STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1950-009

Een stelling van Petr uit de getallentheorie

"Actualiteiten"

1950

Voordracht door C. Schogt in de serie
Actualiteiten op 29 April 1950.

Een stelling van Petr uit de getallentheorie.

De volgende stelling is door K. Petr afgeleid:
Is D een natuurlijk getal, geen quadraat, dan heeft van het stelsel vergelijkingen:

(1) $$D_1 u^2 - D_2 v^2 = e,$$

waarbij D_1 en D_2 alle mogelijke natuurlijke getallen doorlopen, zodat $D_1 D_2 = D$ en $D_1 < D_2$, en e telkens de waarden 1, -1, 2, -2 doorloopt, behalve voor $D_1 = 1$, waarvoor de waarde e = 1 uitgesloten is, één en slechts één vergelijking een oplossing in natuurlijke getallen u, v, waarvoor geldt:

(2) $$(u, D_2) = (v, D_1) = 1.$$

(Door (a,b) wordt de g.g.d. van a en b aangeduid).

Deze stelling is een gevolg van de volgende bekende stelling uit de getallentheorie:
Voor elk natuurlijk getal D, dat geen quadraat is, is de vergelijking van Pell:

$$x^2 - Dy^2 = 1$$

in natuurlijke getallen oplosbaar.

Petr heeft zijn stelling bewezen met behulp van de kettingbreukontwikkeling van $\sqrt{D}$. (Časopis pro pěstovani matematiky a fysiky, Praag 1927, blz. 57).

Het bewijs, dat hier gegeven zal worden, is afkomstig van S. Lubelski.

Onder een integriteitsgebied verstaat men een verzameling elementen met de volgende eigenschappen:

1. aan twee elementen a en b is eenduidig toegevoegd een element a + b, de som, en een element a b, het product.
2. (a+b)+ c = a + (b+c).
3. a + b = b + a.
4. bij a en b is steeds een element x te vinden, zodat a + x = b.
5. (ab)c = a(bc).
6. ab = ba.
7. a(b+c)= ab + ac.

Uit 1, 2, 3, 4 volgt, dat de verzameling t.o.v. de optelling een commutatieve groep is. Hieruit volgt:

Er is één en slechts één nulelement 0 met de eigenschap, dat $a + 0 = a$ voor iedere a. Bij ieder element a behoort één en slechts één tegengestelde $-a$, zodat $-a + a = 0$.

De aftrekking is eenduidig, d.w.z. er is bij gegeven a en b slechts één element x, waarvoor $a + x = b$, n.l. $x = -a + b$. We noemen x het verschil van b en a; we schrijven $x = b - a$.

We kunnen nu bewijzen dat $a\,0 = 0$ voor iedere a:

$$a\,0 = a\,(0 + 0) = a0 + a0$$

en $$a\,0 = a\,0 + 0$$

Uit de eenduidigheid van de aftrekking volgt dus, dat $a0 = 0$.

Voor een integriteitsgebied moeten nu verder nog de volgende eigenschappen gelden:

8. Er is tenminste één van 0 verschillend element.

9. Uit $a\,b = ac$ en $a \neq 0$ volgt $b = c$.

Deling door een van 0 verschillend element is, indien mogelijk, eenduidig. Is $d = ab$ en $a \neq 0$, dan schrijven we $b = \frac{d}{a}$. Men noemt a een deler van d.

Van belang is de volgende stelling:
Is I een integriteitsgebied en J een deelverzameling van I, die ten minste één van 0 verschillend element bevat en met a en b ook hun verschil en hun product bevat, dan is J t.o.v. optelling en vermenigvuldiging in I weer een integriteitsgebied.

Bewijs: J bevat een element a en dus ook $a - a = 0$. Met een element b bevat J dus ook het tegengestelde $-b = 0 - b$. Met a en b bevat J dus de som $a + b = a - (-b)$. Dat J aan de eigenschappen van een integriteitsgebied voldoet, is dan duidelijk.

Van bijzonder belang zijn integriteitsgebieden met een eenelement. Een element e is eenelement, als voor iedere a geldt, dat $ea = a$.

