Mijn jeugdliefde

Frans Oort

2 november 2009

Lustrum van A-Eskwadraat, februari 2001

Lees niet verder! Want ontboezemingen van deze aard, met een dergelijke titel, horen misschien wel thuis in de “Privé”, maar toch niet in een lustrum-nummer van een eerbiedwaardige vereniging als A-Es^2?

Toen ik als student een onderwerp zocht voor een eind-scriptie kwam ik als vanzelf op het onderwerp “elliptische krommen”. En, vanaf het eerste moment was ik verloren, gefascineerd, bekoord, en kon ik aan weinig anders meer denken. Dat was niet omdat het ook het onderwerp van het proefschrift van mijn vader was, maar het was omdat dit onderwerp die fascinerende combinatie van meetkunde en algebra heeft, die me altijd heeft geboeid (en pas later zag ik de aritmetische aspecten en toepassingen), ik was voorgoed verloren. En dit onderwerp, in allerlei verschijningsvormen, heeft me steeds meer geboeid in de afgelopen 45 jaar.

In dit korte essay zal ik proberen iets over te brengen van al die fascinerende eigenschappen. Als je een grondiger en betere behandeling van dit onderwerp wilt: er is heel veel literatuur over, en ik zal een paar verwijzingen geven.

1 Elliptische krommen

Voor een betere behandeling van deze aspecten, zie: [4], [10], [13] VI.7, [3] IV.4, om maar een paar referenties te noemen uit de enorme hoeveelheid literatuur over dit onderwerp).

De definitie van een elliptische kromme kan op vele manier gegeven worden:
- een kromme van geslacht één (met een rationaal punt over het grondlichaam),
- een abelse variëteit van dimensie één,
- een *niet-singuliere vlakke kromme van de graad* 3 (met een buigpunt rationaal over het grondlichaam),
- een complexe torus van dimensie één (als we over $\mathbb{C}$ werken),
$\cdots$.

In vele toepassingen gebruiken we eerst de ene definitie, stappen dan over op een andere equivalente; zo vertalen we bij voorbeeld meetkundige informatie in eigenschappen in getaltheorie, etc. We zullen hier een heel toegankelijke definitie geven (we nemen aan dat de karakteristiek van het grondlichaam $\neq 2$ en $\neq 3$). we beschouwen het projectieve vlak met als coördinaat functies X, Y, Z.

(1.1) Definitie. *Een elliptische kromme is een vlakke projectieve kromme gegeven door een vergelijking van de vorm $Y^2 = X^3 + AX + B$, met $4A^3 + 27B^2 \neq 0$.*

Hiermee bedoelen we: maak de vergelijking homogeen: $ZY^2 = X^3 + AXZ^2 + BZ^3$. Dat geeft een nulpuntenverzameling $E \subset \mathbb{P}^2$, een "vlakke kromme van graad 3". De eigenschap $4A^3 + 27B^2 \neq 0$ zorgt ervoor dat het polynoom $X^3 + AX + B$ drie verschillende nulpunten heeft (kun je dat inzien ?), en als bovendien de karakteristiek van het grondlichaam $\neq 2$ is blijkt deze kromme E geen singulariteiten te bezitten. De rechte $Z = 0$ snijdt deze kromme in het punt $(0 : 1 : 0) =: 0 \in E$, en dat punt is een *buigpunt*: de rechte $Z = 0$ raakt aan E in het punt $0 \in E$ en snijdt daar de kromme "met multipliciteit 3";

$$E = \{(x, y) \mid y^2 = x^3 + Ax + B\} \cup \{0\}.$$

(1.2) *Punten op een elliptische kromme vormen een groep.* Hier begint het avontuur! Kies een punt op de kromme (vaak nemen we $0 \in E$ daarvoor). We definiëren de groepswet door een "optelling" op E te geven:

de optelling op een cubische kromme

voor gegeven punten $P, Q \in E$ nemen we de lijn door P en Q, noemen het derde snijpunt $S = S(P, Q)$, verbinden S met 0, en noemen het derde snijpunt $P + Q$.
Feit: *Dit geeft op E de structuur van een groep* ! Het blijkt dat dit niet zo moeilijk is, behalve dan dat het bewijs van de associativiteit van deze "optelling" enig werk vergt (er zijn bewijzen die met elementaire middelen gaan, bewerkelijk; er zijn ook bewijzen die van iets meer techniek gebruikt maken, en dan is het verder gemakkelijk). - Het feit dat hier een algebraïsche structuur (een groep) plaats vindt op een meetkundig object, we krijgen een "algebraïsche groep", geeft toegang tot krachtige hulpmiddelen, zoals we zullen zien.

