Gaten tussen Pythagoreïsche drietallen

Mike Daas

Universiteit Leiden

26 april 2023

Universiteit Leiden

Een observatie

Een drietal positieve gehele getallen (a, b, c) heet Pythagoreïsch als

$$a^2 + b^2 = c^2.$$

Een observatie

Een drietal positieve gehele getallen (a, b, c) heet Pythagoreïsch als

$$a^2 + b^2 = c^2.$$

Voorbeelden zijn

$$(3, 4, 5), \quad (6, 8, 10), \quad (5, 12, 13), \quad (9, 12, 15), \quad (8, 15, 17), \quad \ldots$$

Deze drietallen corresponderen met rechthoekige driehoeken.

Een observatie

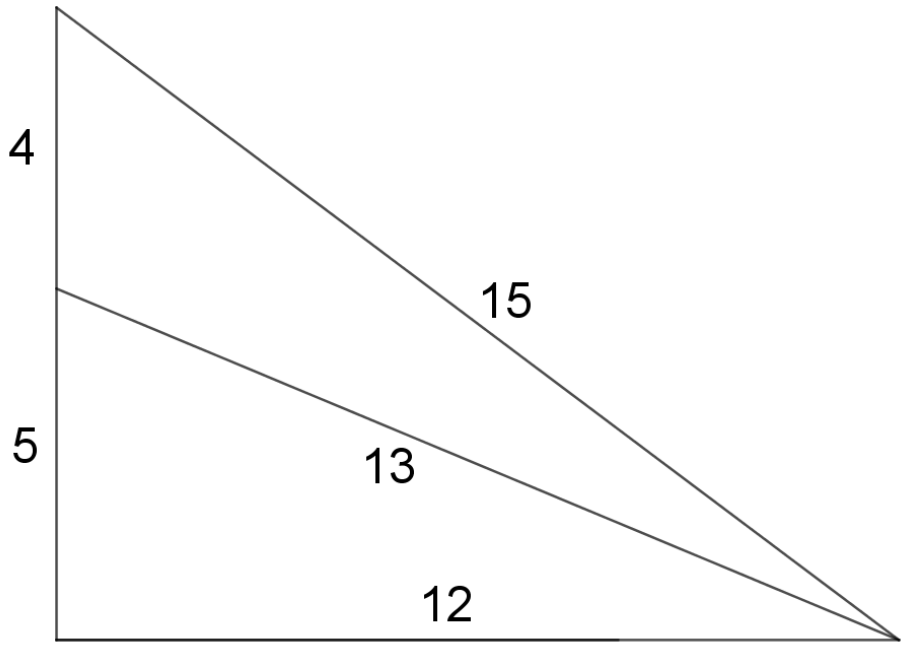
Een drietal positieve gehele getallen (a, b, c) heet Pythagoreïsch als

$$a^2 + b^2 = c^2.$$

Voorbeelden zijn

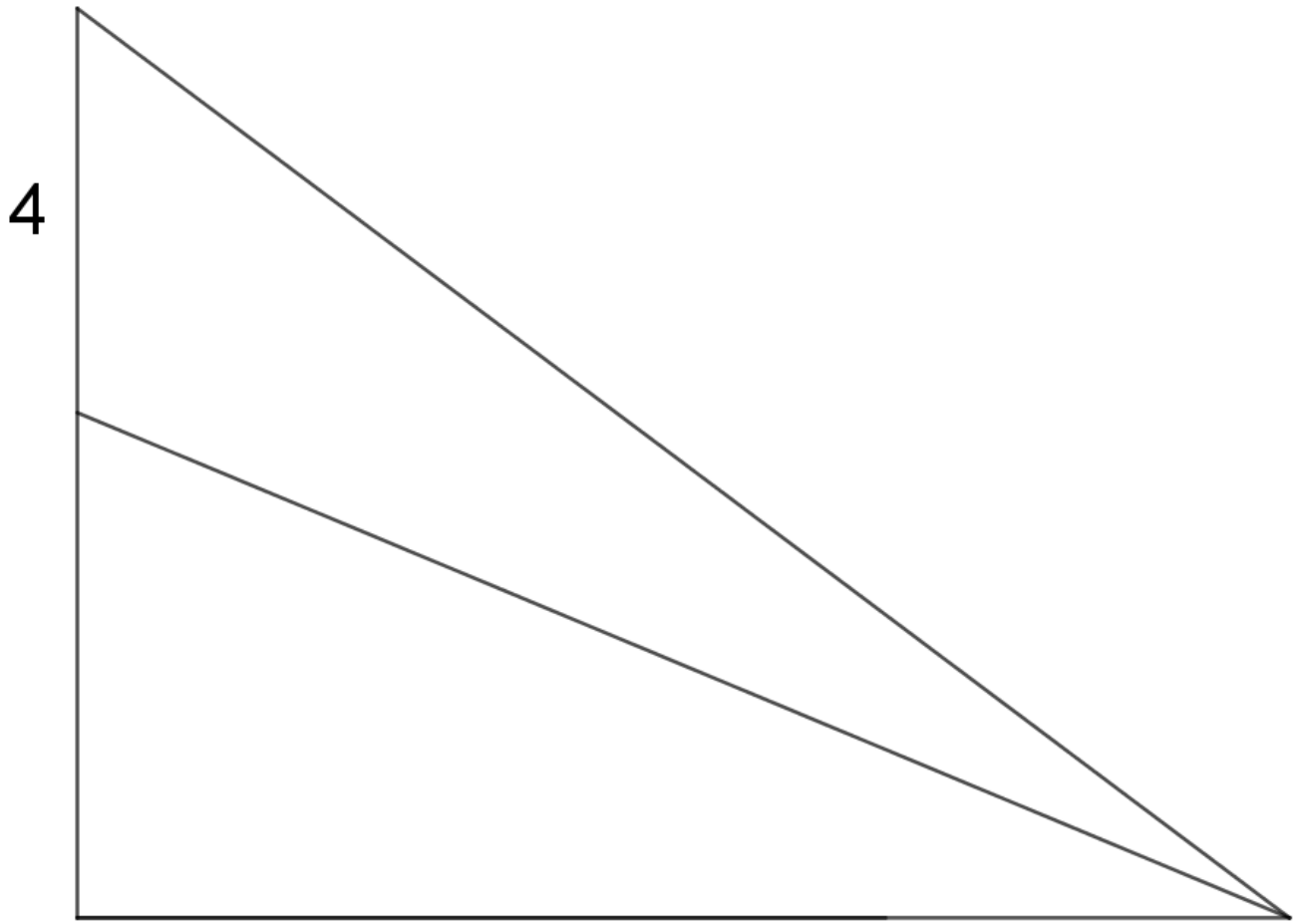
$$(3, 4, 5), \quad (6, 8, 10), \quad (5, 12, 13), \quad (9, 12, 15), \quad (8, 15, 17), \quad \ldots$$

Deze drietallen corresponderen met rechthoekige driehoeken. In het bijzonder hebben we de volgende configuratie:



Een vraag

Zijn er oneindig veel manieren om met gehele zijdelengtes een diagram zoals hieronder te maken?



De eerste stap

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+4)^2 = d^2. \end{cases}$$

De eerste stap

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+4)^2 = d^2. \end{cases}$$

Er valt wat weg als we schrijven $d = c + u$ voor een zekere $u \in \mathbb{Z}$:

$$a^2 + (b+4)^2 = (c+u)^2 \implies 8b + 16 = 2cu + u^2.$$

De eerste stap

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+4)^2 = d^2. \end{cases}$$

Er valt wat weg als we schrijven $d = c + u$ voor een zekere $u \in \mathbb{Z}$:

$$a^2 + (b+4)^2 = (c+u)^2 \implies 8b + 16 = 2cu + u^2.$$

Merk op dat u even moet zijn; dus $u = 2k$ voor een $k \in \mathbb{Z}$. Dan

$$8b + 16 = 2cu + u^2 \implies 2b + 4 = ck + k^2.$$

De eerste stap

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+4)^2 = d^2. \end{cases}$$

Er valt wat weg als we schrijven $d = c + u$ voor een zekere $u \in \mathbb{Z}$:

$$a^2 + (b+4)^2 = (c+u)^2 \implies 8b + 16 = 2cu + u^2.$$

Merk op dat u even moet zijn; dus $u = 2k$ voor een $k \in \mathbb{Z}$. Dan

$$8b + 16 = 2cu + u^2 \implies 2b + 4 = ck + k^2.$$

We moeten dus oplossen:

