# Elliptische krommen

Frans Oort

## Project,
## Utrecht, november 2013 - januari 2014

## 1 Inleiding

**Doel.** In deze activiteit leren we zelfstandig werken (vraagstukken, opdrachten), samenwerken, een syllabus schrijven en begrijpelijk uitleggen (een voordracht houden) aan de hand van een fascinerend onderwerp: *elliptische krommen*.

We proberen dit te doen met een minimum aan technische voorbereidingen (algebra, commutatieve algebra, algebraïsche meetkunde). Zo komen we al gauw tot de kern van mooie problemen. Als wiskundigen, en zeker in een opleiding wiskunde, zijn we gewend alles van de grond af op te bouwen. Als we dat met dit onderwerp zouden doen, dan zijn we vele semesters verder voor we aan echte problemen toekomen.

Deze opzet vergt van het gehoor zich snel vertrouwd te maken zonder veel ondergrond, en "black boxes" te leren hanteren, wel door de juiste formulering en definities te kennen, zonder bewijzen compleet te begrijpen. Dat is een methode die wiskundigen vaak wel moeten toepassen in ons mooie maar ook moeilijke vak.

Ook zullen verschillende technieken aan de orde komen. Het vergt van het gehoor te kunnen overschakelen tussen meetkunde - algebra - getaltheorie. Maar dat is ook de grote charme en schoonheid van dit vak. Probeer in jouw systeem op te nemen: overschakelen van (elliptische krommen over $\mathbb{C}$) naar (arithmetiek, elliptische krommen over $\mathbb{Q}$) naar (elliptische krommen over een eindig lichaam) en weer terug.

Dit onderwerp past in de "*arithmetische algebraïsche meetkunde*": getaltheorie begrijpen met behulp van meetkundige methoden.

**Werkwijze, practische informatie.**

- Er zijn 6 colleges: **donderdag 10:00 - 13:00 uur**, vanaf 13 – XI – 2013 tot en met 19 – XII – 2013.
- We formeren groepje van elk hooguit 3 studenten. Elke groep verzorgt in het tweede deel een voordracht.
- Een **opgave**: wordt op college behandeld (als illustratie van de theorie);
  een **vraagstuk**: kan gemaakt en ingeleverd worden.
- Inleveren van de oplossingen van 8 vraagstukken (meer mag ook, minder geeft een lager cijfer): uiterste inlever-datum: 12 – XII – 2013 (harde deadline; begin niet te laat aan die vraagstukken). Iedereen mag zelf een keuze maken uit vraagstukken in dit pamflet.

- Inleveren van oplossingen van 5 opdrachten. Uiterste inlever datum: 14 – I – 2014 (harde deadline; begin niet te laat).
- Vanaf 7 – I – 2014 tot en met 23 – I – 2011: 6 bijeenkomsten; voordrachten worden gehouden op **dinsdag 13:15 − 15** en op **donderdag 9:00 − 11:00 uur.**
- Bij het nakijken van vraagstukken en opdrachten zal er zeer kritische gekeken worden naar het ingeleverde materiaal. Wees zorgvuldig, precies en correct. Bij de voordrachten is er een kritisch publiek: maak er iets moois van.
- Aanwezigheids-plicht. Studenten worden verondersteld bij alle 12 bijeenkomsten aanwezig te zijn. Ja, ik weet, als jouw voordracht geweest is, dat het verleidelijk is niet meer te komen, maar de anderen hebben ook recht op jouw aandacht.
- Zorg dat je de checklist afwerkt. Er komt niet ook nog een tentamen na afloop; ik neem aan dat studenten op dit niveau zelf hun verantwoordelijkheid kennen.
- Het eindcijfer wordt verkregen door middelen over de drie prestaties, waar de individuele prestaties zwaarder tellen dan de gezamenlijke voordracht.
- Aarzel niet om vragen te stellen, hulp in te roepen, te laten weten wat je mooi/moeilijk vindt. Interactie student - docent is een belangrijk onderdeel van deze activiteit.
- Dit pamflet is niet een syllabus. Veel theorie kan de student halen uit de colleges en uit de literatuur zonder dat volledige informatie hier te vinden is. Wel probeer ik verwijzingen te geven, zodat zelfstudie mogelijk is.
- Lang niet alles is compleet en goed gedefinieerd in dit pamflet. Aarzel niet om verdere uitleg te vragen.
- In de bibliotheek komt een plank met literatuur over deze activiteit. Materiaal daar kan in de bibliotheek bestudeerd worden, en mag niet meegenomen worden buiten de bibliotheek

