Uitwerking puzzel 97-7 **Lieke de Rooij**
Vakantie puzzel: Goochelen **Wobien Doyer**

Misschien iets voor de laatste les voor de vakantie of voor vrienden en familie thuis.
Bij deze puzzel kan kennis van getal- en groepentheorie misschien helpen, maar is zeker niet noodzakelijk, maar modulo rekenen kan wel handig zijn. Wellicht een leuke toepassing bij wiskunde D?
Er liggen n kaarten op een voor een goochelaar bekende volgorde. Een toeschouwer trekt zonder dat de goochelaar dat kan zien een kaart en stopt die ergens in de stapel terug.
De goochelaar schudt de kaarten een aantal keer en bekijkt dan de kaarten . Weet hij vervolgens welke kaart de toeschouwer had getrokken?
Hij gebruikt daarvoor de volgende schudmethode: Splits de kaarten in twee gelijke of bijna gelijke stapeltjes en schuif ze om en om in elkaar. Dat kan door te zorgen dat of de bovenste kaart van het bovenste stapeltje daarna boven ligt, of de bovenste kaart van het onderste stapeltje komt boven. Zie afbeelding hoe een ervaren schudder dat doet. Het schijnt dat je dat met een goed spel kaarten snel kan leren. Omdat het resultaat vastligt, kan de goochelaar meestal bepalen welke kaart was getrokken.

Er zijn vier verschillende methoden van schudden:

n is even:
Methode A: De bovenste kaart wordt de op een na bovenste.
Methode B: De onderste en de bovenste kaarten blijven op hun plaats.

n is oneven
Methode C: De onderste kaart blijft onder.
Methode D: De bovenste kaart blijft boven.

Als de goochelaar meerdere keren schudt, gebruikt hij steeds dezelfde methode.
Om formules te kunnen formuleren moet je de kaarten nummers geven, maar dat hoeft niet per se voor elke methode bij 1 te beginnen.

Opgave 1a: Bepaal voor methode A een zo eenvoudig mogelijke formule/methode om te bepalen waar een gegeven kaart na i keer schudden terechtkomt.

Uitwerking opgave 1a: Het aantal kaarten is bij methode A even, de twee stapeltjes zijn dan even groot, dus $2k$ kaarten, in elk stapeltje k kaarten, vóór de eerste keer schudden in het ene nr 1, 2,....,k, in de ander $k+1$,....,$2k$.
Omdat de bovenste kaart de één na bovenste wordt is na de eerste keer schudden de volgorde van boven naar beneden:
$k+1$, 1, $k+2$, 2, $k+3$, 3...., $2k$, k. Conclusie: als een kaart op plaats x_0 ligt vóór het

schudden , dan ligt die kaart na de eerste keer schudden op plaats $x_1 = 2x_0 \bmod (2k + 1)$. Schudden we nog eens, dan komt die kaart op plaats $x_2 = 2x_1 \bmod (2k + 1) = 4x_0 \bmod (2k + 1)$.
Na *i* keer schudden ligt diezelfde kaart dan op plaats $x_i = x_0 \cdot 2^i \bmod (2k + 1)$.
Het ligt dus voor de hand om bij methode A de kaarten te nummeren beginnend met 1, zodat na *i* keer schudden de kaart met nummer *m* op plaats $m \cdot 2^i \bmod (2k + 1)$ ligt.

Opgave 1b: Als je een formule hebt voor methode A kun je daar een recept voor de andere drie methoden uit afleiden. Bepaal zo formules voor alle vier de methodes.

Uitwerking opgave 1b: Bij de methoden B, C en D zijn er kaarten die bij het schudden op dezelfde plaats blijven liggen. En omdat de goochelaar steeds dezelfde methode gebruikt blijven bij de volgende keer schudden opnieuw dezelfde kaarten op hun plaats. Bij methode B zijn dat de eerste en de laatste kaart, bij C is het de laatste kaart en bij D de eerste.

