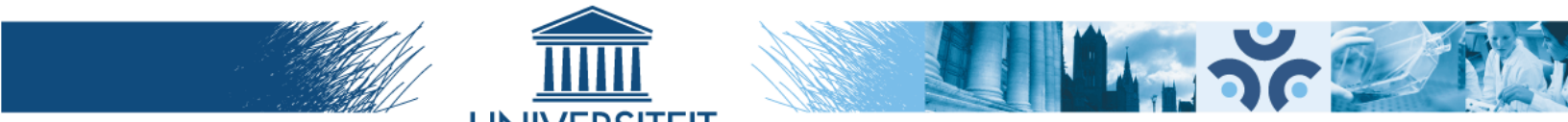

Vakgroep Zuivere Wiskunde

De stelling van Bruck-Ryser

Tine De Plekker
Promotor: Jan De Beule

3^e Bachelor wiskunde
Academiejaar 2014-2015

Inhoudsopgave

1 Inleiding

1.1 Projectieve vlakken

Definitie 1.1. *Een **projectieve vlakke meetkunde** π is een mathematisch systeem samengesteld uit ongedefinieerde elementen, **punten** genaamd, en ongedefineerde verzamelingen van punten (minimum twee), **rechten** genaamd, dat voldoet aan volgende voorwaarden:*

(i) Twee verschillende punten liggen op een unieke rechte.

(ii) Twee verschillende rechten bevatten een uniek gemeenschappelijk punt.

(iii) Elke rechte heeft minimum drie punten.

Het projectieve vlak π is eindig als het bestaat uit een eindig aantal punten. Als π eindig is, dan bestaat er een natuurlijk getal N zo dat elke rechte van π exact $N+1$ verschillende punten heeft en elk punt bevat is in exact $N+1$ verschillende rechten. Bovendien heeft π dan exact N^2+N+1 verschillende punten en N^2+N+1 verschillende rechten.

In alle gekende eindige projectieve vlakken is N een macht van een priemgetal. Inderdaad, voor elk priemgetal p en voor elk positief geheel getal n zijn er eindige meetkundes geconstrueerd door middel van de Galoisvelden $\mathrm{GF}(p^n)$. Het is nog altijd een onbeantwoorde vraag of N een macht van een priemgetal moet zijn. Er is wel al bewezen dat er geen eindige meetkunde bestaat voor $N=6$ en $N=10$. Het doel van deze paper is een grondige studie van de volgende stelling.

Stelling 1.2 (Bruck-Ryser)**.** *Als $N \equiv 1$ of $2 \pmod 4$ en als het kwadraatvrije deel van N ten minste 1 priemfactor van de vorm $4k+3$ bevat, dan bestaat er geen eindige projectieve vlakke meetkunde met $N+1$ punten op een rechte.*

Deze stelling verklaart in het bijzonder dat er geen meetkunde bestaat voor $N=2p$ met p priem van de vorm $4k+3$.

1.2 De incidentiematrix

Een vierkante $n \times n$ -matrix A waarvan elk element 0 of 1 is, is een incidentiematrix als het voldoet aan de volgende drie voorwaarden:

(a) Als r_1 en r_2 twee verschillende rijen zijn van A, dan bestaat er een uniek natuurlijk getal j zodat rijen r_1 en r_2 elk het natuurlijk getal 1 hebben staan in de j-de kolom.

(b) Als c_1 en c_2 twee verschillende kolommen zijn van A, dan bestaat er een uniek natuurlijk getal i zodat de kolommen c_1 en c_2 elk het natuurlijk getal 1 hebben staan op de i-de rij.

(c) Elke rij van A bevat ten minste drie 1-en.

Stelling 1.3. *Als π een eindig projectief vlak met $N+1$ punten op een rechte is, dan bestaat er een incidentiematrix A van orde $n=N^2+N+1$. Als A^T de getransponeerde is van A, dan geldt dat*

$$B = AA^T = A^TA$$

met B een matrix waarvan de elementen gehele getallen zijn: de diagonaalelementen zijn $N+1$ en alle andere elementen zijn 1.

Bewijs. We nummeren de N^2+N+1 punten in gelijk welke volgorde $1, 2, \ldots, N^2+N+1$ en sommen ze op in een rij. We nummeren de N^2+N+1 rechten gelijkaardig en sommen ze op in een kolom. Vervolgens stellen we een tabel op met N^2+N+1 rijen en N^2+N+1 kolommen. Het element op rij i en kolom j is gelijk aan 1 als rechte i punt j bevat en anders gelijk aan nul. Door de eigenschappen van het vlak π, gegeven in de vorige sectie, volgt nu dat de tabel een incidentiematrix voortbrengt:

(i) Twee verschillende punten liggen op een unieke rechte $\Rightarrow$ (b): twee verschillende kolommen hebben op een unieke rij een 1 staan.

(ii) Twee verschillende rechten bevatten een uniek punt $\Rightarrow$ (a): twee verschillende rijen hebben in een unieke kolom een 1 staan.

(iii) Elke rechte heeft minimum drie punten $\Rightarrow$ (c): elke rij bevat minstens drie 1-en.

Tot slot moeten we nog aantonen dat deze matrix voldoet aan $B = AA^T = A^TA$. Als we de bekomen matrix A noemen, weten we dat elke rij van A met elke kolom van A^T exact één 1 gemeen heeft, aangezien elke twee rechten in 1 punt snijden. Dit geldt niet voor de diagonaalelementen omdat daar de rij van A en de kolom van A^T dezelfde rij voorstellen en dus $N+1$ punten gemeen hebben. □

Stelling 1.4. *Als een matrix A met niet-negatieve gehele getallen en van orde $n > 1$ voldoet aan $B = AA^T = A^TA$, met $N \geq 2$, dan is A een incidentiematrix en definieert A een eindig projectief vlak met $N+1$ punten op een rechte.*

Bewijs. De matrix A moet volledig gemaakt worden met 0-en en 1-en. Als a_{ij} immers een element is van A in rij i en kolom j en als a_{ij} groter zou zijn dan 1, dan zou door $B = AA^T = A^TA$ elk element in kolom j van A buiten a_{ij} nul moeten zijn. Bovendien zou dan elk element in rij i van A buiten a_{ij} nul moeten zijn. Dan zou de matrix AA^T echter een nulelement bevatten, en dit is onmogelijk als A moet voldoen aan $B = AA^T = A^TA$. Aangezien A dus bestaat uit 0-en en 1-en en voldoet aan $B = AA^T = A^TA$ met $N \geq 2$, volgt dat A een incidentiematrix is en deze kan gebruikt worden om een eindig projectief vlak te definiëren. □

2 De p-adische getallen

2.1 De p-adische getallen

2.1.1 De p-adische afstand

We hebben in $\mathbb{Q}$ onderstaande absolutewaardefunctie en bijhorende afstandsfunctie $d(x, y) = |x-y|$.

$$|x| = \begin{cases} x, & \text{als } x \geq 0, \\ -x, & \text{als } x < 0. \end{cases}$$

De afstandsfunctie voldoet aan de driehoeksongelijkheid $d(x, z) \leq d(x, y) + d(y, z)$. Men zegt dat een rij $(x_n)_{n\in\mathbb{N}}$ van rationale getallen naar een rationaal getal x convergeert, als er voor elke $\epsilon > 0$ een $N \in \mathbb{N}$ bestaat, zodat $|x_n - x| < \epsilon$ voor alle $n \geq N$. Een Cauchy-rij in $\mathbb{Q}$ is een rij $(x_n)_{n\in\mathbb{N}}$ van rationale getallen, zodat er voor elke $\epsilon > 0$ een $N \in \mathbb{N}$ bestaat met $|x_n - x_m| < \epsilon$ voor alle $n, m \geq N$. Door de driehoeksongelijkheid is elke convergente rij een Cauchy-rij ($|x_n - x_m| \leq |x_n - x| + |x - x_m| < \epsilon + \epsilon = 2\epsilon$). Er bestaan echter Cauchy-rijen die niet naar een rationaal

getal convergeren. Zo bekomt men de reële getallen als vervollediging van de rationale getallen met betrekking tot de afstandsfunctie d:

$$\mathbb{R} = \{\text{Cauchy-rijen } (x_n)_{n\in\mathbb{N}} \text{ in } \mathbb{Q}\}/\sim,$$

waarbij de equivalentierelatie $\sim$ door

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \Leftrightarrow (x_i - y_i)_{i\in\mathbb{N}} \text{ is een nulrij}$$

gegeven is (een nulrij is een rij die naar 0 convergeert). Het veld $\mathbb{R}$ van de reële getallen is compleet, i.e. elke Cauchy-rij convergeert naar een reëel getal. We kunnen een reëel getal voorstellen als een punt op de getallenrechte. We gaan nu een gelijkaardig proces op $\mathbb{Q}$ uitvoeren, maar met een andere afstandsfunctie. Hierbij is geen intuïtieve interpretatie mogelijk zoals bij $\mathbb{R}$.

Zij p een willekeurig priemgetal. Elk van nul verschillend rationaal getal r heeft een eenduidige voorstelling van de vorm

$$r = \frac{a}{b}p^n$$

met $a, b, n \in \mathbb{Z}, b > 0$ en $(a, b) = (a, p) = (b, p) = 1$.

Definitie 2.1. *Het in de bovenstaande vergelijking voorkomende gehele getal*

$$n =: v_p(r)$$

heet de ***p-valuatie*** *van r. (Afspraak: $v_p(0) = \infty$)*

Lemma 2.2. *Voor $x, y \in \mathbb{Q}$ geldt*

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq \min(v_p(x), v_p(y))$
3. *Als $v_p(x) \neq v_p(y)$, dan geldt $v_p(x + y) = \min(v_p(x), v_p(y))$.*

Bewijs. Neem $x, y \in \mathbb{Q}$ en stel $x = \frac{a}{b}p^n$ en $y = \frac{c}{d}p^m$ met a, b, c, d, n, m zoals in de definitie.

1. $xy = \frac{a}{b}p^n\frac{c}{d}p^m = \frac{ac}{bd}p^{n+m} \Rightarrow v_p(xy) = n + m = v_p(x) + v_p(y)$
2. $x + y = \frac{a}{b}p^n + \frac{c}{d}p^m$. Stel z.v.v.a. $n < m$ dus $n = \min(n, m)$, dan is $x + y = p^n(\frac{a}{b} + \frac{c}{d}p^{m-n})$. Als $n = m$ dan is $x + y = p^n(\frac{a}{b} + \frac{c}{d}) = p^n(\frac{ad+bc}{bd})$. bd kan geen macht van p bevatten. $ad + bc$ zou echter wel een macht van p kunnen bevatten, waardoor $v_p(x + y) \geq \min(v_p(x), v_p(y))$.
3. Als $n \neq m$ dan geldt dat $x + y = p^n(\frac{a}{b} + \frac{c}{d}p^{m-n}) = p^n(\frac{ad+bcp^{m-n}}{bd})$. bd kan opnieuw geen macht van p bevatten. $ad + bcp^{m-n}$ kan enkel een macht van p bevatten als ad een macht van p bevat, wat niet kan. Hierdoor is $v_p(x + y) = \min(v_p(x), v_p(y))$.

□

Definitie 2.3. *Voor een rationaal getal r heet*

$$|r|_p = \begin{cases} p^{-v_p(r)}, & \text{als } r \neq 0, \\ 0, & \text{als } r = 0. \end{cases}$$

de ***p-waarde*** *van r. (Afspraak: $p^{-\infty} = 0$)*

Men observeert dat de p-waarde van een rationaal getal r klein wordt, als de teller van r door een grote p-macht deelbaar is. Een geheel getal heeft een p-waarde kleiner of gelijk aan 1 en deze wordt steeds kleiner hoe meer het getal deelbaar is door p.