**Opmerking.** Elliptische krommen over $\mathbb{C}$ of over $\mathbb{Q}$ vormen een fascinerend onderwerp (zoals we zullen zien). Toch beschouwen we dit onderwerp ook over een lichaam van positieve karakteristiek (met beperkingen, maar ook met mooie eigenschappen). Waarom? Niet alleen is dat een mooi onderwerp, maar ook zullen we die theorie gebruiken in beschouwingen in karakteristiek nul, in het bijzonder in de getaltheorie: "reductie modulo $p$" levert veel informatie. Vandaar.

We geven iets van de theorie die we nodig hebben in §§ 2 – 10.

In appendices §§ 11 – 14 geven we wat informatie over enkele begrippen uit de algebra, de getaltheorie, en de commutatieve algebra die we gebruiken. Die paragrafen bevatten een aantal eenvoudig en mooie vraagstukken. In §§ 15 – 17 geven we vraagstukken, opdrachten en onderwerpen voor voordrachten. Lees vooral geregeld § 19 om te kijken of je de onderwerpen die je geacht wordt te beheersen ook echt kent.

**Literatuur, speciaal aanbevolen.**

[31] J. Silverman & J. Tate – *Rational points on elliptic curves.*

[11] A. Knapp – *Elliptic curves.*
[29] J. Silverman – *The arithmetic of elliptic curves.*
[19] J. Milne – *Elliptic curves.*
[53] = [HAG] Hartshorne, R. – *Algebraic geometry.*

## 2 Algebraïsche krommen

Op het college zal ik definiëren / uitleg geven over: $\mathbb{A}^n(L)$, en over de affiene ruimte $\mathbb{A}^n_K$; uitleg over: $\mathbb{P}^n(L)$, over de projectieve ruimte $\mathbb{P}^n_K$ en uitleg over de Zariski-topologie.

**(2.1) Opgave.** Zij $I$ het interval $I := \{x \mid 0 \leq x \leq 1\} \subset \mathbb{R}$. Laat zien dat $I \subset \mathbb{A}^1_{\mathbb{C}}$ een Zariski-dichte deelverzameling is.

**(2.2) Algebraïsche krommen in het affiene vlak.** Neem een lichaam $K$, en een polynoom $f \in K[X,Y]$ met $f \notin K$. We schrijven $C = \mathcal{Z}(f)$ voor de vlakke kromme gegeven door $f$; het symbool $\mathcal{Z}(-)$ staat voor de "nulpunten-verzameling" (de Z van "zero-set"). Hieronder verstaan we: voor elke uitbreiding van lichamen $K \subset L$ geldt

$$C(L) = \mathcal{Z}(f)(L) := \{(x,y) \in \mathbb{A}^2_K(L) = L \times L \mid f(x,y) = 0\}.$$