Een integriteitsgebied heeft ten hoogste één eenelement. Geldt n.l. voor iedere a, dat $ea = e'a = a$, dan geldt dit dus ook voor een van 0 verschillende a; uit de eenduidigheid van de deling door een van 0 verschillend element volgt dan $e = e'$. Is $ea = a$ voor zeker van 0 verschillend element a, dan is e eenelement. Voor een willekeurig element b geldt n.l. $(be)a = b(ea) = ba$; uit de eenduidigheid van de deling door a volgt dan $be = b$.

We zullen nu eenheden definiëren in een integriteitsgebied met eenelement. Onder een eenheid verstaat men een deler van het eenelement. Ieder integriteitsgebied met eenelement heeft ten minste één eenheid, n.l. het eenelement zelf.

Is e het eenelement, ε een eenheid, dan noemen we $\frac{e}{\varepsilon}$ het inverse element van ε, geschreven ε^{-1}.

Nu geldt de volgende stelling:
In een integriteitsgebied I met een eenelement vormen de eenheden een commutatieve groep t.o.v. de vermenigvuldiging.

De vermenigvuldiging van eenheden is n.l. associatief en commutatief. Onder de eenheden komt het eenelement van I voor, dat ook eenelement is voor de vermenigvuldiging van de eenheden. Bij iedere eenheid behoort een inverse eenheid. We moeten nu nog aantonen, dat het product van twee eenheden weer een eenheid is. Dat is ook gemakkelijk in te zien. Bij het product van twee eenheden behoort n.l. als invers element het product van de inversen der factoren. Het product is dus ook een eenheid.

Hiermee is aangetoond, dat de eenheden t.o.v. de vermenigvuldiging een commutatieve groep vormen.

Heeft ieder van 0 verschillend element een invers, dan is deling door een van 0 verschillend element steeds mogelijk en hebben we een <u>lichaam</u>. Is omgekeerd deling door een van 0 verschillend element steeds mogelijk, dan is er een eenelement en heeft ieder van 0 verschillend element een invers.

Zij D een natuurlijk getal, dat geen quadraat is. We beschouwen nu de verzameling $G[\sqrt{D}]$, bestaande uit de getallen $a_1 + a_2\sqrt{D}$, waarin a_1 en a_2 gehele rationale getallen. $G[\sqrt{D}]$ is een deelverzameling van het lichaam van de reële getallen, die met de getallen α en β ook $\alpha - \beta$ en $\alpha\beta$ bevat en zeker een van 0 verschillend getal bevat, is dus een integriteitsgebied, en wel een integriteitsgebied met een eenelement, want het getal 1 behoort er toe.

Is $\alpha = a_1 + a_2\sqrt{D}$, waarin a_1 en a_2 gehele rationale getallen, dan verstaat men onder het <u>geconjugeerde</u> getal $\bar{\alpha}$ het getal $a_1 - a_2\sqrt{D}$. Nu zijn $\alpha + \bar{\alpha}$ en $\alpha\bar{\alpha}$ gehele rationale getallen. Het is ook duidelijk, dat $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$ en $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$.

<u>Stelling</u>: $G[\sqrt{D}]$ bevat een getal ε, groter dan 1, zodat de getallen $\pm \varepsilon^n$, waarin n de gehele rationale getallen doorloopt, juist alle eenheden van $G[\sqrt{D}]$ zijn.

<u>Bewijs</u>: Neem aan, dat α een eenheid is. Zij $\alpha^{-1} = \rho$. Uit $\alpha\rho = 1$ volgt nu $\bar{\alpha}\bar{\rho} = 1$. Dus: $(\alpha\bar{\alpha})(\rho\bar{\rho}) = 1$. Hier zijn beide factoren gehele rationale getallen. Dus $\alpha\bar{\alpha} = 1$ of $\alpha\bar{\alpha} = -1$. Dan is dus $\bar{\alpha} = \alpha^{-1}$ of $\bar{\alpha} = -\alpha^{-1}$.

Uit de oplosbaarheid van de vergelijking van Pell volgt het bestaan in $G[\sqrt{D}]$ van een eenheid, die groter dan 1 is.

Immers $x^2 - Dy^2 = 1$, waarin x en y natuurlijke getallen. Dus:

$$(x + y\sqrt{D})(x - y\sqrt{D}) = 1.$$

$x + y\sqrt{D}$ is dus eenheid en $x + y\sqrt{D} > 1$. Zij $\alpha = a_1 + a_2\sqrt{D}$, waarin a_1 en a_2 gehele rationale getallen, een eenheid, groter dan 1. Dan zijn a_1 en a_2 positief.

