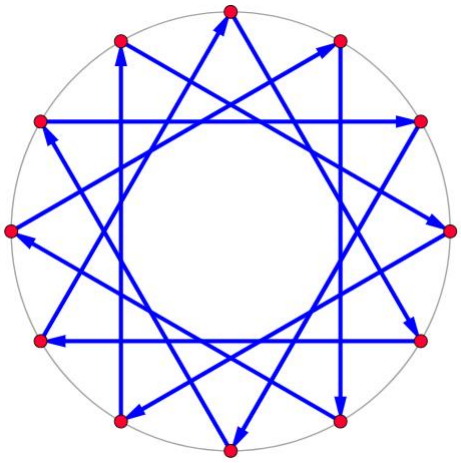
Pijlenklokken

1 Inleiding



In bovenstaande tekening zie je 12 rode punten. Er staan blauwe pijlen van elk rood punt naar een ander rood punt 4 plaatsen verder op de cirkel. Een dergelijke afbeelding noemen we een *pijlenklok* . In dit artikel gaan we dergelijke pijlenklokken bestuderen. Een paar onderzoeksvragen die we ons kunnen stellen in het begin van het onderzoek zijn:

- Hoe ziet de tekening eruit als we niet 4 maar 5 of 6 plaatsen opschuiven?
- Wat als we niet starten met 12 maar 13 rode punten of een ander aantal?
- Wat zijn de eigenschappen van de bekomen figuur?
- Wat gebeurt er als we een andere formule gebruiken om de blauwe pijlen te construeren?

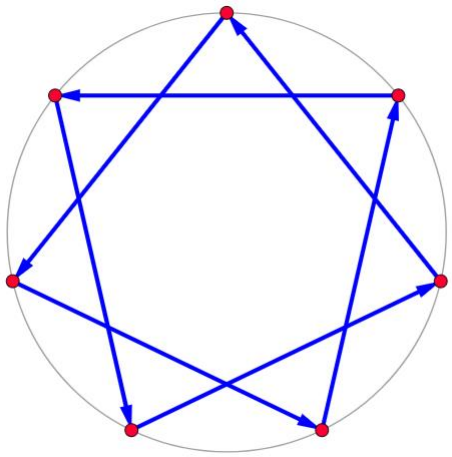
2 Notaties, definities en begrippen

2.1 Notaties en definities

- We noteren de n rode punten met de getallen $0, 1, 2, \cdots, n-1$. Het bovenste rode punt op de cirkel komt overeen met het getal 0, en dan gaan we verder met de klok mee: $1, 2, \cdots$.
- De verzameling van alle rode punten noteren we met $\mathbb{Z}_n$.
- Een rood punt waar de knop van een blauwe pijl uitkomt heet een *doelpunt* . Een rood punt waar de staart van een blauwe pijl vanuit gaat heet een *startpunt* .

2.2 Permutaties

- Een afbeelding in $\mathbb{Z}$, zodat in elk element juist 1 blauwe pijl toekomt en juist 1 blauwe pijl vertrekt, noemen we een *permutatie* . Een voorbeeld:



We noteren de permutatie met

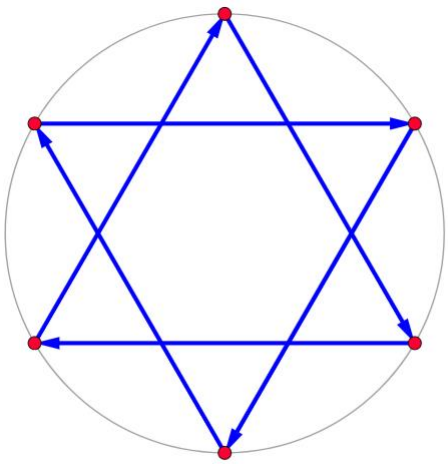
$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

De bovenste lijn geeft de startpunten weer en de onderste lijn de overeenkomstige doelpunten. Een andere mogelijkhied om te op te schrijven is: $(0, 5, 3, 1, 6, 4, 2)$. We bedoelen hiermee dat 0 afgebeeld wordt op 5. Dan wordt 5 afgebeeld op 3 en zo verder tot op het laatst 2 terug afgebeeld wordt op 0. Deze notatie noemen we de *cykelnotatie* . De

lengte van een cykel is het aantal elementen van haar baan. Een cykel van lengte k wordt ook wel een k-cykel genoemd. Hier hebben we een 7-cykel.

- Als er geen misverstand kan ontstaan dan mag je in e cykelnotatie ook de komma's weglaten : (0531642)

- Onderstaande pijlenklok is ook een permutatie, die genoteerd wordt door:$(0, 2, 4)(1, 3, 5)$. De permutatie bestaat uit twee 3-cykels.



- Een punt dat op zichzelf wordt afgebeeld, noemen we een *vast punt* van de permutatie. In de cykelnotatie wordt dat gewoon weggelaten. De permutatie

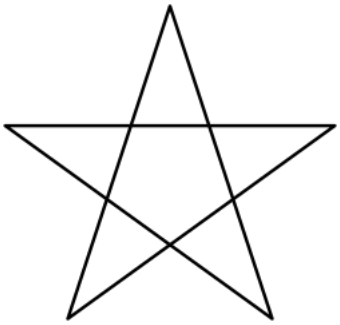
$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

wordt dan genoteerd als $(0, 2)$. In de pijlenklok zien we dan een baluwe lus bij 1 en 3.

2.3 Veelhoeken

- Een regelmatige veelhoek is een veelhoek waarvan de zijden alle dezelfde lengte hebben, en alle hoeken aan elkaar gelijk zijn. Een regelmatige n-hoek is dus opgebouwd uit n paarsgewijs met elkaar verbonden even lange lijnstukken die n keer dezelfde hoek met elkaar maken. De hoekpunten liggen op een cirkel. een regelmatige n-hoek wordt genoteerd door $\{n\}$ of $\{\frac{n}{1}\}$. Zo is bijvoorbeeld $\{4\}$ een vierkant.

- Een regelmatige sterveelhoek, genoteerd als $\{\frac{n}{m}\}$ met $1 < m < \frac{n}{2}$ is een figuur met n even lange zijden en n even grote hoeken. Een regelmatige sterveelhoek wordt gevormd door bepaalde diagonalen van een regelmatige n-hoek; steeds wordt een hoekpunt verbonden met de hoekpunten m hoekpunten verderop. Bij de notatie $\{\frac{n}{m}\}$ betekent het eerste getal het aantal hoekpunten en het tweede getal geeft weer dat de sterveelhoek zich m keer rond haar centrum windt. Hierbij zijn n en m onderling ondeelbaar zijn. Een voorbeeld is het pentagram, genoteerd door $\frac{5}{2}$:



2.4 Modulorekenen

- Stel $a, b, m \in \mathbb{Z}, m > 1$. Indien a en b bij deling door m dezelfde rest geven, d.w.z. indien $a - b = cm$ voor zekere $c \in \mathbb{Z}$, heten a en b congruent modulo m. We noteren $a \equiv b$ mod m

- Eigenschappen :

  1. Als $a \equiv b$ mod m en $b \equiv c$ mod m, dan is $a \equiv c$ mod m.
  2. Als $a \equiv b$ mod m en $c \equiv d$ mod m, dan is $a + c \equiv b + d$ mod m.
  3. Als $a \equiv b$ mod m en $n \in \mathbb{N}$, dan is $a^n \equiv b^n$ mod m.
  4. Als $a \equiv b$ mod m dan is voor elke $c \in \mathbb{Z}$: $ac \equiv bc$ mod m.
  5. Als $a \equiv b$ mod m en $c \equiv d$ mod m, dan is $ac \equiv bd$ mod m.