Een eenvoudig voorbeeld. Neem $K = \mathbb{Q}$ en $f = X^2+Y^2+1$. We zien dat voor elke $\mathbb{Q} \subset L \subset \mathbb{R}$ de verzameling $C(L) = \emptyset$; echter $C$ is "helemaal niet leeg".
Nog een voorbeeld (Selmer). Er geldt: $\mathcal{Z}(3X^3+4Y^3+5)(\mathbb{Q}) = \emptyset$; zie (17.10) voor verwijzingen.
Nog een voorbeeld. Beschouw $C = \mathcal{Z}(-Y^2 + X^3 - X)$. We zien direct oplossingen; het kan bewezen worden dat

$$C(\mathbb{Q}) = \{(-1,0),\ (0,0),\ (1,0)\};$$

zie (9.5) en (17.2); deze kromme heeft interessante arithmetische eigenschappen. Dat lijkt toch een rare "kromme" die (over $\mathbb{Q}$) maar uit 3 punten bestaat. Teken een plaatje van $C(\mathbb{R})$. Als je voldoende kennis hebt van topologie: probeer de topologische ruimte (met de klassieke topologie) $C(\mathbb{C})$ te beschrijven.

We zien dat affiene krommen interessant kunnen zijn, zonder dat ze veel punten over $\mathbb{Q}$ hebben.

**(2.3) Een intuïtieve benadering.** Een meetkundige kijkt vaak tegen de voorgaande definitie als volgt aan. Beschouw een lichaam $K$, en een lichaam $K \subset k$, waar $k$ algebraïsch afgesloten is; bij voorbeeld $K = \mathbb{Q} \subset \overline{\mathbb{Q}} = k$ of $K = \mathbb{Q} \subset \mathbb{C}$. We kunnen dan $\mathbb{A}^2_K$ ons voorstellen als de ruimte $\mathbb{A}^2_K(k) = k^2$ of $\mathbb{A}^2_K(\mathbb{C}) = \mathbb{C}^2$, waarin elke algebraïsche kromme gegeven wordt door een vergelijking met coëfficienten in $K$. Pas goed op met deze manier van denken. Bij voorbeeld, een automorfisme $\varphi$ van $\mathbb{C}$ (en er zijn er heel veel) geeft een automorfisme van $\mathbb{C}^2$ (door $\varphi$ op de coördinaten te laten werken), maar voor $\varphi \neq \mathrm{id}$. geeft dit niet een automorfisme van $\mathbb{A}^2_{\mathbb{Q}}$

**(2.4) Homogeen maken van een polynoom.** Een polynoom $G \in K[X,Y,Z]$ heet *homogeen* als alle monomen in $G$ dezelfde (totale) graad hebben; equivalent: er is een $m \in \mathbb{Z}_{\geq 0}$ ("de graad van $G$") zodanig dat

$$G(TX,TY,TZ) = T^m G(X,Y,Z)$$

in $K[X,Y,Z,T]$. Zij $f \in K[X,Y]$. We schrijven $f^h \in K[X,Y,Z]$ voor het polynoom dat $f$ op "de zuinigste manier homogeen maakt". Precieze definitie:
(1) $f^h$ is homogeen;
(2) $f^h(X,Y,1) = f$ en $Z$ deelt niet $f^h$.

**(2.5) Projectieve vlakke algebraïsche krommen.** Laat $K$ een lichaam zijn, en $G \in K[X,Y,Z]$ een homogeen polynoom van positieve graad. We definiëren $C = \mathcal{Z}(G) \subset \mathbb{P}^2_K$ door:

$$C(L) = \mathcal{Z}(G)(L) = \{[x:y:z] \in \mathbb{P}^2_K(L) \mid G(x,y,z) = 0\}, \quad K \subset L.$$

**Opmerking.** Voor $[x:y:z] \in \mathbb{P}^2_K(L)$ is de waarde $G(x,y,z)$ in het algemeen niet goed gedefinieerd (waarom niet? ga na! dit begrijpen s.v.p.); maar de uitspraak $G(x,y,z) = 0$ is zinvol.

Waarom is dit nuttig? Laat zien dat voor $\mathbb{A}^2_K \subset \mathbb{P}^2_K$ gegeven door $(x,y) \mapsto [x:y:1]$ geldt dat

$$\mathcal{Z}(f^h) \cap \mathbb{A}^2_K = \mathcal{Z}(f)$$

en $\mathcal{Z}(f^h)$ is de Zariski-afsluiting van $\mathcal{Z}(f)$ in $\mathbb{P}^2_K$. (Op college wordt uitleg gegeven over de Zariski topologie; zie één van de standaard boeken, bv. [53].)