Het aantal kaarten dat wel beweegt tijdens het schudden is dus altijd even. Als we het aantal bewegende kaarten $2k$ noemen, dan bewegen de bewegende kaarten op precies dezelfde manier als bij methode A met $2k$ kaarten. Het is dan handig om bij methode B en D de eerste (stilliggende) kaart nummer 0 te geven, zodat de eerste bewegende kaart nummer 1 heeft. Bij methode C is de eerste kaart een bewegende kaart, die geven we nummer 1. Dan zijn de formules voor de bewegende kaarten precies hetzelfde als bij methode A.

Opgave 2a: Geef een methode om te berekenen hoe vaak je moet schudden (bij gegeven aantal kaarten *n*) met methode A tot de kaarten voor de eerste keer weer in de oorspronkelijke volgorde liggen, en leg uit dat het aantal keren dat je moet schudden nooit groter is dan *n*.

Uitwerking opgave 2a: We zagen in opgave 1a dat na *i* keer schudden de kaart met nummer *m* op plaats $m \cdot 2^i \bmod (2k + 1)$ ligt (met $2k = n$). Voor $m = 1$ dus: kaart 1 ligt na *i* keer schudden voor het eerst weer op z'n plaats als *i* het kleinste getal is waarvoor $2^i \bmod (2k + 1) \equiv 1$

We laten eerst zien dat er zo'n getal *i* bestaat:

Bij elke keer schudden komt er een kaart op plaats 1 terecht die daarna, met één of meer stappen achterstand, hetzelfde pad volgt als kaart 1.

Omdat het aantal kaarten eindig is, vormen alle kaarten die hetzelfde pad volgen een cykel. Het gezochte getal *i* is dus de lengte van die cykel en is $\leq n$.

Conclusie: er is een getal $i \leq n$ waarvoor geldt: na i maal schudden ligt kaart 1 voor de eerste keer weer op plaats 1.

Dat betekent (zoals we zagen in opgave 1a) dat $1 \cdot 2^i \bmod (2k + 1) \equiv 1$
Ook zagen we dat voor elke kaart *m* geldt: na *i* keer schudden ligt de kaart met nummer *m*

op plaats $m \cdot 2^i \bmod (2k+1)$, en met $2^i \bmod (2k+1) \equiv 1$ wordt dat $m \cdot 2^i \bmod (2k+1) \equiv m$. Daarom: als kaart 1 voor de eerste keer terug is op zijn oorspronkelijke plaats, dan liggen alle kaarten weer op hun oorspronkelijke plaats, en het aantal keren dat je daarvoor moet schudden is $i \leq n$

Om de waarde van *i* te bepalen voor een bepaalde waarde van *n* kun je tellen hoeveel kaarten hetzelfde pad volgen als kaart 1, bijvoorbeeld met *n* = 16:
Schrijf de volgorde van de kaarten aan het begin en na 1x schudden uit zoals hieronder.
Op de plaats van 1 komt 9, dus 9 volgt hetzelfde pad als 1: geef die 9 een kleurtje.
Op de plaats van 9 komt 13, ook 13 volgt dan hetzelfde pad, etc. tot je weer bij 1 uitkomt en tel het aantal , en dat is 8. Conclusie: bij 16 kaarten moet je 8x schudden.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8

Merk ook op dat de kaarten die in de eerste rij elkaars spiegelbeeld zijn dat in de tweede rij ook zijn (bijvoorbeeld 3 en 14 in de eerste rij derde van links en derde van rechts, in de tweede rij 6e van links en 6e van rechts). Dat is natuurlijk het directe gevolg van de manier van schudden, en dan blijft die symmetrie gedurende het hele schudproces bewaard.

Opgave 2b: Hebben ze dan daarvoor al in omgekeerde volgorde gelegen? Hoe kun je dat bepalen? En geef een voorbeeld.

Uitwerking opgave 2b: Als de kaarten na i maal schudden in omgekeerde volgorde liggen dan ligt in elk geval kaart 1 op plaats $2k$.

We zagen in opgave 2a dat dat gebeurt als kaart $2k$ hetzelfde pad volgt als kaart 1.