Gevolg 2.4. *Voor $x, y \in \mathbb{Q}$ geldt*

1. $|xy|_p = |x|_p|y|_p$
2. $|x+y|_p \leq \max(|x|_p, |y|_p)$
3. *Als $|x|_p \neq |y|_p$, dan geldt $|x+y|_p = \max(|x|_p, |y|_p)$.*

Bewijs. Neem $x, y \in \mathbb{Q}$ en stel $x = \frac{a}{b}p^n$ en $y = \frac{c}{d}p^m$ met a, b, c, d, n, m zoals in de definitie.

1. $|xy|_p = p^{-v_p(xy)} = p^{-(v_p(x)+v_p(y))} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$
2. $|x+y|_p = p^{-v_p(x+y)} \leq p^{-\min(v_p(x),v_p(y))} = \max(p^{-v_p(x)}, p^{-v_p(y)}) = \max(|x|_p, |y|_p)$
3. $|x|_p \neq |y|_p \Rightarrow v_p(x) \neq v_p(y) \Rightarrow |x+y|_p = p^{-v_p(x+y)} = p^{-\min(v_p(x),v_p(y))} = \max(|x|_p, |y|_p)$

□

Definitie 2.5. *Zij $x, y \in \mathbb{Q}$. Het getal*

$$d_p(x, y) = |x - y|_p$$

*heet de **p-adische afstand** van x en y.*

Voorbeeld 2.6. *Aangezien $12 = 2.2.3$ geldt dat $v_2(12) = 2$, $v_3(12) = 1$ en $v_p(12) = 0, \forall p > 3$.*

- $d_2(4, 16) = |12|_2 = 2^{-2} = \frac{1}{4}$
- $d_3(4, 16) = |12|_3 = 3^{-1} = \frac{1}{3}$
- $d_5(4, 16) = |12|_5 = 5^{-0} = 1$

$|r|_p = 0$ enkel voor $r = 0$, omdat $|r|_p$ dan gelijk is aan $p^{-v_p(r)} = p^{-\infty} = 0$. Hieruit volgt dat $d_p(x, y) = 0 \Leftrightarrow x = y$. Bovendien geldt dat

$$\begin{aligned} d_p(x, z) = |x - z|_p &= |(x - y) + (y - z)|_p \\ &\leq \max(|x - y|_p, |y - z|_p) \\ &= \max(d_p(x, y), d_p(y, z)) \end{aligned}$$

Deze relatie noemt men de **versterkte driehoeksongelijkheid**. Wegens $\max(d_p(x, y), d_p(y, z)) \leq d_p(x, y) + d_p(y, z)$ geldt natuurlijk ook de gewone driehoeksongelijkheid. Op volledig dezelfde manier als het bewijs met de gewone afstand bewijst men dat een rij $(x_n)_{n\in\mathbb{N}}$ van rationale getallen een **p-adische Cauchy-rij** is, als er voor elke $\epsilon > 0$ een $N \in \mathbb{N}$ bestaat waarvoor $d_p(x_n, x_m) < \epsilon$ voor alle $n, m \geq N$. Door de versterkte driehoeksongelijkheid kan men deze uitdrukking ook in de vorm $d_p(x_n, x_N) < \epsilon$ voor alle $n \geq N$ schrijven, wat voor de normale afstand vals is. We hebben immers dat

$$\begin{aligned} d_p(x_n, x_N) \leq |x_n - x_N|_p &= |(x_n - x_m) + (x_m - x_N)|_p \\ &\leq \max(|x_n - x_m|_p, |x_m - x_N|_p) = \max(d_p(x_n, x_m), d_p(x_m, x_N)) < \epsilon \end{aligned}$$

Maar bij de gewone absolute waarde is $|(x_n - x_m) + (x_m - x_N)| \leq |x_n - x_m|_p + |x_m - x_N|_p < 2\epsilon$. Er bestaan p-adische Cauchy-rijen die geen limiet in $\mathbb{Q}$ hebben. Om een duidelijker onderscheid te hebben, zullen we vanaf nu de gewone absolute waarde $|x|$ en afstand $d(x, y)$ schrijven als $|x|_\infty$ en $d_\infty(x, y)$.

Lemma 2.7. *(i) Is $(x_n)_{n\in\mathbb{N}}$ een p-adische Cauchy-rij, dan is de rij $(|x_n|_p)_{n\in\mathbb{N}}$ ook een Cauchy-rij m.b.t. de gewone afstand.*

(ii) De rij $(x_n)_{n\in\mathbb{N}}$ is een p-adische nulrij als de rij $(|x_n|_p)_{n\in\mathbb{N}}$ m.b.t. de gewone afstand naar 0 convergeert.

(iii) Zij $(x_n)_{n\in\mathbb{N}}$ een p-adische Cauchy-rij, maar geen p-adische nulrij. Dan bestaat er een $N \in \mathbb{N}$ en een $k \in \mathbb{Z}$, zo dat $|x_n|_p = p^k$ voor alle $n \geq N$.

Bewijs. Voor rationale getallen x en y impliceert de driehoeksongelijkheid voor de p-adische afstand de ongelijkheden

$$-|x - y|_p \leq |x|_p - |y|_p \leq |x - y|_p. \tag{1}$$

Daaruit volgt

$$\left||x|_p - |y|_p\right|_\infty \leq |x - y|_p. \tag{2}$$

Zij nu (x_n) een p-adische Cauchy-rij. Dan bestaat er voor elke $\epsilon > 0$ een $N \in \mathbb{N}$ met $|x_n - x_m|_p < \epsilon$ voor alle $n, m \geq N$. Uit (2) volgt dat voor $n, m \geq N$

$$\left||x_n|_p - |x_m|_p\right|_\infty \leq |x_n - x_m|_p < \epsilon.$$

Daardoor is de rij $(|x_n|_p)$ een Cauchy-rij m.b.t. de gewone afstand, wat (i) bewijst.
Een rij (x_n) van rationale getallen is een p-adische nulrij als er voor alle $\epsilon > 0$ een $N \in \mathbb{N}$ bestaat waarvoor $|x_n|_p < \epsilon$ voor alle $n \geq N$. Nu is $|x_n|_p$ een niet-negatief rationaal getal waardoor de uitdrukking $|x_n|_p < \epsilon$ equivalent is met de uitdrukking $\left||x_n|_p\right|_\infty < \epsilon$. Hieruit volgt dat (x_n) een p-adische nulrij is als $(|x_n|_p)$ een nulrij is m.b.t. de gewone afstand, wat (ii) bewijst.
De p-adische afstand $|x|_p$ neemt slechts de aftelbaar vele waarden $p^k, k \in \mathbb{Z}$ en 0 aan. Zij nu (x_n) een p-adische Cauchy-rij, die geen nulrij is. Dan moet volgens (i) en (ii) de rij $(|x_n|_p)$ statisch worden. Er bestaat m.a.w. een $k \in \mathbb{Z}$ met $|x_n|_p = p^k$ voor voldoende grote $n \in \mathbb{N}$. Dit bewijst (iii).

□

2.1.2 Het veld van de p-adische getallen

Definitie 2.8. *Het **veld van de p-adische getallen** $\mathbb{Q}_p$ is de vervollediging van $\mathbb{Q}$ m.b.t. de p-adische afstand d_p.*

M.a.w.: De elementen van $\mathbb{Q}_p$, de zogenaamde p-adische getallen, zijn equivalentieklassen van de p-adische Cauchy-rijen $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ m.b.t. de equivalentierelatie

$$(x_i)_{i\in\mathbb{N}} \sim (y_i)_{i\in\mathbb{N}} \Leftrightarrow (x_i - y_i)_{i\in\mathbb{N}} \text{ is een } p\text{-adische nulrij.}$$

Het is makkelijk in te zien dat dit een equivalentierelatie is. Als (x'_n) een deelrij is van de Cauchy-rij (x_n), dan is $(x'_n) \sim (x_n)$. Voor een Cauchy-rij die geen nulrij is, willen we stilzwijgend aannemen dat al zijn elementen van nul verschillen. Hiervoor gaan we over op een geschikte deelrij zonder daarbij van equivalentieklasse te veranderen.

Lemma 2.9. *Zij $(x_n), (y_n)$ en $(x'_n), (y'_n)$ Cauchy-rijen met $(x_n) \sim (x'_n)$ en $(y_n) \sim (y'_n)$, dan geldt ook $(x_n + y_n) \sim (x'_n + y'_n)$ en $(x_n y_n) \sim (x'_n y'_n)$. Is $(y_n) \sim (y'_n)$ geen nulrij, dan geldt $\left(\frac{x_n}{y_n}\right) \sim \left(\frac{x'_n}{y'_n}\right)$.*

Bewijs. Volgens de definitie is $(x_n + y_n) \sim (x'_n + y'_n) \Leftrightarrow (x_n + y_n - x'_n - y'_n)$ een p-adische nulrij is, m.a.w. als $|x_n + y_n - x'_n - y'_n|_p$ naar nul convergeert voor $n \to +\infty$. Aangezien $|x_n + y_n - x'_n - y'_n|_p \leq |x_n - x'_n|_p + |y_n - y'_n|_p$ en $(x_n) \sim (x'_n)$ en $(y_n) \sim (y'_n)$, volgt dat dit inderdaad zo is.
Om aan te tonen dat $(x_n y_n) \sim (x'_n y'_n)$ gaan we analoog te werk:

$$\begin{aligned}
|x_n y_n - x'_n y'_n|_p &= \left|\frac{1}{2}((x_n - x'_n)(y_n + y'_n) + (y_n - y'_n)(x_n + x'_n))\right|_p \\
&= \left|\frac{1}{2}\right|_p (|((x_n - x'_n)(y_n + y'_n) + (y_n - y'_n)(x_n + x'_n))|_p) \\
&\leq \epsilon(|(x_n - x'_n)(y_n + y'_n)|_p + |(y_n - y'_n)(x_n + x'_n)|_p) \\
&= \epsilon(|x_n - x'_n|_p |y_n + y'_n|_p + |y_n - y'_n|_p |x_n + x'_n|_p)
\end{aligned}$$

Want als $p = 2$, dan is $\left|\frac{1}{2}\right|_p = p$, anders gelijk aan 1. We stellen $\epsilon = 2$ als $p = 2$ en $\epsilon = 1$ anders. Aangezien $(x_n) \sim (x'_n)$ en $(y_n) \sim (y'_n)$ gaat dit naar 0.
Tot slot bewijzen we dat $\left(\frac{x_n}{y_n}\right) \sim \left(\frac{x'_n}{y'_n}\right)$.
Er geldt dat $\left|\frac{x_n}{y_n} - \frac{x'_n}{y'_n}\right|_p = \left|\frac{x_n y'_n - x'_n y_n}{y_n y'_n}\right|_p = |x_n y'_n - x'_n y_n|_p |(y_n y'_n)^{-1}|_p$. Analoog aan het vorige deel zal de eerste factor naar nul gaan, wat het bewijs vervolledigt. □

Gevolg 2.10. *De operatoren optelling en vermenigvuldiging $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$ en deling $\mathbb{Q}_p \times (\mathbb{Q}_p \setminus \{0\}) \to \mathbb{Q}_p$ die door optelling, vermenigvuldiging en deling van de representerende Cauchy-rijen gegeven zijn, zijn goed gedefinieerd. Door deze operatoren wordt $\mathbb{Q}_p$ een veld.*

De p-adische absolute waarde zet zich door de regel $|(x_n)_{n\in\mathbb{N}}|_p = \lim_{n\to\infty} |x_n|_p$ op natuurlijke wijze van $\mathbb{Q}$ naar $\mathbb{Q}_p$ voort. Lemma 2.2 impliceert dat de limiet bestaat en onafhankelijk is van de keuze van de representant van de Cauchy-rij. Er geldt dat $|(x_n)_{n\in\mathbb{N}}|_p = 0$ a.s.a. $(x_n)_{n\in\mathbb{N}}$ een p-adische nulrij is. Als de Cauchy-rij $(x_n)_{n\in\mathbb{N}}$ geen nulrij is, dan wordt de rij van p-valuaties $(v_p(x_n))_{n\in\mathbb{N}}$ stationair en we noemen zijn limiet, die een geheel getal is, de p-valuatie van het door die rij $(x_n)_{n\in\mathbb{N}}$ gerepresenteerde p-adische getal. Als men de afspraak maakt om een nulrij p-valuatie ∞ toe te kennen, dan zet ook de p-valuatie zich op natuurlijke wijze van $\mathbb{Q}$ naar $\mathbb{Q}_p$ voort. Verder zijn de p-adische absolute waarde en de p-valuatie door volgende regel met elkaar verbonden:

$$|(x_n)_{n\in\mathbb{N}}|_p = p^{-v_p((x_n)_{n\in\mathbb{N}})}$$

Met behulp van de p-adische afstand

$$d_p((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) = |(x_n - y_n)_{n\in\mathbb{N}}|_p$$

bekomen we op natuurlijke wijze begrippen zoals een convergente rij van p-adische getallen, open deelverzamelingen van $\mathbb{Q}_p$, gesloten deelverzamelingen van $\mathbb{Q}_p$, enz.