Daar $\alpha > 1$ is, is immers $0 < \alpha^{-1} < 1$. Is $\bar{\alpha} = \alpha^{-1}$, dan is dus: $0 < \alpha - \alpha^{-1} = \alpha - \bar{\alpha} = 2a_2\sqrt{D}$. Dus: $a_2 > 0$.

Dan is verder: $a_1 = \bar{\alpha} + a_2\sqrt{D} = \alpha^{-1} + a_2\sqrt{D} > 0$. Is $\bar{\alpha} = -\alpha^{-1}$, dan is: $0 < \alpha - \alpha^{-1} = \alpha + \bar{\alpha} = 2a_1$. Dus: $a_1 > 0$. Dan is ook: $0 < \alpha^{-1} + a_1 = -\bar{\alpha} + a_1 = a_2\sqrt{D}$. Dus: $a_2 > 0$.

Zij η een eenheid, $\eta > 1$. Opdat de eenheid $\alpha = a_1 + a_2\sqrt{D}$ tussen 1 en η ligt, is nu noodzakelijk, dat $0 < a_1 < \eta$ en $0 < a_2 < \eta$. Er kunnen dus slechts eindig veel eenheden tussen 1 en η liggen. Er is dus een kleinste eenheid, die groter dan 1 is. Deze noemen we ε. Het is duidelijk, dat alle getallen $\pm\varepsilon^n$, waarin n de gehele rationale getallen doorloopt, eenheden zijn.

Nu is: $1 < \varepsilon < \varepsilon^2 < \varepsilon^3 < \ldots\ldots$

Zij η weer een eenheid, groter dan 1. Er zijn slechts eindig veel eenheden tussen 1 en η. Er is dus een natuurlijk getal n, zodat:

$$\varepsilon^n \leqq \eta < \varepsilon^{n+1}$$

Dan is: $1 \leqq \frac{\eta}{\varepsilon^n} < \varepsilon$.

$\frac{\eta}{\varepsilon^n}$ is weer een eenheid. Daar er tussen 1 en ε geen eenheden zijn, is dus $\frac{\eta}{\varepsilon^n} = 1$, dus $\eta = \varepsilon^n$.

Is ζ een eenheid, waarvoor $0 < \zeta < 1$ geldt, dan is $\zeta^{-1} > 1$ en dus $\zeta^{-1} = \varepsilon^n$, waarin n een natuurlijk getal. Dus: $\zeta = \varepsilon^{-n}$.

Daar $1 = \varepsilon^0$, is dus iedere pos. eenheid een macht van ε. Een neg. eenheid is het tegengestelde van een pos. eenheid, dus van een macht van ε. Hiermee is de stelling bewezen.

Nu komt het bewijs van de stelling van Petr:

I. We bewijzen eerst, dat ten minste één van de vergelijkingen (1) in natuurlijk getallen oplosbaar is, die voldoen aan (2). De vergelijking $x^2 - Dy^2 = 1$ is in natuurlijke getallen oplosbaar.

Zij w de kleinst mogelijke natuurlijke waarde voor y, t de bijbehorende waarde voor x. Nu is:

$$\begin{aligned} t^2 - D\,w^2 &= 1 \\ t^2 - 1 &= Dw^2 \\ (t+1)(t-1) &= Dw^2 . \end{aligned}$$

t+1 en t-1 hebben geen gemeenschappelijke priemfactoren, behalve eventueel één factor 2. Van de priemfactoren van w wordt dus ten hoogste één factor 2 over beide factoren t + 1 en t - 1 verdeeld. Dan is dus:

$$(3)\qquad \begin{cases} t + 1 = 2^{a} D_1' v_1^2 \\ t - 1 = 2^{a} D_2' v_2^2 \end{cases}$$

waarin a = 0 of a = 1; D_1', D_2', v_1, v_2 natuurlijke getallen, zodat $D_1' D_2' = D$ en $2^a v_1 v_2 = w$. Nu is:

$$2 = 2^{a} (D_1' v_1^2 - D_2' v_2^2).$$

Daar D geen quadraat is, zijn D_1' en D_2' verschillend. Het kleinste van deze twee getallen noemen we nu D_1, het grootste D_2. Dan is:

$$D_1 u^2 - D_2 v^2 = e ,$$

waarin e = 1, -1, 2 of -2; u en v zijn de getallen v_1 en v_2.

