzondere geval:

- Als $a \equiv b \pmod{n}$ en c is een geheel getal, dan is $a \cdot c \equiv b \cdot c \pmod{n}$.

En hier het bewijs: stel dat $a \equiv b \pmod{n}$, dan is $b - a$ een n-voud. Dus dan is ook $c(b - a)$ een n-voud. Oftewel: $bc - ac$ is een n-voud en we concluderen dat $a \cdot c \equiv b \cdot c \pmod{n}$.

Nu passen we deze hulpregel toe om de derde rekenregel te bewijzen. Stel $a \equiv b \pmod{n}$ en $a' \equiv b' \pmod{n}$, dan geldt ook dat $a \cdot a' \equiv b \cdot a' \pmod{n}$ (beide zijden van de eerste congruentie maal a') en $b \cdot a' \equiv b \cdot b' \pmod{n}$ (beide zijden van de tweede congruentie maal b). We concluderen dat $a \cdot a' \equiv b \cdot a' \equiv b \cdot b' \pmod{n}$, dus $a \cdot a' \equiv b \cdot b' \pmod{n}$.

Nu we kunnen vermenigvuldigen modulo n, kunnen we natuurlijk ook machtsverheffen, als we de exponenten maar hetzelfde nemen.

- Als $a \equiv b \pmod{n}$ en k is een positief geheel getal, dan is $a^k \equiv b^k \pmod{n}$.

Dat komt omdat machtsverheffen niets anders is dan herhaald vermenigvuldigen, dus je kunt $k - 1$ keer de vermenigvuldigregel toepassen.

Delen gaat echter niet in het algemeen goed. We weten bijvoorbeeld dat $4 \equiv 28 \pmod{24}$, maar $2 \equiv 14$ gaat modulo 24 niet meer op. In dit geval zou je de modulus kunnen meedelen; dan klopt het wel: $2 \equiv 14 \pmod{12}$. Maar dat wil je soms niet en dat lukt ook niet altijd. Bijvoorbeeld $20 \equiv 140 \pmod{24}$ en delen door 10 gaat weer verkeerd (want het is niet zo dat $2 \equiv 14 \pmod{24}$). Bovendien is dat nu niet meer op te lossen door 24 dan ook maar te delen door 10.

Opgave 1. Verklaar de volgende 'rekenregels' door modulo 2 te werken:
- even + oneven = oneven;
- oneven + oneven = even;
- even · oneven = even;
- oneven · oneven = oneven.

Opgave 2. Bewijs dat $26^k - 2^k$ deelbaar is door 24 voor alle positieve gehele k.

Opgave 3. Op welk cijfer eindigt 3^{100}?

Opgave 4. Bewijs dat er geen gehele getallen m en n zijn zodanig dat $m^2 + n^2 = 10000003$.

DE IMO-OPGAVE Nu we weten wat modulorekenen inhoudt, kunnen we het proberen toe te passen bij IMO2009-1. De opgave luidt als volgt:

IMO2009-I. We bekijken verschillende gehele getallen $a_1, a_2, ..., a_k$ die allemaal tussen 1 en n zitten (waarbij 1 en n ook mee mogen doen). Gegeven is dat voor elke i van 1 tot en met $k - 1$ het getal $a_i(a_{i+1} - 1)$ deelbaar is door n. Bewijs dat het getal $a_k(a_1 - 1)$ niet deelbaar is door n.

Laten we eerst eens een voorbeeld bekijken om een beetje feeling met de opgave te krijgen. Neem bijvoorbeeld $n = 24$ en $k = 5$ en bekijk de vijf getallen 24, 8, 16, 4 en 13 (in die volgorde). Inderdaad is $24 \cdot 7$ deelbaar door 24, en hetzelfde geldt voor $8 \cdot 15$, $16 \cdot 3$ en $4 \cdot 12$. Volgens de opgave zou nu moeten gelden dat $13 \cdot 23$ niet deelbaar is door 24. Dat is inderdaad waar.