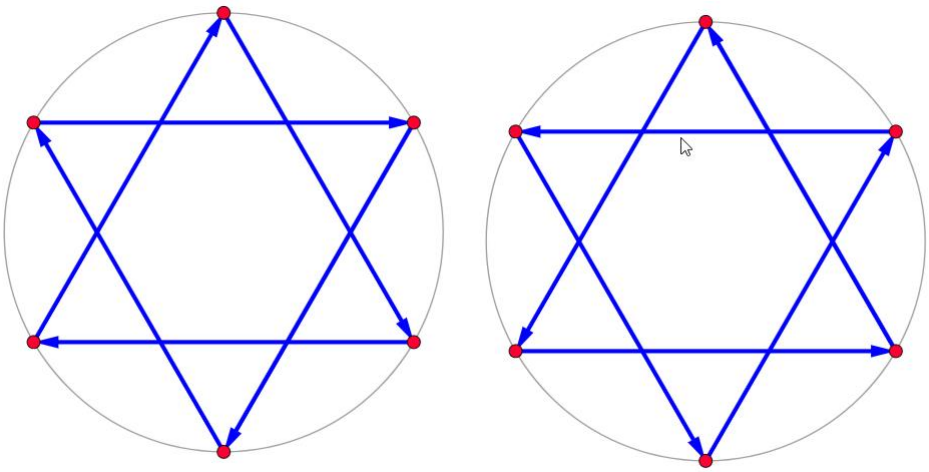
3 De afbeelding $f(x) = x + b$

Voor we met het onderzoek beginnen kunnen we een aantal eenvoudige zaken opmerken:

- Het onderzoek heeft eigenlijk pas zin voor $n \geq 5$. Voor kleinere waarden van n is er weinig te onderzoeken.

- Als $b = 0$ dan wordt elk rood punt op zichzelf afgebeeld en krijgen we een pijlenklok met n lussen.

- Voor $b = i$ en $b = n - i$ krijgen we dezelfde pijlenklok, maar wordt de richting van de pijlen gewoon omgekeerd. Zie onderstaand voorbeeld voor $n = 6$, $b = 2$ en $b = 4$:



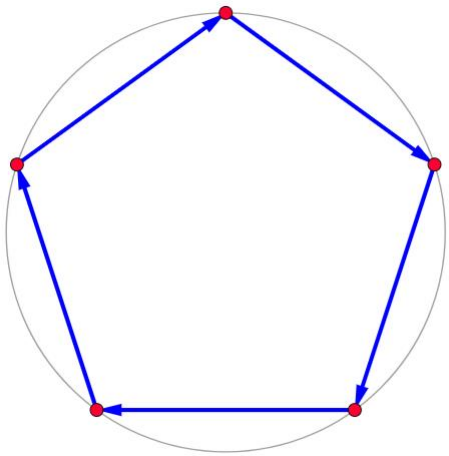
  De verklaring hiervoor is dat $n - i \equiv -i \bmod n$, zodat de afbeeldingen $f(x) = x + i$ en $f(x) = x - i$ zijn: ofwel i plaatsen doorschuiven met de klok mee ofwel n plaatsen doorschuiven naar links.

- Door vorige opmerkingen moeten wij, bij de studie van $f(x) = x + b$, enkel rekening houden met natuurlijke waarden van b waarvoor geldt dat $1 \leq b \leq \frac{n}{2}$.

3.1 Empirisch onderzoek voor n=5

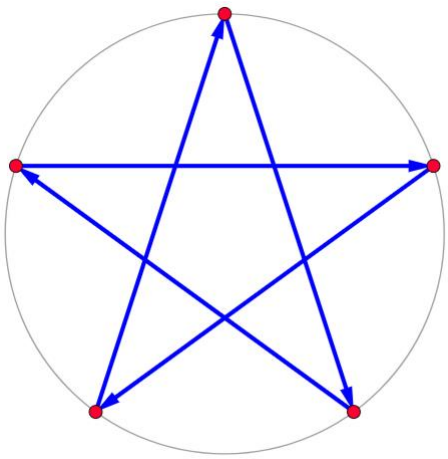
Er zijn twee mogelijkheden voor b, namelijk $b = 1$ en $b = 2$.

3.1.1 b=1



- De afbeelding f is de permutatie: (01234).
- De pijlenklok is de regelmatige vijfhoek $\{\frac{5}{1}\}$.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.72°$ met $k \in \{0, 1, 2, 3, 4\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 5 *symmetrie assen* : de middellijnen door elk rood punt.

3.1.2 b=2

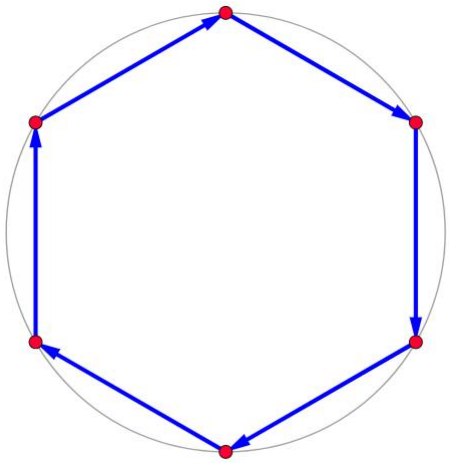


- De afbeelding f is de permutatie : (02413).
- De pijlenklok is een regelmatige ster vijfhoek $\{\frac{5}{2}\}$: het pentagram.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.72°$ met $k \in \{0, 1, 2, 3, 4\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 5 symmetrie assen: de middellijnen door elk rood punt.
- Binnenin zie je een regelmatige vijfhoek ontstaan.

3.2 Empirisch onderzoek voor n=6

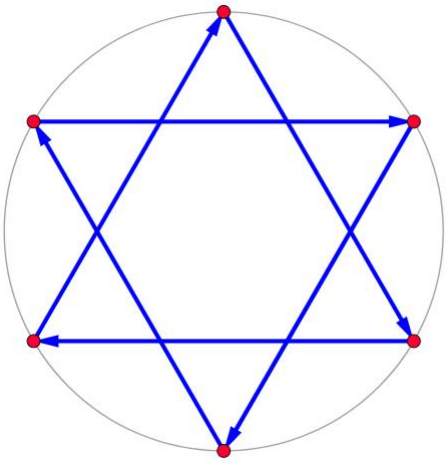
Er zijn drie mogelijkheden voor b, namelijk $b = 1$, $b = 2$ en $b = 3$.

3.2.1 b=1



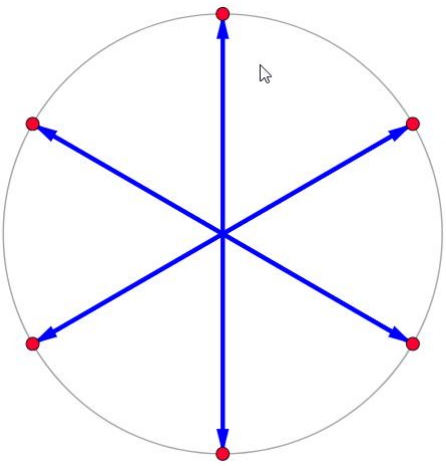
- De afbeelding f is de permutatie: (012345).
- De pijlenklok is de regelmatige zeshoek $\{\frac{6}{1}\}$
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.60°$ met $k \in \{0, 1, 2, 3, 4, 5\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 6 *symmetrie assen* : de 3 middellijnen door elk rood punt en 3 middellijnen die loodrecht staan op de middens van de zijden van de zeshoek.

3.2.2 b=2



- De afbeelding f is de permutatie : $(024)(135)$.
- De pijlenklok bestaat uit 2 gelijkzijdige driehoeken.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.60°$ met $k \in \{0, 1, 2, 3, 4, 5\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 6 symmetrie assen: de 3 middellijnen door elk rood punt en 3 middellijnen door de snijpunten van de twee driehoeken.
- Binnenin zie je een regelmatige zeshoek ontstaan.