De mogelijkheid $D_1 = 1$, e = 1 is uitgesloten. In dat geval zou $u^2 - Dv^2 = 1$ zijn, waarin 2 u v = w, dus $v < w$. Daar w de kleinste natuurlijke waarde voor y in de vergelijking $x^2 - Dy^2 = 1$ is, is dit onmogelijk.

Hiermee is de oplosbaarheid van een van de vergelijkingen (1) in natuurlijke getallen aangetoond. Nu moet nog bewezen worden, dat bij geschikte keuze aan (2) voldaan is. Is aan (2) niet voldaan, dan moet $|e| = 2$ zijn en $(u, D_2) = 2$ of $(v, D_1) = 2$. In (3) is dan a = 0 en $(v_1, D_2') = 2$ of $(v_2, D_1') = 2$. Laat aan (3) voldaan zijn door:

$$a = 0,\ D_1' = \Delta_1,\ D_2' = \Delta_2,\ v_1 = w_1,\ v_2 = w_2,\ \text{waarbij } (w_1, \Delta_2) = 2 \text{ of } (w_2, \Delta_1) = 2.$$

Zij $(w_1, \Delta_2) = 2$. We voeren dan in:

$$\bar{\Delta}_1 = 2\Delta_1,\ \bar{\Delta}_2 = \tfrac{1}{2}\Delta_2,\ \bar{w}_1 = \tfrac{1}{2} w_1 .$$

Nu is:

$$t + 1 = \Delta_1 w_1^2 = 2 \bar{\Delta}_1 \bar{w}_1^2$$

$$t - 1 = \Delta_2 w_2^2 = 2 \bar{\Delta}_2 w_2^2$$

$$\bar{\Delta}_1 \bar{\Delta}_2 = \Delta_1 \Delta_2 = D ,\ 2 \bar{w}_1 w_2 = w_1 w_2 = w .$$

Aan (3) is dus ook voldaan door:

$$a = 1,\ D_1' = \bar{\Delta}_1,\ D_2' = \bar{\Delta}_2,\ v_1 = \bar{w}_1,\ v_2 = w_2 .$$

Ook als $(w_2, \Delta_1) = 2$, is aan (3) te voldoen met a = 1. Uit a = 1 volgt onmiddellijk, dat $|e| = 1$ en dat dus aan (2) voldaan is. Bij geschikte keuze is dus steeds aan (2) voldaan.

II. Alle eenheden van $G[\sqrt{D}]$ kunnen worden voorgesteld door $\pm \varepsilon^n$.

Nu is $t + w\sqrt{D}$ zo'n eenheid, die groter dan 1 is. Dus $t + w\sqrt{D} = \varepsilon^g$, waarin g een natuurlijk getal.

Laat de natuurlijke getallen t', w' nu een willekeurige oplossing van de vergelijking $x^2 - D y^2 = 1$ vormen.

Dan is: $t' + w'\sqrt{D} = \varepsilon^h$,

waarin h weer een natuurlijk getal. Zij d = (g,h). De getallentheorie leert ons, dat er dan twee gehele rationale getallen a en b zijn, zodat d = g a + h b.

Zij $\varepsilon^d = T + W\sqrt{D}$.

Daar $\varepsilon^d > 1$ is, zijn T en W positief. Nu is:

$$T + W\sqrt{D} = (t + w\sqrt{D})^a (t' + w'\sqrt{D})^b$$

Dan is: $T - W\sqrt{D} = (t - w\sqrt{D})^a (t' - w'\sqrt{D})^b$

Dus: $T^2 - D W^2 = (t^2 - D w^2)^a (t'^2 - D w'^2)^b = 1.$

T, W voldoet dus aan de vergelijking van Pell.

Nu is $d \leqq g$, dus $T + W\sqrt{D} \leqq t + w\sqrt{D}$. Dan moet $T \leqq t$ en $W \leqq w$ zijn. w is de kleinste natuurlijke waarde voor y in de vergelijking van Pell, dus W = w. Dan is T = t en dus d = g. Dus g is deler van h.