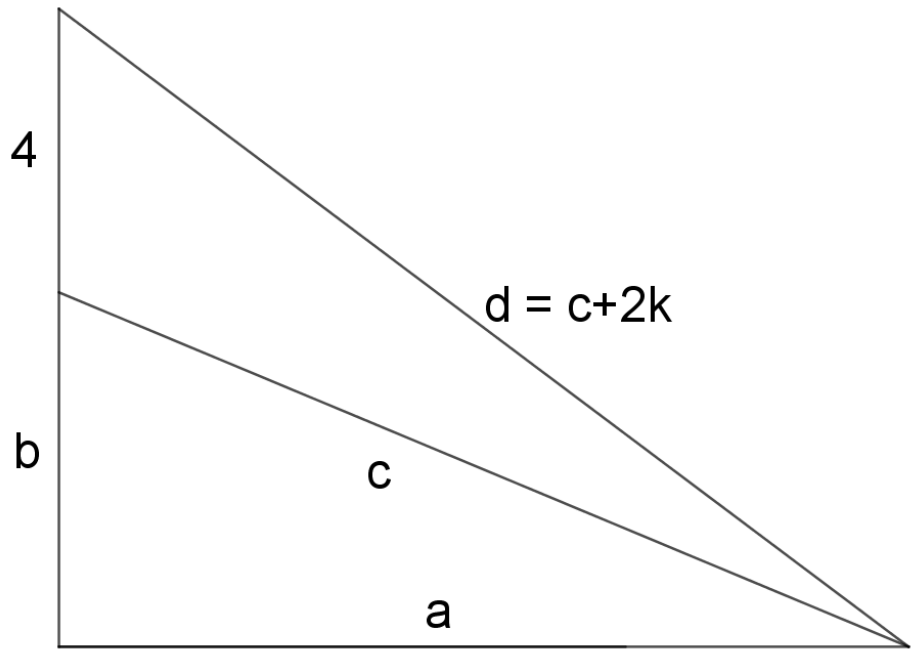
$$\begin{cases} a^2 + b^2 = c^2 \\ 2b + 4 = ck + k^2. \end{cases}$$

Vergeet de meetkunde niet!

Het is soms verleidelijk om alles direct algebraïsch aan te pakken en de meetkunde te vergeten. Echter, als de praktijk ons een ding leert, is dat algebra vaak erg krachtig ondersteund kan worden door meetkunde.

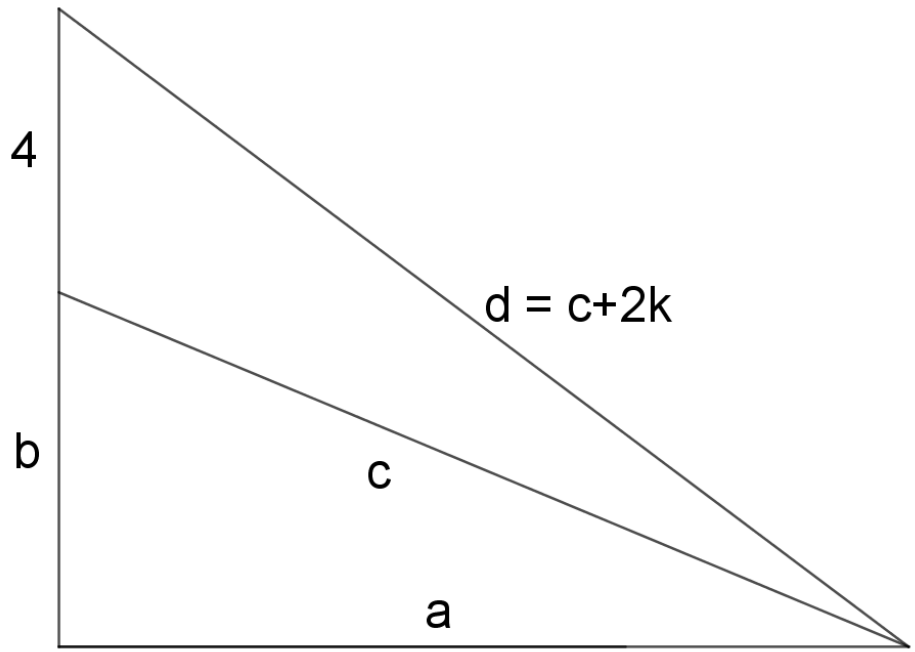
Vergeet de meetkunde niet!

Het is soms verleidelijk om alles direct algebraïsch aan te pakken en de meetkunde te vergeten. Echter, als de praktijk ons een ding leert, is dat algebra vaak erg krachtig ondersteund kan worden door meetkunde. Herinner namelijk:



Vergeet de meetkunde niet!

Het is soms verleidelijk om alles direct algebraïsch aan te pakken en de meetkunde te vergeten. Echter, als de praktijk ons een ding leert, is dat algebra vaak erg krachtig ondersteund kan worden door meetkunde. Herinner namelijk:



Volgens de driehoeksongelijkheid:

$$c < d < c + 4 \implies 2k \in \{1, 2, 3\} \implies k = 1.$$

Een grote stap vooruit

We reduceren dus tot het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ 2b + 4 = c + 1. \end{cases}$$

Dit kunnen we snel reduceren tot een enkele vergelijking:

$$a^2 + b^2 = (2b + 3)^2 \implies a^2 = 3b^2 + 12b + 9.$$

Een grote stap vooruit

We reduceren dus tot het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ 2b + 4 = c + 1. \end{cases}$$

Dit kunnen we snel reduceren tot een enkele vergelijking:

$$a^2 + b^2 = (2b + 3)^2 \implies a^2 = 3b^2 + 12b + 9.$$

Dit kunnen we herschrijven tot

$$a^2 - 3(b + 2)^2 = -3.$$

Met andere woorden, we vinden een vergelijking van de vorm

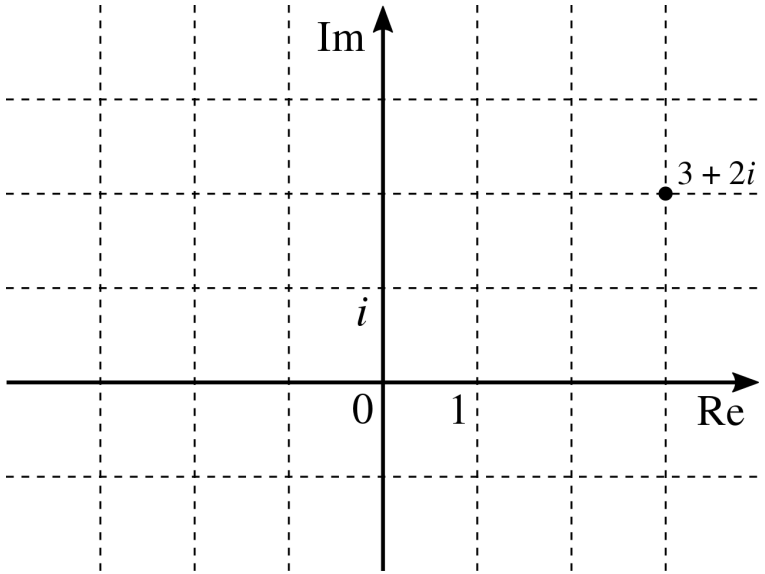
$$X^2 - 3Y^2 = -3.$$

Dit is een zogeheten *vergelijking van Pell*.

Norm op $\mathbb{Z}[i]$

De inclusie $\mathbb{Z}[i] \subset \mathbb{C}$ induceert een natuurlijke norm:

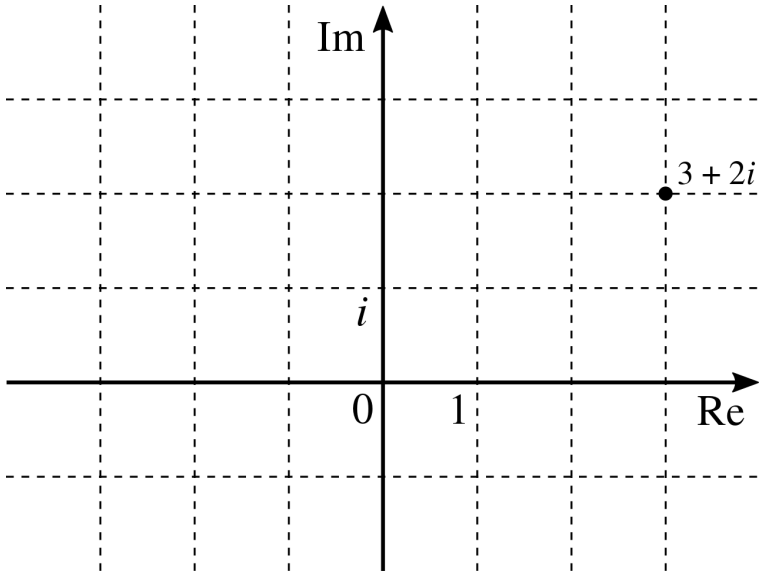
$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$



Norm op $\mathbb{Z}[i]$

De inclusie $\mathbb{Z}[i] \subset \mathbb{C}$ induceert een natuurlijke norm:

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$



Deze norm is multiplicatief:

$$N(z_1)N(z_2) = N(z_1 z_2).$$

Eenheden zijn elementen van norm 1. Deze liggen op de eenheidscirkel: in dit geval enkel ± 1 en $\pm i$.