3.2.3 b=3

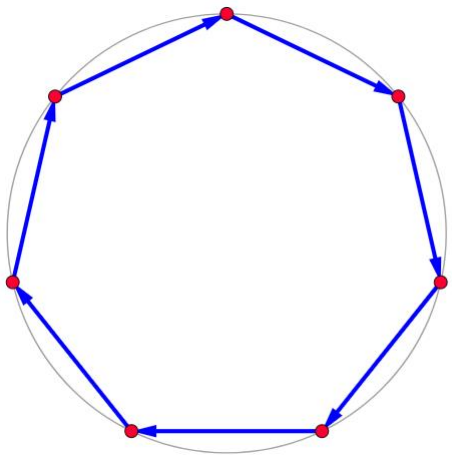


- De afbeelding f is de permutatie (03)(14)(25).
- De pijlenklok bestaat uit 3 lijnstukken.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.60°$ met $k \in \{0, 1, 2, 3, 4, 5\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 6 symmetrie assen: de 3 middellijnen door elk rood punt en 3 middellijnen die de deellijnen zijn van de gegeven lijnstukken.

3.3 Empirisch onderzoek voor n=7

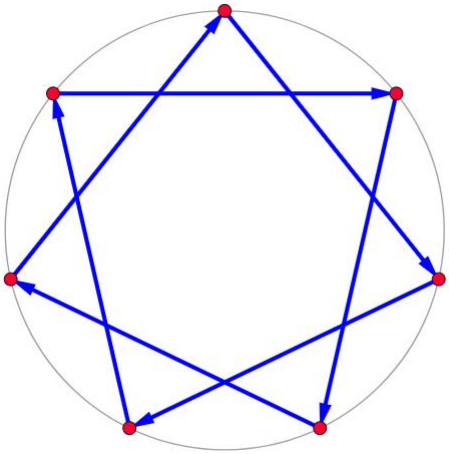
Er zijn drie mogelijkheden voor b, namelijk $b = 1$, $b = 2$ en $b = 3$.

3.3.1 b=1



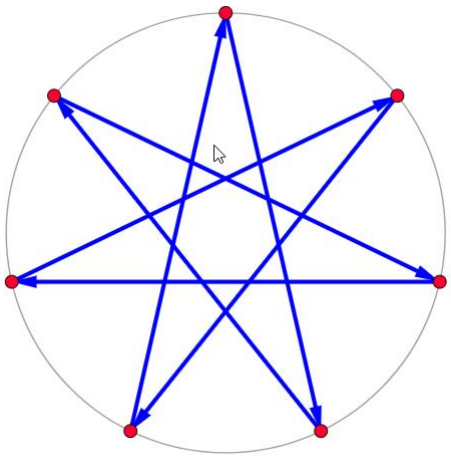
- De afbeelding f is de permutatie: (0123456).
- De pijlenklok is de regelmatige zeshoek $\{\frac{7}{1}\}$
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.\left(\frac{360}{7}\right)^{\circ}$ met $k \in \{0, 1, 2, 3, 4, 5, 6\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 7 *symmetrie assen* : de 7 middellijnen door elk rood punt .

3.3.2 b=2



- De afbeelding f is de permutatie : (0246135).
- De pijlenklok is een regelmatige ster zevenhoek $\{\frac{7}{2}\}$.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.\left(\frac{360}{7}\right)^{\circ}$ met $k \in \{0, 1, 2, 3, 4, 5, 6\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 7 *symmetrie assen* : de 7 middellijnen door elk rood punt .
- Binnenin zie je een regelmatige zevenhoek ontstaan.

3.3.3 b=3

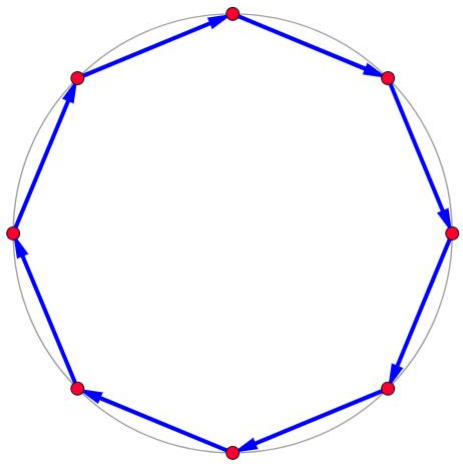


- De afbeelding f is de permutatie (0362514).
- De pijlenklok is een regelmatige ster zevenhoek $\{\frac{7}{3}\}$: het heptagram.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.\left(\frac{360}{7}\right)^{\circ}$ met $k \in \{0, 1, 2, 3, 4, 5, 6\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 7 *symmetrie assen* : de 7 middellijnen door elk rood punt .
- Binnenin zie je een regelmatige zevenhoek ontstaan.

3.4 Empirisch onderzoek voor n=8

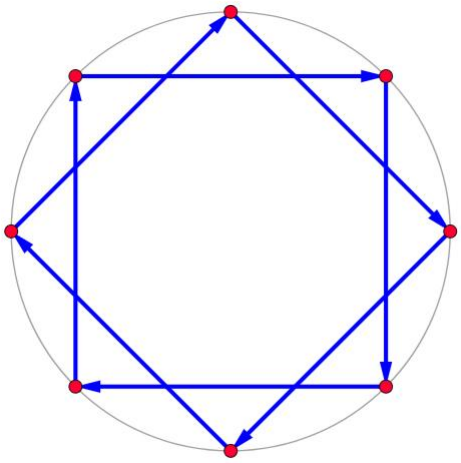
Er zijn drie mogelijkheden voor b, namelijk $b = 1$, $b = 2$, $b = 3$ en $b = 4$

3.4.1 b=1



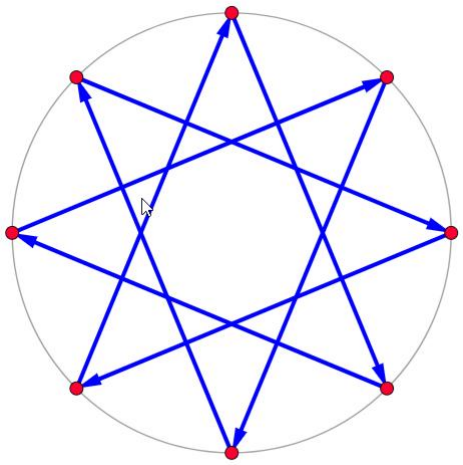
- De afbeelding f is de permutatie: (01234567).
- De pijlenklok is de regelmatige achthoek $\{\frac{8}{1}\}$
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.45)^{\circ}$ met $k \in \{0, 1, 2, 3, 4, 5, 6, 7\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 8 *symmetrie assen* : de 4 middellijnen door elk rood punt en 4 middellijnen die loodrecht staan op de middens van de zijden van de achthoek. .

3.4.2 b=2



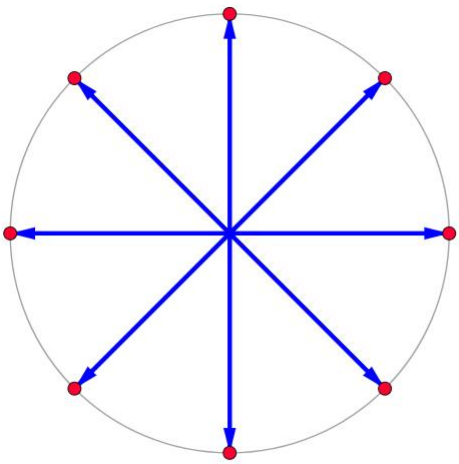
- De afbeelding f is de permutatie : $(0246)(1357)$.
- De pijlenklok bestaat uit 2 vierkanten.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.45°$ met $k \in \{0, 1, 2, 3, 4, 5, 6\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 8 *symmetrie assen* : de 4 middellijnen door elk rood punt en 4 middellijnen door de snijpunten van de twee vierkanten.
- Binnenin zie je een regelmatige achthoek ontstaan.