Zij n een natuurlijk getal.

$$(t + w\sqrt{D})^n = t_n + w_n\sqrt{D},$$

waarin t_n en w_n natuurlijke getallen.

$$(t - w\sqrt{D})^n = t_n - w_n\sqrt{D}$$

Dus: $t_n^2 - D w_n^2 = (t^2 - D w^2)^n = 1.$

t_n, w_n vormen dus een oplossing van de vergelijking van Pell.

We krijgen zo alle oplossingen. Gaan we uit van een willekeurige oplossing t', w', dan is n.l. $t' + w'\sqrt{D} = \varepsilon^h = (t+w\sqrt{D})^{\frac{h}{g}}$, waarin $\frac{h}{g}$ een natuurlijk getal is, want we hebben gezien, dat g deler van h is.

III. $$\left(\frac{\sqrt{D_1}\,u + \sqrt{D_2}\,v}{\sqrt{|e|}}\right)^2 = \frac{D_1 u^2 + D_2 v^2 + 2uv\sqrt{D}}{|e|} =$$

$$= \frac{D_1' v_1^2 + D_2' v_2^2 + 2 v_1 v_2\sqrt{D}}{2^{1-a}} =$$

$$= \frac{2^a D_1' v_1^2 + 2^a D_2' v_2^2 + 2^{1+a} v_1 v_2\sqrt{D}}{2} =$$

$$= \frac{(t+1)+(t-1)+2w\sqrt{D}}{2} = t + w\sqrt{D}.$$

Voor ieder natuurlijk getal m is dus:

$$\left(\frac{\sqrt{D_1}\,u + \sqrt{D_2}\,v}{\sqrt{|e|}}\right)^{2m} = t_m + w_m\sqrt{D}.$$

Beschouw nu een willekeurige vergelijking uit het stelsel (1) en neem aan, dat deze een oplossing heeft, die voldoet aan (2):

$d_1 x_1^2 - d_2 x_2^2 = e_1$, $(x_1,d_2)= (x_2,d_1)= 1$.

$d_1 d_2 = D$, $0 < d_1 < d_2$, $|e_1| = 1$ of $|e_1| = 2$,

$x_1 > 0$, $x_2 > 0$, niet $d_1 = e_1 = 1$.

Dan is: $$\left(\frac{\sqrt{d_1}x_1 + \sqrt{d_2}\,x_2}{\sqrt{|e_1|}}\right)^2 = \frac{d_1x_1^2 + d_2x_2^2 + 2\,x_1x_2\sqrt{D}}{|e_1|} =$$

$$= \frac{e_1 + 2\,d_2x_2^2 + 2\,x_1x_2\sqrt{D}}{|e_1|} =$$

$$= r + s\sqrt{D},$$

waarin r en s natuurlijke getallen.

$$\left(\frac{\sqrt{d_1}x_1 - \sqrt{d_2}x_2}{\sqrt{|e_1|}}\right)^2 = r - s\sqrt{D}.$$

Nu is:

$$r^2 - Ds^2 = (r+s\sqrt{D})(r-s\sqrt{D}) = \left(\frac{\sqrt{d_1}x_1 + \sqrt{d_2}x_2}{\sqrt{|e_1|}}\right)^2 \cdot \left(\frac{\sqrt{d_1}x_1 - \sqrt{d_2}x_2}{\sqrt{|e_1|}}\right)^2 =$$

$$= \left(\frac{d_1x_1^2 - d_2x_2^2}{|e_1|}\right)^2 = \left(\frac{e_1}{|e_1|}\right)^2 = 1 .$$

Er is dus een natuurlijk getal n, zodat $r = t_n$, $s = w_n$ (zie II).