Stelling 2.11. *De voorgaande eigenschappen in verband met de p-adische absolute waarde, de p-valuatie en de p-adische afstand op $\mathbb{Q}$ zetten zich op natuurlijke wijze om naar $\mathbb{Q}_p$. In het bijzonder blijven lemma 2.2, gevolg 2.4 en lemma 2.7 waar, als men in de opgaves $\mathbb{Q}$ door $\mathbb{Q}_p$ vervangt.*

De velden $\mathbb{Q}_p$ staan volkomen gelijkwaardig naast het veld $\mathbb{R}$ van de reële getallen. Er bestaat echter een belangrijk verschil. De ordening, i.e. de $\leq$-relatie op $\mathbb{Q}$, bestaat niet in $\mathbb{Q}_p$. Het is niet mogelijk om de elementen van $\mathbb{Q}_p$ op een zinvolle manier te ordenen. In dit opzicht zijn de velden $\mathbb{Q}_p$ vergelijkbaar met het veld van de complexe getallen $\mathbb{C}$.
Volgende stelling is de p-adische versie van de Stelling van Bolzano-Weierstrass. We vermelden deze zonder bewijs.

Stelling 2.12. *Het veld $\mathbb{Q}_p$ is compleet: elke Cauchy-rij in $\mathbb{Q}_p$ convergeert. Elke in $\mathbb{Q}_p$ begrensde rij heeft een limietpunt. Elke gesloten en begrensde deelrij in $\mathbb{Q}_p$ is compact.*

Van nu af aan zullen we p-adische getallen als 'echte' getallen beschouwen en hen ook enkel met een eenvoudige letter benoemen.

2.1.3 Gehele p-adische getallen

De geldigheid van de versterkte driehoeksongelijkheid heeft een merkwaardig gevolg. Als namelijk $|x|_p \leq 1$ en $|y|_p \leq 1$, dan is ook $|x+y|_p \leq \max(|x|_p, |y|_p) \leq 1$. Hetzelfde geldt voor het product. Bovendien is de verzameling van zo'n p-adische getallen onder optelling en vermenigvuldiging gesloten en is dus een ring.

Definitie 2.13. *De elementen $x \in \mathbb{Q}_p$ met $|x|_p \leq 1$ heten **gehele p-adische getallen**. Zij vormen een ring die $\mathbb{Z}_p$ genoemd wordt. Equivalent hiermee is: $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | v_p(x) \geq 0\}$.*

Lemma 2.14. *De ring $\mathbb{Z}_p$ is als deelverzameling van $\mathbb{Q}_p$ begrensd, open en gesloten. In het bijzonder is $\mathbb{Z}_p$ compact.*

Lemma 2.15. *De verzameling $\mathbb{Z}$ van gehele getallen is dicht in $\mathbb{Z}_p$. M.a.w. elke geheel p-adisch getal kan als limiet van een rij van gehele getallen geschreven worden.*

Bewijs. Zij $a \in \mathbb{Z}_p$ willekeurig. Het is voldoende om te bewijzen dat er voor elke $n \in \mathbb{N}$ een $A_n \in \mathbb{Z}$ met $v_p(a - A_n) \geq n$ bestaat. De rij $(A_n)_{n\in\mathbb{N}}$ convergeert dan namelijk p-adisch naar a. Zij nu $n \in \mathbb{N}$ vast en zij $(a_i)_{i\in\mathbb{N}}$ een rij van rationale getallen, die p-adisch naar a convergeren. Aangezien $v_p(a) \geq 0$ kunnen we door het weglaten van een eindig aantal elementen in het begin van de rij de geldigheid van de ongelijkheden

$$v_p(a_i) \geq 0, \quad v_p(a_i - a_j) \geq n \text{ voor alle } i, j \in \mathbb{N}$$

aannemen. Zij nu $a_i = \frac{c_i}{d_i}, c_i \in \mathbb{Z}, d_i \in \mathbb{N}, p \nmid d_i$ en zij $A_n \in \mathbb{Z}$ een geheel getal met $d_1 A_n \equiv c_1 \pmod{p^n}$. A_n bestaat aangezien $\overline{d}_1 \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Zij $i \in \mathbb{N}$ willekeurig. Dan geldt dat

$$a_i - a_1 = \frac{c_i}{d_i} - \frac{c_1}{d_1} = p^n \frac{c}{d}, \quad c \in \mathbb{Z}, d \in \mathbb{N}, p \nmid d.$$

Er geldt ook dat $d(c_i d_1 - c_1 d_i) = p^n c d_1 d_i$, en doordat $p \nmid d$ volgt dat $p^n | c_i d_1 - c_1 d_i$. Door de keuze van A_n geldt dat $p^n | (c_i d_1 - d_1 A_n d_i)$. Omdat $d \nmid d_1$ vinden we ook een $b \in \mathbb{Z}$ met $p^n b = c_i - A_n d_i$. We bekomen $a_i - A_n = p^n \frac{b}{d_i}$ en $v_p(a_i - A_n) \geq n$. Omdat i willekeurig was, volgt dat $v_p(a - A_n) \geq n$. $\square$

Volgende stelling is een eerste stap in de algebraïsche karakterisering van de gehele p-adische getallen.

Stelling 2.16. *De natuurlijke inclusie $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induceert voor elk natuurlijk getal n een isomorfisme*

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

Gevolg 2.17. *Elke $a \in \mathbb{Z}_p$ definieert dus een rij $(a_n \in \mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$, namelijk de rij van zijn restklassen modulo p^n. Deze rij voldoet aan de compatibiliteitsvoorwaarde*

$$a_{n+1} \equiv a_n \ (mod\ p^n)$$

aangezien a_n een lineaire combinatie is van $\{p^1, \ldots, p^n\}$ en a_{n+1} van $\{p^1, \ldots, p^{n+1}\}$.

We onderzoeken nu enkele ringtheoretisch eigenschappen van $\mathbb{Z}_p$.

Lemma 2.18. *Een element $u \in \mathbb{Q}_p$ is een eenheid in $\mathbb{Z}_p$ als $v_p(u) = 0$ of dus als $|u|_p = 1$.*

Bewijs. Stel $v_p(u) = 0$, dan is $v_p(u^{-1}) = -v_p(u) = 0$, waardoor $u, u^{-1} \in \mathbb{Z}_p$. Is omgekeerd $u \in \mathbb{Z}_p^\times$, dan is $uv = 1$ voor een $v \in \mathbb{Z}_p^\times$ en daarom is $v_p(u) + v_p(v) = 0$ ($v_p(uv) = v_p(1) = 0$ en $v_p(uv) = v_p(u) + v_p(v)$). Aangezien $v_p(u) \geq 0$ en $v_p(v) \geq 0$ volgt dat $v_p(u) = 0$. □

Gevolg 2.19. *Een element $u \in \mathbb{Z}_p$ is een eenheid als zijn restklasse $u_1 \in \mathbb{Z}/p\mathbb{Z}$ verschillend is van nul.*

Bewijs. Voor $u \in \mathbb{Z}_p$ geldt: $u \in \mathbb{Z}_p^\times \Leftrightarrow v_p(u) = 0 \Leftrightarrow u \in \mathbb{Z}_p \setminus p\mathbb{Z}_p \Leftrightarrow u_1 \neq 0$. □

Lemma 2.20. *Elke $a \in \mathbb{Q}_p$ heeft een eenduidige voorstelling van de vorm*

$$a = p^n u, \quad n \in \mathbb{Z}, \quad u \in \mathbb{Z}_p^\times.$$

Bewijs. Stel $n = v_p(a)$. Dan is $v_p(ap^{-n}) = v_p(a) + v_p(p^{-n}) = n + (-n) = 0$. Hierdoor is $u = ap^{-n} \in \mathbb{Z}_p^\times$, waardoor $a = p^n u$ zoals in de opgave. Is nu omgekeerd $a = p^n u, u \in \mathbb{Z}_p^\times$, dan volgt dat $n = v_p(a), u = ap^{-n}$, wat de eenduidigheid van de voorstelling bewijst. □

2.1.4 De p-adische ontwikkeling

Elk reëel getal kan als een decimaalgetal geschreven worden, waarbij er oneindig veel cijfers na de komma zijn toegestaan. Een analoge beschrijving bestaat ook voor de p-adische getallen. Elk niet-negatief geheel getal N bezit een eenduidige **p-adische ontwikkeling**, namelijk een voorstelling van de vorm

$$N = a_0 + a_1 p + \ldots + a_n p^n,$$

met $a_i \in \{0, 1, \ldots, p-1\}$. Men bekomt deze door N achtereenvolgens met rest door p te delen:

$$\begin{aligned} N &= a_0 + pN_1 \\ N_1 &= a_1 + pN_2 \\ &\vdots \\ N_{n-1} &= a_{n-1} + pN_n \\ N_n &= a_n \end{aligned}$$

In een getallensysteem met basis p zal men nu $N = a_n \ldots a_1 a_0$ schrijven. Omdat op p-adische wijze de machten p^n bij toenemende n steeds kleiner worden, geven we de voorkeur aan de schrijfwijze $N = 0, a_0 a_1 \ldots a_n$. Met deze afspraak krijgen we bijvoorbeeld

$$\begin{aligned} &\text{2-adisch: } 10 = 0,0101 \\ &\text{3-adisch: } 10 = 0,101 \\ &\text{5-adisch: } 10 = 0,02 \end{aligned}$$

Nu kan men ook cijfers voor de komma toelaten. We stellen

$$a_{-m}a_{-m+1}\ldots a_{-1}, a_0a_1\ldots = \sum_{i=-m}^{n} a_i p^i \in \mathbb{Q}.$$

Doordat p^n voor $n \to \infty$ p-adisch naar 0 convergeert, kunnen we ook oneindig veel cijfers na de komma toelaten. We stellen

$$a_{-m}a_{-m+1}\ldots a_{-1}, a_0a_1\ldots = \sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}.$$

Wegens de versterkte driehoeksongelijkheid is de rij van partieelsommen $\sum_{i=-m}^{n} a_i p^i$ een p-adische Cauchy-rij. We moeten hiervoor aantonen dat er voor elke $\epsilon > 0$ een $N \in \mathbb{N}$ bestaat zodat $\left|\sum_{i=-m}^{n} a_i p^i - \sum_{i=-m}^{n'} a_i p^i\right|_p < \epsilon, \forall n, n' \geq N$. Stel nu zonder verlies van algemeenheid dan $n > n'$. Dan is

$$\left|\sum_{i=-m}^{n} a_i p^i - \sum_{i=-m}^{n'} a_i p^i\right|_p = \left|\sum_{i=n'+1}^{n} a_i p^i\right|_p \leq \max_{i\in\{n'+1,\ldots,n\}} |a_i p^i|_p = p^{-(n'+1)}$$

Kies dus N groot genoeg zodat $p^{-(n'+1)}$ kleiner is dan ϵ. Daarom definieert die rij een goed-gedefinieerd p-adisch getal.