We hebben dan: na i maal schudden ligt kaart 1 op plaats $2^i \bmod (2k+1) \equiv 2k$
(en $2k \bmod 2k+1 \equiv -1$)

Omgekeerd, als $2^i \bmod (2k+1) \equiv -1$ dan geldt voor elke m:
$m \cdot 2^i \bmod (2k+1) \equiv m \cdot (-1) \equiv 2k+1-m$ en alle kaarten liggen in omgekeerde volgorde.

De kaarten komen dan en slechts dan in omgekeerde volgorde te liggen als kaart $2k$ hetzelfde pad volgt als kaart 1.

Dan is $2^{2i} \bmod (2k+1) \equiv (-1)^2 \equiv 1$, en liggen de kaarten na $2i$ keer schudden in de oorspronkelijke volgorde.

Of kaart $2k$ hetzelfde pad volgt, kunnen we aflezen uit een schema zoals we dat maakten in opgave 2a. Voor 16 kaarten zien we daarin dat 16 hetzelfde pad volgt als 1, dus komen de kaarten eerst in omgekeerde volgorde voordat ze terug zijn op hun plaats.

We kijken weer naar methode A:

In opgave 2 bepaalden we het aantal keren dat je moet schudden voordat bij een bepaald aantal kaarten n de kaarten weer in de oorspronkelijke volgorde liggen, en we zagen dat het aantal keren schudden nooit groter is dan n. Als het aantal keren dat geschud moet worden gelijk is aan n, dan noemen we het aantal keren schudden maximaal.
Het blijkt dat als $n + 1$ priem is de kaarten vaak na $n(= 2k)$ keer schudden voor het eerst weer op hun plaats liggen, en n is dan maximaal. Dat is echter niet altijd het geval, bijvoorbeeld voor $n = 42$, met $n + 1 = 43$ (priem).

Bij opgave 3 gebruiken we weer methode A:
Opgave 3a: Het aantal kaarten is dan even, met n=$2k$. Laat zien dat als $2k + 1$ geen priemgetal is het aantal keren schudden nooit maximaal kan zijn.
(Ook als opgave 3a niet lukt mag je natuurlijk bij de volgende vragen aannemen dat als het aantal keer schudden maximaal is, $2k + 1$ priem moet zijn.)

Uitwerking opgave 3a:
Bij opgave 3a werd door enkele inzenders de kleine stelling van Fermat ingezet, of de stelling van Euler waarbij de totiënt van n + 1 werd gebruikt. Dat geeft mooie oplossingen, maar we kozen er hier voor om dat niet te gebruiken, niet iedereen heeft deze kennis paraat en het was ook niet nodig.

We schrijven om een beeld te krijgen een voorbeeld uit waarin $2k + 1 = 9$ en geen priemgetal (het kleinste voorbeeld dat mogelijk is)
We geven in een tabel de volgorde van de 8 kaarten na 0 tot en met 6 keer schudden:

0	1	2	3	4	5	6	7	8
1	5	1	6	2	7	3	8	4
2	7	5	3	1	8	6	4	2
3	8	7	6	5	4	3	2	1
4	4	8	3	7	2	6	1	5
5	2	4	6	8	1	3	5	7
6	1	2	3	4	5	6	7	8

Je ziet direct in het schema dat er kolommen zijn waarin 6 en 3 elkaar afwisselen. Het aantal plaatsen waar kaart 1 kan liggen is dan kleiner dan n, en kan het aantal keren schudden nooit maximaal zijn. We moeten natuurlijk nog wel bewijzen dat dat altijd geldt als $2k + 1$ geen priemgetal is:

Als $2k + 1$ geen priemgetal is hebben we $2k + 1 = p \cdot q$, waarin p en q oneven >2,
Kaart 1 ligt dan na i keer schudden op plaats $2^i \bmod (2k + 1) = 2^i \bmod (p \cdot q)$, en kan alleen op plaats p terechtkomen als $2^i \bmod (p \cdot q) \equiv p$. Dan moet 2^i een factor p bevatten, en dat kan natuurlijk niet, want p is oneven.
Kaart 1 kan dus niet op alle n plaatsen komen, en dan is het aantal keren schudden niet maximaal.