Dan is: $$\left(\frac{\sqrt{d_1}x_1 + \sqrt{d_2}x_2}{\sqrt{|e_1|}}\right)^2 = \left(\frac{\sqrt{D_1}u + \sqrt{D_2}v}{\sqrt{|e|}}\right)^{2n}$$

$$\frac{\sqrt{d_1}x_1 + \sqrt{d_2}x_2}{\sqrt{|e_1|}} = \left(\frac{\sqrt{D_1}u + \sqrt{D_2}v}{\sqrt{|e|}}\right)^n$$

Neem n oneven aan. Dan is:

$$(\sqrt{D_1}\,u + \sqrt{D_2}\,v)^n = \sqrt{D_1}\,u_n + \sqrt{D_2}\,v_n ,$$

waarin u_n en v_n natuurlijke getallen.

$$(\sqrt{|e|})^n = 2^b\sqrt{|e|} ,$$

waarin $b = 0$ voor $|e| = 1$

$b = \frac{n-1}{2}$ voor $|e| = 2$

Dus: $$\frac{\sqrt{d_1}x_1 + \sqrt{d_2}x_2}{\sqrt{|e|}} = \frac{\sqrt{D_1}u_n + \sqrt{D_2}v_n}{2^b\sqrt{|e|}}$$

$$2^b(\sqrt{|e|\,d_1}x_1 + \sqrt{|e|\,d_2}x_2) = \sqrt{|e_1|\,D_1}\,u_n + \sqrt{|e_1|\,D_2}\,v_n$$

Stel: $|e_1| D_1 = A_1^2 B_1$
$|e_1| D_2 = A_2^2 B_2$
$|e| d_1 = a_1^2 b_1$
$|e| d_2 = a_2^2 b_2$,

waarin A_1, A_2, B_1, B_2, a_1, a_2, b_1, b_2 natuurlijke getallen en B_1, B_2 b_1, b_2 quadraatvrij.

(Een quadraatvrij natuurlijk getal is een natuurlijk getal, dat door geen quadraat > 1 deelbaar is). Dan is:

$$2^b (a_1 x_1 \sqrt{b_1} + a_2 x_2 \sqrt{b_2}) = A_1 u_n \sqrt{B_1} + A_2 v_n \sqrt{B_2} .$$

Nu is: $A_1^2 A_2^2 B_1 B_2 = |e_1|^2 D$, dus $B_1 B_2$ is geen quadraat (want D is geen quadraat), dus $B_1 \neq B_2$. Dan is: $B_1 = b_1$ en $B_2 = b_2$

of $B_1 = b_2$ en $B_2 = b_1$.

Dus: $2^b (a_{i_1} x_{i_1} \sqrt{B_1} + a_{i_2} x_{i_2} \sqrt{B_2}) = A_1 u_n \sqrt{B_1} + A_2 v_n \sqrt{B_2}$,

waarin $i_1 = 1$, $i_2 = 2$

of $i_1 = 2$, $i_2 = 1$.

Daar A_1^2 deler is van $|e_1| D_1$, is A_1 deler van D_1 . Evenzo is A_2 deler D_2 , a_1 deler van d_1, a_2 deler van d_2 . Uit $(u, D_2) = (v, D_1) = (x_1, d_2) = (x_2, d_1) = 1$ volgt dus $(u, A_2) = (v, A_1) = (x_1, a_2) = (x_2, a_1) = 1$.

Zijn D_1 en D_2 beide oneven, dan zijn dus ook A_1 en A_2 beide oneven.

Nu is: $2^b a_{i_1} x_{i_1} = A_1 u_n$, $2^b a_{i_2} x_{i_2} = A_2 v_n$. Dan zijn dus u_n en v_n beide deelbaar door 2^b.

Zijn D_1 en D_2 beide even, dan zijn, daar

$$u_n = D_1^{\frac{n-1}{2}} u^n + \binom{n}{3} D_1^{\frac{n-3}{2}} D_2 u^{n-2} v^2 + \ldots + n D_2^{\frac{n-1}{2}} u v^{n-1}$$

$$v_n = D_2^{\frac{n-1}{2}} v^n + \binom{n}{2} D_2^{\frac{n-3}{2}} D_1 v^{n-2} u^2 + \ldots + n D_1^{\frac{n-1}{2}} v u^{n-1},$$

u_n en v_n beide deelbaar door $2^{\frac{n-1}{2}}$, dus door 2^b.

Is D_1 oneven, D_2 even, dan is u oneven, daar $(u, D_2) = 1$, en dus $D_1 u^2 - D_2 v^2 = e$ oneven, dus $|e| = 1$, dan is dus $b = 0$. Als D_1 even en D_2 oneven is, is eveneens $b = 0$.

Steeds zijn u_n en v_n dus door 2^b deelbaar.

Zij: $u_n = 2^b u_n'$, $v_n = 2^b v_n'$.