Stelling 2.21. *Elk p-adisch getal $x \in \mathbb{Q}_p$ heeft een eenduidig bepaalde voorstelling*

$$x = \sum_{i>>-\infty}^{\infty} a_i p^i = a_{-m}a_{-m+1}\ldots a_{-1}, a_0a_1\ldots$$

met $a_i \in \{0, 1, \ldots, p-1\}$. Zijn p-adische valuatie $v_p(x)$ is het kleinste getal $i \in \mathbb{Z}$ met $a_i \neq 0$. In het bijzonder ligt x in $\mathbb{Z}_p$ als alle cijfers voor de komma nul zijn, dus als $a_i = 0$ voor $i < 0$.

Bewijs. Zij $x = \sum_{i=r}^{\infty} a_i p^i, a_r \neq 0$. Door lemma 2.2 geldt voor elke partieelsom dat

$$v_p\left(\sum_{i=r}^{n} a_i p^i\right) = v_p\left(a_r p^r + \sum_{i=r+1}^{n} a_i p^i\right) = \min\left(a_r p^r, \sum_{i=r+1}^{n} a_i p^i\right) = r$$

en dus ook $v_p(x) = r$. In het bijzonder ligt x in $\mathbb{Z}_p$ als alle cijfers voor de komma nul zijn, aangezien $x \in \mathbb{Z}_p \Leftrightarrow |x|_p \leq 1 \Leftrightarrow p^{-v_p(x)} \leq 1 \Leftrightarrow v_p(x) \geq 0$. Als we x met een vaste p-macht vermenigvuldigen, verschuift enkel de komma. Daardoor kunnen we ons zowel bij het bewijs van het bestaan als bij het bewijs van de eenduidigheid beperken tot het geval $x \in \mathbb{Z}_p$. Zij nu

$$x = a_0 + a_1 p + a_2 p^2 + \ldots.$$

Dan geldt dat $x - (a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}) \in p^n \mathbb{Z}_p$ en

$$N = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}$$

is de p-adische ontwikkeling van het volgens stelling 2.16 eenduidig bepaalde gehele getal N_n met $0 \leq N_n < p^n$ en $x \equiv N_n \pmod{p^n}$. Dit bewijst de eenduidigheid van de rijenvoorstelling. Zij nu

omgekeerd, voor $n \in \mathbb{N}$, N_n het eenduidig bepaalde gehele getal met $0 \leq N_n < p^n$ en $x \equiv N_n \pmod{p^n}$. Doordat $N_{n+1} \equiv N_n \pmod{p}$, stemmen de eerste n plaatsen van de p-adische ontwikkeling van N_{n+1} overeen met die van N_n. Er bestaat dus een rij $a_0, a_1, \ldots$ van gehele getallen, $a_i \in \{0, 1, \ldots, p-1\}$, met $N_n = a_0 + a_1 p + \ldots + a_{n-1}p^{n-1}$ voor alle n. We verkrijgen

$$x = \lim_{n\to\infty} N_n = \sum_{i=0}^{\infty} a_i p^i$$

Dit bewijst het bestaan van de p-adische ontwikkeling. □

2.1.5 p-adische vergelijkingen

We beschouwen een systeem van diophantische vergelijkingen

$$\begin{aligned} f_1(X_1, \ldots, X_r) &= 0 \\ \vdots \qquad &\vdots \\ f_n(X_1, \ldots, X_r) &= 0 \end{aligned}$$

met p-adische gehele polynomen $f_i \in \mathbb{Z}_p[X_1, \ldots, X_r]$, en we zoeken naar oplossingen in $\mathbb{Z}_p^r$. Volgende stelling hebben we nodig voor het volgende deel, maar we laten het topologische bewijs achterwege.

Stelling 2.22. *Bovenstaand systeem heeft een oplossing in $\mathbb{Z}_p^r$ a.s.a. er een oplossing modulo p^m bestaat voor elke $m \in \mathbb{N}$.*

2.2 Het Hilbert-symbool

2.2.1 Het Hilbert-symbool

Zij K gelijk aan $\mathbb{R}$ of aan een van de lichamen $\mathbb{Q}_p$ voor een priemgetal p.

Definitie 2.23. *Voor $a, b \in K^\times$ stellen we het symbool (a, b) gelijk aan 1 als de vergelijking*

$$aX^2 + bY^2 = Z^2$$

een van $(0, 0, 0)$ verschillende oplossing in K^3 bezit. Anders stellen we $(a, b) = -1$. Het zo gedefinieerde symbool $(a, b) \in \{\pm 1\}$ heet het Hilbert-symbool van a en b.

Het Hilbert-symbool verandert niet als je a of b met een kwadraat vermenigvuldigt. In de vergelijking $ac^2X^2 + bY^2 = Z^2$ kan je c^2X^2 gelijkstellen aan X'^2 waardoor de vergelijking waarvoor je een niet-nuloplossing moet vinden, hetzelfde blijft. Het geval waarbij je b vermenigvuldigt met een kwadraat is analoog. M.a.w. voor $a, b, c \in K^\times$ geldt dat $(a, bc^2) = (a, b) = (ac^2, b)$. Daardoor induceert het Hilbert-symbool een afbeelding

$$K^\times/K^{\times 2} \times K^\times/K^{\times 2} \to \{\pm 1\}.$$

Volgende stelling levert ons de belangrijkste eigenschappen van het Hilbert-symbool. We zullen enkele van deze verderop bewijzen.

Stelling 2.24. *Voor het Hilbert-symbool gelden de volgende eigenschappen:*

(i) $(a,b) = (b,a)$,

(ii) $(a,-a) = 1$ *en* $(a,1-a) = 1$,

(iii) $(aa',b) = (a,b)(a',b)$ *en* $(a,bb') = (a,b)(a,b')$,

(iv) uit $(a,b) = 1, \forall b$ *volgt dat* $a \in K^{\times 2}$,

(v) als $a \equiv b \not\equiv 0 \pmod{p}$, *dan is* $(a,p) = (b,p)$.

Hierbij zijn $a, a', b, b' \in K^\times$ *en* $a \neq 1$ *in de tweede uitspraak van (ii).*

Wegens zijn multiplicativiteit en symmetrie wordt het Hilbert-symbool door de volgende stelling volledig beschreven. Daar gebruiken we voor $a \in \mathbb{Z}_2$ de notatie: $(-1)^a = (-1)^{a \pmod 2}$.

Stelling 2.25. *Het Hilbert-symbool wordt als volgt berekend:*

(i) Als $K = \mathbb{R}$, *dan geldt dat* $(a,b) = 1$ *als* a *of* b *positief is. Voor* $a < 0$ *en* $b < 0$ *geldt dat* $(a,b) = -1$.

(ii) Als $k = \mathbb{Q}_p$ *en* $u, v \in \mathbb{Z}_p^\times$, *dan geldt dat*

$$(p,p) = (-1)^{\frac{p-1}{2}}, \quad (p,u) = \left(\frac{u}{p}\right), \quad (u,v) = 1, \text{ als } p \neq 2,$$

$$(2,2) = 1, \quad (2,u) = (-1)^{\frac{u^2-1}{8}}, \quad (u,v) = (-1)^{\frac{u-1}{2}\frac{v-1}{2}}, \text{ als } p = 2.$$

Om voorgaande stellingen te bewijzen, moeten we het Hilbert-symbool voor alle mogelijke waarden uit $(K^\times/K^{\times 2}) \times (K^\times/K^{\times 2})$ berekenen. Het aantal symbolen dat hiervoor berekend moet worden is groot, wat niet elegant, maar wel doenbaar is.

Voor we een deel van de eigenschappen van stelling 2.24 bewijzen, stellen we eerst een verbinding tussen het Hilbert-symbool en normgroepen voor. Voor een willekeurige $d \in K^\times$ verkrijgen we de deelverzameling

$$N_d := \{x \in K^\times | \exists a, b \in K \text{ met } x = a^2 - db^2\}$$

die wegens $(a^2 - db^2)(a'^2 - db'^2) = (aa' + bb'd)^2 - d(ab' + a'b)^2$ en

$$\frac{1}{a^2 - db^2} = \left(\frac{a}{a^2 - db^2}\right)^2 - d\left(\frac{b}{a^2 - db^2}\right)^2$$

zelfs een deelgroep van $K^\times$ is. Als $d = c^2, c \in K^\times$, dan geldt voor elke $x \in K^\times$ dat

$$x = \left(\frac{x+1}{2}\right)^2 - d\left(\frac{x-1}{2c}\right)^2.$$

Aangezien N_d een deelgroep is van $K^\times$ en we zo aangetoond hebben dat $K^\times$ ook een deelgroep is van N_d, geldt dan dat $N_d = K^\times$ als d een kwadraat is.

Stelling 2.26. *Zij* $a, b \in K^\times$. *Dan geldt dat*

$$(a,b) = 1 \Leftrightarrow a \in N_b.$$

In het bijzonder geldt dat $a \in N_b \Leftrightarrow b \in N_a$.

Bewijs. Is $b = c^2, c \in K$, dan is $(0, 1, c)$ een niet-triviale oplossing van $aX^2 + bY^2 = Z^2$, dus $(a, b) = 1$. In dit geval is ook $N_b = K^\times$.
Zij nu b geen kwadraat. Is $a = z^2 - by^2$, dan is $(1, y, z)$ een niet-triviale oplossing van de vergelijking, dus $(a, b) = 1$. Is omgekeerd $(a, b) = 1$ en $(x, y, z) \neq (0, 0, 0)$ een oplossing van de vergelijking, dan geldt $x = 0$ aangezien b anders een kwadraat is. We bekomen

$$x = \frac{z^2}{x^2} - b\frac{y^2}{x^2}$$

en hierdoor volgt dat $a \in N_b$. De tweede bewering volgt nu uit de eerste en uit de symmetrie van het Hilbert-symbool. □

We bewijzen nu volgend nuttig lemma dat een aantal eigenschappen van stelling 2.24 bevat.

Lemma 2.27. *Voor $a, a', b \in K^\times$ gelden de volgende uitspraken:*

(i) $(a, b) = (b, a)$,

(ii) $(a, -a) = 1$ *en* $(a, 1 - a) = 1$ *als* $a \neq 1$,

(iii) $(a, b) = 1 \Rightarrow (aa', b) = (a', b)$,

(iv) $(a, 1) = 1$,

(v) $(a, a) = (-1, a)$.

Bewijs. Uitspraak (i) volgt direct uit de definitie van het Hilbert-symbool. Als $aX^2 + bY^2 = Z^2$ een niet-triviale oplossing (x, y, z) heeft, zal $bX^2 + aY^2 = Z^2$ een niet-triviale oplossing (y, x, z) hebben. Als de eerste vergelijking geen niet-triviale oplossing heeft, zal de andere dat ook niet hebben. $(1, 1, 0)$ is een niet-triviale oplossing van $aX^2 - aY^2 = Z^2$ en $(1, 1, 1)$ is een niet-triviale oplossing van $aX^2 + (1 - a)Y^2 = Z^2$, wat (ii) bewijst. Als nu geldt dat $(a, b) = 1$, dan is door stelling 2.26 $a \in N_b$, en omdat $N_b \subset K^\times$ een deelgroep is, geldt dat $a' \in N_b \Leftrightarrow aa' \in N_b$. Als we stelling 2.26 hier opnieuw op toepassen, bewijzen we uitspraak (iii). Aangezien $N_1 = K^\times$, geldt dat $(a, 1) = 1$ voor alle a door stelling 2.26. Dit bewijst uitspraak (iv). Uit (ii) volgt dat $(-a, a) = 1$, waaruit door (iii) en (iv) de gelijkheden $(a, a) = (-a^2, a) = (-1, a)$ volgen. Dit bewijst (v). □

2.2.2 De productformule

Het veld $\mathbb{Q}$ van de rationale getallen ligt als deelveld in $\mathbb{R}$ en in elke $\mathbb{Q}_p$. Om eenduidigheid in notatie te bekomen, voeren we de benaming $\mathbb{R} = \mathbb{Q}_\infty$ in en duiden de standaard absolute waarde van $\mathbb{R}$ aan met $|\ |_\infty$. Stel P gelijk aan de verzameling van priemgetallen samen met het symbool ∞. Men noemt P de verzameling van de **plaatsen van** $\mathbb{Q}$.