2 Meetkundige aspecten

(2.1) Een elliptische kromme als topologische groep. Beschouw een elliptische

kromme E over $\mathbb{C}$. We schrijven S^1 voor de "cirkelgroep" (de topologische ruimte gegeven door een cirkel, met als optelling het optellen van argumenten); merk op $S^1 \approx \mathbb{R}/\mathbb{Z}$, de cirkelgroep is homeomorf met de groep van reële getallen modulo gehele getallen.
Feit. *Er is een isomorfisme van topologische groepen*:

$$E(\mathbb{C}) \quad \approx \quad S^1 \times S^1$$

(een dergelijke groep heet een "torus"; meetkundig kunnen we het zien als een "ringoppervlak").

(2.2) Een elliptische kromme als analytische groep. Voor een complex getal $\tau \in \mathbb{C}$ dat niet reëel is, schrijven $\Lambda_\tau := \mathbb{Z}{\cdot}1 + \mathbb{Z}{\cdot}\tau$.
Feit. *Voor elke elliptische kromme E over $\mathbb{C}$ is er een $\tau \in \mathbb{C} - \mathbb{R}$ en een isomorfisme van analytische groepen*:

$$E(\mathbb{C}) \quad \cong \quad T_\tau := \mathbb{C}/\Lambda_\tau.$$

We zien dat de meetkunde op een elliptische kromme eenvoudig te begrijpen is. Hier zijn een paar eenvoudige oefeningen
Opgave: *Zij E een elliptische kromme over $\mathbb{C}$, zij $n \in \mathbb{Z}_{>0}$, dan is*

$$\mathrm{Ker}(E(\mathbb{C}) \xrightarrow{\times n} E(\mathbb{C})) =: E(\mathbb{C})[n] \cong (\mathbb{Z}/n)^2.$$

Opgave: *Bewijs dat $P \in E$ een punt is met $3{\cdot}P = 0$ desda $P \in E \subset \mathbb{P}^2$ een* buigpunt *is.* [We nemen nog steeds aan dat $0 \in E$ een buigpunt is.]
Opgave: *Zij E een elliptische kromme over $\mathbb{C}$; laat zien dat E precies 9 buigpunten heeft. Laat zien dat een lijn die twee buigpunten verbindt weer in een buigpunt als derde snijpunt snijdt.*
Opgave: *Zij E een elliptische kromme over over $\mathbb{R}$. Bewijs dat E precies een of precies 3 buigpunten over $\mathbb{R}$ heeft.* [Deze opgave is volstrekt elementair op te lossen; er is ook een doorzichtiger, geavanceerd bewijs dat gebruik maakt van de "Weil-paring", maar dat valt buiten de context van deze onze beschrijvingen.]

3 Een meetkundige toepassing

We geven een beschrijving van een bewijs van de "sluitingsstelling van Poncelet". Voor meer details, en voor verwijzingen, zie [1].

(3.1) We beschouwen twee kegelsneden $C, D \subset \mathbb{P}^2$,
allebei niet onaard, over een algebraïsch afgesloten
grondlichaam, van karakteristiek $\neq 2$.
Verder nemen we aan dat $\#(C \cap D) = 4$, d.w.z.
C en D raken nergens aan elkaar.
We schrijven $D^\wedge$ voor de verzameling van raaklijnen aan D. We nemen een punt $P_0 \in C$ en een raaklijn $L_0 \in D^\wedge$ aan D met $P_0 \in L_0$. Dan voeren we de "Poncelet constructie uit": we

noemen $P_1 \in C$ het tweede snijpunt van L_0 met C, en $L_1 \in D^\wedge$ de tweede raaklijn door P_1 aan D.

de Poncelet constructie

Iteratie van deze contructie geeft een rij $\{(P_i, L_i) \mid i \in \mathbb{Z}_{\geq 0}\}$.