Dan is: $a_{i_1} x_{i_1} = A_1 u_n'$, $a_{i_2} x_{i_2} = A_2 v_n'$.

We zullen nu aantonen, dat $|e_1| = |e|$ is.

$|e_1|^2 D = |e_1| D_1 . |e_1| D_2 = A_1^2 B_1 . A_2^2 B_2 = A_1^2 A_2^2 B_1 B_2$
$|e|^2 D = |e| d_1 . |e| d_2 = a_1^2 b_1 . a_2^2 b_2 = a_1^2 a_2^2 b_1 b_2 = a_1^2 a_2^2 B_1 B_2$

Dus: $|e_1| a_1 a_2 = |e| A_1 A_2$.

Is D oneven, dan zijn A_1, A_2, a_1, a_2 ook oneven; het zijn immers delers van D. Dan is $|e_1|=|e|$. Is $D \equiv 2 \pmod 4$, dan is van de getallen D_1 en D_2 er één even, het andere oneven; hetzelfde geldt voor de getallen d_1 en d_2. Dan is $|e_1|=|e|=1$. Is $D \equiv 4 \pmod 8$, dan kunnen D_1 en D_2 niet beide even zijn. Dan zou n.l. $D_1 \equiv D_2 \equiv 2 \pmod 4$ zijn. Daar u en v oneven zouden moeten zijn, zou dan $D_1 u^2 - D_2 v^2 \equiv 0 \pmod 4$, wat niet kan. Van de getallen D_1 en D_2 is er dus weer één even, het ander oneven, en hetzelfde geldt weer voor d_1 en d_2. Dus $|e_1|=|e|=1$.

We hebben nu nog het geval $D \equiv 0 \pmod 8$ te beschouwen. Zij $|e|=$ Dan is $(D_1, D_2)=2$, dus:

$$D_1 \equiv 2 \pmod 4,\ D_2 \equiv 0 \pmod 4$$
$$\text{of}\quad D_1 \equiv 0 \pmod 4,\ D_2 \equiv 2 \pmod 4.$$

Neem het geval, dat $D_1 \equiv 2 \pmod 4$ is. Daar u en v oneven zijn, is in u_n de eerste term door geen hogere macht van 2 dan $2^{\frac{n-1}{2}} = 2^b$ deelbaar alle andere termen zijn door hogere machten van 2 deelbaar. In v_n is de laatste term door geen hogere macht dan 2^b deelbaar, alle andere termen door hogere machten. Dus: $(u_n, 2^{b+1})=(v_n, 2^{b+1})=2^b$. Dan zijn u_n' en v_n' oneven.

Hetzelfde vindt men natuurlijk in het geval, dat $D_2 \equiv 2 \pmod 4$ is. Uit $a_{i_1} x_{i_1} = A_1 u_n'$, $a_{i_2} x_{i_2} = A_2 v_n'$ volgt nu, dat $a_1 a_2$ niet meer factoren 2 bevat dan $A_1 A_2$.

Uit $|e_1| a_1 a_2 = 2 A_1 A_2$ volgt dan, dat $|e_1| = 2$ is. Laat nu gegeven zijn, dat $|e_1| = 2$ is. Dan is $(d_1, d_2)=2$. x_1 en x_2 zijn oneven. Men vindt nu op dezelfde wijze, dat $|e|=2$ is.

Voor $D \equiv 0 \pmod 8$ is dus $|e_1|=|e|=2$ of $|e_1|=|e|=1$. Steeds is dus $|e_1|=|e|$. Hieruit volgt $a_1 a_2 = A_1 A_2$.

Neem $A_1 > a_{i_1}$ aan. Dan is $\frac{A_1}{(A_1, a_{i_1})} > 1$. $\frac{A_1}{(A_1, a_{i_1})}$ is deler van x_{i_1}, want A_1 is deler van $a_{i_1} x_{i_1}$.