Norm op $\mathbb{Z}[\sqrt{D}]$

Zij $D < 0$. Dan opnieuw $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ dus krijgen we dezelfde complexe norm

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

Opnieuw liggen eenheden op de eenheidscirkel. Wat als $D > 0$?

Norm op $\mathbb{Z}[\sqrt{D}]$

Zij $D < 0$. Dan opnieuw $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ dus krijgen we dezelfde complexe norm

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

Opnieuw liggen eenheden op de eenheidscirkel. Wat als $D > 0$? We gebruiken dezelfde formule! Zo geldt bijvoorbeeld

$$N(\sqrt{3}) = -3, \quad N(1 + \sqrt{3}) = -2 \quad \text{en} \quad N(2 + \sqrt{3}) = 1.$$

Norm op $\mathbb{Z}[\sqrt{D}]$

Zij $D < 0$. Dan opnieuw $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ dus krijgen we dezelfde complexe norm

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

Opnieuw liggen eenheden op de eenheidscirkel. Wat als $D > 0$? We gebruiken dezelfde formule! Zo geldt bijvoorbeeld

$$N(\sqrt{3}) = -3, \quad N(1 + \sqrt{3}) = -2 \quad \text{en} \quad N(2 + \sqrt{3}) = 1.$$

Merk nu op dat

$$X^2 - 3Y^2 = -3 \iff N(X + Y\sqrt{3}) = -3.$$

We zoeken dus naar elementen in $\mathbb{Z}[\sqrt{3}]$ van norm -3.

Elementen van vaste norm

Observatie

Voor elke $\alpha \in \mathbb{Z}[\sqrt{D}]$ en eenheid $\epsilon \in \mathbb{Z}[\sqrt{D}]^\times$ met $N(\epsilon) = 1$, geldt er

$$N(\alpha\epsilon^n) = N(\alpha)N(\epsilon)^n = N(\alpha).$$

Elementen van vaste norm

Observatie

Voor elke $\alpha \in \mathbb{Z}[\sqrt{D}]$ en eenheid $\epsilon \in \mathbb{Z}[\sqrt{D}]^\times$ met $N(\epsilon) = 1$, geldt er

$$N(\alpha\epsilon^n) = N(\alpha)N(\epsilon)^n = N(\alpha).$$

Dus hoe vinden we oneindig veel X en Y zodat

$$N(X + Y\sqrt{3}) = -3?$$

Een mogelijke oplossing is $X = 0$, $Y = 1$, want $N(\sqrt{3}) = -3$. Dan vinden we oneindig veel verschillende

$$X + Y\sqrt{3} = \sqrt{3}(2 + \sqrt{3})^n.$$

Terug naar driehoeken

Herinner dat

$$a = X, \quad b = Y - 2, \quad c = 2b + 3, \quad d = c + 2.$$

Terug naar driehoeken

Herinner dat

$$a = X, \quad b = Y - 2, \quad c = 2b + 3, \quad d = c + 2.$$

We berekenen nu voor $n \geqslant 2$ dat

$$\sqrt{3}(2+\sqrt{3})^n \in \{12 + 7\sqrt{3},\ 45 + 26\sqrt{3},\ 168 + 97\sqrt{3}, \ldots\}.$$

Terug naar driehoeken

Herinner dat

$$a = X, \quad b = Y - 2, \quad c = 2b + 3, \quad d = c + 2.$$

We berekenen nu voor $n \geqslant 2$ dat

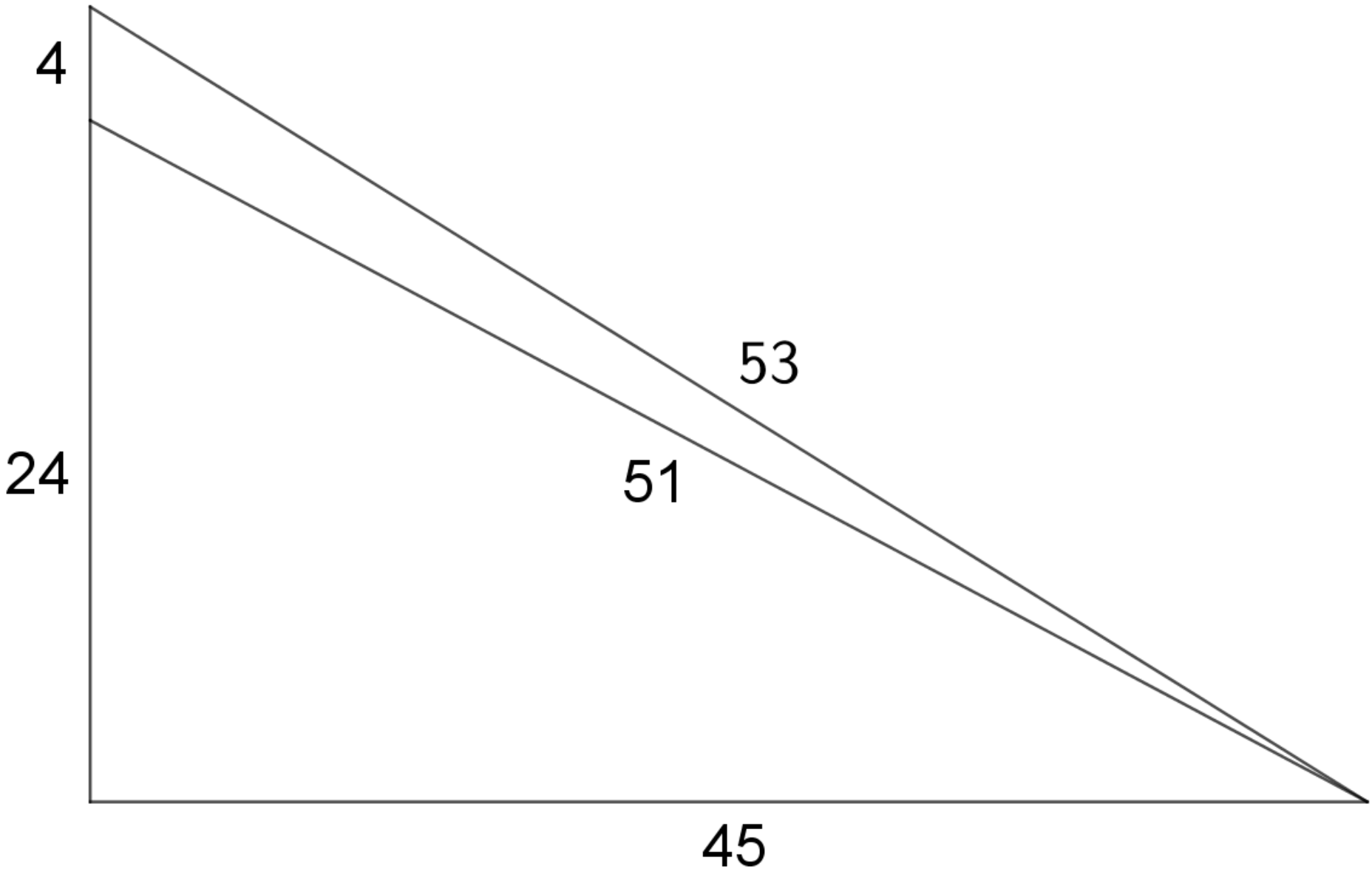
$$\sqrt{3}(2+\sqrt{3})^n \in \{12 + 7\sqrt{3},\ 45 + 26\sqrt{3},\ 168 + 97\sqrt{3}, \ldots\}.$$

We vinden zo

$$\begin{aligned}
n = 0 &\implies (X, Y) = (0, 1) \implies b < 0 \text{ dus geen geldige oplossing;} \\
n = 1 &\implies (X, Y) = (3, 2) \implies b = 0 \text{ dus geen geldige oplossing;} \\
n = 2 &\implies (X, Y) = (12, 7) \implies (a, b, c, d) = (12, 5, 13, 15); \\
n = 3 &\implies (X, Y) = (45, 26) \implies (a, b, c, d) = (45, 24, 51, 53); \\
n = 4 &\implies (X, Y) = (168, 97) \implies (a, b, c, d) = (168, 95, 193, 195).
\end{aligned}$$