Opgave 3b: Wat kun je zeggen over de volgorde van de kaarten na ½ $n = k$ keer schudden als het aantal keren schudden voor n maximaal is?

Uitwerking opgave 3b: Als het aantal keren schudden maximaal is dan komt kaart 1 op alle *n* plaatsen te liggen. Dat wil zeggen dat alle kaarten hetzelfde pad volgen als kaart 1, dus is er maar één cykel en alle kaarten bezoeken alle plaatsen. De lengte van die cykel moet dan $2k$ zijn.

We zagen in opgave 2b dat de kaarten in omgekeerde volgorde komen als kaart $2k$ hetzelfde pad volgt als kaart 1. Dat is zeker zo als het aantal keren schudden maximaal is.

Als dat gebeurt na *x* keer schudden, dan heeft kaart 1 het pad gevolgd van plaats 1 naar plaats $2k$ en kaart $2k$ heeft het pad gevolgd van plaats $2k$ naar plaats 1. Samen is dat de hele cykel, dus is $x=2k/2$.

We kunnen dus zeggen: Als het aantal keer schudden maximaal is dan liggen de kaarten na *k* keer schudden in de omgekeerde volgorde.

Opgave 3c: Geef een functie waarmee je zo eenvoudig mogelijk kan bepalen of voor een bepaalde *n* de volgorde na *k* keer schudden voldoet aan wat je vond in 3b.
(3c geeft een noodzakelijke voorwaarde voor *n* maximaal, maar bewijst niet dat dan *n* maximaal is)

Uitwerking opgave 3c: We kunnen bepalen of de kaarten in omgekeerde volgorde liggen na ½ $n = k$ keer schudden door te kijken of na ½ $n = k$ keer schudden kaart 1 op plaats $n = 2k$ ligt. Immers, volgens de formule die we vonden in opgave 1a is dat zo als:
$2^k \bmod (2k + 1) \equiv 2k \equiv -1$

Als je dit criterium gebruikt weten we echter niet zeker of *n* maximaal is. Misschien is er een $i < k$ die voldoet aan bovenstaande vergelijking. Zie hiervoor opgave **3d**.

(Zie voor de extra opgave **3d** het eind van de uitwerking.)

Met methode B liggen 52 kaarten na 8 keer schudden weer in de oorspronkelijke volgorde. Dat maakt methode B erg populair bij goochelaars!

Opgave 4: Bepaal het maximale aantal kaarten dat ook na precies 8 keer schudden weer voor het eerst in de oorspronkelijk volgorde liggen met methode A. Geef ook een bewijs van je resultaat.

Uitwerking opgave 4:
We zoeken een zo groot mogelijke waarde van *n* waarbij de lengte van de cykel die kaart 1 doorloopt gelijk is aan 8.
Dan moet $2^8 \bmod (2k + 1) \equiv 1$ met zo groot mogelijke waarde van *k*.
Dat is het geval als $2k = 2^8$, dus met 256 kaarten

En dan de goocheltruc: De goochelaar hoeft daarvoor niet zo vaak te schudden dat de kaarten weer in de oorspronkelijke volgorde liggen.
Opgave 5a: Kan de goochelaar altijd precies weten welke kaart werd getrokken? Wanneer niet?

Uitwerking 5a: In elk geval niet als de kaart op dezelfde plaats wordt teruggelegd als waar hij vandaan komt. En als de kaart 1 hoger of 1 lager wordt teruggestoken, kan de goochelaar nooit weten welk van de 2 verwisselde kaarten getrokken is.