We zullen vaak zowel een affiene kromme $\mathcal{Z}(g) \subset \mathbb{A}^2_K$ als de bij behorende projectieve kromme $\mathcal{Z}(g^h) \subset \mathbb{P}^2_K$ beschouwen. Op het college wordt meer uitleg gegeven.

**(2.6) Opgave.** We beschouwen $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ met de klassieke topologie. Laat zien dat $\mathbb{A}^n(\mathbb{C})$ voor $n > 0$ niet een compacte ruimte is.

We beschouwen $\mathbb{P}^n(\mathbb{C})$ met de klassieke topologie. Laat zien dat voor $n > 0$ dit wel een compacte ruimte is.
(Doe dit voor $n = 1$, dat is al interessant genoeg.)

**(2.7) Niet-singuliere punten.** Zij $(x,y) = P \in \mathcal{Z}(f) =: C^0 \subset \mathbb{A}^2_K$ (notatie als boven). Neem en lichaamsuitbreiding $K \subset L$, en $P \in C^0(L)$. We zeggen dat $P$ *niet-singulier* is op $C^0$ als $f_X(P) \neq 0$ of $f_Y(P) \neq 0$ (het "zwakke of": beide kunnen ook ongelijk aan nul zijn"); we schrijven $f_X = (d/dX)f$; hier is $(d/dX)(aX^m) := maX^{m-1}$. We zeggen dat $P \in \mathcal{Z}(f)(L)$ *singulier* is als $f_X(P) = 0$ en $f_Y(P) = 0$. Op college zal meer uitleg volgen.

Ga na dat in de volgende gevallen het om een singulier punt gaat: $(0,0) \in \mathcal{Z}(-Y^2 + X^3)$, respectievelijk $(0,0) \in \mathcal{Z}(-Y^2 + X^3 + X^2)$ (teken plaatjes). Soms wordt wel de terminologie "een glad punt" gebruikt, of "$C$ is glad in het punt $P$". Deze terminologie, afkomstig uit de differentiaal meetkunde, zal ik niet gebruiken voor een niet-singulier punt in de algebraïsche meetkunde.

**(2.8) Opmerking.** Als $P = (0,0) \in \mathcal{Z}(f) = C \subset \mathbb{A}^2_K$ dan is de constante term van $f$ gelijk aan nul, want $f(x,y) = 0$, en $P$ een singulier punt van $C$ desda (dan en slechts dan als) de coëfficienten van de lineaire termen van $f$ gelijk aan nul zijn:
$\mathcal{Z}(X + X^3Y^4 + X^2Y^9)$ is niet-singulier in $P = (0,0)$;
$\mathcal{Z}(X^2 + X^3Y^4 + X^2Y^9)$ is singulier in $P = (0,0)$.

**(2.9) Opmerking/waarschuwing.** Als ($f_X(P) = 0$ en $f_Y(P) = 0$ maar) $P \notin \mathcal{Z}(f)$ dan gebruiken we de terminologie "singulier - niet-singulier" niet.

**(2.10) Opmerking/waarschuwing.** Vaak werken we over een grondlichaam, maar singuliere punten worden ook gedefinieerd/bestudeerd over uitbreidingslichamen. Zie ook (3.2).
**Opgave.** Zij $f := X^3 + Y^3 + XY^2 + X^2Y - X - Y \in \mathbb{Q}[X, Y]$. Bepaal alle singuliere punten van $C := \mathcal{Z}(f)$.

**(2.11) Snijpuntsmultipliciteit.** Dit is een veelzijdig onderwerp. Geheel in de stijl van dit college geven we de definitie in een speciaal geval, en verwijzen voor algemenere definities en eigenschappen naar algemenere theorie. Zie verder § 3.