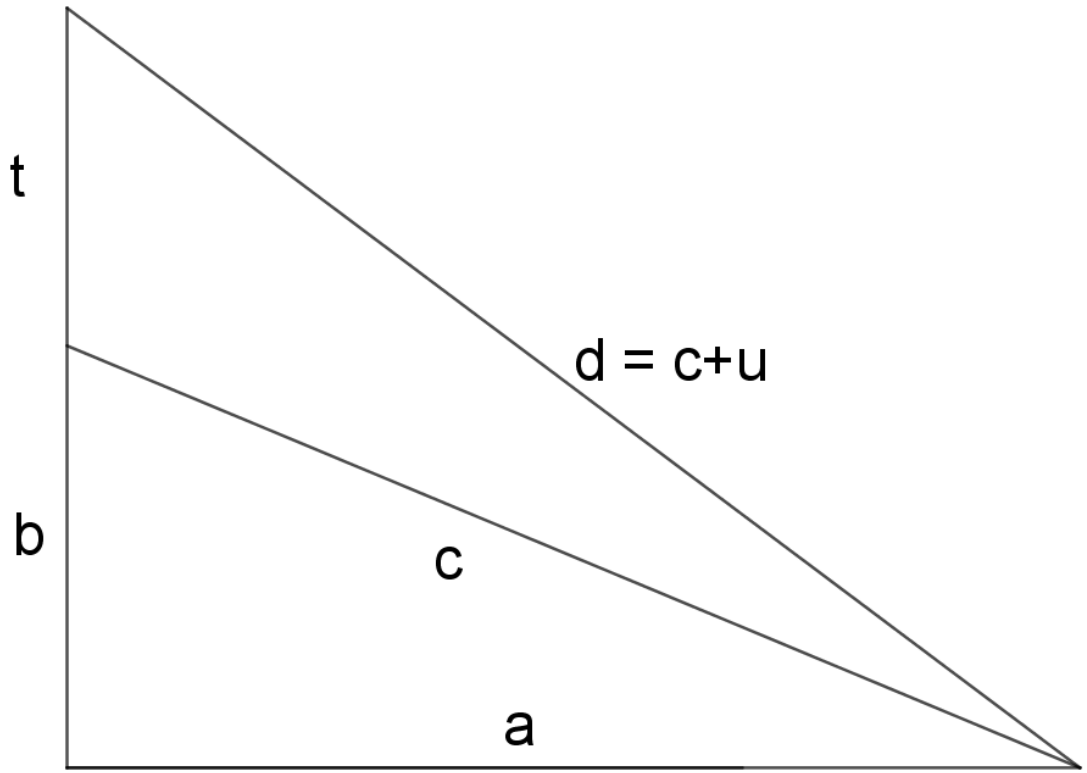
Zo vinden we oneindig veel oplossingen.

Vier je overwinningen (pun intended)



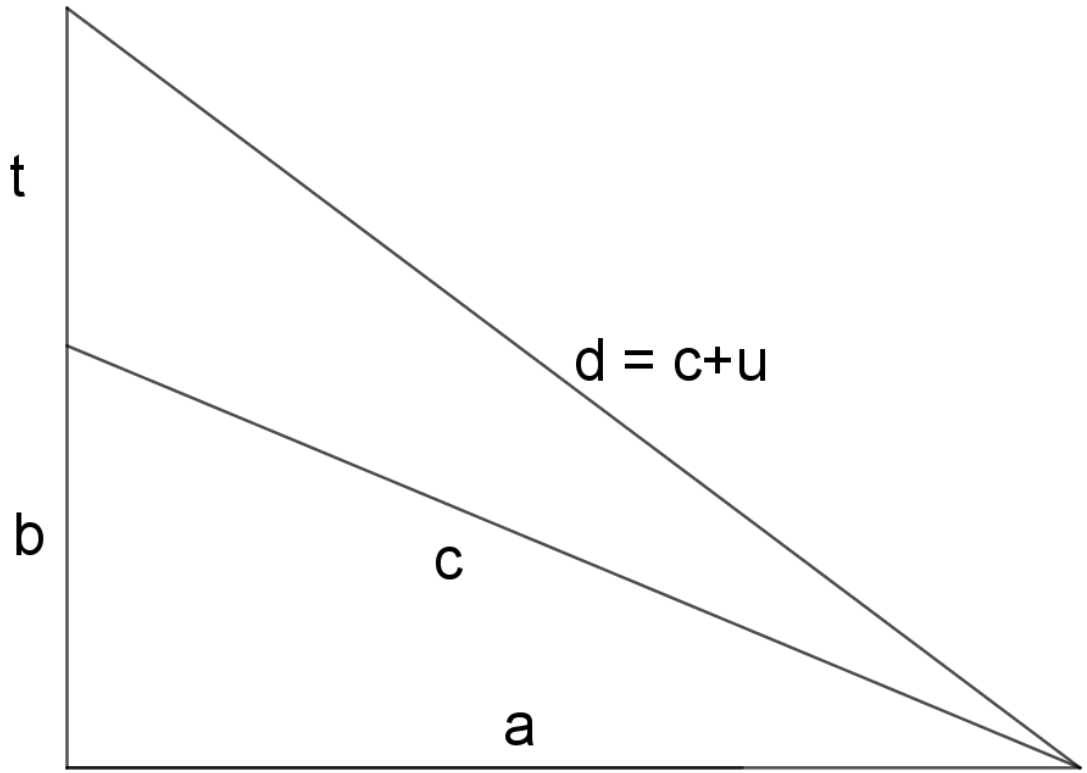
Hoe zit het in het algemeen?

Zij nu $t > 0$ willekeurig doch vast gekozen. Kunnen we dan voor elke waarde van t oneindig veel van zulke configuraties vinden?



Hoe zit het in het algemeen?

Zij nu $t > 0$ willekeurig doch vast gekozen. Kunnen we dan voor elke waarde van t oneindig veel van zulke configuraties vinden?



Opnieuw geeft de driehoeksongelijkheid

$$c < d = c + u < c + t \implies 0 < u < t.$$

Kleine waarden van t

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b + t)^2 = d^2. \end{cases}$$

Kleine waarden van t

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+t)^2 = d^2. \end{cases}$$

Schrijf opnieuw $d = c + u$ voor een zekere $u \in \mathbb{Z}$:

$$a^2 + (b+t)^2 = (c+u)^2 \implies 2bt + t^2 = 2cu + u^2.$$

Kleine waarden van t

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+t)^2 = d^2. \end{cases}$$

Schrijf opnieuw $d = c + u$ voor een zekere $u \in \mathbb{Z}$:

$$a^2 + (b+t)^2 = (c+u)^2 \implies 2bt + t^2 = 2cu + u^2.$$

We zien dat t en u dezelfde pariteit moeten hebben. We zien nu:

- Als $t = 1$, dan is $0 < u < 1$ direct een tegenspraak.

Kleine waarden van t

Laat (a, b, c) zo'n gezocht drietal zijn. We zoeken dan naar oplossingen van het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + (b+t)^2 = d^2. \end{cases}$$

Schrijf opnieuw $d = c + u$ voor een zekere $u \in \mathbb{Z}$:

$$a^2 + (b+t)^2 = (c+u)^2 \implies 2bt + t^2 = 2cu + u^2.$$

We zien dat t en u dezelfde pariteit moeten hebben. We zien nu:

- Als $t = 1$, dan is $0 < u < 1$ direct een tegenspraak.
- Als $t = 2$, dan volgt met $0 < u < 2$ dat $u = 1$; een tegenspraak met de pariteitseis; dus ook hier geen oplossingen.

Het algemene geval

Met wat omschrijven kwamen we tot het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ 2bt + t^2 = 2cu + u^2. \end{cases}$$

Het algemene geval

Met wat omschrijven kwamen we tot het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ 2bt + t^2 = 2cu + u^2. \end{cases}$$

Herschrijf het stelsel als volgt:

$$\begin{cases} (2au)^2 + (2bu)^2 = (2cu)^2 \\ 2bt + t^2 - u^2 = 2cu. \end{cases}$$

Het algemene geval

Met wat omschrijven kwamen we tot het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ 2bt + t^2 = 2cu + u^2. \end{cases}$$

Herschrijf het stelsel als volgt:

$$\begin{cases} (2au)^2 + (2bu)^2 = (2cu)^2 \\ 2bt + t^2 - u^2 = 2cu. \end{cases}$$

We kunnen nu substitueren en als $D = t^2 - u^2$ vinden we

$$(2au)^2 + (2bu)^2 = (2bt + D)^2 .$$

Een ogenschijnlijk onooglijke vergelijking

We moeten dus oplossingen zoeken van

$$(2au)^2 + (2bu)^2 = (2bt)^2 + 4btD + D^2.$$

Een ogenschijnlijk onooglijke vergelijking

We moeten dus oplossingen zoeken van

$$(2au)^2 + (2bu)^2 = (2bt)^2 + 4btD + D^2.$$

Zo vinden we dat

$$(2au)^2 - D(2b)^2 - 4btD = D^2.$$

Dit kunnen we netjes samenpakken tot

$$(2au)^2 - D(2b + t)^2 = -u^2D.$$

Een ogenschijnlijk onooglijke vergelijking

We moeten dus oplossingen zoeken van

$$(2au)^2 + (2bu)^2 = (2bt)^2 + 4btD + D^2.$$

Zo vinden we dat

$$(2au)^2 - D(2b)^2 - 4btD = D^2.$$

Dit kunnen we netjes samenpakken tot

$$(2au)^2 - D(2b + t)^2 = -u^2D.$$

Dus we zoeken eigenlijk naar elementen in $\mathbb{Z}[\sqrt{D}]$ van norm $-u^2D$.
Dat valt best mee!