In de opgave is gegeven dat $a_i(a_{i+1} - 1) = a_i a_{i+1} - a_i$ deelbaar is door n voor i van 1 tot en met $k - 1$. Volgens de definitie van het modulorekenen staat hier niets anders dan dat $a_i \equiv a_i a_{i+1} \pmod{n}$ voor $i = 1, ..., k - 1$. (Voor het gemak laten we de indicatie '(mod n)' vanaf nu steeds weg; we rekenen steeds modulo n.) Dus $a_1 \equiv a_1 a_2$. Op zijn beurt

geldt weer dat $a_2 \equiv a_2a_3$. Als we dat links en rechts met a_1 vermenigvuldigen, krijgen we dat $a_1a_2 \equiv a_1a_2a_3$, wat gecombineerd met de eerste observatie leidt tot $a_1 \equiv a_1a_2a_3$. We kunnen vervolgens de a_3 vervangen door a_3a_4 en het is duidelijk dat we zo nog wel even kunnen doorgaan. De laatste stap die we toepassen is voor $i = k - 1$: dat $a_{k-1} \equiv a_{k-1}a_k$. Uiteindelijk vinden we hiermee: $a_1 \equiv a_1a_2a_3...a_k$.

We moeten laten zien dat $a_k(a_1 - 1) = a_ka_1 - a_k$ niet deelbaar is door n. Dat betekent dus dat we moeten laten zien dat $a_k \not\equiv a_ka_1$. Delen door a_k is helaas verboden. Maar als we de rechterkant uitrekenen met hetzelfde trucje als net, komt er: $a_ka_1 \equiv a_ka_1a_2 \equiv ... \equiv a_ka_1a_2...a_{k-1}$. Hier staat in feite dat $a_ka_1 \equiv a_1a_2a_3...a_k$. Van deze rechter uitdrukking hadden we hierboven al gezien dat hij congruent is aan a_1. Conclusie: $a_ka_1 \equiv a_1$, terwijl we juist moeten bewijzen dat $a_ka_1 \not\equiv a_k$. We zijn dus ook klaar als we kunnen bewijzen dat $a_1 \not\equiv a_k$. En deze laatste uitspraak is overduidelijk waar. Immers, twee verschillende getallen tussen 1 en n kunnen nooit congruent zijn modulo n, want ze verschillen hoogstuit $n - 1$.

BRONS EN ZILVER Met de techniek van modulorekenen lijkt dit plotseling een vrij eenvoudige opgave. Niets is minder waar. Deze oplossing is zeker elegant, maar je moet er maar net opkomen. Er zijn vele wegen in te slaan en als je eenmaal op een ander spoor zit, is het soms moeilijk daar weer van af te stappen.

Wouter en David hebben in Bremen deze aanpak gekozen en daarmee de opgave volledig opgelost. De vier andere Nederlandse teamleden daarentegen maakten in hun oplossingsstrategie gebruik van de priemfactorontbinding van n en van de grootste gemene deler van n met elk van de a_i'tjes. Raymond en Harm losten de opgave hiermee ook volledig op. Uiteindelijk hebben Harm en David hiervoor een eervolle vermelding ontvangen; Raymond en Wouter hebben wegens hun oplossingen voor andere opgaven zelfs een bronzen respectievelijk zilveren medaille gewonnen!

MEER INFORMATIE

www.wiskundeolympiade.nl: site van de Nederlandse Wiskunde Olympiade; op 30 januari is weer de eerstvolgende eerste ronde op je school.
www.imo2009.de: site van de 50ste Internationale Wiskunde Olympiade in Bremen, afgelopen zomer.
www.imo-official.org: site met daarop alle IMO-opgaven en resultaten over alle jaren. ■

ANTWOORDEN

1. $0 + 1 = 1$; $1 + 1 = 2 \equiv 0 \pmod 2$;
$0 \cdot 1 = 0$; $1 \cdot 1 = 1$.

2. We rekenen modulo 24. Er geldt dat $26 \equiv 2 \pmod{24}$, dus geldt ook $26^k \equiv 2^k \pmod{24}$.

3. Omdat we alleen maar geïnteresseerd zijn in het laatste cijfer, rekenen we modulo 10. Als we de eerste machten van 3 uitrekenen, zien we al snel dat $3^4 = 81 \equiv 1 \pmod{10}$.
Dat kunnen we goed gebruiken:
$3^{100} = (3^4)^{25} \equiv 1^{25} = 1 \pmod{10}$.
Het eindigt dus op een 1.

4. Stel dat zulke getallen m en n er wel waren, dan zou modulo 4 gelden dat $m^2 + n^2 \equiv 3$.
Een kwadraat is echter altijd 0 of 1 modulo 4: $0^2 = 0$; $1^2 = 1$; $2^2 = 4 \equiv 0$ en $3^2 = 9 \equiv 1$. De som van twee kwadraten is dus 0 of 1 plus 0 of 1, en daar kan alleen maar 0, 1 of 2 uitkomen modulo 4; niet 3.