Zij $g \in K[X, Y, Z]$ een homogeen polynoom en schrijf $C := \mathcal{Z}(g) \subset \mathbb{P}^2_K$. Zij $\ell := \mathcal{Z}(aX + bY + cZ) \subset \mathbb{P}^2_K$ een lijn; we nemen aan $a \neq 0$ of $b \neq 0$ of $c \neq 0$; beschouw $P = [x : y : z] \in C \cap \ell$. We definiëren $i(C, \ell; P)$, de *snijpuntsmultipliciteit* van $C$ en $\ell$ in $P$, als volgt. Onderstel dat $a \neq 0$. Substitueer:

$$g(-(bY + cZ)/a, Y, Z).$$

Als dit polynoom in $Y$ en $Z$ gelijk aan nul is, dan deelt $aX + bY + cZ$ het polynoom $g$, en we schrijven $i = \infty$. Zo niet, dan is dit poynoom na substitutie niet gelijk aan nul en we schrijven

$$g(-(bY + cZ)/a, Y, Z) = (yZ - zY)^\alpha . h(Y, Z)$$

met $h(y, z) \neq 0$ (m.a.w. we splitsen de factor $(yZ - zY)$ af zo vaak als dat kan). Terzijde: we weten dat $\alpha > 0$ (is dit duidelijk ?). We schrijven in dit geval

$$i(C, \ell; P) \quad := \quad \alpha.$$

Overigens, als $Q \notin C \cap \ell$, dan schrijven we $i(C, \ell; Q) = 0$.

**(2.12) Opmerking/Opgave.** Als de graad van $g$ gelijk aan $m$ is, en $aX + bY + cZ$ deelt niet $g$ dan is

$$\sum_{P \in \mathbb{P}^2(k)} i(C, \ell; P) \quad = \quad m$$

(ga na). Dit is een bijzonder geval van de stelling van Bezout (zie verderop).

**(2.13) De raaklijn in een punt aan een kromme.** Zij $P = (x, y)$, en $f \in K[X, Y]$, en veronderstel dat

$$(x, y) = P \in C^0 := \mathcal{Z}(f) \subset \mathbb{A}^2_K$$

een niet-singulier punt is. Dan wordt de raaklijn $L = \mathfrak{t}_{C^0,P}$ in $P$ aan $C^0$ gegeven door:

$$\mathfrak{t}_{C^0,P} = \mathcal{Z}\left(f_X(P)(X - x) + f_Y(P)(Y - y)\right) \subset \mathbb{A}^2_K.$$

Voor $g \in K[X, Y, Z]$ en $P = [x : y : z] \in C = \mathcal{Z}(g) \subset \mathbb{P}^2_K$ een niet-singulier punt wordt de raaklijn gegeven door

$$\mathfrak{t}_{C,P} = \mathcal{Z}\left(g_X(P)X + g_Y(P)Y + g_Z(P)Z\right) \subset \mathbb{P}^2_K.$$

Herinnering: we schrijven $G_X$ voor $(d/dX)G$. Hier volgt uitleg.

**(2.14) Vraagstuk.** Voor $(x, y) = P \in \mathcal{Z}(f)(K)$ (met notatie als boven) en $P = [x : y : 1]$ en $g := f^h$ laat zien:

$$g_X(P)x + g_Y(P)y + g_Z(P)z = 0;$$

(maak goed onderscheid tussen de variabele $X$ en een waarde $x \in K$ daarvan). Concludeer

$$f_X(P)(X - x) + f_Y(P)(Y - y) = (g_X(P)X + g_Y(P)Y + g_Z(P)Z)_{Z=1};$$

m.a.w. de twee definities van de raaklijn hierboven gegeven komen op hetzelfde neer.