Opmerking: Zij K een veld. Een functie $|\ | : K \to \mathbb{R}$ met eigenschappen

(i) $|x| \geq 0$ en $|x| = 0 \Leftrightarrow x = 0$,

(ii) $|xy| = |x||y|$,

(iii) $|x + y| \leq |x| + |y|$

heet de **absolute waarde** van K en definieert door $d(x,y) = |x-y|$ een afstandsbegrip. Op elk veld bestaat de **triviale** absolute waarde, die door $|0| = 0$ en $|x| = 1$ voor alle $x \neq 0$ gegeven is. Twee absolute waarden zijn **equivalent** als de door hen gedefinieerde verzamelingen van Cauchy-rijen in K gelijk zijn. Elke plaats $v \in P$ definieert een absolute waarde $|\ |_v$ op $\mathbb{Q}$. Volgende omkering geldt: Op $\mathbb{Q}$ is elke niet-triviale absolute waarde equivalent met een van de absolute waarden $|\ |_v, v \in P$. Voor $a, b \in \mathbb{Q}^\times$ en een plaats $v \in P$ is $(a,b)_v$ het Hilbert-symbool van a en b in $\mathbb{Q}_v$. Voor we de producformule bewijzen, tonen we eerst een lemma aan dat we verderop nodig hebben.

Lemma 2.28. *Voor p een oneven priemgetal en voor elk positief geheel getal n geldt dat*

(i) $(n, n+1)_p = (-1, n+1)_p$,

(ii) $(n, n^2+n+1)_p = 1$,

(iii) $\prod_{i=1}^{n} (i, i+1)_p = ((n+1)!, -1)_p$.

Bewijs. (i) Om deze gelijkheid te bewijzen, bekijken we de mogelijke gevallen apart. Stel dat $p \not| n$ en $p \not| n+1$, dan volgt hieruit door stelling 2.25 dat $(n, n+1)_p = 1$ en $(-1, n+1)_p = 1$. Als $p|n$, dan geldt dat $n+1 \equiv 1 \pmod p$, dus $(n, n+1)_p = 1 = (-1, n+1)_p$ want $p \not| -1$ en $p \not| n+1$. Stel tot slot dat $p|n+1$, dan is $n \equiv -1 \pmod p$ waardoor $(n, n+1)_p = (-1, n+1)_p$. De laatste 2 gevallen volgen uit de definitie van het Hilbert-symbool.

(ii) Ook voor deze ongelijkheid maken we een gevallenonderscheid. Het geval waarbij zowel n als n^2+n+1 niet deelbaar zijn door p is triviaal. Stel dat $p|n$. Hieruit volgt dat $n^2+n+1 \equiv 1 \pmod p$ waardoor $nx^2 + (n^2+n+1)y^2 \equiv y^2 \pmod p$ en dus $(n, n^2+n+1)_p = 1$. Stel vervolgens dat $p|n^2+n+1$. Hierdoor is $n \equiv n^2+2n+1 \equiv (n+1)^2 \pmod p$ waardoor $(n, n^2+n+1)_p = (n, (n+1)^2)_p$. We weten dat we kwadraten uit het Hilbert-symbool kunnen schrappen waardoor dit gelijk is aan $(n,1)_p = 1$.

(iii) Deze gelijkheid kunnen we a.d.h.v. de vorige puntjes en stelling 2.24 (i) en (iii) uitrekenen.

$$\begin{aligned}\prod_{i=1}^{n}(i,i+1)_p &= \prod_{i=1}^{n}(-1,i+1)_p = (-1, \prod_{i=1}^{n}(i+1))_p \\ &= (-1, 2.3.\ldots.(n+1))_p = (-1,(n+1)!)_p = ((n+1)!,-1)_p\end{aligned}$$

□

Volgende productformule geldt voor de Hilbert-symbolen $(a,b)_v, a, b \in \mathbb{Q}^\times, v \in P$.

Stelling 2.29 (Productformule voor het Hilbert-symbool)**.** *Voor $a, b \in \mathbb{Q}^\times$ geldt dat $(a,b)_v = 1$ voor bijna alle $v \in P$ en*

$$\prod_{v \in P} (a,b)_v = 1.$$

Bewijs. We kunnen, zonder het Hilbert-symbool te veranderen, a en b met kwadraten vermenigvuldigen en daarom aannemen dat a en b geheel en kwadraatvrij zijn. Omdat een geheel getal maar eindig veel priemdelers heeft, geldt $a, b \in \mathbb{Z}_p^\times$ voor bijna alle p en door stelling 2.25 (ii) volgt dat $(a,b)_v = 1$ voor bijna alle $v \in P$.
Om nu de productformule te bewijzen, kunnen we ons door de multiplicativiteit en de symmetrie van het Hilbert-symbool beperken tot de gevallen $(a,b) = (-1,-1), (a,b) = (-1,p)$, p priem, en $(a,b) = (p,q)$, p, q priem.

- $(a,b) = (-1,-1)$: er geldt dat $(-1,-1)_p = 1$ voor $p \neq 2$, $(-1,-1)_\infty = -1$ en $(-1,-1)_2 = (-1)^{\frac{-1-1}{2}\frac{-1-1}{2}} = (-1)^1 = -1$. De twee minnen heffen elkaar op waardoor we de productformule krijgen.

- $(a,b) = (-1,p)$, $p \neq 2$ priem: er geldt dat $(-1,p)_\infty = 1, (-1,p)_q = 1$ voor $q \not| 2p$, $(-1,p)_p = (-1)^{\frac{p-1}{2}}$ en $(-1,p)_2 = (-1)^{\frac{p-1}{2}}$. Net zoals bij het vorige puntje heffen de 2 eventuele minnen elkaar op.

- $(a,b) = (-1,2)$: doordat $(-1).1^2 + 2.1^2 = 1^2$ geldt dat $(-1,2)_v = 1$ voor alle $v \in P$ en de productformule is triviaal.

- $(a,b) = (p,q)$ met p,q oneven priemgetallen: Er geldt dat $(p,q)_\infty = 1, (p,q)_r = 1$ voor $r \not| 2pq$, $(p,q)_p = \left(\frac{q}{p}\right), (p,q)_q = \left(\frac{p}{q}\right)$ en $(p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Uit de kwadratische reciprociteitsstelling $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$ volgt de productformule.

- $(a,b) = (2,p)$ met p een oneven priemgetal: er geldt dat $(2,p)_\infty = 1, (2,p)_r = 1$ voor $r \not| 2p$, $(2,p)_p = \left(\frac{2}{p}\right), (2,p)_2 = (-1)^{\frac{p^2-1}{8}}$. Een vervollediging van de kwadratische reciprociteitsstelling zegt dat $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ waaruit de profuctformule volgt.

- $(a,b) = (2,2)$: er geldt dat $(2,2)_p = 1$ voor alle $p \in P$ waarmee ook hier de productformule bewezen is.

□

2.3 De Stelling van Bruck-Ryser

2.3.1 Congruentie van matrices

Met de theorie van de p-adische getallen en het Hilbert-symbool zijn we al een stap verder richting het bewijs van de stelling van Bruck-Ryser. Deze maakt gebruik van invarianten en hiervoor hebben we congruentie van matrices nodig.

Definitie 2.30. *Stel A en B twee symmetrische matrices van orde n met rationale elementen. Deze matrices zijn **congruent**, genoteerd als $A \sim B$, als er een niet-singuliere matrix C bestaat met rationale elementen zodat $A = C^T BC$.*

Congruentie van matrices is een equivalentierelatie:

- Reflexiviteit: $A \sim A$ want $A = I^T AI$ met I de eenheidsmatrix van orde n.

- Symmetrie: $A \sim B \Rightarrow A = C^T BC \Rightarrow (C^T)^{-1}A(C)^{-1} = B \Rightarrow (C^{-1})^T A(C^{-1}) = B \Rightarrow B \sim A$.

- Transitiviteit: stel dat $A \sim B$ en $B \sim C$, m.a.w. $A = D^T BD$ en $B = E^T CE$. Dan geldt dat $A = D^T E^T CED = (ED)^T C(ED)$ en dus $A \sim C$.

Stel nu dat A een symmetrische matrix van gehele getallen is van orde en rang n. Dan kan men een diagonaalmatrix $D = [d_1, d_2, \ldots, d_n]$ van gehele getallen construeren met $d_i \neq 0$ voor $i = 1, 2, \ldots, n$ zodat $D \sim A$. Het aantal negatieve termen ι in deze diagonaal wordt de **index** van A genoemd. De traagheidswet van Sylvester stelt dat ι een invariant is van A.

Stel $d = (-1)^\iota \delta$, waarbij δ het kwadraatvrije positieve deel is van de determinant $|A|$ van de matrix A. Het kwadraatvrije deel van een geheel getal is het deel van dit getal dat overblijft wanneer alle kwadratische factoren uitgedeeld zijn. Bijvoorbeeld, het kwadraatvrije deel van $24 = 2^3.3$ is $2.3 = 6$. Uit de matrixvergelijking $B = C^T AC$ volgt dat $|B| = |C|^2|A|$. Aangezien δ het kwadraatvrije deel is van de determinant van B, zal de determinant van C bij deze berekening wegvallen, waardoor de δ's van A en B gelijk zijn. Hieruit volg dat d een tweede invariant is van A.

Minkowski en Hasse hebben een derde invariant c_p geintroduceerd, die met de vorige twee het systeem vervolledigt. Om deze c_p te definiëren hebben we het Hilbert-symbool $(m, n)_p$ nodig dat we in de vorige sectie hebben besproken. Stel A een niet-singuliere, symmetrische matrix van gehele getalen van orde n, stel D_r de hoofdminor van orde r en neem aan dat $D_r \neq 0$ voor $r = 1, 2, \ldots, n$. De invariant c_p is dan gedefinieerd voor elk oneven priemgetal p door de vergelijking

$$c_p = c_p(A) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_i, -D_{i+1})_p.$$

Aangezien een natuurlijk getal slechts door een eindig aantal priemgetallen deelbaar is, is $c_p = -1$ voor alleen een eindig aantal priemgetallen. Het laatste wat we nog nodig hebben om de stelling van Bruck-Ryser te bewijzen is de fundamentele Minkowski-Hasse stelling.

