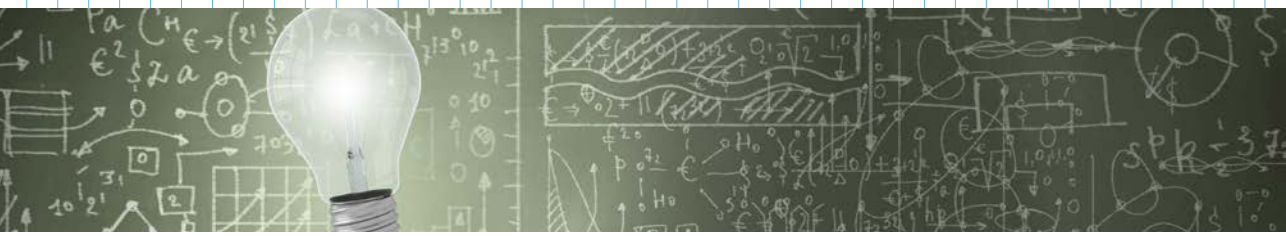
MODULO BENJAMIN

De redactie van Pythagoras ontving een brief van Willem Bouman, een Nederlands rekenwonder. Willem Bouman heeft 6 wereldrecords hoofdrekenen op zijn naam staan, waarvan het laatste dateert van 2022 toen hij uit het hoofd de derdemachtswortel trok uit het getal 7182 3714 0592 5428 0312 3253 9125 6146 6729 in 8 minuten 46 seconden! Hieronder kan je de volledige brief lezen. We geven tussendoor wat duiding.



door **Willem Bouman** en **Paul Levrie**

Voor wie mij nog niet kent: mijn naam is Willem Bouman, ik ben 85 jaar en Nederlands enige rekenwonder. In de kring van de toprekenaars sta ik bekend als "King of the Primes" en "Grandmaster of Modulo" vanwege mijn grote interesse in deze deelgebieden van de getallenwereld. Dat is de reden waarom Benjamin Magdalena, een rekenaar uit Spanje, mij de volgende vraag voorlegde.

$4^{80} \bmod 7 = ?$
$5^{68} \bmod 7 = ?$

HOE ZIT HET WEER MET DAT MODULOREKENEN?

In dit verhaal zullen we enkel werken met natuurlijke getallen. Twee natuurlijke getallen kan je door elkaar delen, en we doen dat hier op een speciale manier, we werken met een gehele deling. Als we bijvoorbeeld 17 delen door 5, dan kijken we hoeveel keer 5 in 17 past, dat is 3 keer – het quotiënt – en we houden dan nog 17 – 3 · 5 = 2 over – de rest. (Merk op dat de rest kleiner is dan 5, anders was het quotiënt minstens 4 geweest.)

Rekenen modulo een zeker getal m wil zeggen dat we alle getallen waarmee we werken voorstellen door de rest ervan bij deling door m. Zo'n getal is natuurlijk niet gelijk aan de rest ervan. Nemen we even het vorige voorbeeld: 17 = 3 · 5 + 2, 17 is niet gelijk aan 2, daarom voeren we een nieuwe notatie in. We zeggen dat 17 congruent is met 2 modulo 5 omdat de deling van 17 door 5 rest 2 geeft.

Meer algemeen zeggen we:
Twee getallen a en b zijn congruent modulo m als a en b dezelfde rest hebben bij deling door m.

Notatie: $a \equiv b \pmod{m}$.
De notatie $a \bmod m$ staat voor de rest bij deling van a door m.

Dus we noteren $17 \equiv 2 \pmod 5$ en ook $17 \bmod 5 = 2$. Maar we hebben bijvoorbeeld ook $17 \equiv 12 \pmod 5$.

OPGAVE 1

De rest bij deling van een natuurlijk getal door m kan enkel de waarden 0, 1, 2, …, m – 1 aannemen. Waarom?

OPGAVE 2

Ga zelf na met wat voorbeelden dat het volgende waar is:
als $a \equiv b \pmod{m}$ dan is m een deler van $a - b$.