**(2.15) Opmerking. Een formule van Euler.** Zij $g \in K[X, Y, Z]$ een homogeen polynoom van de graad $m$. Dan geldt

$$g_X X + g_Y Y + g_Z Z = mg;$$

een analoge formule geldt voor homogene polynomen in een ander aantal variabelen; een bewijs is eenvoudig: laat zien dat de formule geldt voor een monoom $aX^\alpha Y^\beta Z^{m-\alpha-\beta}$.

Echter (in het geval de karakteristiek van $K$ het getal $m$ deelt) helpt dit niet om het voorgaande vraagstuk op te lossen.

**(2.16) Opgave.** We beschouwen $-Y^2 - Y + X^3 - X^2 =: f \in \mathbb{Q}[X, Y]$ en de algebraïsche kromme gegeven door $C := \mathcal{Z}(f) \subset \mathbb{A}^2_{\mathbb{Q}}$. M.a.w. "de kromme gegeven door

$$Y^2 + Y = X^3 - X^2. \ \text{"}$$

Laat zien dat deze kromme niet-singulier is. We zien dat $P_0 := (x = 1, y = 0) \in C(\mathbb{Q})$. We gaan verder $P_1, P_2, \cdots$ construeren op de volgende recursieve manier: als $P_i$ bekend is, dan construeren de $P_{i+1}$ door de raaklijn $\ell_i$ in $P_i$ aan C te construeren, die snijden we met $C$, en we zien dat die lijn de kromme $C$ tweemaal snijdt in $P_i$ en ook nog snijdt in een nieuw punt, dat we $P_{i+1}$ noemen. In het geval hier beschouwd, construeer deze rij punten $\{P_i \mid i \geq 0\}$. Teken een plaatje van deze raaklijnen $\ell_i$ voor alle $i \geq 0$ en van de kromme. (Deze kromme komt nog terug hieronder, en in (7.17)).

**(2.17) Opgave.** We kiezen een priemgetal $p$, kiezen $-Y^2 - Y + X^3 - X^2 =: f \in \mathbb{F}_p[X, Y]$, en geven $C$ door $C := \mathcal{Z}(f) \subset \mathbb{A}^2_{\mathbb{F}_p}$. Voor welke keuze van $p$ geeft dit een singuliere kromme ?

**(2.18) Opmerking.** We nemen $g \in K[X, Y]$ en $G := g^h \in K[X, Y, Z]$ met

$$C^0 := \mathcal{Z}(g) \subset \mathbb{A}^2_K, \quad C^0 \subset \mathcal{Z}(G) =: C \subset \mathbb{P}^2_K.$$

Voor $P = (x, y) = [x : y : 1] \in \mathbb{A}^2(K)$ geldt:

$$\big(P = [x : y : 1] \in C^0 \ \text{ en } \ P \in C^0 \ \text{ is singulier}\big) \implies (G_X(P) = 0 = G_Y(P) = G_Z(P)).$$

**Opgave.** Als de karakteristiek van het grondlichaam gelijk is aan nul, dan geldt de omkering (ga na).
Het voorbeeld

$$g = X^3Y + XY^3 + 1, \ \ g^h = X^3Y + XY^3 + Z^4, \ \ \text{char}(K) = 2, \ \ P = [a : a : 1], \ \ a \in K$$

laat zien dat de omkering in het algemeen niet geldt (ga na).

**(2.19) Vraagstuk. Uitleg raaklijn.** Zij $(x, y) = P \in C^0 = \mathcal{Z}(f)$ met notatie als boven, en zij $P \in L = \mathcal{Z}(aX + bY + c)$ met $a \neq 0$ of $b \neq 0$. Bewijs: dan is $i(C, L; P) > 0$ en

$$i(C^0, L; P) = 1 \quad \Longleftrightarrow \quad \big(P \in C^0 \quad \text{is niet-singulier en} \quad L \neq \mathfrak{t}_{C^0,P}\big)\,.$$

M.a.w. de raaklijn is in een niet-singulier punt de enige lijn die met hogere multipliciteit snijdt en in een singulier punt snijden alle lijnen door dat punt met een multipliciteit groter dan een.