Opgave 5b: Een goochelaar oefent om de juiste kaart te vinden ook als de kaarten nog niet in de oorspronkelijke volgorde liggen. Hij gebruikt een beperkt aantal kaarten, alleen schoppen aas, en schoppen 2 tot en met schoppen 10.
Nadat een kaart is getrokken en weer terug is gestopt, schudt hij een onbekend aantal keer en ziet het resultaat: schoppen aas, 8, 5, 3, 2, 9, 6, 4, 7, 10.
Bepaal welke kaart was getrokken en hoe vaak er is geschud, en dat met zo min mogelijk rekenwerk en/of geheugen van de goochelaar. Leg uit hoe je erachter bent gekomen.

Uitwerking 5b:
Aan het resultaat is te zien dat methode B is gebruikt: kaart 1 is bovenop blijven liggen en kaart 10 onderaan

We schrijven de rijen uit met 10 kaarten met methode B, zonder verplaatste kaart.
Daaronder het resultaat na het schudden waarbij een kaart verplaatst is:

Aantal keer schudden	1	2	3	4	5	6	7	8	9	10
1	1	6	2	7	3	8	4	9	5	10
2	1	8	6	4	2	9	7	5	3	10
3	1	9	8	7	6	5	4	3	2	10
4	1	5	9	4	8	3	7	2	6	10
5	1	3	5	7	9	2	4	6	8	10
6	1	2	3	4	5	6	7	8	9	10

Resultaat:	1	8	5	3	2	9	6	4	7	10

Als een kaart is weggenomen en ergens anders is teruggestoken zijn er 2 mogelijkheden: de weggenomen kaart is vóór of achter zijn oorspronkelijke plek teruggestoken.
Tussen de plaats waar de kaart is getrokken en de plaats waar de kaart is terug gestoken, zijn alle kaarten 1 naar links of naar rechts opgeschoven. De kaarten daarvoor en daarna zijn onveranderd.
We kijken daarom naar grote getallen en kleine getallen die gelijk zijn in één van de rijen uit het schema en de onderste reeks.
Dan zien we dat 1, 2, 8, 9 en 10 gelijk zijn in het resultaat en in rij 2.
Verder zien we dat op de plaatsen van 4, 5, 6 en 7 in rij 2 in het resultaat 3, 4, 5 en 6 zijn.
En waar in rij 2 een 3 staat, staat in het resultaat een 7.
Conclusie: de 7 zit op de plaats waar de 3 zou zitten zonder verandering van de volgorde, dus de 7 is ingestoken tussen de 2 en de 3, en 3 tot en met de 6 zijn een plaats naar rechts opgeschoven. 7 is dan de getrokken kaart.

Voor de goochelaar is bovenstaande redenering lastig uit zijn hoofd te doen, maar hij weet iets dat wij niet wisten: hij heeft zelf geschud en hij weet dat hij 2 keer geschud heeft.

Na 2 keer schudden zonder dat een kaart is verplaatst is er een grote regelmaat in de reeks: (behalve 1 en 10) eerst alle even getallen van groot naar klein, dan alle oneven getallen van groot naar klein.
Als de goochelaar de kaarten één voor één bekijkt kan hij achtereenvolgens de volgende conclusie trekken:
Hij ziet eerst kaart 1, dan kaart 8: die zijn op hun plaats gebleven.
Dan ziet hij kaart 5. Daar had 6 moeten liggen, en kaart 5 ligt op de plaats van kaart 6. Dus is de getrokken kaart vóór kaart 5 ingestoken.
Daarna kaart 3, en daar had 4 moeten liggen, en kaart 3 ligt op de plaats van kaart 4. Dus is de getrokken kaart vóór kaart 3 ingestoken.
Dan kaart 2. Die is op z'n plaats gebleven , dus de getrokken kaart is tussen kaart 2 en 3 ingestoken.
Kaart 9 is op z'n plaats gebleven. De getrokken kaart is dus <9
Kaart 6 ligt op de plaats van kaart 7. Kaart 7 is er dus tussenuit getrokken, en moet de getrokken kaart zijn.
Ter contrôle nog:
Kaart 4 ligt op de plaats van kaart 5. De getrokken kaart is dus voor kaart 4 ingestoken (wisten we al).
Kaart 7 ligt op de plaats van kaart 3. Kaart 7 is dus getrokken en ingevoegd voor kaart 3 (wisten we al)
Kaart 10 is op z'n plaats gebleven. Klopt, de veranderingen zitten tussen 7 en 3.