Je kan dat ook zelf bewijzen: als a een m-voud is plus r (de rest), en b is ook een m-voud plus r (dezelfde rest), wat kan je dan zeggen over $a - b$?

Mijn antwoord was, met daarin onvermijdelijk nogal wat cijferreeksen, te beginnen met modulo 7. Ik begin met een getal en dan volgen de moduli 7 bij het machtsverheffen.

1 – 1 blijft 1
2 – 4 – 1
3 – 2 – 6 – 4 – 5 – 1
4 – 2 – 1
5 – 4 – 6 – 2 – 3 – 1
6 – 1

In deze tabel staan naast elkaar de resten modulo 7 van de opeenvolgende machten van de getallen links, tot je op de rest 1 stuit. Bijvoorbeeld voor 3:

$3^1 \bmod 7 = 3$ $3^2 \bmod 7 = 2$ $3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$ $3^5 \bmod 7 = 5$ $3^6 \bmod 7 = 1$

Merk op dat je bij de getallen van 1 tot 6 (in de rijtjes hierboven) steeds een 1 tegen–komt bij een macht die kleiner is dan 7.

Voor de volledigheid: deze kwestie heeft alles te maken met de kleine stelling van Fermat. Bij het wiskundig gedeelte van mijn antwoord kreeg ik de onmisbare hulp van mijn vriend Dr. B. de Weger, universitair hoofddocent aan de TU Eindhoven.

De kleine stelling van Fermat luidt: $a^{p-1} \equiv 1 \pmod{p}$ waarbij a een getal is groter dan of gelijk aan 1 en kleiner dan p en waarbij p een priemgetal is.

Aan de stelling op zich mankeert niets, die is onomstotelijk bewezen, ik ben helaas geen wiskundige, maar rekenaar. De Engelse rekencrack Robert Fountain vond voor mij de treffende omschrijving "number practitioner", getallen practicus.

DE KLEINE STELLING VAN FERMAT

Dit is wat de stelling uit 1640 zegt:
Als een natuurlijk getal a niet deelbaar is door het priemgetal p, dan geldt:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Merk op dat p een priemgetal is, dus een getal dat enkel deelbaar is door 1 en door zichzelf.

Willem Bouman neemt a kleiner dan p, maar dat is zelfs niet nodig.

We zien hierboven dat de mogelijke machten om bij priemgetal 7 als resultaat 1 te krijgen respectievelijk zijn 1, 2, 3, 6. En deze getallen zijn de delers van 6, wat $p - 1$ is. Dat was voor mij een interessante verrassing. Wel kon ik zien aankomen dat toen ik bij 6 (7) aankwam, dat het kwadraat hiervan 1 (7) is, en daarmee kom je bij de zesde macht dus ook op 1(7).

Met de notatie $a(7)$ bedoelt Willem Bouman a mod 7.

Merk op dat $6^2 = (7 - 1)^2 = 7 \cdot 7 - 2 \cdot 7 + 1$ en daarom is $6^2 \bmod 7 = 1$.

OPGAVE 3

Ga nu zelf na dat voor elk natuurlijk getal $m > 1$ geldt dat:
$(m - 1)^2 \bmod m = 1$.

>

We gebruiken in het vervolg nog een extra eigenschap van congruenties.

We illustreren ze met een voorbeeld: stel dat we 600 mod 7 willen berekenen. Dan kunnen we dat doen door 600 te delen door 7 en de rest te bepalen. Maar we kunnen dat ook sneller klaarkrijgen door gebruik te maken van de volgende eigenschap:

$a \equiv r \pmod m$ en $b \equiv s \pmod m$,
dan is $a \cdot b \equiv r \cdot s \pmod m$.