Stelling 2.31. *Stel A en B twee symmetrische matrices van gehele getallen van orde en rang n. Stel verder dat de hoofdminoren van A en B verschillend van nul zijn. Dan is $A \sim B$ a.s.a. A en B dezelfde invarianten ι, d en c_p hebben voor elk priemgetal p.*

2.3.2 De stelling van Bruck-Ryser

Bewijs. Stel N een natuurlijk getal en stel B_n de matrix van gehele getallen van orde n waarvan de elementen op de diagonaal $N+1$ zijn en de elementen op andere plaatsen 1 zijn. Om de determinant van deze matrix te berekenen voeren we er eerst enkele rij- en kolomoperaties op uit. We trekken kolom 1 van deze matrix af van de andere kolommen en vervolgens tellen we bij rij 1 alle andere rijen op.

$$\begin{pmatrix} N+1 & 1 & \ldots & 1 \\ 1 & N+1 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & N+1 \end{pmatrix} \rightarrow \begin{pmatrix} N+1 & -N & \ldots & -N \\ 1 & N & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \ldots & N \end{pmatrix} \rightarrow \begin{pmatrix} N+n & 0 & \ldots & 0 \\ 1 & N & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \ldots & N \end{pmatrix}$$

Hierdoor is $|B_n| = (N+n)N^{n-1}$. In het bijzonder als $n = N^2 + N + 1$, dan is B_n de matrix B in de vergelijking $B = AA^T = A^T A$ van stelling 1.3 en dan is $|B|$ is het kwadraat van een geheel getal, namelijk van de determinant van de matrix A in de vergelijking $B = AA^T = A^T A$.
Als rij n van B_n wordt afgetrokken van alle andere rijen van B_n en als kolom n daarna wordt afgetrokken van alle andere kolommen, dan krijgen we dat:

$$\begin{pmatrix} N+1 & 1 & \ldots & 1 \\ 1 & N+1 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & N+1 \end{pmatrix} \rightarrow \begin{pmatrix} N & 0 & \ldots & -N \\ 0 & N & \ldots & -N \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & N+1 \end{pmatrix} \rightarrow \begin{pmatrix} 2N & N & \ldots & -N \\ N & 2N & \ldots & -N \\ \vdots & \vdots & \ddots & \vdots \\ -N & -N & \ldots & N+1 \end{pmatrix}.$$

De bekomen matrix noemen we Q_n en deze is congruent met B_n. Er geldt immers dat $Q_n = C^T B_n C$, waarbij

$$C = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ -1 & -1 & \dots & 1 \end{pmatrix}.$$

We hebben dus dat voor elk oneven priemgetal p, $c_p(B_n) = c_p(Q_n)$. Bovendien, als E_i de determinant is van orde i met als diagonaalelementen $2N$ en als overige elementen N, dan is $E_i = N^i(i+1)$. Daardoor, als $n = N^2 + N + 1$ en als p een oneven priemgetal is, wordt de invariant $c_p(B) = c_p(Q_n)$ van de matrix B uit de vergelijking $B = AA^T = A^T A$ gegeven door

$$c_p(B) = (E_{n-1}, -1)_p \prod_{i=1}^{n-2} (E_i, -E_{i+1})_p.$$

We tonen dit aan als volgt:

$$c_p(B) = c_p(Q_n) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_i, -D_{i+1})_p = (-1, D_n)_p \prod_{i=1}^{n-2} (E_i, -E_{i+1})_p (E_{n-1}, -D_n)_p,$$

waarbij D_i de hoofdminor van orde i is zoals in de definitie van c_p. Omdat D_n een kwadraat is ($D_n = Q_n$ en deze determinant is gelijk aan die van B), mogen we D_n uit het Hilbert-symbool schrappen. We krijgen dan dat $(-1, D_n)_p = (-1, -1)_p = 1$. Hieruit volgt ook nog dat $(E_{n-1}, -D_n)_p = (-1, E_{n-1})_p$, waaruit de formule volgt.
In volgende berekeningen bewijzen we dat

$$c_p(B) = (-1, N)_p^{\frac{N(N+1)}{2}}.$$

Door de stellingen en lemma's van het Hilbert-symbool toe te passen, krijgen we dat

$$\begin{aligned} \prod_{i=1}^{n-2} (E_i, -E_{i+1})_p &= \prod_{i=1}^{n-2} (N^i(i+1), -N^{i+1}(i+2))_p \\ &= \prod_{i=1}^{n-2} \left[(N^i, -N^{i+1}(i+2))_p . (i+1, -N^{i+1}(i+2))_p \right] \\ &= \prod_{i=1}^{n-2} \left[(N^i, -N^{i+1})_p . (N^i, i+2)_p . (i+1, N^{i+1})_p . (i+1, -(i+2))_p \right] \\ &= \prod_{i=1}^{n-2} (N^i, -N^{i+1})_p \prod_{i=1}^{n-2} (i+1, -(i+2))_p \prod_{i=1}^{n-2} \left[(N^i, i+2)_p . (i+1, N^{i+1})_p \right] \end{aligned}$$

We berekenen alle stukken van bovenstaande uitdrukking apart.

$$\begin{aligned} \prod_{i=1}^{n-2} (N^i, -N^{i+1})_p &= \prod_{i=1}^{n-2} \left[(N^i, -N^i)_p . (N^i, N)_p \right] = \prod_{i=1}^{n-2} 1 . (N^i, N)_p \\ &= \left(N^{\sum_{i=1}^{n-2} i}, N \right)_p = \left(N^{\frac{(n-2)(n-1)}{2}}, N \right)_p = (N, N)_p^{\frac{(n-2)(n-1)}{2}} = (N, -1)_p^{\frac{(n-2)(n-1)}{2}} \end{aligned}$$

$$\begin{aligned}\prod_{i=1}^{n-2}(i+1,-(i+2))_p &= \prod_{i=1}^{n-2}(i+1,-1)_p \prod_{i=1}^{n-2}(i+1,i+2)_p \\ &= \prod_{i=1}^{n-2}(i+1,i)_p \prod_{i=2}^{n-1}(i,i+1)_p.1 \\ &= ((n-1)!,-1)_p \prod_{i=2}^{n-1}(i,i+1)_p.(1,2)_p = ((n-1)!,-1)_p \prod_{i=1}^{n-1}(i,i+1)_p \\ &= ((n-1)!,-1)_p \,.\, (n!,-1)_p \\ &= (1,-1)_p^2 \,.\, (2,-1)_p^2 \,.\, \ldots \,.\, (n-1,-1)_p^2 \,.\, (n,-1)_p = (n,-1)_p\end{aligned}$$

$$\begin{aligned}\prod_{i=1}^{n-2}\left[(N^i,i+2)_p.(i+1,N^{i+1})_p\right] &= \prod_{i=1}^{n-2}(N^i,i+2)_p \prod_{i=0}^{n-3}(N^{i+2},i+2)_p \\ &= \prod_{i=1}^{n-2}(N^i,i+2)_p \prod_{i=0}^{n-3}(N^i,i+2)_p.(N^2,i+2)_p \\ &= (N^0,0+2)_p \,.\, (N^{n-2},n-2+2)_p = (1,2)_p \,.\, (N^{n-2},n)_p \\ &= (N,n)_p^{n-2} = (n^2+n+1,n)_p^{n-2} = 1^{n-2} = 1\end{aligned}$$

Uit deze berekeningen volgt nu dat:

$$\begin{aligned}c_p(B) &= (E_{n-1},-1)_p \prod_{i=1}^{n-2}(E_i,-E_{i+1})_p = (N^{n-1}n,-1)_p.(N,-1)_p^{\frac{(n-2)(n-1)}{2}}.(n,-1)_p.1 \\ &= (N^{n-1},-1)_p.(n,-1)_p.(N,-1)_p^{\frac{(n-2)(n-1)}{2}}.(n,-1)_p \\ &= (N^{n-1},-1)_p.(N,-1)_p^{\frac{(n-2)(n-1)}{2}} \\ &= (N,-1)_p^{n-1}.(N,-1)_p^{\frac{(n-2)(n-1)}{2}}\end{aligned}$$

Om nu nog aan te tonen dat dit gelijk is aan $(-1,N)_p^{\frac{N(N+1)}{2}}$ maken we een gevallenonderscheid. We weten dat $n = N^2+N+1$ en dat we N kunnen schrijven als $4k$, $4k+1$, $4k+2$ of $4k+3$ met $k \in \mathbb{N}$. We tonen nu aan dat in allevier deze gevallen, $(n-1)+\frac{(n-1)(n-2)}{2}$ en $\frac{N(N+1)}{2}$ van dezelfde vorm zijn. In $(N,-1)_p^{n-1}.(N,-1)_p^{\frac{(n-2)(n-1)}{2}}$ is het symbool $(N,-1)_p$ gelijk aan 1 of -1, we stellen dit gelijk aan ϵ waardoor we de vorm $\epsilon^{n-1}.\epsilon^{\frac{(n-2)(n-1)}{2}}$ krijgen.

- $N = 4k$: $N^2+N+1 = 16k^2+4k+1 = 4(4k^2+k)+1 = 4l+1$, $l \in \mathbb{N}$
  - $n-1 = 4l$: hierdoor kunnen we ϵ^{n-1} schrappen.
  - $\frac{(n-1)}{2} = 2l$ en $n-2 = 4l-1 = 4l'+3 = 2l''+1$: $\frac{(n-1)(n-2)}{2} = 2l(2l''+1)$.
  - $\frac{N(N+1)}{2} = \frac{4k(4k+1)}{2} = 2k(2k'+1)$.

  $\frac{(n-1)(n-2)}{2}$ en $\frac{N(N+1)}{2}$ zijn dus van dezelfde vorm.

- $N = 4k+1$: $N^2+N+1 = 16k^2+8k+1+4k+1+1 = 4(4k^2+3k)+3 = 4l+3$, $l \in \mathbb{N}$
  - $n-1 = 4l+2$: hierdoor kunnen we ϵ^{n-1} schrappen.
  - $\frac{(n-1)}{2} = 2l+1$ en $n-2 = 4l+1$: $\frac{(n-1)(n-2)}{2} = (2l+1)(4l+1)$.
  - $\frac{N(N+1)}{2} = \frac{(4k+1)(4k+2)}{2} = (4k+1)(2k+1)$.

  $\frac{(n-1)(n-2)}{2}$ en $\frac{N(N+1)}{2}$ zijn dus van dezelfde vorm.
- $N = 4k+2$: $N^2+N+1 = 16k^2+16k+4+4k+2+1 = 4(4k^2+5k+1)+3 = 4l+3$, $l \in \mathbb{N}$
  - $n-1 = 4l+2$: hierdoor kunnen we ϵ^{n-1} schrappen.
  - $\frac{(n-1)}{2} = 2l+1$ en $n-2 = 4l+1 = 2l'+1$: $\frac{(n-1)(n-2)}{2} = (2l+1)(2l'+1)$.
  - $\frac{N(N+1)}{2} = \frac{(4k+2)(4k+3)}{2} = (2k+1)(2k'+1)$.

  $\frac{(n-1)(n-2)}{2}$ en $\frac{N(N+1)}{2}$ zijn dus van dezelfde vorm.
- $N = 4k+3$: $N^2+N+1 = 16k^2+24k+9+4k+3+1 = 4(4k^2+7k+3)+1 = 4l+1$, $l \in \mathbb{N}$
  - $n-1 = 4l$: hierdoor kunnen we ϵ^{n-1} schrappen.
  - $\frac{(n-1)}{2} = 2l$ en $n-2 = 4l-1 = 4l'+3$: $\frac{(n-1)(n-2)}{2} = 2l(4l'+3)$.
  - $\frac{N(N+1)}{2} = \frac{(4k+3)(4k+4)}{2} = (4k+3)2k'$

  $\frac{(n-1)(n-2)}{2}$ en $\frac{N(N+1)}{2}$ zijn dus van dezelfde vorm.