Nu is: $$\frac{a_{i_1}}{(A_1, a_{i_1})}\, a_{i_2} = \frac{A_1}{(A_1, a_{i_1})}\, A_2 .$$

Daar $A_1 > a_{i_1}$, volgt hieruit: $$\left(\frac{A_1}{(A_1, a_{i_1})}, a_{i_2} \right) > 1.$$

Dan zou dus ook $(x_{i_1}, a_{i_2}) > 1$ zijn.
Daar echter $(x_{i_1}, a_{i_2})=1$, is dus $A_1 \leq a_{i_1}$. Eveneens is: $A_2 \leq a_{i_2}$.
Dan is: $a_{i_1} = A_1$, $a_{i_2} = A_2$. Hieruit volgt: $d_{i_1} = D_1$, $d_{i_2} = D_2$.
Daar $d_1 < d_2$ en $D_1 < D_2$, is dus $d_1 = D_1$, $d_2 = D_2$.

We tonen nu nog aan, dat $e_1 = e$ is.

$$x_1 = u_n' , \quad x_2 = v_n' .$$

Nu is: $$(\sqrt{D_1}\, u + \sqrt{D_2}\, v)^n = \sqrt{D_1}\, u_n + \sqrt{D_2}\, v_n = 2^b (\sqrt{D_1}\, u_n' + \sqrt{D_2}\, v_n') =$$
$$= 2^b (\sqrt{d_1}\, x_1 + \sqrt{d_2}\, x_2).$$
$$(\sqrt{D_1}\, u - \sqrt{D_2}\, v)^n = \sqrt{D_1}\, u_n - \sqrt{D_2}\, v_n = 2^b (\sqrt{d_1}\, x_1 - \sqrt{d_2}\, x_2).$$

Dus:

$$(D_1 u^2 - D_2 v^2)^n = 2^{2b} (d_1 x_1^2 - d_2 x_2^2)$$
$$e^n = 2^{2b} e_1 .$$

Daar n oneven is, zijn e_1 en e dus beide pos. of beide neg.; daar $|e_1| = |e|$, is dus $e_1 = e$. Kunnen we aantonen, dat n oneven moet zijn, dan is hiermee bewezen, dat slechts één van de vergelijkingen (1) een oplossing in natuurlijke getallen heeft, die aan (2) voldoet.

Voor even n is:

$$\frac{\sqrt{d_1}x_1 + \sqrt{d_2}x_2}{\sqrt{|e_1|}} = t_{\frac{1}{2}n} + w_{\frac{1}{2}n} \sqrt{D}.$$

Voor $|e_1| = 1$ moet dus $d_{i_1} = q^2$ zijn, waarin q een natuurlijk getal. Dan is $D = q^2 d_{i_2}$, $t_{\frac{1}{2}n} = q x_{i_1}$, $x_{i_2} = q w_{\frac{1}{2}n}$. Daar $(x_{i_2}, d_{i_1}) = 1$ is. is dus $q = 1$. Dan is $d_1 = 1$, $d_2 = D$, $x_1 = t_{\frac{1}{2}n}$, $x_2 = w_{\frac{1}{2}n}$. Dus: $e_1 = d_1 x_1^2 - d_2 x_2^2 = t_{\frac{1}{2}n}^2 - D w_{\frac{1}{2}n}^2 = 1$. Dit kan niet; bij $d_1 = 1$ moet $e_1 \neq 1$ zijn. Voor $|e_1| = 2$ moet $d_{i_1} = 2 q^2$ zijn.

$D = 2 q^2 d_{i_2}$, $t_{\frac{1}{2}n} = q x_{i_1}$, $x_{i_2} = 2 q w_{\frac{1}{2}n}$.

Dit is onmogelijk, want $(x_{i_2}, d_{i_1}) = 1$. n moet dus oneven zijn, waarmee het bewijs voltooid is.

Hieronder volgen enige oplossingen:

D	D_1	D_2	e	u	v
2	1	2	-1	1	1
3	1	3	-2	1	1
5	1	5	-1	2	1
6	2	3	-1	1	1
7	1	7	2	3	1
8	2	4	-2	1	1
10	1	10	-1	3	1
11	1	11	-2	3	1
12	3	4	-1	1	1
13	1	13	-1	18	5
14	2	7	1	2	1
15	3	5	-2	1	1
17	1	17	-1	4	1
18	2	9	-1	2	1
19	1	19	-2	13	3
20	4	5	-1	1	1
21	3	7	-1	3	2
22	2	11	-1	7	3
23	1	23	2	5	1
24	4	6	-2	1	1
26	1	26	-1	5	1
27	1	27	-2	5	1
28	4	7	1	4	3