We kunnen deze eigenschap als volgt toepassen in dit geval:

$60 \equiv 4 \pmod 7$ en $10 \equiv 3 \pmod 7$,
dan is $600 \equiv 12 \pmod 7$,

en hieruit volgt dat 600 mod 7 = 12 mod 7 = 5. Erg handig om de rest te bepalen (modulo m) van een getal dat uit verschillende factoren bestaat! De bovenstaande eigenschap zegt dat je dit als volgt kunt doen:
Als je de rest wil bepalen (modulo m) bij een product, dan doe je dat voor elk van de factoren in dat product en je neemt van de resultaten het product (modulo m).

Het werkt ook met meer dan 2 factoren. Probeer het zelf eens uit op
600 = 25 · 8 · 3 mod 7.

Het antwoord op de vragen van Benjamin is:
in 4^{80} passen 13 × 6, dat is dus
$1^{13} = 1(7) + 4^2 = 2(7)$ en
in 5^{68} passen 11 × 6, dat is dus
$1^{11} = 1(7)$ en $5^2 = 4(7)$

Willem Bouman gaat voor de berekening bij 4^{80} als volgt te werk. De kleine stelling van Fermat zegt voor een macht van 4 dit:

$4^6 \equiv 1 \pmod 7$.

En dat willen we gebruiken! Daarom zoeken we het grootste veelvoud van 6 op dat kleiner is dan de exponent 80 : 80 = 6 · 13 + 2, en dus kunnen we schrijven:

$$4^{80} = 4^{6\cdot 13+2} = (4^6)^{13} \cdot 4^2 = \overbrace{4^6 \cdot 4^6 \cdot \cdots 4^6}^{13 \text{ factoren}} \cdot 4^2$$

door eigenschappen van machten te gebruiken. Nu hebben we 4^{80} geschreven als een product en kunnen we elk van de factoren modulo 7 doen, zoals we hierboven hebben gezien. Dit geeft m.b.v. de kleine stelling:

$$4^{80} = \overbrace{4^6 \cdot 4^6 \cdot \cdots 4^6}^{13 \text{ factoren}} \cdot 4^2 \equiv 1^{13} \cdot 2 = 2 \pmod 7$$

We gebruiken hier ook dat $4^2 \equiv 2 \pmod 7$. Klaar!

OPGAVE 4

Gebruik nu de kleine stelling van Fermat om 5^{68} mod 7 te berekenen.

Het kon niet uitblijven dat ik door weetgierigheid gedreven naar andere priemgetallen ging kijken, te beginnen bij $p = 11$.

Het resultaat:
1 – 1
2 – 4 – 8 – 5 – 10 – 9 – 7 – 3 – 6 – 1
3 – 9 – 5 – 4 – 1
4 – 5 – 9 – 3 – 1
5 – 3 – 4 – 9 – 1
6 – 3 – 7 – 9 – 10 – 5 – 8 – 4 – 2 – 1
7 – 5 – 2 – 3 – 10 – 4 – 6 – 9 – 8 – 1
8 – 9 – 6 – 4 – 10 – 3 – 2 – 5 – 7 – 1
9 – 4 – 3 – 5 – 1
10 – 1

Voor wiskundigen waarschijnlijk niet, maar voor mij is dit een leuke verrassing, want het beeld is hetzelfde: de delers van 10, immers p – 1, zijn 1, 2, 5 en 10 en dat zien we hier ook weer terug: de mogelijke machten zijn uitsluitend de delers van 10.

Hierdoor aangemoedigd ging ik verder met $p = 13$ met als resultaat:

1 – 1
2 – 4 – 8 – 3 – 6 – 12 – 11 – 9 – 5 – 10 – 7 – 1
3 – 9 – 1
4 – 3 – 12 – 9 – 10 – 1
5 – 12 – 8 – 1
6 – 10 – 8 – 9 – 2 – 12 – 7 – 3 – 5 – 4 – 11 – 1
7 – 10 – 5 – 9 – 11 – 12 – 6 – 3 – 8 – 4 – 2 – 1

8 – 12 – 5 – 1
9 – 3 – 1
10 – 9 – 12 – 3 – 4 – 1
11 – 4 – 5 – 3 – 7 – 2 – 9 – 8 – 10 – 6 – 1
12 – 1

We zien – natuurlijk! – ook hier hetzelfde beeld: het aantal mogelijkheden om tot 1 te komen vertegenwoordigt ook hier weer de delers van p – 1, nu 12, het zijn 1, 2, 3, 4, 6, 12.