Een ogenschijnlijk onooglijke vergelijking

We moeten dus oplossingen zoeken van

$$(2au)^2 + (2bu)^2 = (2bt)^2 + 4btD + D^2.$$

Zo vinden we dat

$$(2au)^2 - D(2b)^2 - 4btD = D^2.$$

Dit kunnen we netjes samenpakken tot

$$(2au)^2 - D(2b + t)^2 = -u^2D.$$

Dus we zoeken eigenlijk naar elementen in $\mathbb{Z}[\sqrt{D}]$ van norm $-u^2D$.
Dat valt best mee!
Een element van norm $-u^2D$ hebben we altijd: $u\sqrt{D}$.
Hebben we ook genoeg eenheden?

Een slimme truc

De grap is om hier de juiste waarden voor u te kiezen:

- Stel dat $t \neq 1$ oneven is. Kies $u = 1$. Dan is $D = t^2 - 1$ geen kwadraat. We krijgen een gratis eenheid

$$\epsilon = t + \sqrt{D} \implies N(\epsilon) = t^2 - D = 1.$$

Een slimme truc

De grap is om hier de juiste waarden voor u te kiezen:

- Stel dat $t \neq 1$ oneven is. Kies $u = 1$. Dan is $D = t^2 - 1$ geen kwadraat. We krijgen een gratis eenheid

$$\epsilon = t + \sqrt{D} \implies N(\epsilon) = t^2 - D = 1.$$

- Stel dat $t \neq 2$ even is en kies $u = 2$. Dan is $D = t^2 - 4$ geen kwadraat. Opnieuw

$$\epsilon = \frac{t + \sqrt{D}}{2} \implies N(\epsilon) = \frac{t^2 - D}{4} = 1.$$

Een slimme truc

De grap is om hier de juiste waarden voor u te kiezen:

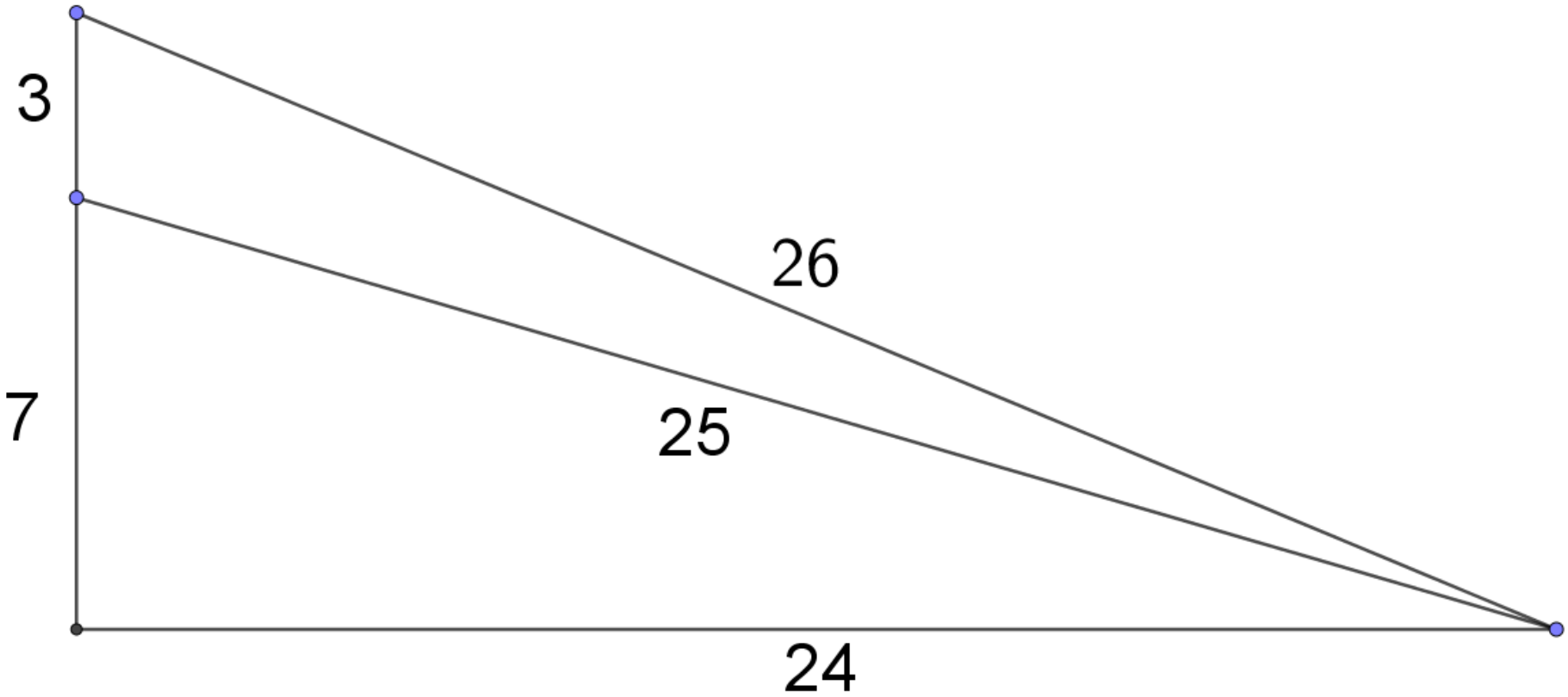
- Stel dat $t \neq 1$ oneven is. Kies $u = 1$. Dan is $D = t^2 - 1$ geen kwadraat. We krijgen een gratis eenheid
$$\epsilon = t + \sqrt{D} \implies N(\epsilon) = t^2 - D = 1.$$
- Stel dat $t \neq 2$ even is en kies $u = 2$. Dan is $D = t^2 - 4$ geen kwadraat. Opnieuw
$$\epsilon = \frac{t + \sqrt{D}}{2} \implies N(\epsilon) = \frac{t^2 - D}{4} = 1.$$
We genereren dan oplossingen middels
$$X + Y\sqrt{D} = u\sqrt{D}\epsilon^n.$$

Stelling

Zij $t \geqslant 3$ willekeurig. Dan bestaan er oneindig veel Pythagoreïsche drietallen (a, b, c) zodat $(a, b + t, d)$ voor een d ook Pythagoreïsch is.