(3.2) Stelling (de sluitingssteling van Poncelet): *Als $C, D \subset \mathbb{P}^2$ als boven, en als voor een keuze van (P_0, L_0) en een getal $n \in \mathbb{Z}_{>1}$ bestaat, zodanig dat $(P_0, L_0) = (P_n, L_n)$* (we zeggen dat de Poncelet-constructie sluit na n stappen) *dan is er voor elke uitgangspositie $(Q_0, M_0) \in C \times D^\wedge$, met $Q_0 \in M_0$, sluiting na n stappen.*

de Poncelet constructie sluit na 3 stappen

Het blijkt al snel, dat expliciet uitschrijven van dit procedé (met als doel een bewijs te geven via berekeningen) vreselijk ingewikkeld is.

We schetsen een bewijs. We schrijven

$$E := \{(P_0, L_0) \in C \times D^\wedge \mid P_0 \in L_0\}.$$

We schrijven

$$\tau : (P_0, L_0) \mapsto (P_1, L_1)$$

voor de Poncelet constructie. Gemakkelijk in te zien: *$\tau : E \to E$ heeft geen dekpunten.* Niet erg moeilijk: *E is een elliptische kromme.* [We maken steeds gebruik van $\#(C \cap D) = 4$.] Nu komt een niet-triviale stap: *een morfisme $f : E \to E$ van krommen van geslacht één is een homomorfisme op een translatie na*, d.w.z. $\varphi(x) := f(x) - f(0)$ is een homomorfisme van groepen. Hieruit valt gemakkelijk af te leiden: bij de gegevens zoals in de stelling hoort een punt $t \in E$ zo dat $\tau(x) = x + t$. We zien dan in: de constructie, uitgaande van $x_0 = (P_0, L_0)$, sluit na n stappen desda $n{\cdot}t = 0$; daaruit volgt sluiting na n stappen uitgaande van $(Q_0, M_0) \in E$. Einde bewijs !

Wil je gevoel krijgen voor de schoonheid van dit bewijs, probeer dan maar eens een bewijs met elementaire middelen te geven. Of, lees hoe Poncelet het in 1822 deed. De (enige) niet-triviale stap in het bewijs vergt geavanceerde middelen uit de algebraïsche meetkunde, zie b.v. [3], IV Lemma 4.9; het volgt ook uit geavanceerde methoden uit de functie-theorie: bestudering van de Weierstrass-$\wp$-functie, of uit bestudering van de exponentiaal-afbeelding uit de theorie van de complexe Lie groepen: *een analytische afbeelding van complexe tori die $0 \mapsto 0$ is "automatisch" een homomorfisme.* - We zien dat het ontwikkelen van een geavanceerd wiskundig apparaat het bewijs van een gecompliceerde stelling inzichtelijk en kort (modulo diepe eigenschappen) maakt. Dat doet zuivere wiskunde voor je!

4 Aritmetische toepassingen

In het bewijs van de laatste stelling van Fermat door Frey-Ribet-Wiles spelen elliptische krommen een cruciale rol. We geven kort aan wat het nieuwe idee is (onbekend vóór 1985, een doorbraak door middel van een heel eenvoudige constructie van Frey):

neem aan dat er een tegenvoorbeeld zou zijn van FLT, dat wil zeggen, $n \in \mathbb{Z}_{\geq 3}$ en $a, b, c \in \mathbb{Z}$ met $abc \neq 0$, en $\text{ggd}(a, b) = 1$ en

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

We zullen aannemen dat n een priemgetal is; we zullen (voor het gemak) aannemen dat $n \geq 7$. We schrijven

$$A := a^n, \quad B := b^n, \quad C := c^n; \quad \text{dus} \quad A + B = C.$$

De cruciale suggestie van Gerhard Frey is: *uitgaande van dat hypothetische tegenvoorbeeld construeer de elliptische kromme over $\mathbb{Q}$ gegeven door*:

$$E = E_{A,B,C} : \qquad Y^2 = X{\cdot}(X - A){\cdot}(X + B).$$

"Ervaring" leert dat deze kromme niet hoort te bestaan (en dan zouden we concluderen dat het hypothetische tegenvoorbeeld tot een tegenspraak leidt).