Er is nog meer aardigs, bijvoorbeeld bij 13. We zien af van het laatste getal, 1 en nemen dan $2 \times 7 = 1(13)$; $4 \times 10 = 1(13)$, 12 moeten we kwadrateren, het resultaat is steeds 1(13). Nieuwsgierig geworden keek ik nog naar de volgende priemen: 17, 19, 23, 29, 37, 41, 59 en 61 met als steeds dezelfde bevindingen.

Willem Bouman merkt op dat de resten modulo 13 (behalve 0) twee per twee een product opleveren gelijk aan 1 modulo 13. Enkel bij rest 1 en 12 is dat anders, als je die kwadrateert, dan krijg je 1 modulo 13. Dit is eenvoudig te verklaren aan de hand van de kleine stelling van Fermat. We nemen hiervoor een van de 'lange lijnen' in de vorige tabel, omdat op deze lijn alle resten modulo 13 behalve 0 voorkomen:

	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
mod 13	2	4	8	3	6	12	11	9	5	10	7	1

Uit de kleine stelling van Fermat weten we dat $2^{12} \equiv 1 \pmod{13}$. En omdat we 12 kunnen schrijven als $12 = 1 + 11 = 2 + 10 = 3 + 9 = 4 + 8 = 5 + 7 = 6 + 6$, zegt Fermat dus dat modulo 13 geldt:

$2^1 \cdot 2^{11} \equiv 1$, $2^2 \cdot 2^{10} \equiv 1$, $2^3 \cdot 2^9 \equiv 1$,
$2^4 \cdot 2^8 \equiv 1$, $2^5 \cdot 2^7 \equiv 1$, $2^6 \cdot 2^6 \equiv 1$

Of nog, als we de factoren in de linkerleden modulo 13 nemen (zie tabel):

$2 \cdot 7 \equiv 1$, $4 \cdot 10 \equiv 1$, $8 \cdot 5 \equiv 1$,
$3 \cdot 9 \equiv 1$, $6 \cdot 11 \equiv 1$, $12 \cdot 12 \equiv 1$

OPGAVE 5

Uit het vorige volgt dadelijk dat $12! \equiv 12 \pmod{13}$. Hoe?
Herinner je dat $12! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$.
Meer algemeen geldt voor elk priemgetal p dat $(p-1)! \equiv p-1 \pmod{p}$.

Voor het geval dat de lezer een vraagstuk als beschreven tegenkomt, bijvoorbeeld hoeveel 10^{35} modulo 17 is, dan is dit de oplossing: p – 1 is hier 16. In 35 passen 2×16, de rest is 3. $10^3 = 1000 = 14(17)$ dus dit is de oplossing. Voor de goede orde: het getal 1 heb ik buiten beschouwing gelaten, maar ook p – 1. Als je dat kwadrateert is de uitkomst altijd 1 modulo wat dan ook. Er zijn nogal wat leuke verrassingen. Bijvoorbeeld $2^4 = 16(17)$ dus bij de 2^8 kom je al op 1(17). En $37 : 10^3 = 1000 = 1(37)$. En ook 26^3 is 1(37). p – 1 is wel het maximale aantal machten om op 1 mod p te komen, minder is zeer wel mogelijk. Maar altijd kom je uit op een deler van p – 1.

Zo vond ik ook dat bij modulo 71 de vijfde macht al 1 oplevert: $5^5 = 3125$ en 44×71 is 3124.

En modulo 31 rekenen met het getal 13 levert de volgende reeks op:
13–14–27–10–6–16–22–7–29–5–3–8–11–19–30–18–17–4–21–25–15–9–24–2–26–28–23–20–12–1.

En ziet u het ook: het derde getal is de mod 31 van de twee voorafgaande. 13 + 14 = 27; 14 + 27 = 41 en dat is 10(31) enz.