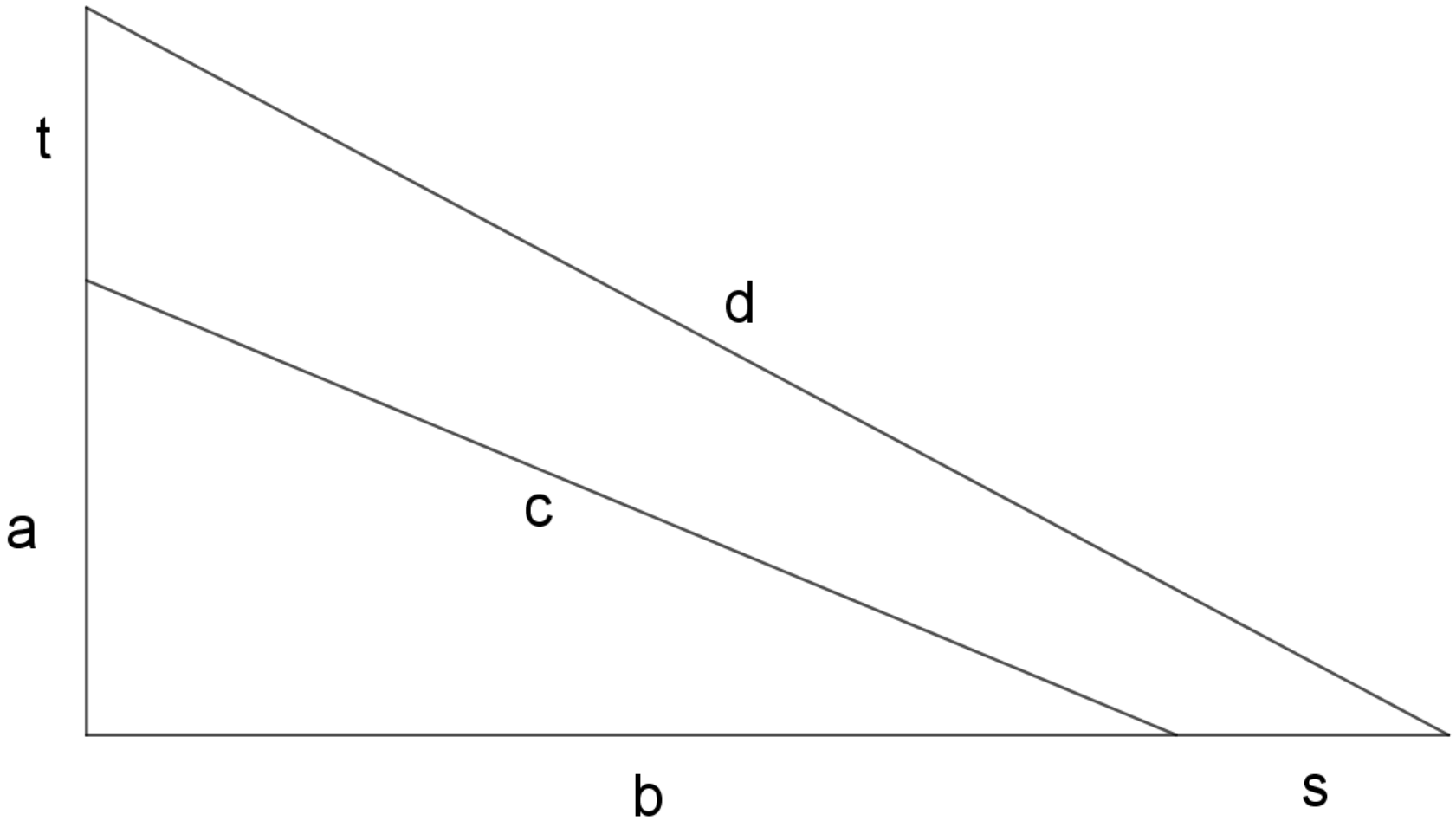
Tel even tot drie

Er zijn dus geen oplossingen voor $t = 1, 2$, maar oneindig veel oplossingen voor $t \geqslant 3$. Zijn we nu helemaal klaar?



Het algemene geval

Zij nu $s, t > 0$ willekeurig doch vast. Voor welke tweetallen kunnen we dan oneindig veel van zulke configuraties vinden?



Onze oude vriend: meetkunde

De eerste vergelijking kunnen we ook direct proberen op te lossen:

$$a^2 + b^2 = c^2 \iff (a/c)^2 + (b/c)^2 = 1.$$

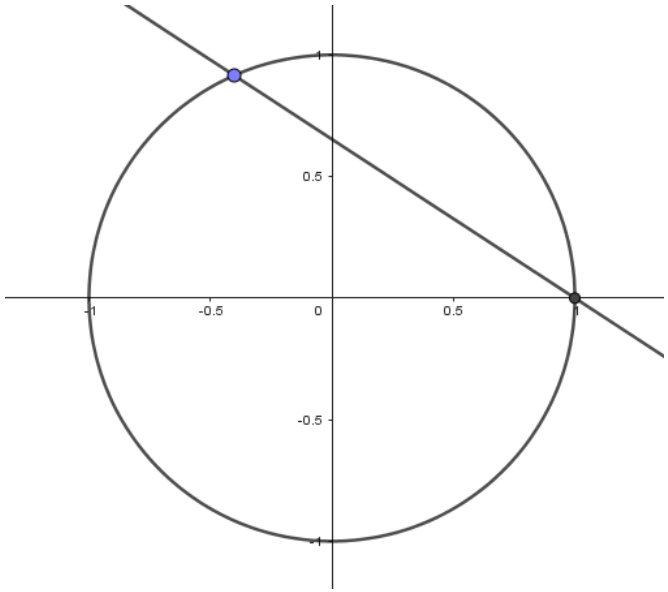
Met andere woorden, we zoeken rationale punten op de eenheidscirkel. Hoe doen we dat?

Onze oude vriend: meetkunde

De eerste vergelijking kunnen we ook direct proberen op te lossen:

$$a^2 + b^2 = c^2 \iff (a/c)^2 + (b/c)^2 = 1.$$

Met andere woorden, we zoeken rationale punten op de eenheidscirkel. Hoe doen we dat?



De helling van een rationaal punt op de cirkel naar $(1, 0)$ is rationaal. Geldt dit ook andersom?

Lijnen zijn punten en punten zijn lijnen

Stel dat $r \in \mathbb{Q}$. Wat is dan het snijpunt van de lijn

$$y = r(x - 1)$$

met de cirkel $x^2 + y^2 = 1$?

Lijnen zijn punten en punten zijn lijnen

Stel dat $r \in \mathbb{Q}$. Wat is dan het snijpunt van de lijn

$$y = r(x - 1)$$

met de cirkel $x^2 + y^2 = 1$? Wel, substitueer en vind

$$x^2 + r^2(x-1)^2 = 1 \implies (x-1)\left(x + 1 + r^2(x-1)\right) = 0.$$

We vinden dus ofwel $x = 1$, ofwel

$$x = \frac{r^2 - 1}{r^2 + 1} \in \mathbb{Q} \implies y = \frac{2r}{r^2 + 1} \in \mathbb{Q}.$$

Lijnen zijn punten en punten zijn lijnen

Stel dat $r \in \mathbb{Q}$. Wat is dan het snijpunt van de lijn

$$y = r(x-1)$$

met de cirkel $x^2 + y^2 = 1$? Wel, substitueer en vind

$$x^2 + r^2(x-1)^2 = 1 \implies (x-1)\left(x+1+r^2(x-1)\right) = 0.$$

We vinden dus ofwel $x = 1$, ofwel

$$x = \frac{r^2-1}{r^2+1} \in \mathbb{Q} \implies y = \frac{2r}{r^2+1} \in \mathbb{Q}.$$

Er bestaan dus $m, n \in \mathbb{N}$ met $r = m/n$ zodat

$$(a/c, b/c) = \left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right).$$

Dus voor een $k \in \mathbb{N}$ geldt dat $(a,b,c) = k(m^2-n^2, 2mn, m^2+n^2)$.

Nog eenmaal omschrijven

We beschouwen dus het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Nog eenmaal omschrijven

We beschouwen dus het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Net als voorheen herschrijven we de tweede vergelijking tot

$$2as + s^2 + 2bt + t^2 = 2cu + u^2$$

waar

$$(a, b, c) = k(m^2 - n^2, 2mn, m^2 + n^2).$$

Nog eenmaal omschrijven

We beschouwen dus het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Net als voorheen herschrijven we de tweede vergelijking tot

$$2as + s^2 + 2bt + t^2 = 2cu + u^2$$

waar

$$(a, b, c) = k(m^2 - n^2, 2mn, m^2 + n^2).$$

Als $D = s^2 + t^2 - u^2$, volgt na substitueren

$$(m(s-u) + tn)^2 - Dn^2 = -D\frac{s-u}{2k}.$$

Nog eenmaal omschrijven

We beschouwen dus het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Net als voorheen herschrijven we de tweede vergelijking tot

$$2as + s^2 + 2bt + t^2 = 2cu + u^2$$

waar

$$(a, b, c) = k(m^2 - n^2, 2mn, m^2 + n^2).$$

Als $D = s^2 + t^2 - u^2$, volgt na substitueren

$$(m(s-u) + tn)^2 - Dn^2 = -D\frac{s-u}{2k}.$$

We zoeken dus elementen van norm $-D\frac{s-u}{2k}$ in $\mathbb{Z}[\sqrt{D}]$. We hebben nu echter geen trucs meer. Hoe zit het met eenheden in $\mathbb{Z}[\sqrt{D}]$?

Eenheden in $\mathbb{Z}[\sqrt{D}]$

Lemma

De groep $\mathbb{Z}[\sqrt{D}]^\times$ is oneindig precies wanneer er een eenheid $\epsilon \in \mathbb{Z}[\sqrt{D}]^\times$ bestaat verschillend van ± 1.