Voor we verdergaan geven we een *notatie*: Neem aan dat $A, B, C \in \mathbb{Z}_{>0}$, met $A + B = C$ en $\text{ggd}(A, B) = 1$; we schrijven $\text{Cond}(A, B, C)$ (spreek uit: de conductor van dit drietal) voor het product van alle priemgetallen p (tot de macht één !) met de eigenschap dat p een deler is van ABC.

Waar komt deze intuïtie dat $E_{A,B,C}$ als boven niet hoort te bestaan vandaan? [Waarschuwing: vanaf nu zullen we een paar speculatieve, onzorgvuldige uitspraken doen; we proberen daarmee het idee achter het bewijs duidelijk te maken, zonder op exactheid aanspraak te maken.] Een dergelijke elliptische kromme levert twee invarianten: de *conductor* en de *discriminant* (ik wandel hier over wat technische moeilijkheden heen; bv. hangt de discriminant af van de gekozen vergelijking). De conductor is het product van alle priemgetallen p waar deze kromme modulo p singulier is; AHA: dit is zo als p een deler is van ABC; kijk maar: als bv. p een deler is van A, dan is $A \bmod p = 0$; idem voor priemdelers van B; als p een deler is van $C = A + B$ dan geldt $A \bmod p = B \bmod p$; hieruit volgt gemakkelijk wat we willen (ik stap over een probleem heen: deze beschouwingen gaan alleen maar op voor zgn. "stabiele reductie"; de eis dat n een priemgetal is, en $n \geq 5$ blijkt dit op te leveren). Conclusie:

$$\mathrm{Cond}(A, B, C) = \mathrm{Cond}(E_{A,B,C}).$$

Verder geldt dat de discriminant van een elliptische kromme gegeven door $Y^2 = (X - e_1)(X - e_2)(X - e_3)$ gelijk is (op een factor 2^8 en op een teken na) aan $(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$. AHA

$$\mathrm{Discr}(E_{A,B,C}) = A^2{\cdot}B^2{\cdot}C^2$$

(op een factor $\pm 2^8$ na).

Een (onbewezen) ervaringsfeit (het "vermoeden van Szpiro") vertelt ons dat voor een elliptische kromme E over $\mathbb{Q}$ er geldt:

$$\mathrm{Discr}(E) < \mathrm{Cond}(E)^6$$

(mijn formulering is wat al te onzorgvuldig, maar het geeft wel het idee aan).

Laten we aannemen dat deze ingrediënten (onzorgvuldig geformuleerd, en onbewezen wat het vermoeden van Szpiro betreft) zouden mogen gebruiken als ware uitspraken. Dan volgt FLT: neem aan dat er een hypothetische oplossing is als boven, dan zien we dat enerzijds

$$N = \mathrm{Cond}(E_{A,B,C}) = \mathrm{Cond}(A, B, C) \leq abc.$$

[AHA hier is de "winst": merk op dat als p een priemgetal is wat $A := a^n$ deelt, dan deel p ook a, allicht.] Ook zien we dat $C < A^2{\cdot}B^2$ (tenminste als $C > 4$), en we zouden kunnen concluderen:

$$C^3 < \mathrm{Discr}(E) = A^2{\cdot}B^2{\cdot}C^2 < N^6 \leq (abc)^6;$$

er komt:

$$(abc)^n = ABC < C^3 < (abc)^6,$$

hetgeen in tegenspraak is met $n \geq 7$.