Voor dit speciale geval, namelijk de machten van 13 modulo 31, heb je inderdaad een merkwaardig iets: de volgende rest in het rijtje is de som van de vorige twee modulo 31. We kunnen dat eenvoudig verklaren. Neem bijvoorbeeld de drie opeenvolgende machten 13^7, 13^8, 13^9. Blijkbaar is het zo dat

$13^9 \equiv 13^8 + 13^7 \pmod{31}$.

>

Waarom? Om dit aan te tonen, gebruiken we het resultaat in Opgave 2. De formule is waar als 31 een deler is van $13^9 - (13^8 + 13^7)$. Maar $13^9 - (13^8 + 13^7) = 13^7 \cdot (13^2 - 13 - 1) = 13^7 \cdot 155$ met $155 = 5 \cdot 31$. Dus het klopt. En precies diezelfde methode kun je gebruiken voor elke drie opeenvolgende machten van 13.

OPGAVE 6

Niet enkel bij 13 en 31 heb je dit fenomeen. Tussen de rijtjes hierboven vind je nog twee andere gevallen. Ga zelf na dat het werkt (zoals bij de machten van 13) indien het tweede getal in zo'n rijtje precies 1 meer is dan het eerste getal. Waarom?

Ik wens u net zo veel plezier toe als ik zelf beleefd heb met modulo rekenen. Voor de enthousiastelingen heb ik de volgende vragen bedacht:

$10^{17} \bmod 41 = ?$
$2^{13} \bmod 17 = ?$

Ik ben benieuwd!!

TOEMAATJE

We weten nu precies genoeg om de kleine stelling van Fermat te bewijzen. We zullen dat doen voor $p = 13$. Dus we willen aantonen dat voor elk getal a dat geen veelvoud is van 13 geldt dat

$$a^{12} \equiv 1 \pmod{13}$$

We nemen daarvoor de volgende veelvouden van a:

$$1 \cdot a,\ 2 \cdot a,\ 3 \cdot a,\ \ldots,\ 12 \cdot a$$

Bewering: als we elk van deze 12 getallen delen door 13 en de rest bepalen, dan vinden we alle resten modulo 13 behalve 0.

Inderdaad:
- 0 komt niet voor als rest want omdat a geen veelvoud is van 13 (gegeven), is $i \cdot a$ voor $i = 1, 2, \ldots 12$ ook geen veelvoud van 13.
- de resten 1, 2, 3, …, 12 komen elk precies 1 keer voor. Er zijn 12 getallen en dus 12 resten ($\neq 0$). Stel dat 2 van die 12 getallen dezelfde rest geven bij deling door 13, neem bijvoorbeeld $2 \cdot a$ en $5 \cdot a$. Anders gezegd: stel dat $5 \cdot a \equiv 2 \cdot a \pmod{13}$. Dan betekent dit dat 13 een deler is van $(5 - 2) \cdot a$, maar dat is natuurlijk niet zo.

We berekenen nu het product modulo 13 van de 12 gegeven getallen. Dan volgt uit het vorige:

$(1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdot \cdots \cdot (12 \cdot a) \equiv$ (product van alle resten ($\neq 0$) modulo 13) (mod 13)

of nog, als we het linker lid uitwerken en het rechterlid uitschrijven.

$$12! \cdot a^{12} \equiv 12! \pmod{13}.$$

Omdat we met Opgave 5 weten dat $12! \equiv 12 \pmod{13}$, kunnen we dit laatste ook zo schrijven:

$$12 \cdot a^{12} \equiv 12 \pmod{13}.$$

We kunnen wat hier staat lezen als $12a^{12} - 12 = 12(a^{12} - 1)$ is een veelvoud van 13. Dat kan alleen zo zijn als $a^{12} - 1$ een 13-voud is, want 12 is het niet.

We kunnen dan besluiten:

$$a^{12} \equiv 1 \pmod{13}.$$

En dat wilden we ook bewijzen. <