3.4.3 b=3



- De afbeelding f is de permutatie (03614725).
- De pijlenklok is een regelmatige ster achthoek $\{\frac{7}{3}\}$: het octagram.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.45°$ met $k \in \{0, 1, 2, 3, 4, 5, 6\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 8 *symmetrie assen* : de 4 middellijnen door elk rood punt en 4 middellijnen door de punten waar de zijden van de ster achthoek elkaar snijden.
- Binnenin zie je een regelmatige achthoek ontstaan.

3.4.4 b=4



- De afbeelding f is de permutatie (04)(15)(26)(37).
- De pijlenklok bestaat uit 4 lijnstukken.
- De pijlenklok is *draaisymmetrisch* met als centrum het middelpunt van de cirkel van de rode punten en als hoeken : $k.45°$ met $k \in \{0, 1, 2, 3, 4, 5, 6, 7\}$.
- De pijlenklok is *lijnsymmetrisch* . Er zijn 8 symmetrie assen: de 4 middellijnen door elk rood punt en 4 middellijnen die de deellijnen zijn van de gegeven lijnstukken.

3.5 Algemene resultaten

Stelling 3.1. *$f(x) = x + b$ is altijd een permutatie van $\mathbb{Z}_n$. Er zijn dus altijd n doelpunten.*

Bewijs. Uit elk rood punt vertrekt juist 1 blauwe pijl. Dit is logisch want er is maar 1 mogelijke uitkomst bij een som. In elk rood punt komt er hoogstens 1 blauwe pijl toe. Want, als $f(x_1) = f(x_2)$ dan is $x_1 + b = x_2 + b$. Omdat b een invers element heeft voor de optelling, volgt hieruit dat $x_1 = x_2$. In elk rood punt komt er ook minstens 1 bauwe pijl toe. Neem nu het rood punt y dan is $f(y - b) = y - b + b = b$, dus er komt een blauwe pijl toe in y en die vertrekt vanuit $y - b$. □

Stelling 3.2. *$f(x) = x + b$ heeft enkel vaste punten als $b = 0$. En in dat geval is elk rood punt een vast punt.*

Bewijs. Voor een vast punt geldt: $f(x) = x$ of $x + b = x$. Hieruit volgt dat $b = 0$. □

Stelling 3.3. *Als b een deler is van n, dan bestaat de pijlenklok uit b regelmatige $\frac{n}{b}$-hoeken.*

Bewijs. Stel $n = b.d$. De baan van 0, door het herhaaldelijk toepassen van de functie f, is: $b, 2b, 3b, \cdots$. Omdat $d.b \equiv 0 \bmod n$ eindigt de baan na d stappen terug bij 0 en krijgen we een regelmatige d-hoek. Neem nu een rood punt dat niet in de baan van 0 ligt en herhaal de procedure. De baan van , bijvoorbeeld a is dan : $a + b, a + 2b, a + 3b, \cdots$. Omdat $a + db \equiv a \bmod n$, vinden we opnieuw een regelmatige d-hoek. We kunnen deze procedure uiteindelijk b keer herhalen. □

Stelling 3.4. *Als b en n onderling ondeelbaar zijn, dan is de pijlenklok een regelmatige n-hoeken of een regelmatige n-ster.*

Bewijs. Als b en n onderling ondeelbaar zijn, dan is hun grootste gemene deler gelijk aan 1. Volgens de stelling van Bezout bestaan er dan gehele getallen r en s, zodat $rb + sn = 1$. Neem nu 0 als startpunt. Dan is $rb \equiv 1 \bmod n$. Dit betekent dat de baan van 0 na r stappen in 1 terechtkomt. Maar je kan ook schrijven dat voor een willekeurig rood punt k geldt dat $k = (kr)b + (ks)n$ of $k \equiv (kr)b \bmod n$. Dus ook k ligt op de baan van 0. Met andere woorden elk rood punt ligt op de baan van het punt 0 en dus krijgen we een baan die uiteindelijk terug eindigt in 0. Hieruit volgt het gestelde. □

Stelling 3.5. *Als de grootste gemene deler van b en n gelijk is aan d en als b geen deler is van n, dan bestaat de pijlenklok uit d regelmatige $\frac{n}{d}$ sterhoeken.*

Bewijs. Veronderstel dat $n = dn'$ en $b = db'$, met b' en n' onderling ondeelbaar. We werken per groepje van d punten. Er zijn n' van dergelijke groepjes. Als nieuwe functie, op die groepjes , nemen we $f(x) = x + b'$. Omdat b' en n' onderling ondeelbaar zijn, kunnen we stelling 3.4 toepassen. Omdat b geen deler is van n, is $b' \neq 1$ en is de pijlenklok een regelmatige sterveelhoek met $n' = \frac{n}{d}$ zijden. Voor elk rood punt van een groepje heb je dan zo een regelmatige sterveelhoek. □

Stelling 3.6. *Als n een priemgetal is dan vindt je, door $b \neq 0$ te laten variëren, 1 regelmatige n-hoek en $\frac{n-3}{2}$ regelmatige n- sterveelhoeken.*

Bewijs. Als n een priemgetal is dan zijn er in $\mathbb{Z}_n$ $n-1$ getallen die onderling ondeelbaar zijn met n, namelijk $1, 2, \cdots, n-1$. Voor $b = 1$ en $b = n-1$ is de pijlenklok een regelmatige n-hoek en voor de andere waarden vinden we een regelmatige sterveelhoek. Als we pijlenklokken die in een andere richting worden afgelegd, als gelijk beschouwen, vinden we nog $\frac{n-3}{2}$ sterveelhoeken. □

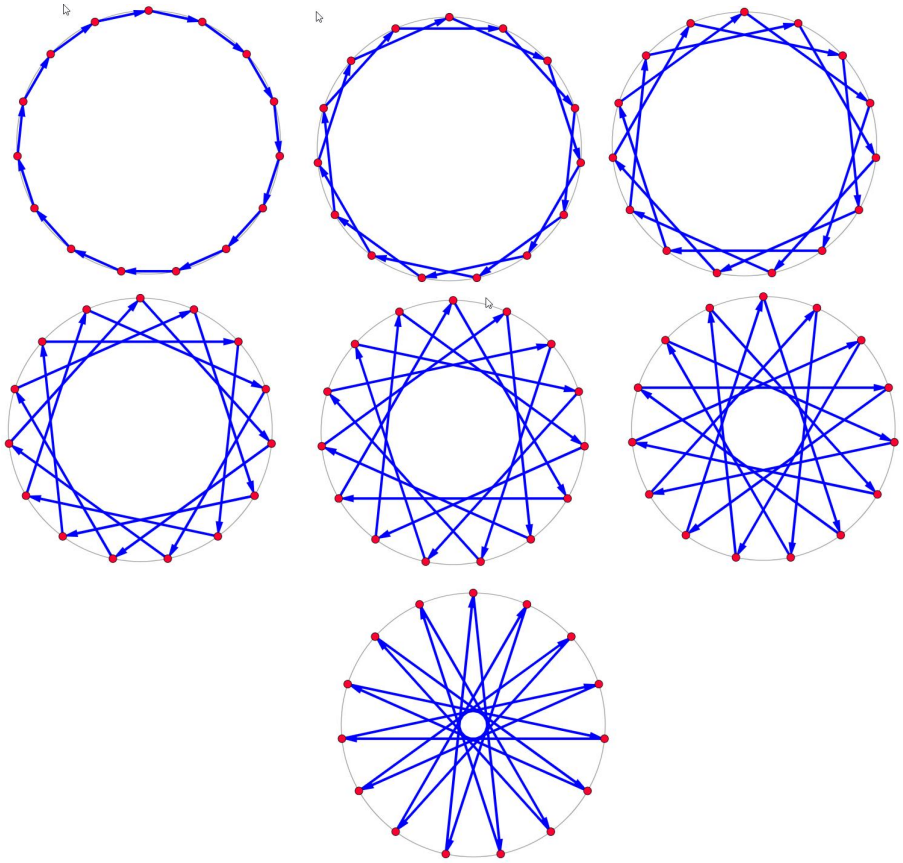
Stelling 3.7. *Als n even is, dan is er een pijlenklok die bestaat uit $\frac{n}{2}$ middellijnen. We noemen dit een ontaarde pijlenklok.*

Bewijs. De baan die in 0 vertrekt is na twee stappen terug in 0, want $2.\frac{n}{2} \equiv 0 \bmod n$. Pas nu stelling 3.3 toe. $\square$

De symmetrie eigenschappen volgen uit de symmetrieën van een regelmatige n-hoek. Er zijn steeds n draaisymmetrieën en n lijnsymmetrieën.