Bovenstaande gedachtengang is slordig (hier en daar ontbreken wat kleine factoren), en is gebaseerd op een nog onbewezen vermoeden. Maar het geeft wel aan welke kant we op zouden willen gaan. Inderdaad bewees Ken Ribet dat die Frey kromme $E_{A,B,C}$ zoals boven geconstrueerd niet bestaat, mist aan een vermoeden het zo genaamde Shimura-Taniyama-Weil vermoeden is voldaan (dat vermoeden geeft een parametrizatie van elliptische krommen over $\mathbb{Q}$, en zodoende een toegang tot het al of niet bestaan van een kromme van de vorm $E_{A,B,C}$). Dat STW-vermoeden werd in 1995 door Andrew Wiles bewezen (voor het "stabiele geval" wat we hier nodig hebben), zie [14]. Alhoewel het Szpiro vermoeden nog niet bewezen is, geeft toch die suggestie van Frey toegang tot het probleem, en via de omweg STW is nu FLT bewezen.

Wat is de rol van de theorie van elliptische krommen in dit geheel? Een kromme gegeven door $X^n + Y^n = Z^n$ voor $n > 3$ is een vlakke kromme, waarvan de meetkunde "moeilijk" is. Parametriseren van een dergelijke kromme met *transcendente functies* is mogelijk, zoals Poincaré ons al lang geleden ziet zien; maar daar hebben we niet zoveel aan voor *aritmetische toepassingen.*

Nu komt een weergave van het exacte bewijs van FLT. Via de Frey-kromme wordt het bestaan van één hypothetische oplossing met $abc \neq 0$ vertaald in het hypothetisch bestaan van de elliptische kromme $E_{A,B,C}$; daarvan krijgen we een rationale parametrizatie (met behulp van een modulaire kromme, mits STW bewezen is, de grote bijdrage van Wiles); via het bewijs van Ribet concluderen we dat die elliptische kromme $E_{A,B,C}$ niet bestaat (zoals Frey onmiddellijk aanvoelde), en het bewijs is rond.

(4.1) Het A-B-C-vermoeden. Zie [2], [8], [6]. Een recent vermoeden in de (elementaire) getaltheorie leek onbenaderbaar. We gaan weer uit van $A, B \in \mathbb{Z}_{>0}$ met $\text{ggd}(A, B) = 1$, en $C := A + B$. Voor een $\alpha \in \mathbb{Z}_{\geq 2}$ is (een eenvoudige vorm van het) vermoeden:
ABC$(\alpha)_?$:

$$C < \text{Cond}(A, B, C)^\alpha.$$

[Het juiste vermoeden dient zorgvuldiger geformuleerd te worden ...]

Als je dit gedrag van gehele getallen niet kent (het grillige gedrag van factorizatie van een som van twee getallen waarvan je de summanden al kunt factoriseren), dan lijkt het ABC-vermoeden bizar. Neem bv. maar eens aan dat $2^{49} + 1$ gelijk zou zijn aan 3^{31}; voor $A = 2^{48}$ en $B = 1$ zou er komen dat $N := \text{Cond}(A, B, C) = 6$, en $3^{31} < 6^\alpha$ zou geven $\alpha > 19$. Maar dit voorbeeld werkt niet: de getallen A en $C = 3^{31}$ zijn wel ongeveer even groot, maar $2^{49} + 1 \neq 3^{31}$. Het ABC-vermoeden zegt zoiets als: neem aan dat zowel A als B (of A en C) deelbaar zijn door hoge factoren van priemfactoren, dan geldt dit juist niet voor $A + B$ (respectievelijk voor $C - A$).

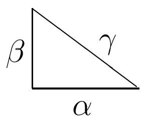
We kennen geen tegenvoorbeelden tegen het vermoeden ABC(2) (en voorbeelden met een exponent dicht bij 2 zijn al heel moeilijk te vinden!). [Advies: ga niet in "het wilde weg" proberen.]

Waar moet je beginnen met een bewijs van het ABC-vermoeden? Elementaire middelen lijken te falen. Maar ik weet dat er momenteel onderzoek verricht wordt; daarin wordt het vermoeden vertaald in eigenschappen van elliptische krommen. Vervolgens wordt geprobeerd dit bewijzen met methoden uit de meetkunde en de aritmetiek. Het ziet er veel belovend uit! Het zou een enorme doorbraak in de getaltheorie zijn. Dankzij, jawel, elliptische krommen.