Opgave 3d: Dit is een extra opgave buiten de puntentelling. Als 3c geen uitsluitsel geeft of het aantal keren schudden maximaal is, hoe kun je daar dan wel uitsluitsel over krijgen?

Uitwerking opgave 3d:
Als we in opgave 3c geen uitsluitsel kregen, dan weten we dat de kaarten na ½ $n = k$ keer schudden in omgekeerde volgorde liggen en na $n = 2k$ keer schudden in de oorspronkelijke volgorde. Als dat de eerste keer is dat dat gebeurt, dan is het aantal keren schudden maximaal, dus we moeten uitsluiten dat het al eerder is gebeurd.
Stel dat de eerste keer dat ze in omgekeerde volgorde lagen was na x keer schudden. Dan lagen ze in de oorspronkelijke volgorde na $2x$ keer schudden. Nadat ze in dezelfde volgorde liggen gaat het zich herhalen, dus liggen ze in de oorspronkelijke volgorde na $2x$, $4x$, $6x$, $8x$ etc. keer schudden en na x, $3x$, $5x$, $7x$, $9x$ etc. keer schudden in de omgekeerde volgorde. We kunnen ook zeggen: voor elke gehele waarde van $j \geq 0$ liggen de kaarten in omgekeerde volgorde na $(2j + 1) \cdot x$ keer schudden (maar we kennen de waarden van j en x niet).
We constateerden dat ze na k keer schudden in omgekeerde volgorde lagen, dus moet $k = (2j + 1) \cdot x$.
We kennen de waarde van k, en dan is het aantal mogelijkheden voor j en x beperkt.
En omdat de kaarten steeds in omgekeerde volgorde liggen bij x, $3x$, $5x$ etc. keer schudden is het alleen de eerste keer na k keer schudden als $j = 0$.

Als k geen oneven delers heeft dan is $j = 0$, en was het bij k keer schudden de eerste keer dat ze zo lagen, en is dus het aantal keren schudden maximaal.
Als k wel oneven delers heeft moeten we verder zoeken.

We bekijken een voorbeeld: $n = 42$ dus $k = 21$:

1): geldt $2^k \bmod (2k+1) \equiv -1$?
Ja, $2^{21} \bmod (42+1) \equiv 43 \equiv -1$
Het zou dus maximaal kunnen zijn, maar meer onderzoek is nodig.
2): heeft k oneven delers?
Ja, dus meer onderzoek is nodig
3): Als $k = (2j+1) \cdot x$ met $k = 21$ zijn er 4 mogelijkheden:
$2j+1 = 21$ en $x = 1$ of $2j+1 = 7$ en $x = 3$ of $2j+1 = 3$ en $x = 7$ of
$2j+1 = 1$ en $x = 21$.
Alleen als $x = 21$ is het aantal keren schudden maximaal,
We moeten dus uitsluiten dat *x* is 1, 3 of 7.
Als $x = 1$ dan liggen de kaarten in omgekeerde volgorde na 1, 3, 5, 7 etc. keer schudden.
Als $x = 3$ dan liggen de kaarten in omgekeerde volgorde na 3, 9, 15, 21 etc. keer schudden.
Als $x = 7$ dan liggen de kaarten in omgekeerde volgorde na 7, 21, 35 etc. keer schudden.

We weten al dat ze na 21 keer schudden in omgekeerde volgorde liggen.
Als ze niet in omgekeerde volgorde liggen na 3 of 7 keer schudden, dan weten we dus dat het na 21 keer schudden voor de eerste keer is dat ze in omgekeerde volgorde liggen.

We bepalen dus $2^3 \bmod (42+1) \equiv 8$
en $2^7 \bmod (42+1) \equiv 42 \equiv -1$
$n = 42$ is dus niet maximaal, want na 7 keer schudden liggen de kaarten in omgekeerde volgorde en dus na 14 keer schudden in de oorspronkelijke volgorde.