We werken, als voorbeeld, $n = 15$ uit:

b	pijlenklok
1	een regelmatige 15-hoek
2	een regelmatige 15-sterveelhoek
3	drie regelmatige vijfhoeken
4	een regelmatige 15-sterveelhoek
5	vijf gelijkzijdige driehoeken
6	drie regelmatige 5-sterveelhoeken
7	een regelmatige 15-sterveelhoek



4 De afbeelding $f(x) = ax + b$

Omdat de vermenigvuldiging in $\mathbb{Z}_n$ nu een belangrijke rol gaat spelen, is het belangrijk te weten welke getallen een inverse hebben voor die vermenigvuldiging. Verder veronderstellen we steeds dat $a \neq 1$.

Stelling 4.1. *Als a en n onderling ondeelbaar zijn dan heeft a een uniek invers element voor de vermenigvuldiging in $\mathbb{Z}_n$.*

Bewijs. Het invers element van a is de unieke oplossing van de vergelijking $ax \equiv 1 \bmod n$. Stel dat $ax_1 \equiv ax_2 \bmod n$, dan is $a(x_1 - x_2) \equiv 0 \bmod n$. Dus is $a(x_1 - x_2)$ deelbaar door n. Maar a en n zijn onderling ondeelbaar. Bijgevolg is n een deler van $x_1 - x_2$ of $x_1 \equiv x_2 \bmod n$. Met andere woorden: de vermenigvuldiging van alle elementen van $\mathbb{Z}_n$ met a levert n verschillende uitkomsten. Er is dus zeker een x, die vermenigvuldigd met a, de waarde 1 aanneemt. Hiermee is het gestelde bewezen. □

De verzameling van de elementen van $\mathbb{Z}_n$ die onderling ondeelbaar zijn met n, wordt genoteerd door $\mathbb{Z}_n^\times$. Het aantal elementen in die verzameling wordt bepaald door de *indicator of totiënt* van n. Notatie: $\varphi(n)$. Een paar eigenschappen:

- $\varphi(m.n) = \varphi(m)\varphi(n)$.
- Als n priem is, dan is $\varphi(n) = n - 1$.
- Als $n = p^k$ met p een priemgetal, dan is $\varphi(n) = (p-1)p^{k-1}$.

4.1 a en n zijn onderling ondeelbaar

Stelling 4.2. *Als a en n onderling ondeelbaar zijn, dan is $f(x) = ax + b$ altijd een permutatie van $\mathbb{Z}_n$. Er zijn dus altijd n doelpunten.*

Bewijs. Uit elk rood punt vertrekt juist 1 blauwe pijl. Dit is logisch want er is maar 1 mogelijke uitkomst bij een som of product. In elk rood punt komt

er hoogstens 1 blauwe pijl toe. Want, als $f(x_1) = f(x_2)$ dan is $ax_1 + ba = x_2 + b$. Omdat b een invers element heeft voor de optelling, volgt hieruit dat $ax_1 = ax_2$. Omdat a een invers element heeft voor de vermenigvuldiging, volgt hieruit dat $x_1 = x_2$. In elk rood punt komt er ook minstens 1 bauwe pijl toe. Neem nu het rood punt y dan is $f(a^{-1}(y-b)) = a(a^{-1}(y-b)) + b = y - b + b = y$, dus er komt een blauwe pijl toe in y en die vertrekt vanuit $a^{-1}(y-b)$. □

4.1.1 $f(x) = -x + b$

Stelling 4.3. *$f(x) = -x + b$ heeft 0,1 of 2 vaste punten.*

Bewijs. x is een vast punt van f als $-x+b \equiv x \bmod n$ of $2x \equiv b \bmod n$. Als n oneven is, dan heeft 2 een invers element voor de vermenigvuldiging en is heeft f juist 1 vast punt: $2^{-1}b$. Als n even is en b oneven dan zijn er geen vaste punten. Als n en b beiden even zijn , dan zijn er steeds 2 vaste punten, voor $x = \frac{b}{2}$ en $x = n + \frac{b}{2}$. □

Stelling 4.4. *$f(x) = -x + b$ is involutief of $f(f(x)) = x$.*
Met andere woorden: elke blauwe pijl is een heen en weer pijl.

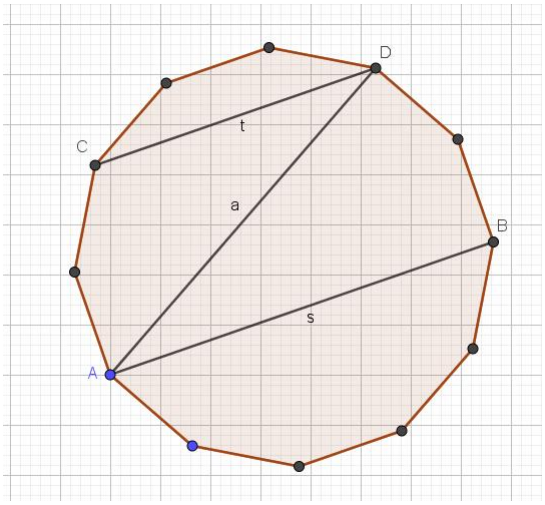
Bewijs. $f(f(x)) = f(-x + b) = -(-x + b) + b = x - b + b = x$.

□

Als we een blauwe pijl als een rechte beschouwen, kunnen we nagaan wanneer deze rechten evenwijdig zijn. Voor de eenvoud spreken we van evenwijdige pijlen. Om verwarring te vermijden zullen we punten op de cirkel niet met elementen van $\mathbb{Z}_n$ aanduiden, maar wel met letters. De optelling in $\mathbb{Z}_n$ dragen we over op de letters. Een lus kan je beschouwen als een pijl waar vertrekpunt en doelpunt samenvallen. Als lijn hierdoor kan je dan de raaklijn tekenen aan de gegeven cirkel.

Stelling 4.5. *Een pijl door A en B is evenwijdig met een pijl door C en D als en slechts als $A + B \equiv C + D \mod n$.*

Bewijs. Als de boog tussen A en C en de boog tussen B en D even groot is, dan zijn de omtrekshoeken $\widehat{ADC}$ en $\widehat{DAB}$ gelijk. Volgens de eigenschap van de verwisselende binnenhoeken is dan AB evenwijdig met CD.