Bewijs: Inderdaad, als $\epsilon \neq \pm 1$, dan omdat $\epsilon \in \mathbb{R}$, kan ϵ geen eenheidswortel zijn. Dus ϵ heeft oneindige orde in $\mathbb{Z}[\sqrt{D}]^\times$. □

Eenheden in $\mathbb{Z}[\sqrt{D}]$

Lemma

De groep $\mathbb{Z}[\sqrt{D}]^\times$ is oneindig precies wanneer er een eenheid $\epsilon \in \mathbb{Z}[\sqrt{D}]^\times$ bestaat verschillend van ± 1.

Bewijs: Inderdaad, als $\epsilon \neq \pm 1$, dan omdat $\epsilon \in \mathbb{R}$, kan ϵ geen eenheidswortel zijn. Dus ϵ heeft oneindige orde in $\mathbb{Z}[\sqrt{D}]^\times$. □
De volgende stelling zegt dus precies wat we willen.

Stelling

Zij $D > 0$ een geheel getal dat geen kwadraat is.
Dan bevat $\mathbb{Z}[\sqrt{D}]$ een eenheid $\epsilon \neq \pm 1$.

Eenheden in $\mathbb{Z}[\sqrt{D}]$

Lemma

De groep $\mathbb{Z}[\sqrt{D}]^\times$ is oneindig precies wanneer er een eenheid $\epsilon \in \mathbb{Z}[\sqrt{D}]^\times$ bestaat verschillend van ± 1.

Bewijs: Inderdaad, als $\epsilon \neq \pm 1$, dan omdat $\epsilon \in \mathbb{R}$, kan ϵ geen eenheidswortel zijn. Dus ϵ heeft oneindige orde in $\mathbb{Z}[\sqrt{D}]^\times$. □
De volgende stelling zegt dus precies wat we willen.

Stelling

Zij $D > 0$ een geheel getal dat geen kwadraat is.
Dan bevat $\mathbb{Z}[\sqrt{D}]$ een eenheid $\epsilon \neq \pm 1$.

Hoe bewijst men zo'n resultaat? Idee: als $X^2 - DY^2 = 1$, dan is $X/Y \approx \sqrt{D}$. Bieden benaderingen van $\sqrt{D}$ met breuken uitkomst?

Benaderende breuken nestelen

Stel dat we het getal π zouden willen benaderen met een breuk. Hoe zouden we dat doen?

Benaderende breuken nestelen

Stel dat we het getal π zouden willen benaderen met een breuk. Hoe zouden we dat doen?
Een allereerste benadering zou zijn $\pi \approx \lfloor \pi \rfloor = 3$.

Benaderende breuken nestelen

Stel dat we het getal π zouden willen benaderen met een breuk. Hoe zouden we dat doen?
Een allereerste benadering zou zijn $\pi \approx \lfloor \pi \rfloor = 3$.
Hoe groot is onze fout? Wel, $\pi - 3 \approx 0.14159$ en $1/(\pi - 3) \approx 7.0625$.
We vinden zo de betere benadering

$$\pi \approx 3 + \frac{1}{7} = \frac{22}{7}.$$

Benaderende breuken nestelen

Stel dat we het getal π zouden willen benaderen met een breuk. Hoe zouden we dat doen?
Een allereerste benadering zou zijn $\pi \approx \lfloor \pi \rfloor = 3$.
Hoe groot is onze fout? Wel, $\pi - 3 \approx 0.14159$ en $1/(\pi - 3) \approx 7.0625$.
We vinden zo de betere benadering

$$\pi \approx 3 + \frac{1}{7} = \frac{22}{7}.$$

We krijgen een betere benadering als we iets preciezer zijn over

$$7.0625 = 7 + 0.0625 \quad \text{waar} \quad 1/0.0625 = 16.$$

Zo vinden we een betere benadering

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{16}} = \frac{355}{113}.$$

Kettingbreuken

Merk nu op dat

$$\pi - \left(3 + \frac{1}{7 + \frac{1}{16}}\right) = \pi - \frac{355}{113} = -0.000000266764\ldots$$

Dit is al heel goed!

Kettingbreuken

Merk nu op dat

$$\pi - \left(3 + \frac{1}{7 + \frac{1}{16}}\right) = \pi - \frac{355}{113} = -0.000000266764\ldots$$

Dit is al heel goed!
Een *kettingbreuk* is een uitdrukking van de vorm

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}} =: \langle a_0, a_1, a_2, \ldots \rangle.$$

Kettingbreuken

Merk nu op dat

$$\pi - \left(3 + \frac{1}{7 + \frac{1}{16}}\right) = \pi - \frac{355}{113} = -0.000000266764\ldots$$

Dit is al heel goed!
Een *kettingbreuk* is een uitdrukking van de vorm

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}} =: \langle a_0, a_1, a_2, \ldots \rangle.$$

Voor $\alpha \in \mathbb{R}$, laat $\lfloor \alpha \rfloor = n$ het grootste gehele getal $n \leqslant \alpha$ zijn en schrijf $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$ voor het fractionele deel.

Kettingbreuken

Merk nu op dat

$$\pi - \left(3 + \frac{1}{7 + \frac{1}{16}}\right) = \pi - \frac{355}{113} = -0.000000266764\ldots$$

Dit is al heel goed!
Een *kettingbreuk* is een uitdrukking van de vorm

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}} =: \langle a_0, a_1, a_2, \ldots \rangle.$$

Voor $\alpha \in \mathbb{R}$, laat $\lfloor \alpha \rfloor = n$ het grootste gehele getal $n \leqslant \alpha$ zijn en schrijf $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$ voor het fractionele deel. We de kettingbreukexpansie middels $\alpha_0 = \alpha$ en het algoritme

$$a_k = \lfloor \alpha_k \rfloor \quad \text{en} \quad \alpha_{k+1} = 1/\{\alpha_k\}.$$

Voorbeeld met $\sqrt{2}$

Hoe bepalen we de kettingbreuk van $\sqrt{2}$? Wel, $\alpha_0 = \sqrt{2}$ en:

$$a_0 = \lfloor \sqrt{2} \rfloor = 1 \quad \text{en} \quad \alpha_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1;$$

$$a_1 = \lfloor \sqrt{2}+1 \rfloor = 2 \quad \text{en} \quad \alpha_2 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1;$$

$$a_2 = \lfloor \sqrt{2}+1 \rfloor = 2 \quad \text{en} \quad \alpha_3 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1\ldots$$

Voorbeeld met $\sqrt{2}$

Hoe bepalen we de kettingbreuk van $\sqrt{2}$? Wel, $\alpha_0 = \sqrt{2}$ en:

$$a_0 = \lfloor \sqrt{2} \rfloor = 1 \quad \text{en} \quad \alpha_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1;$$

$$a_1 = \lfloor \sqrt{2}+1 \rfloor = 2 \quad \text{en} \quad \alpha_2 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1;$$

$$a_2 = \lfloor \sqrt{2}+1 \rfloor = 2 \quad \text{en} \quad \alpha_3 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1\ldots$$

We concluderen dat

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2+\ldots}}}} = \langle 1, 2, 2, \ldots \rangle =: \langle 1, \overline{2} \rangle.$$

Van benaderingen naar eenheden

Welke benaderingen van $\sqrt{2}$ vinden we zo? Wel:

$$\sqrt{2} \approx 1, \quad \sqrt{2} \approx 1 + \frac{1}{2} = \frac{3}{2}, \quad \sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2}} = \frac{8}{5}$$

en wat grotere voorbeelden

$$\sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{17}{12} \quad \text{en} \quad \sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = \frac{41}{29}.$$

Van benaderingen naar eenheden

Welke benaderingen van $\sqrt{2}$ vinden we zo? Wel:

$$\sqrt{2} \approx 1, \quad \sqrt{2} \approx 1 + \frac{1}{2} = \frac{3}{2}, \quad \sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2}} = \frac{8}{5}$$

en wat grotere voorbeelden

$$\sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{17}{12} \quad \text{en} \quad \sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = \frac{41}{29}.$$

Vergelijk dit met $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$, en

$$\left(1 + \sqrt{2}\right)^1 = 1 + \sqrt{2}; \quad \left(1 + \sqrt{2}\right)^2 = 3 + 2\sqrt{2};$$
$$\left(1 + \sqrt{2}\right)^3 = 8 + 5\sqrt{2}; \quad \left(1 + \sqrt{2}\right)^4 = 17 + 12\sqrt{2};$$
$$\left(1 + \sqrt{2}\right)^5 = 41 + 29\sqrt{2} \ldots$$

Dit kan toch zeker geen toeval zijn?