In bovenstaand voorbeeld zien we hoe we zekerheid kunnen krijgen als *k* het product is van twee verschillende oneven priemgetallen (3 en 7). We willen graag een algoritme voor het algemene geval.
Bij $n = 42$ was het nodig om $2^i \bmod (42+1)$ te bepalen voor $i = 21, 7$ en 3. Dat zijn alle oneven delers van 42. Maar dat hoeft bij grotere aantallen oneven delers niet.
We weten dat als na *x* keer schudden de kaarten voor de eerste keer in omgekeerde volgorde liggen, dat ook zo is voor alle oneven veelvouden van *x*.
Daaruit volgt dat als *r* een oneven deler van *k* is en na *r* keer schudden liggen de kaarten niet in omgekeerde volgorde, dan is *r* geen oneven veelvoud van *x*.
Het loont dus om de waarden van *r* waarvoor we $2^r \bmod (2k+1)$ bepalen zo groot mogelijk te kiezen, want daarmee sluiten we veel mogelijke waarden van *x* uit.

Het algoritme om te bepalen of voor $n = 2k$ het aantal keren schudden maximaal is:

1) geldt $2^k \bmod (2k+1) \equiv -1$?
   Als dat niet zo is is het aantal keren schudden niet maximaal
2) Als het wel zo is en k heeft geen oneven delers dan is het aantal keren schudden maximaal
3) Als $2^k \bmod (2k+1) \equiv -1$ en k heeft oneven delers gaan we als volgt verder:
   Laat $p_1, p_2, p_3, \ldots p_m$ de oneven priemdelers van *k* zijn. Kies voor elke p_s:
   $i = k/p_s$ (de grootst mogelijke delers van *k* dus!) en bepaal of
   $2^i \bmod (2k+1) \equiv -1$
   Als dat waar is het aantal keren schudden voor $n = 2k$ niet maximaal.
   Als het niet waar is ga dan verder met de volgende p_s

Als je klaar bent en de modulowaarde was geen enkele keer -1 dan is het aantal keren schudden voor $n = 2k$ maximaal. We gaan dat bewijzen.

Als $2^k \bmod (2k+1) \equiv -1$ dan liggen de kaarten na *k* maal schudden in omgekeerde volgorde. Als dat de eerste keer is dat dat gebeurt, dan is het aantal keren schudden maximaal. We bewijzen dat als in bovenstaand algoritme geen enkele keer -1 is gevonden dan is er geen getal $i < k$ waarvoor $2^i \bmod (2k+1) \equiv -1$.

Bewijs uit het ongerijmde:

Stel er zijn getallen *i* kleiner dan *k* waarvoor na *i* keer schudden de kaarten in omgekeerde volgorde liggen.

Laat *x* het kleinste getal zijn waarbij dat gebeurt. Dan is dus
$x < k$ en $2^x \bmod (2k+1) \equiv -1$.

We zagen eerder dat dan de kaarten ook in omgekeerde volgorde liggen na x, $3x$, $5x$, $7x$, $9x$, … keer schudden en dat $k = (2j+1) \cdot x$.

Omdat $x < k$ bevat $(2j+1)$ minstens één oneven priemfactor p die dus ook in k zit.
En omdat $k = (2j+1) \cdot x$ geldt $\frac{k}{p} = \left(\frac{2j+1}{p}\right) \cdot x$ waarin p een deler is van $2j+1$.
Dus is k/p een oneven veelvoud van x en dus liggen de kaarten na k/p keer schudden in omgekeerde volgorde.

Maar omdat p een oneven deler is van k is k/p één van de waarden waarvoor we in het algoritme hebben getest. Toen constateerden we dat na k/p maal schudden de kaarten **niet** in omgekeerde volgorde liggen want we hadden $2^i \bmod (2k+1) \equiv -1$

Dat is dus een tegenspraak en dus zijn er geen getallen *i* kleiner dan *k* waarvoor na *i* keer schudden de kaarten in omgekeerde volgorde liggen. QED.
Het algoritme klopt dus.