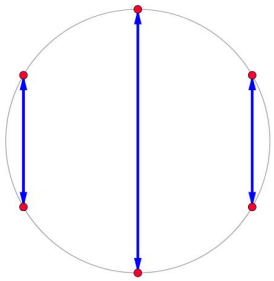


De pijlen tussen A en B en tussen C en D zijn dus evenwijdig als $B - D \equiv C - A \mod n$ of $A + B \equiv C + D \mod n$. □

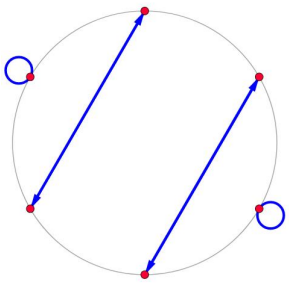
Stelling 4.6. *De pijlenklok $f(x) = -x + b$ bestaat uit evenwijdige pijlen.*

Bewijs.

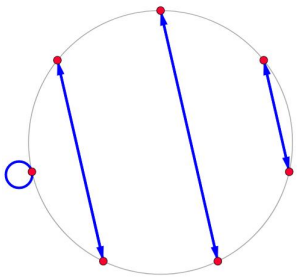
- Als n even is en b oneven, wordt elk even rood punt $2x'$ afgebeeld op $b - 2x'$. De som van die twee rode punten is constant gelijk aan b. Dus zijn alle $\frac{n}{2}$ lijnen evenwijdig. Zie voorbeeld met $n = 6$ en $b = 3$:



- Als n en b allebei even zijn, bestaan er 2 vaste punten, voor $x = \frac{b}{2}$ en $x = n + \frac{b}{2}$. Net zoals in vorig deel is de som van twee rode punten die op elkaar worden afgebeeld constant gelijk aan b. Als we in een vast punt de som maken van het punt met zichzelf komen we ook , modulo n, aan de waarde b. Dus alle $\frac{n-2}{2}$ blauwe lijnen en de 2 raaklijnen in de vaste punten zijn allemaal evenwijdig. In het totaal heb je $\frac{n}{2} + 1$ evenwijdige lijnen. Zie voorbeeld met $n = 6$ en $b = 4$:



- Als n oneven is heb je 1 vast punt : $2^{-1}b$. Als we in het vast punt de som maken van het punt met zichzelf komen we ook aan de waarde b, net zoals bij de andere blauwe lijnen. Dus alle $\frac{n-1}{2}$ blauwe lijnen en de ene raaklijn in het vaste punt zijn allemaal evenwijdig. In het totaal heb je $\frac{n+1}{2}$ evenwijdige lijnen. Zie voorbeeld met $n = 7$ en $b = 3$:



$\square$

4.1.2 $f(x) = ax$

We zien duidelijk dat 0 steeds een vast punt is. Zijn er nog andere?

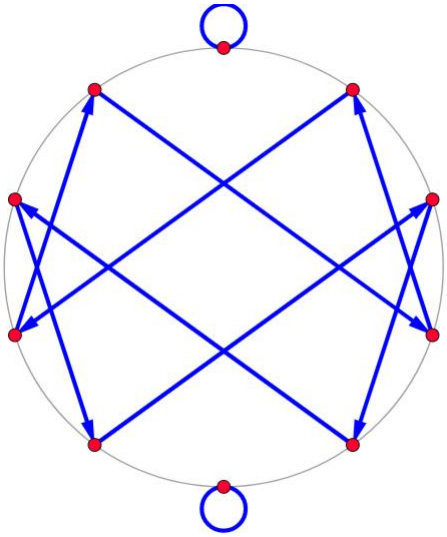
Stelling 4.7. *De pijlenklok $f(x) = ax$ heeft d vaste punten, waarbij $d = \ ggd(a-1, n)$.*

Bewijs. x is een vast punt van f als $ax \equiv x \bmod n$ of $(a-1)x \equiv 0 \bmod n$. Omdat d de grootste gemene deler is van $a-1$ en n, kunnen we stellen dat $a-1 = d.r$ en $n = d.s$, waarbij r en s onderling ondeelbaar zijn. De op te lossen vergelijking wordt dan $drx \equiv ds \bmod n$. Deze vergelijking heeft juist d oplossingen: $0, s, 2s, \cdots,$
$(d-1)s$. □

Stelling 4.8. *Veronderstel dat de orde van a in $\mathbb{Z}_n^\times$ gelijk is aan m. Dan bestaat de pijlenklok van $f(x) = ax$, buiten de lussen, uit $\frac{n-d}{m}$ veelhoeken met m zijden. (Een veelhoek met 2 zijden is een lijnstuk, met andere woorden: een blauwe heen en weer pijl)*

Bewijs. 0 is zeker al een vast punt. 1 is dat zeker niet, omdat we hier veronderstellen dat $a \neq 1$. De baan van 1 is dan: $1, a, a^2, \cdots, a^{m-1}$. We komen terug in 1 terecht want $a^m = 1$. Neem een ander element dat geen lus is en niet in de baan zit van 1. Noem dit element p. Dan is de baan van p gegeven door $p, ap, a^2p, \cdots, a^{m-1}$. je komt terug in p, want $a^m p = p$. Blijf dit doen tot alle elementen zijn opgebruikt. Je krijgt $\frac{n-d}{m}$ veelhoeken met m zijden. □

Neem bijvoorbeeld $n = 10$ en $a = 7$. dan is $d = 2$ en $s = 5$. Er zijn er 2 vaste punten: 0 en 5. Verder is $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$. De permutatie f is dan gelijk aan: (1793)(2486). Er zijn 2 veelhoeken met 4 zijden.



We zien in bovenstaande tekening dat de zijden van de twee vierhoeken twee aan twee evenwijdig zijn. Hoe komt dat? Noteer $d' = \text{ggd}(a+1, n)$.

Stelling 4.9. *De pijlenklok $f(x) = ax$ heeft $\frac{n}{d'}$ evenwijdige lijnen, waarbij $d' = ggd(a+1, n)$.*

Bewijs. Als de blauwe pijl die vertrekt uit x evenwijdig moet zijn met de pijl die uit y vertrekt, dan moet $x + ax \equiv y + ay$ of $(a+1)(x-y) \equiv 0 \bmod n$. Veronderstel dat $a + 1 = r'd'$ en $n = d's'$, dan krijgen we $r'(x-y) \equiv 0 \bmod s'$.Omdat $'$ en s' onderling ondeelbaar zijn, moet $x \equiv y \bmod s'$. Zo krijgen we s' evenwijdige paren. □

4.1.3 $f(x) = ax + b$ met $b \neq 0$

Stelling 4.10. *De pijlenklok $f(x) = ax + b$ heeft d vaste punten, waarbij $d = ggd(a-1, n)$, als d een deler is van b. Anders zijn er geen vaste punten.*

Bewijs. x is een vast punt van f als $ax+b \equiv x \bmod n$ of $(a-1)x \equiv -b \bmod n$. Omdat d de grootste gemene deler is van $a-1$ en n, kunnen we stellen

dat $a-1=d.r$ en $n=d.s$, waarbij r en s onderling ondeelbaar zijn. Veronderstel verder dat $b=k.d$. De op te lossen vergelijking wordt dan $drx \equiv (s-k)d \bmod n$. We kunnen dit vereenvoudigen tot $rx \equiv -k \bmod s$. Deze vergelijking heeft d oplossingen omdat r en s onderling ondeelbaar zijn:$-r^{-1}k, -r^{-1}k+s, -r^{-1}k+2s, \cdots, -r^{-1}k+(d-1)s$. $\square$

Bestuderen we nu de mogelijke pijlen in een pijlenklok van $f(x)=ax+b$ met b een veelvoud van d, de grootste gemene deler avn $a-1$ en n. Neem een willekeurig rood punt x. Na twee stappen ben je bij $a(ax+b)+b=a^2x+(a+1)b$. Na drie stappen kom je terecht bij $a^3x+(a^2+a+1)b$. Algemeen: na p stappen ben je in het rood punt $a^px+(a^{p-1}+a^{p-2}+\cdots+a+1)b$. De pijlenklok vertoont een veelhoek met p zijden als $a^px+(a^{p-1}+a^{p-2}+\cdots+a+1)b \equiv x \bmod n$. Hieruit volgt dat $(a^p-1)x+(a^{p-1}+a^{p-2}+\cdots+a+1)b \equiv 0 \bmod n$ of $(a^{p-1}+a^{p-2}+\cdots+a+1)\{(a-1)x+b\} \equiv 0 \bmod n$. Stel $n=ds$, $a-1=rs$ en $b=ks$, dan kan je vorige equivalentie herleiden tot:

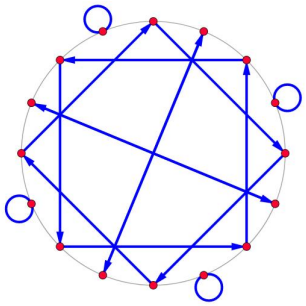
$$(a^{p-1}+a^{p-2}+\cdots+a+1)\{rx+k\} \equiv 0 \bmod s$$

Een voorbeeld:

Neem $f(x)=5x+b$ met $n=16$. Dan is $d=$ ggd$(a-1,n)=4$ en $m=4$. Neem $b=4k$. We onderzoeken voor welke waarden van p er een veelhoek met p zijden bestaat in de pijlenklok van f. Noteer $A_p=a^{p-1}+a^{p-2}+\cdots+a+1$.

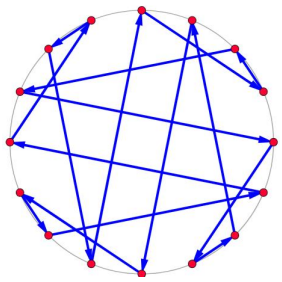
- De formule wordt:$A_p(4x+4k) \equiv 0 \bmod 16$ of $A_p(x+k) \equiv 0 \bmod 4$.
- We weten al dat er 4 lussen zijn.
- Is er een tweehoek? $A_2=1+5 \equiv 2 \bmod 4$, zodat we krijgen dat $2(x+k) \equiv 0 \bmod 4$ of $x+k \equiv 2 \bmod 4$. Als we bijvoorbeeld $b=4$, dan is $k=1$ en vinden we als oplossingen voor x: $1,3,5,9$. Er is een blauwe pijl heen en weer (een tweehoek) tussen 1 en 9 en ook tussen 5 en 13.
- Is er een driehoek? $A_3=1+5+25 \equiv 3 \bmod 4$. De vergelijking wordt: $3(x+k) \equiv 0 \bmod 4$. Deze vergelijking heeft geen oplossingen, tenzij $k=0$, maar dat hebben we al besproken in het beval $f(x)=ax$. Er zijn dus geen driehoeken.

- Een vierhoek? $A_4 = 1 + 5 + 25 + 125 \equiv 0 \bmod 4$. Er zijn nog $16 - 4 - 2 - 2 = 8$ rode punten over. We krijgen dus nog twee vierhoeken.



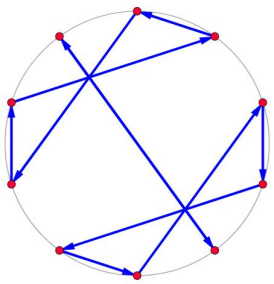
Uiteindelijk rest ons nog het geval dat b geen veelvoud is van d, de grootste gemene deler van $a - 1$ en n. Er zijn geen lussen en we hebben een veelhoek met p zijden als $(a^{p-1} + a^{p-2} + \cdots + a + 1)\{(a - 1)x + b\} \equiv 0 \bmod n$.

Nemen we volgend voorbeeld: $f(x) = 5x + 3$ met $n = 16$. We krijgen een veelhoek met p zijden als $(a^{p-1} + a^{p-2} + \cdots + a + 1)(4x + 3) \equiv 0 \bmod 16$. Nu kan $4x + 3$ nooit een deler zijn van 16, dus moeten we zoeken naar een mogelijkheid om $A_p \equiv 0 \bmod 16$. Omdat de orde van a gelijk is aan 4, is $A_{16} = 4A_4 \equiv 0 \bmod 16$. Alle punten zijn dan oplossingen : we krijgen een veelhoek met 16 zijden.



Een ander voorbeeld is $f(x) = 3x + 7$ met $n = 10$. We krijgen een veelhoek met p zijden als $(a^{p-1} + a^{p-2} + \cdots + a + 1)(4x + 3) \equiv 0 \bmod 16$. Als $x = 4$ of $x = 9$ dan is $2x + 7 \equiv 5 \bmod 10$ en kunnen we $(a^{p-1} + a^{p-2} + \cdots + a + 1)(4x + 3) \equiv 0 \bmod 16$ maken als A_p even is. Nu is $A_2 = 1 + 3 = 4$ dus hebben we een tweehoek die de rode punten 4 en 9 verbindt. Verder is ook

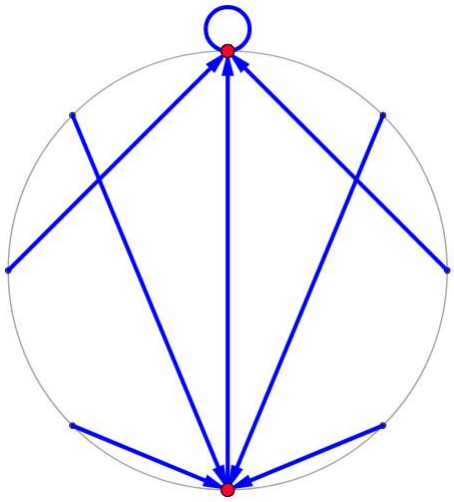
$A_4 \equiv 0 \bmod 10$ zodat de overige 8 rode punten verbonden worden door 2 vierhoeken.



Merk op dat de stelling over evenwijdige blauwe lijnen, die we gezien hebben bij $f(x) = ax$, ook hier geldig is.

4.2 a en n hebben een gemene deler

Noteer de grootste gemene deler van a en n door g. Zoals onderstaande grafiek ($f(x) = 4x$ met $n = 8$) laat zien, is f geen permutatie meer. Sommige rode punten zijn geen doelpunten. In andere rode punten komen meerdere blauwe pijle toe. Dergelijke punten noemen we *aantrekkingspunten* of *attractoren* .



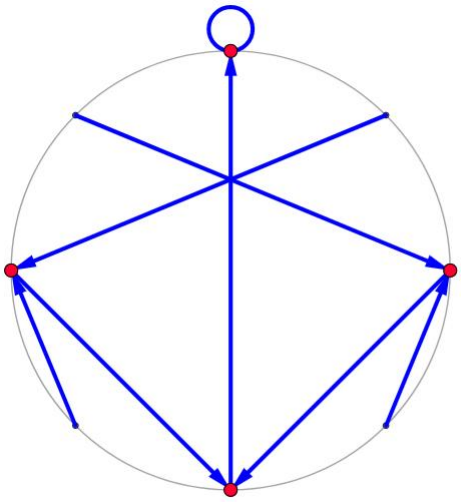
4.2.1 $f(x) = ax$

Stelling 4.7 blijft geldig: $f(x) = ax$ heeft d vaste punten, waarbij $d = \text{ggd}(a - 1, n)$.

Stelling 4.11. *f heeft $\frac{n}{g}$ doelpunten. In elk doelpunt komen g blauwe pijlen toe (lussen meegeteld).*

Bewijs. $y \in \mathbb{Z}_n$ is een doelpunt van f als er een $x \in \mathbb{Z}_n$ bestaat zodat $ax = y$. Er zijn $\frac{n}{g}$ veelvouden van g in $\mathbb{Z}_n$. Al deze rode punten zijn doelpunten van f. Veronderstel immers dat $y = kg$. Stel verder dat $a = ga'$ en $n = gn'$. dan is $ax \equiv y \bmod n \iff ga'x \equiv kg \bmod gn' \iff a'x \equiv ky \bmod n'$. Omdat a' en n' onderling ondeelbaar zijn, volgt hieruit dat $x \equiv a'^{-1}k \bmod n'$. Dit geeft $\frac{n}{n'} = g$ oplossingen. □

Neem als voorbeeld $f(x) = 6x$ met $n = 8$. Dan is $g = \text{ggd}(6, 8) = 2$ en $d = \text{ggd}(6 - 1, 8) = 1$. Er is dus 1 vast punt, namelijk 0. Er zijn 4 aantrekkingspunten, waar telkens 2 blauwe pijlen toekomen.