Stel nu dat π een eindig projectief vlak is met $N+1$ punten op een rechte. Dan is door vergelijking $B = AA^T = A^TA$ de matrix B congruent met de eenheidsmatrix I (want $B = A^TIA$). Aangezien $c_p(I) = 1$ voor elk oneven priemgetal p, volgt dat als π bestaat, dat dan voor elk oneven priemgetal p

$$c_p(B) = (-1, N)_p^{\frac{N(N+1)}{2}} = 1.$$

Als nu $N \equiv 1$ of $2 \pmod 4$, dan is de exponent $\frac{N(N+1)}{2}$ oneven zoals we bij het gevallenonderscheid opmerkten. Als een priemgetal p het kwadraatvrije deel van N deelt, dan is $(-1, N)_p = \left(\frac{-1}{p}\right)$. Als p van de vorm $4k+3$ is, dan is -1 geen kwadraat (mod p), dus is $\left(\frac{-1}{p}\right) = -1$. Dit is een contradictie aangezien $c_p(B)$ gelijk aan 1 moet zijn. Er bestaat dus niet zo een π. □

3 Kwadraatsommen

3.1 De stelling van Lagrange

We willen de stelling van Bruck-Ryser nu op een andere manier bewijzen. Dit bewijs gebruikt de stelling van Lagrange.

Stelling 3.1 (Lagrange)**.** *Elk natuurlijk getal is de som van vier kwadraten.*

Voor we dit bewijzen, kijken we eerst naar een lemma dat ons kan helpen bij dit bewijs.

Lemma 3.2 (Euler-Identiteit)**.** *Voor $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ geldt de identiteit:*

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ &\quad + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ &\quad + (x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\ &\quad + (x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2\end{aligned}$$

Bewijs. Om deze identiteit te bewijzen, rekenen we beide leden uit.

$$\begin{aligned}\text{LL} &= x_1^2y_1^2+x_1^2y_2^2+x_1^2y_3^2+x_1^2y_4^2+x_2^2y_1^2+x_2^2y_2^2+x_2^2y_3^2+x_2^2y_4^2+x_3^2y_1^2+x_3^2y_2^2+x_3^2y_3^2+x_3^2y_4^2 \\ &\quad + x_4^2y_1^2+x_4^2y_2^2+x_4^2y_3^2+x_4^2y_4^2 \\ \text{RL} &= x_1^2y_1^2+x_2^2y_2^2+x_3^2y_3^2+x_4^2y_4^2+2x_1x_2y_1y_2+2x_1x_3y_1y_3+2x_1x_4y_1y_4+2x_2x_3y_2y_3 \\ &\quad + 2x_2x_4y_2y_4+2x_3x_4y_3y_4+x_1^2y_2^2+x_2^2y_1^2+x_3^2y_4^2+x_4^2y_3^2-2x_1x_2y_1y_2+2x_1x_3y_2y_4 \\ &\quad - 2x_1x_4y_2y_3-2x_2x_3y_1y_4+2x_2x_4y_1y_3-2x_3x_4y_3y_4+x_1^2y_3^2+x_2^2y_4^2+x_3^2y_1^2+x_4^2y_2^2 \\ &\quad - 2x_1x_2y_3y_4-2x_1x_3y_1y_3+2x_1x_4y_2y_3+2x_2x_3y_1y_4-2x_2x_4y_2y_4-2x_3x_4y_1y_2 \\ &\quad + x_1^2y_4^2+x_2^2y_3^2+x_3^2y_2^2+x_4^2y_1^2+2x_1x_2y_3y_4-2x_1x_3y_2y_4-2x_1x_4y_1y_4-2x_2x_3y_2y_3 \\ &\quad - 2x_2x_4y_1y_3+2x_3x_4y_1y_2\end{aligned}$$

□

Dit lemma zegt dus dat het product van twee sommen van vier kwadraten opnieuw een som van vier kwadraten is. Deze identiteit vindt zijn oorsprong in de quaternionen.

Definitie 3.3. *Een **quaternion** of **hypercomplex getal** is een uitdrukking van de vorm*

$$z = x_1 + x_2i + x_3j + x_4k$$

waarbij $x_1, x_2, x_3, x_4 \in \mathbb{R}$ en i, j, k symbolen zijn die voldoen aan volgende regels:

- $-1 = i^2 = j^2 = k^2$
- $ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$

Definitie 3.4. *Enkele belangrijke uitdrukkingen van een quaternion zijn:*

- *De **quaternionennorm**: $N(z) = x_1^2 + x_2^2 + x_3^2 + x_4^2$.*
- *De **vermenigvuldigingswet** voor de quaternionennorm: $N(z)N(z') = N(zz')$*

Stel $z = x_1 + x_2i + x_3j + x_4k$ en $z' = y_1 + y_2i + y_3j + y_4k$. De uitwerking van het linkerlid (resp. rechterlid) van de vermenigvuldigingswet levert ons het linkerlid (resp. rechterlid) van de Euler-Identiteit.

$$
\begin{aligned}
N(z)N(z') &= (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \text{LL}\\
N(zz') &= N((x_1+x_2i+x_3j+x_4k)(y_1+y_2i+y_3j+y_4k))\\
&= N(x_1y_1+x_1y_2i+x_1y_3j+x_1y_4k+x_2y_1i+x_2y_2i^2+x_2y_3ij+x_2y_4ik+x_3y_1j+x_3y_2ji\\
&\quad +x_3y_3j^2+x_3y_4jk+x_4y_1k+x_4y_2ki+x_4y_3kj+x_4y_4k^2)\\
&= N((x_1y_1-x_2y_2-x_3y_3-x_4y_4)+(x_1y_2+x_2y_1+x_3y_4-x_4y_3)i\\
&\quad +(x_1y_3-x_2y_4+x_3y_1+x_4y_2)j+(x_1y_4+x_2y_3-x_3y_2+x_4y_1)k)\\
&= (x_1y_1-x_2y_2-x_3y_3-x_4y_4)^2+(x_1y_2+x_2y_1+x_3y_4-x_4y_3)^2\\
&\quad +(x_1y_3-x_2y_4+x_3y_1+x_4y_2)^2+(x_1y_4+x_2y_3-x_3y_2+x_4y_1)^2\\
&= x_1^2y_1^2+x_1^2y_2^2+x_1^2y_3^2+x_1^2y_4^2+x_2^2y_1^2+x_2^2y_2^2+x_2^2y_3^2+x_2^2y_4^2+x_3^2y_1^2+x_3^2y_2^2+x_3^2y_3^2+x_3^2y_4^2\\
&\quad +x_4^2y_1^2+x_4^2y_2^2+x_4^2y_3^2+x_4^2y_4^2\\
&\quad -2x_1x_2y_1y_2-2x_1x_3y_1y_3-2x_1x_4y_1y_4+2x_2x_3y_2y_3+2x_2x_4y_2y_4+2x_3x_4y_3y_4\\
&\quad +2x_1x_2y_1y_2+2x_1x_3y_2y_4-2x_1x_4y_2y_3+2x_2x_3y_1y_4-2x_2x_4y_1y_3-2x_3x_4y_3y_4\\
&\quad -2x_1x_2y_3y_4+2x_1x_3y_1y_3+2x_1x_4y_2y_3-2x_2x_3y_1y_4-2x_2x_4y_2y_4+2x_3x_4y_1y_2\\
&\quad +2x_1x_2y_3y_4-2x_1x_3y_2y_4+2x_1x_4y_1y_4-2x_2x_3y_2y_3+2x_2x_4y_1y_3-2x_3x_4y_1y_2\\
&= \text{RL}
\end{aligned}
$$

We kunnen nu de Stelling van Lagrange bewijzen.

Bewijs. Door de Euler-Identiteit volstaat het om te bewijzen dat elk priemgetal de som van vier kwadraten is. Elk natuurlijk getal kan immers op een unieke manier ontbonden worden als het product van priemgetallen. Aangezien het product van twee sommen van vier kwadraten ook een som van vier kwadraten is volgens de Euler-Identiteit, zal de ontbinding in priemgetallen dan een som van vier kwadraten geven.
Zij p een priemgetal. Dan kunnen we zonder beperking aannemen dat p oneven is. Voor $p=2$ geldt immers: $2=1^2+1^2+0^2+0^2$. In $\mathbb{Z}/p\mathbb{Z}$ zijn er $\frac{p-1}{2}$ kwadratische resten en dit zijn dus kwadraten modulo p. Ook $0=0^2$ is een kwadraat modulo p en we krijgen $\frac{p+1}{2}$ kwadraten modulo p (en dus $\frac{p-1}{2}$ niet-kwadraten modulo p). Er zijn dus ook $\frac{p+1}{2}$ restklassen van de vorm $-1-x^2$: de vergelijking $-1-x^2 \equiv y \pmod p$ heeft $\frac{p+1}{2}$ verschillende oplossingen y omdat er $\frac{p+1}{2}$ verschillende kwadraten x^2 zijn. Er zijn in totaal p verschillende restklassen ($a \sim b \Leftrightarrow a \equiv b \pmod p$ en $a = 0, 1, \ldots, p-1$). Omdat er $\frac{p+1}{2}$ restklassen van de vorm $-1-x^2$ zijn en er $\frac{p-1}{2}$ niet-kwadraten zijn, moet minstens $\frac{p+1}{2}-\frac{p-1}{2}=1$ restklasse een kwadraat zijn. M.a.w. de vergelijking $x^2+y^2+1=0$ heeft een oplossing modulo p. Kiezen we de representanten x, y met $-\frac{p}{2} < x, y < \frac{p}{2}$, dan volgt dat

$$0 < x^2+y^2+1 < 3\left(\frac{p}{2}\right)^2 < p^2.$$

Door het interval waar x en y in liggen, is $x^2 < \left(\frac{p}{2}\right)^2$ en $y < \left(\frac{p}{2}\right)^2$. Aangezien p een oneven priemgetal is, is $p \geq 3$ waardoor $\frac{p}{2} \geq \frac{3}{2} > 1$ en dus $\left(\frac{p}{2}\right)^2 \geq \left(\frac{3}{2}\right)^2 > 1^2$.
Er bestaat dus een $n \in \mathbb{N}, n < p$, zodat np de som is van drie kwadraten en dus in het bijzonder ook van vier kwadraten als je er nog 0^2 bij optelt. Zij m het kleinste natuurlijk getal zo dat mp de som van vier kwadraten is. Het is duidelijk dat $m < p$ aangezien we al hebben aangetoond dat er

een $n \in \mathbb{N}, n < p$ bestaat, waarvoor np de som van vier kwadraten is. We tonen aan dat $m = 1$. Stel dat m strikt groter is dan 1 en

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \tag{3}$$

Zij nu $x_i \equiv y_i \pmod{m}$ met $-\frac{m}{2} < y_i \leq \frac{m}{2}$ voor $i = 1, 2, 3, 4$. Dan geldt dat $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{m} \equiv mp \pmod{m} \equiv 0 \pmod{m}$. Er bestaat dus een $r \in \mathbb{Z}, r \geq 0$, met

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2. \tag{4}$$

Aangezien $y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} = m^2$, geldt dat $r \leq m$. Als we (3) en (4) vermenigvuldigen, dan bekomen we $rpm^2 = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$. We krijgen dus een voorstelling van rpm^2 als de som van vier kwadraten wegens de Euler-Identiteit.

$$rpm^2 = A^2 + B^2 + C^2 + D^2 \tag{5}$$

Hierbij zijn A, B, C en D de termen uit het rechterlid van de Euler-Identiteit. Door dat $x_i \equiv y_i \pmod{m}$, zijn B, C en D deelbaar door m:

$$B = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv y_1y_2 - y_2y_1 + y_3y_4 - y_4y_3 \equiv 0 \pmod{m}$$
$$C = x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2 \equiv y_1y_3 - y_2y_4 - y_3y_1 + y_4y_2 \equiv 0 \pmod{m}$$
$$D = x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \equiv y_1y_4 + y_2y_3 - y_3y_2 - y_4y_1 \equiv 0 \pmod{m}$$

Ook A is deelbaar door m:

$$A = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}$$

Hieruit volgt dat $rp = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2$ ook een som van vier kwadraten is. We bewijzen nu dat r niet kan gelijk zijn aan 0 noch aan m.
Uit $r = 0$ volgt dat $y_1 = y_2 = y_3 = y_4 = 0$ en dus x_1, x_2, x_3, x_4 deelbaar zijn door m. Omdat x_i^2 voor $i = 1, 2, 3, 4$ dan deelbaar is door m^2, volgt uit (3) dat $m^2 | mp$ en dus $m | p$.
Uit $r = m$ volgt dat $y_i = \frac{m}{2}$ voor $i = 1, 2, 3, 4$ aangezien y_i niet groter kan zijn dan dit. In het bijzonder is m even omdat elke x_i en dus elke y_i een geheel getal is. Er geldt dat $x_i = \frac{m}{2} + c_i m$ met $c_i \in \mathbb{Z}, i = 1, 2, 3, 4$. We bekomen dat $x_i^2 = \frac{m^2}{4} + c_i m^2 + c_i^2 m^2 \equiv \frac{m^2}{4} \pmod{m^2}$. Door optelling van deze volgt dat $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv m^2 \pmod{m^2}$, waardoor $m^2 | mp$ en dus $m | p$. In beide gevallen bekomen we dat $m | p$, wat in tegenspraak is met $1 < m < p$, doordat p priem is. Hieruit volgt dat $1 \leq r \leq m - 1$. rp is dus een som van vier kwadraten met r strikt kleiner dan m, wat in tegenspraak is met de minimaliteit van m. Uit deze strijdigheid volgt dat m gelijk moet zijn aan 1, wat bewijst dat elke priemgetal kan geschreven worden als de som van vier kwadraten.