(4.2) Congruente getallen. Een positief geheel getal N heet een *congruent getal* als er bestaan positieve rationale getallen α, β, γ zodanig dat:

$$\alpha^2 + \beta^2 = \gamma^2, \quad \text{en} \quad \alpha{\cdot}\beta/2 = N,$$

d.w.z. *als N de oppervlakte is van een rechthoekige driehoek met zijden van rationale lengte.* Als N een congruent getal is, dan zullen we het drietal $(\alpha, \beta, \gamma) \in (\mathbb{Q}_{>0})^3$ als hierboven een *presentatie* van het congruente getal noemen.



$\alpha \cdot \beta/2 = N \in \mathbb{Z}_{>0}$,
$\alpha^2 + \beta^2 = \gamma^2, \quad \alpha, \beta, \gamma \in \mathbb{Q}_{>0}$;
een voorbeeld: $\alpha = 9/6, \quad \beta = 40/6, \quad \gamma = 41/6, \quad N = 5$.

Het blijkt niet moeilijk te zijn om een (oneindige) lijst te maken waarin álle congruente getallen voorkomen. Maar, probeer maar eens te besluiten of 13 een congruent getal is. Of, moeilijker of 157 een congruent getal is. De moeilijkheid is: we kennen niet een effectieve manier om te besluiten hoe groot de noemers zijn die bij gegeven N we in een presentatie nodig hebben; en als je de moed opgegeven hebt om te besluiten of 157 een congruent getal is, raadpleeg dan [5], pagina 5, waar dit voorbeeld van Don Zagier staat: in de eenvoudigste presentatie van dit congruente getal heeft het getal γ een noemer van 46 cijfers. De sleutel tot dit probleem is - ja! alweer - de theorie van elliptische krommen:

(4.3) Feit (zie [5], Prop. 1 op pagina 4, en Prop. 19 op pp. 46/47): *Zij $N \in \mathbb{Z}_{>0}$. Beschouw de elliptische kromme E_N gedefiniëerd door de vergelijking*

$$E_N : \quad Y^2 = X{\cdot}(X - N){\cdot}(X + N).$$

Dan is N een congruent getal dan en slecht dan als er bestaan

$$x, y \in \mathbb{Q} \ \ \textit{met} \ \ y \neq 0 \ \ \textit{en} \ \ (x, y) \in E_N(\mathbb{Q}).$$

Het probleem welke getallen congruente getallen zijn is al meer dan 10 eeuwen bestudeerd. We hebben nog steeds geen bevredigend, effectief antwoord: het probleem is eenvoudig te formuleren, maar 10 eeuwen onderzoek heeft ons nog steeds niet tot de definitieve oplossing gebracht.

Met behulp van elliptische krommen formuleert Tunnell een vermoeden, waarmee op eenvoudige manier alle congruente getallen gekarakteriseerd zouden moeten zijn, zie [12] en zie [5], pag. 221. Het laatste woord over dit probleem, wat zo gemakkelijk lijkt, maar moeilijk blijkt, is nog niet gesproken.

5 Vladimir Nabokov: Lolita

In 1955 publiceerde de schrijver Vladimir Nabokov een boek, opgedragen aan zijn vrouw, wat de wereld schokte: *Lolita.* Het boek beschrijft hoe de hoofdpersoon H.H. (Humbert Humbert) haar ontmoet: *"She was Lo, plain Lo in the morning, standig four feet ten on one sock. She was Lola in slacks. She was Dolly at school. She was Dolores on the dotted line. But in my arms she was always Lolita."* En Nabokov beschrijft hoe H.H. dit meisje van twaalf jaar inpalmt, hoe hij de verantwoordelijkheid over haar krijgt; schitterende beschrijvingen van haar bevalligheid, van hoe ze door de USA reizen, H.H. met zijn "nymphet". Naast een schok, een gevoel van afgrijzen over dit zo abjecte onderwerp, vraagt de lezer zich toch af hoe deze auteur er toe komt hierover te schrijven. En, als je meer van Nabokov leest (vooral doen! bv. "Laughter in the dark" of "Pnin"), en je kent de voorliefde van Nabokov om de ene dubbele bodem in een boek te verbergen in weer een ander, dan blijf je met nog meer vraagtekens zitten.