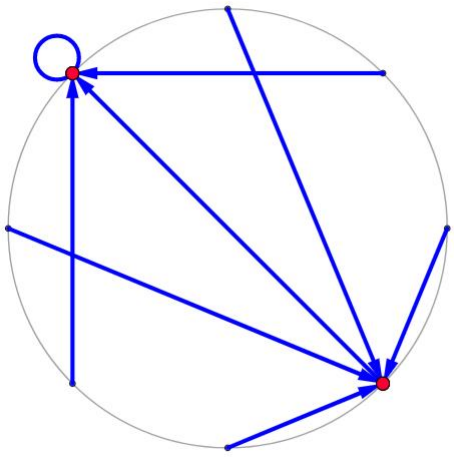
4.2.2 $f(x) = ax + b$

Stelling 4.9 blijft geldig: $f(x) = ax + b$ heeft d vaste punten, waarbij als b een veelvoud is van d. Hierbij is $d = \text{ggd}(a - 1, n)$.

Stelling 4.12. *f heeft $\frac{n}{g}$ doelpunten. In elk doelpunt komen g blauwe pijlen toe (lussen meegeteld).*

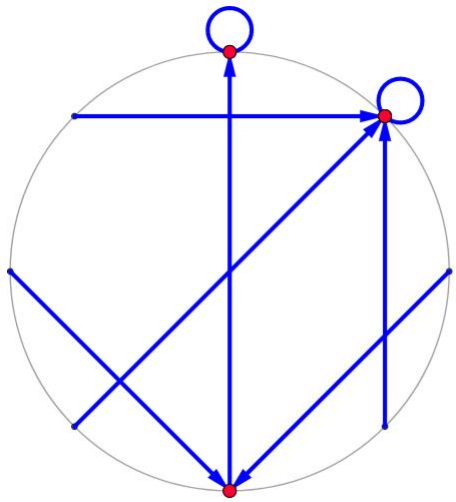
Bewijs. $y \in \mathbb{Z}_n$ is een doelpunt van f als er een $x \in \mathbb{Z}_n$ bestaat zodat $ax + b = y$. Dus moet $y - b$ een veelvoud zijn van g of $y = kg + b$. Al deze rode punten zijn doelpunten van f. Stel verder dat $a = ga'$ en $n = gn'$. dan is $ax + b \equiv y \bmod n \iff ga'x \equiv kg \bmod gn' \iff a'x \equiv ky \bmod n'$. Omdat a' en n' onderling ondeelbaar zijn, volgt hieruit dat $x \equiv a'^{-1}k \bmod n'$. Dit geeft $\frac{n}{n'} = g$ oplossingen. $\square$

Neem als voorbeeld $f(x) = 4x + 3$ met $n = 8$. Dan is $g = \text{ggd}(4, 8) = 2$ en $d = \text{ggd}(4 - 1, 8) = 1$. Er is dus 1 vast punt, namelijk -1. Er zijn 2 aantrekkingspunten, waar telkens 4 blauwe pijlen toekomen.



5 De afbeelding $f(x) = x^2$

Hieronder zien we de pijlenklok van de afbeelding $f(x) = x^2$ voor $n = 8$. Wat zien we op deze tekening? Wat weten we?

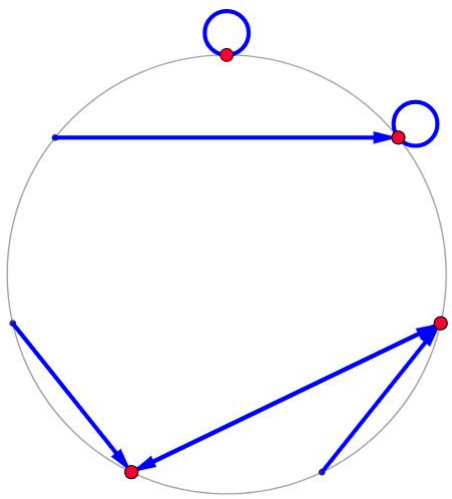


- 0 en 1 zijn altijd vaste punten.
- f is geen permutatie.
- De vaste punten zijn de oplossingen van de vergelijking $x^2 = x$ of $x(x-1) = 0$.
- De doelpunten zijn de rode punten y, waarvoor er een x bestaat met $x^2 = y$. Deze getallen $y \in \mathbb{Z}_{\ltimes}$ noemen we *kwadraatresten modulo n* .
- Als er een blauwe pijl gaat van x naar y, dan gaat er ook een blauwe pijl van $-x$ naar y, want $x^2 = (-x)^2$.
- De vergelijking $x^2 = -1$ is soms toch oplosbaar. Neem bijvoorbeeld $n = 5$, dan is $2^2 = 4 \equiv -1 \bmod 5$.

Laten we een voorbeeld nemen. Bekijk het priemgetal $p = 13$ en bereken wat de kwadraatresten zijn. Dit is makkelijk, we bepalen gewoon $x^2 \bmod p$ voor $x = 1, 2, \cdots, 12$. We vinden : $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 3, 5^2 \equiv 12, 6^2 \equiv 10, 7^10 \equiv 1, 8^2 \equiv 12, 9^2 \equiv 3, 10^2 \equiv 9, 11^2 \equiv 4, 12^2 \equiv 1$.
Merk op dat de rij kwadraatresten $1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1$ symmetrisch is. Uiteraard is dit een gevolg van het feit dat $x^2 = (-x)^2$. Om alle kwadraatresten te vinden is het dus voldoende om $x^2 \bmod p$ te bepalen voor $x = 1, 2, \cdots, \frac{p-1}{2}$. Bovendien zijn de zo gevonden kwadraatresten allemaal

verschillend modulo p. p. Stel namelijk dat $x^2 = y^2 \bmod p$ voor zekere $1 \leq x, y < \frac{p}{2}$. Dan is p een deler van $x^2 - y^2 = (x-y)(x+y)$. Omdat $x + y < p$ kan p geen deler zijn van $x + y$ en dus deelt p het verschil xy. Met andere woorden, $x \equiv y \bmod p$. Maar dit kan alleen als$x = y$. Op deze manier vinden we dus precies $\frac{p-1}{2}$ verschillende kwadraatresten.

Stelling 5.1. *Als p een oneven priemgetal is, dan heeft de pijlenklok van $f(x) = x^2$ voor $n = p$ juist $\frac{p+1}{2}$ doelpunten.*

Bewijs. Uiteraard is 0 een doelpunt, want $0^2 = 0$. Verder kunnen we zoals in het voorbeeld van $p = 13$ bewijzen dat er $\frac{p-1}{2}$ verschillende kwadraatresten zijn. Dit zijn ook allemaal doelpunten. Samen heben we dus $1 + \frac{p-1}{2} = \frac{p+1}{2}$ verschillende doelpunten. $\square$

Het criterium van Euler zegt bovendien dat $a \neq 0$ een doelpunt is, als $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. In onderstaand voorbeeld, met $n = 7$, heeft $\frac{7+1}{2} = 4$ doelpunten. Omdat $1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv -1, 4^3 \equiv 1, 5^3 \equiv -1$ en $6^3 \equiv -1$, zijn de doelpunten van f de rode punten : $0, 1, 2, 4$.