Ons vermoeden sterken

Je kunt nagaan dat

$$\sqrt{3} = \langle 1, 1, 2, 1, 2, \ldots \rangle = \langle 1, \overline{1, 2} \rangle.$$

Hieruit volgen de benaderingen:

$$\sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3}, \quad \sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = \frac{7}{4}$$

en wat grotere voorbeelden

$$\sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}} = \frac{19}{11}. \quad \text{en} \quad \sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}}}} = \frac{26}{15}.$$

Ons vermoeden sterken

Je kunt nagaan dat

$$\sqrt{3} = \langle 1, 1, 2, 1, 2, \ldots \rangle = \langle 1, \overline{1, 2} \rangle.$$

Hieruit volgen de benaderingen:

$$\sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3}, \quad \sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = \frac{7}{4}$$

en wat grotere voorbeelden

$$\sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}} = \frac{19}{11}. \quad \text{en} \quad \sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}}}} = \frac{26}{15}.$$

Dit keer vinden we

$$5^2 - 3 \cdot 3^2 = -2; \quad 7^2 - 3 \cdot 4^2 = 1;$$
$$19^2 - 3 \cdot 11^2 = -2; \quad 26^2 - 3 \cdot 15^2 = 1.$$

Ons vermoeden sterken

Je kunt nagaan dat

$$\sqrt{3} = \langle 1, 1, 2, 1, 2, \ldots \rangle = \langle 1, \overline{1, 2} \rangle.$$

Hieruit volgen de benaderingen:

$$\sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3}, \quad \sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = \frac{7}{4}$$

en wat grotere voorbeelden

$$\sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}} = \frac{19}{11}. \quad \text{en} \quad \sqrt{3} \approx 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}}}} = \frac{26}{15}.$$

Dit keer vinden we

$$5^2 - 3 \cdot 3^2 = -2; \quad 7^2 - 3 \cdot 4^2 = 1;$$
$$19^2 - 3 \cdot 11^2 = -2; \quad 26^2 - 3 \cdot 15^2 = 1.$$

Speelt de lengte van de cykel een rol?

Een bewijsschets

Stelling

Zij $D > 0$ geen kwadraat. Dan bestaan er $a_1, \ldots, a_r$ zodat

$$\sqrt{D} = \langle \lfloor \sqrt{D} \rfloor, \overline{a_1, \ldots, a_r} \rangle.$$

Stel dat $$\langle \lfloor \sqrt{D} \rfloor, a_1, \ldots, a_{r-1} \rangle = \frac{p}{q}.$$

Dan geldt dat $p^2 - Dq^2 = \pm 1$.

Een bewijsschets

Stelling

Zij $D > 0$ geen kwadraat. Dan bestaan er $a_1, \ldots, a_r$ zodat

$$\sqrt{D} = \langle \lfloor \sqrt{D} \rfloor, \overline{a_1, \ldots, a_r} \rangle.$$

Stel dat $$\langle \lfloor \sqrt{D} \rfloor, a_1, \ldots, a_{r-1} \rangle = \frac{p}{q}.$$

Dan geldt dat $p^2 - Dq^2 = \pm 1$.

Bewijsschets: Geheel algemeen hebben we de afschatting

$$\left| \frac{p}{q} - \sqrt{D} \right| < \frac{1}{a_r q^2}.$$

Een bewijsschets

Stelling

Zij $D > 0$ geen kwadraat. Dan bestaan er $a_1, \ldots, a_r$ zodat

$$\sqrt{D} = \langle \lfloor \sqrt{D} \rfloor, \overline{a_1, \ldots, a_r} \rangle.$$

Stel dat $$\langle \lfloor \sqrt{D} \rfloor, a_1, \ldots, a_{r-1} \rangle = \frac{p}{q}.$$

Dan geldt dat $p^2 - Dq^2 = \pm 1$.

Bewijsschets: Geheel algemeen hebben we de afschatting

$$\left| \frac{p}{q} - \sqrt{D} \right| < \frac{1}{a_r q^2}.$$

Men kan aantonen dat $a_r = 2\lfloor \sqrt{D} \rfloor$ in dit geval. Maar dan

$$|p^2 - Dq^2| < 2.$$

Het kan niet nul zijn omdat D geen kwadraat is. □

Back to business

Stelling

Zij $D > 0$ een geheel getal dat geen kwadraat is.
Dan bevat $\mathbb{Z}[\sqrt{D}]$ een eenheid $\epsilon \neq \pm 1$.

Herinner, er gold $D = s^2 + t^2 - u^2$ en we zochten oplossingen tot

$$(m(s-u)+tn)^2 - Dn^2 = -D\frac{s-u}{2k}.$$

Back to business

Stelling

Zij $D > 0$ een geheel getal dat geen kwadraat is.
Dan bevat $\mathbb{Z}[\sqrt{D}]$ een eenheid $\epsilon \neq \pm 1$.

Herinner, er gold $D = s^2 + t^2 - u^2$ en we zochten oplossingen tot

$$(m(s-u)+tn)^2 - Dn^2 = -D\frac{s-u}{2k}.$$

Gebruiken we de stelling, dan reduceren we tot het vinden van een element van norm

$$-D\frac{s-u}{2k}$$

Hoe kiezen we slimme waarden voor u en k?

Back to business

Stelling

Zij $D > 0$ een geheel getal dat geen kwadraat is.
Dan bevat $\mathbb{Z}[\sqrt{D}]$ een eenheid $\epsilon \neq \pm 1$.

Herinner, er gold $D = s^2 + t^2 - u^2$ en we zochten oplossingen tot

$$(m(s-u)+tn)^2 - Dn^2 = -D\frac{s-u}{2k}.$$

Gebruiken we de stelling, dan reduceren we tot het vinden van een element van norm

$$-D\frac{s-u}{2k}$$

Hoe kiezen we slimme waarden voor u en k? Idee: *elke* oplossing van ons stelsel geeft ons zo'n element; ook heel flauwe oplossingen.

De juiste waarde van u

Stel $s = 2r + 1$. Herinner het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Kunnen we hier een oplossing van opschrijven?

De juiste waarde van u

Stel $s = 2r + 1$. Herinner het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Kunnen we hier een oplossing van opschrijven? Heel eenvoudig is

$$a = 0 \implies b = c.$$

De tweede vergelijking wordt

$$(2r+1)^2 + (b+t)^2 = (b+u)^2.$$

De juiste waarde van u

Stel $s = 2r + 1$. Herinner het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a + s)^2 + (b + t)^2 = d^2 = (c + u)^2. \end{cases}$$

Kunnen we hier een oplossing van opschrijven? Heel eenvoudig is

$$a = 0 \implies b = c.$$

De tweede vergelijking wordt

$$(2r + 1)^2 + (b + t)^2 = (b + u)^2.$$

We vinden eenvoudig een mogelijk drietal:

$$(2r + 1)^2 + (2r^2 + 2r)^2 = (2r^2 + 2r + 1)^2 \implies u = t + 1.$$

Wellicht zal $u = t + 1$ altijd een oplossing geven?

De juiste waarde van u

Stel $s = 2r + 1$. Herinner het stelsel

$$\begin{cases} a^2 + b^2 = c^2 \\ (a+s)^2 + (b+t)^2 = d^2 = (c+u)^2. \end{cases}$$

Kunnen we hier een oplossing van opschrijven? Heel eenvoudig is

$$a = 0 \implies b = c.$$

De tweede vergelijking wordt

$$(2r+1)^2 + (b+t)^2 = (b+u)^2.$$

We vinden eenvoudig een mogelijk drietal:

$$(2r+1)^2 + (2r^2+2r)^2 = (2r^2+2r+1)^2 \implies u = t+1.$$

Wellicht zal $u = t + 1$ altijd een oplossing geven? Inderdaad, je kunt nagaan dat met al deze keuzes,

$$N(2r + \sqrt{D}) = -D\frac{s-u}{2k}.$$

Conclusie(?)

Een vergelijkbaar argument werkt voor $s = 2r$ even. Werkt het dan voor alle (s, t)?

Conclusie(?)

Een vergelijkbaar argument werkt voor $s = 2r$ even. Werkt het dan voor alle (s, t)? Neen; uiteindelijk vinden we enkel geen oplossingen voor de volgende paren:

s / t	0	1	2	3	4	5	6	7	8	9
0		X	X							
1	X	X	X							
2	X	X	X	X	X					
3			X							
4			X		X	X	X			
5					X					
6					X			X		
7							X			
8										
9										

Conclusie(?)

Een vergelijkbaar argument werkt voor $s = 2r$ even. Werkt het dan voor alle (s, t)? Neen; uiteindelijk vinden we enkel geen oplossingen voor de volgende paren:

s / t	0	1	2	3	4	5	6	7	8	9
0		X	X							
1	X	X	X							
2	X	X	X	X	X					
3			X							
4			X		X	X	X			
5					X					
6					X			X		
7							X			
8										
9										

Wat als s of t negatief is? Probeer het zelf eens!