Tot ik een bespreking van dit boek las (helaas moet ik uit mijn geheugen citeren). *"Stel je voor dat je in de 19-de eeuw leeft, en een boek over een mooie vrouw wilt schrijven. Bang voor een puriteinse ontvangst, zou je wel eens een mooie vermomming kunnen kiezen: je schrijft een boek over vlinders, en je leeft je steeds uit in lyrische beschrijvingen van hoe mooi vlinders zijn! terwijl je denkt aan* $\cdots$*. Goed, maar, stel dat je in de 20-ste eeuw leeft, en dat je heel veel van vlinders houdt* (zoals Nabokov deed) *en je wilt daarover schrijven; je beseft dat je in dit tijdperk met iets schokkends moet komen, wil je de aandacht trekken, wat doe je dan? Juist ja, je beschrijft een mooie vrouw, je leeft je uit in lyrische beschrijvingen, terwijl je aan vlinders denkt!*

Die bespreking onderbouwt dit argument; deze "verklaring", dat dit boek over vlinders gaat wordt onderbouwd door een passage in *Lolita* te analyseren; daarin reizen Lolita en H.H. door de USA; de auteur geeft het nummerbord van een passerende auto heel precies, de lezer begrijpt niet waarom, denkt dat het nummer nog terug komt, maar nee hoor; de criticus vindt de prachtige beschrijving van Lolita die daar gegeven wordt precies terug in een vlinder-encyclopedie op de pagina en de regel gegeven door het nummer van die auto. Nabokov heeft deze dubbele bodem ongetwijfeld bedoeld! Maar er zijn er vast nog wel meer. Nabokov bewondert zelf deze hoofdpersoon H.H., de tweede in zijn voorkeurslijst van favoriete hoofdpersonen na "Pnin" in zijn werk. Het is een mooi proces, over iets moois te schrijven of denken, terwijl je heel iets anders bedoelt.

Referenties

[1] H. J. M. Bos, C. Kers, F. Oort & D. W. Raven - *Poncelet's closure theorem.* Expos. Math. **5** (1987), 269 - 364.

[2] G. Frey - *Links between solutions of A-B=C and elliptic curves.* In: Number theory, Ulm 1987 (Ed. H. P. Schlickewei & E. Wirsing). Lect. N. Math. 1380, Springer - Verlag 1989, pp. 31-62.

[3] R. Hartshorne - *Algebraic geometry.* Graduate Texts Math. 52. Springer - Verlag, 1977.

[4] A. W. Knapp - *Elliptic curves.* Math. Notes 40, Princeton Univ. Press, 1992.

[5] N. Koblitz - *Introduction to elliptic curves and modular forms.* Graduate Texts Math. 97, Springer - Verlag, 1984.

[6] S. Lang - *Die abc-Vermutung.* El. Math. 48 (1993), 89 - 99.

[7] Vlaodimir Nabokov – *Lolita.* Eerste druk 1955. Nu verkrijgbaar als Penguin paperback.

[8] J. Oesterlé - *Nouvelles approaches du "théorème"de Fermat.* Sém. Bourbaki **40** (1987/88), Exp. 694. Astérisque 161-162 (1988), 165-186.

[9] F. Oort – *Congruente getallen en elliptische krommen.* Syllabus Nationale Wiskunde Dagen, januari 2001.

[10] J. H. Silverman - *The arithmetic of elliptic curves.* Graduate Texts Math. 106, Springer -Verlag, 1986.

[11] J. H. Silverman & J. Tate - *Rational points on elliptic curves.* Undergraduate Texts Math. Springer - Verlag, 1992.

[12] J. B. Tunnell - *A classical diophantine problem and modular forms.* Invent. Math. **72** (1983), 323 - 334.

[13] R. J. Walker – *Algebraic curves.* Princeton Univ. Press 1950, Dover Publ. 1962.

[14] A. Wiles - *Modular elliptic curves and Fermat's Last Theorem.* Annals of Mathematics **142** (1995), 443-551.

Frans Oort
Mathematisch Instituut
Budapestlaan 6 — Postbus 80010
NL - 3584 CD Utrecht — NL - 3508 TA Utrecht
email: oort@math.uu.nl