□

3.2 De Stelling van Bruck-Ryser

Voor dit bewijs wordt de stelling anders geformuleerd, namelijk als volgt.

Stelling 3.5 (Bruck-Ryser)**.** *Als $n \equiv 1, 2 \pmod{4}$, dan is een nodige voorwaarde voor het bestaan van een eindig projectief vlak van orde n dat er gehele getallen x, y bestaan die voldoen aan de vergelijking $n = x^2 + y^2$.*

We tonen eerst aan dat de twee versies van de stelling op hetzelfde neerkomen. Hiervoor gebruiken we onder andere de **identiteit van Fibonacci**.

Lemma 3.6 (Identiteit van Fibonacci)**.**

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac-bd)^2+(ad+bc)^2\\ &= (ac+bd)^2+(ad-bc)^2\end{aligned}$$

De volgende stelling wordt toegeschreven aan Fermat.

Stelling 3.7 (Fermat)**.** *Veronderstel dat $p > 2$ een priemgetal is, dan is p de som van twee kwadraten als en slechts als $p \equiv 1$ (mod 4).*

Veronderstel nu dat N een natuurlijk getal is en beschouw de factorisatie van N: $N = \prod_{i=1}^{k} p_i^{e_i}$, met alle p_i priem en $1 \leq e_i$. Noem het **kwadraatvrije gedeelte van** N in dit geval het product M van de priemgetallen p_i waarvoor geldt dat de exponent e_i oneven is in de priemfactorisatie van N. Uit deze definitie van M volgt onmiddellijk dat $\frac{N}{M}$ een kwadraat is. Dus uit de identiteit van Fibonacci volgt dat N de som van twee kwadraten is als en slechts als M de som van twee kwadraten is. (Om dit in te zien in één richting volstaat het $a^2 = \frac{N}{M}$, $b = 0$, en $M = c^2 + d^2$ te veronderstellen, de andere richting vergt ook een bewijs).

We noemen een getal x kwadraatvrij als voor elk priemgetal p waarvoor $p \mid x$, geldt dat $p^2 \nmid x$. Voor een gegeven getal N voldoet het kwadraatvrije gedeelte, zoals hierboven gedefinieerd, dus aan deze definitie. Nu geldt de volgende stelling die we ook zonder bewijs vermelden, maar waarvan het bewijs in één richting onmiddellijk volgt uit de identiteit van Fibonacci.

Stelling 3.8. *Een kwadraatvrij getal N is de som van twee kwadraten als en slechts als elke priemfactor de som is van twee kwadraten.*

Samen met Stelling 3.7 kunnen we dus besluiten dat een natuurlijk getal N de som is van twee kwadraten als en slechts als het kwadraatvrij gedeelte van N geen priemfactor p bevat met $p \equiv 3 \pmod 4$.

$n = 10$ voldoet aan de voorwaarde van de nieuwe stelling aangezien $10 = 1^2 + 3^2$. Zoals reeds in de inleiding vermeld, is echter bewezen dat er geen eindig projectief vlak van orde 10 bestaat, waardoor duidelijk is dat deze stelling enkel een nodige voorwaarde levert en zeker geen voldoende. Het bewijs van de stelling gebruikt vier eigenschappen uit de getaltheorie, waaronder de Euler-Identiteit en de Stelling van Lagrange. De andere 2 zijn als volgt:

1. Als p een oneven priemgetal is en er bestaan gehele getallen x_1, x_2 niet beide deelbaar door p, zodat $x_1^2 + x_2^2 \equiv 0 \pmod p$, dan is p de som van twee gehele kwadraten. Het analoge resultaat geldt voor vier kwadraten.

2. Voor elk geheel getal n geldt, als de vergelijking $x^2 + y^2 = nz^2$ een gehele oplossing heeft met x, y, z niet allemaal nul, dat n dan de som van twee gehele kwadraten is. M.a.w. de vergelijking heeft een oplossing als $z = 1$.

We kunnen nu de Stelling van Bruck-Ryser bewijzen.

Bewijs. Beschouw een eindig projectief vlak van orde n, met $n \equiv 1, 2 \pmod 4$. Het aantal punten van een projectief vlak van orde n is $N = n^2 + n + 1$. Hieruit volgt dat $N \equiv 3 \pmod 4$:
$n \equiv 1 \pmod 4 : n^2 + n + 1 \equiv n.n + n + 1 \equiv 1.1 + 1 + 1 \equiv 3 \pmod 4$
$n \equiv 2 \pmod 4 : n^2 + n + 1 \equiv n.n + n + 1 \equiv 2.2 + 2 + 1 \equiv 3 \pmod 4$
Zij I, J, A NxN- matrices waarbij I de identiteitsmatrix is, J de matrix met $j_{ik} = 1, \forall i, k \in \{1, 2, \ldots, N\}$ en A de incidentiematrix van het projectieve vlak. Dan geldt:

$$AA^T = nI + J$$

Immers, als we het inproduct nemen van 2 willekeurige rijen, dan zal dit gelijk zijn aan 1 als ze verschillend zijn en gelijk zijn aan $n + 1$ als ze gelijk zijn. Dit volgt uit de definitie van de orde van een projectief vlak omdat 2 rechten incident zijn met 1 punt en elke rechte incident is met $n + 1$ punten. Zij $x_1, \ldots, x_N$ variabelen en zij $x = (x_1, \ldots, x_N)$. Zij $xA = z = (z_1, \ldots, z_N)$, dan zijn $z_1, \ldots, z_N$ lineaire combinaties van $x_1, \ldots, x_N$ met gehele coëfficiënten. We hebben dat:

$$zz^T = xAA^Tx^T = x(nI + J)x^T = nxx^T + xJx^T$$

wat betekent dat:

$$\begin{aligned} z_1^2 + \ldots + z_N^2 &= n(x_1^2 + \ldots + x_N^2) + \begin{pmatrix} x_1 & \ldots & x_N \end{pmatrix} \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \\ &= n(x_1^2 + \ldots + x_N^2) + x_1^2 + x_1x_2 + \ldots + x_1x_N + \ldots + x_Nx_1 + x_Nx_2 + \ldots + x_N^2 \\ &= n(x_1^2 + \ldots + x_N^2) + (x_1 + \ldots + x_N)(x_1 + \ldots + x_N) \\ &= n(x_1^2 + \ldots + x_N^2) + w^2 \end{aligned}$$

waarbij $w = x_1 + \ldots + x_N$.
We nemen een nieuwe variabele x_{N+1}, voegen nx_{N+1}^2 toe aan beide kanten van bovenstaande vergelijking en bekomen $z_1^2 + \ldots + z_N^2 + nx_{N+1}^2 = n(x_1^2 + \ldots + x_N^2 + x_{N+1}^2) + w^2$. Uit onze voorgaande conclusie dat $N \equiv 3 \pmod 4$, volgt dat $N + 1$ deelbaar is door vier. We hebben onze n zo herverdeeld dat elke som van vier termen een n heeft, wat ons de mogelijkheid geeft om de Stelling van Lagrange te gebruiken. We kunnen n schrijven als $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$ en we gaan vervolgens de termen van de vergelijking als volgt hergroeperen:
We beginnen met $n(x_1^2 + \ldots + x_N^2 + x_{N+1}^2)$. Deze hergroeperen we in sommen van telkens vier termen: $n(x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2) + \ldots + n(x_{g1}^2 + x_{g2}^2 + x_{g3}^2 + x_{g4}^2)$, waarbij $4.g = N + 1$. Aangezien n een som van vier kwadraten is, kunnen we de Euler-Identiteit toepassen:

$$n(x_{i1}^2 + x_{i2}^2 + x_{i3}^2 + x_{i4}^2) = y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2$$

met y_{ij} een lineaire combinatie van de x_{ij} met i vast en $j = 1, 2, 3, 4$. Als we dit in de oorspronkelijke vergelijking stoppen, bekomen we volgende uitdrukking waarbij we de y_{ij} een andere index hebben gegeven overeenkomstig met de oorspronkelijke index van de x_i.

$$z_1^2 + \ldots + z_N^2 + nx_{N+1}^2 = y_1^2 + \ldots + y_{N+1}^2 + w^2$$

Zowel de z_i als de y_i zijn lineaire combinaties van de x_i. Voor elke z_i en y_j nemen we een unieke x_k die een niet-nul coëfficiënt heeft in zowel de uitdrukking van z_i als in die van y_j. Als de coëfficiënten

van x_k hetzelfde zijn in zowel z_i als y_j, dan stellen we $z_i = -y_j$ zodat we x_k kunnen schrijven in termen van de andere x_i zonder x_k kwijt te geraken. Als de coëfficiënten van x_k verschillend zijn, stellen we $z_i = y_j$ en schrijven we x_k in termen van de andere x_i. We herhalen dit proces voor $i = 1, \ldots, N$. We merken op dat geen enkele z_i een lineaire combinatie is van x_{N+1}. We merken dit op omdat we door onze specializering hebben dat $z_i^2 = y_j^2$ waardoor we de termen z_i^2 en y_i^2 uit onze vergelijking kunnen elimineren voor alle $i = 1, \ldots, N$. We houden deze vergelijking over:

$$nx_{N+1}^2 = y_{N+1}^2 + w^2$$

Als we nu kunnen aantonen dat x_{N+1}, y_{N+1} en w gehele getallen zijn, dan volgt uit eigenschap 2. dat n de som is van 2 kwadraten, wat de Stelling van Bruck-Ryser bewijst.
We hebben elke x_i, behalve x_{N+1}, dus geschreven in termen van de andere x_i waaronder ook x_{N+1}. We hebben dus N vergelijkingen in $N + 1$ onbekenden en we hebben het niet opgelost voor x_{N+1}. Dan kunnen alle x_i geschreven worden als rationale functies van x_{N+1}. y_{N+1} en w zijn lineaire combinaties van de x_i dus we kunnen ook hen herschrijven als rationale functies van x_{N+1}. We kunnen x_{N+1} dus zo kiezen dat x_{N+1}, y_{N+1} en w gehele getallen zijn, waardoor n dus een som van 2 gehele kwadraten wordt.

□

4 Bronnen

R. H. Bruck & H. J. Ryser. (1948). The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics*, 1, pp. 88 – 93.

C. D. Moraites. (2011). The Bruck-Ryser Theorem and the Search for a Finite Projective Plane of Order 10.

A. Schmidt. (2007). Einführung in die algebraische Zahlentheorie. (1^{e} druk). Berlin Heidelberg: Uitgeverij Springer.