**(2.20) De stelling van Bezout.*** Een uitvoerig onderwerp. Snijpuntsmultipliciteiten kunnen algemener gedefinieerd worden dan hierboven gedaan is. Ik geef toelichting op het college. Voor twee vlakke krommen $\mathcal{Z}(g_1)$ respectievelijk $\mathcal{Z}(g_2)$ geldt:

$$\sum_{P \in \mathbb{P}^2(k)} i(\mathcal{Z}(g_1), \mathcal{Z}(g_2); P) = \deg(g_1) \cdot \deg(g_2).$$

Uitleg en bewijzen vinden we o.a. in [53], [49], [62].

# 3 Elliptische krommen, algemeen

**(3.1) Definitie.** Zij $K$ een lichaam, en $g \in K[X, Y, Z]$ een homogeen polynoom van de graad 3. Zij $E := \mathcal{Z}(g) \subset \mathbb{P}^2_K$. We zeggen dat $(E, 0)$ een *elliptische kromme* is als $E$ niet-singulier is, en als er een punt $0 \in E(K)$ is dat een buigpunt is van $E \subset \mathbb{P}^2_K$. (Het begrip "buigpunt" wordt in (5.9) gedefinieerd.)

**(3.2) Opmerking.** We zeggen dat $C = \mathcal{Z}(h) \subset \mathbb{P}^2_K$ niet-singulier is, als voor elk punt $P \in C(k)$ tenminste één van de afgeleiden $(d/dX)(h)$, $(d/dY)(h)$, $(d/dZ)(h)$ niet nul is in het punt $P$, zie (2.7).

**Opmerking/Voorbeeld.** Een subtiel punt: om te kijken of $C$ al of niet singulier is moeten we kijken naar punten over $k = \overline{k} \supset K$.

Hier is een voorbeeld van $C$ over $K$ waar alle punten $P \in C(K)$ niet-singulier zijn, maar $C$ wel degelijk singulier is. Neem $C = \mathcal{Z}((Y^2+1)^2 + X^3)$ over $\mathbb{R}$. Laat zien dat $C$ singulier is, maar dat alle punten in $C(\mathbb{R})$ niet-singulier zijn op $C$. – Zie je hoe ik dit voorbeeld gemaakt heb? Maak zelf veel andere voorbeelden.

**(3.3) Opmerking.*** Hier is een voorbeeld van een kromme die singulier is, maar waar het singuliere punt niet coördinaten heeft in het grondlichaam. Neem $K = \mathbb{F}_2(t)$; hier is $t$ transcendent over $\mathbb{F}_2$. Neem

$$C^0 = \mathcal{Z}(Y^2 + X^3 + tX + 1) \subset \mathbb{A}^2_K.$$

Neem $K' := K(\sqrt{t})$. (Merk op: $K \subsetneqq K'$.) Het punt $P = (\sqrt{t}, 1) \in C^0(K')$ is singulier op $C^0$.

**(3.4) Opmerking.*** Als $M$ een perfect lichaam is, en $C \subset \mathbb{A}^2_M$ is een singuliere, absoluut irreducibele, kubische kromme over $M$ dan heeft het singuliere punt coördinaten in $M$. (Een lichaam $M$ heet perfect als het óf karakteristiek nul heeft, óf als $p$ de karakteristiek is, voor elke $a \in M$ ook $\sqrt[p]{a} \in M$.)

**(3.5) Voorbeeld/opgave.** Zij $K$ een lichaam. Zij

$$C = \mathcal{Z}(-Y^2Z + X^3 + AXZ^2 + BZ^3) \subset \mathbb{P}^2_K$$

met $A, B \in K$. We laten zien dat $C$ niet-singulier is desda (dan en slechts dan als)

$$-16\cdot(4A^3 + 27B^2) \neq 0.$$

(S.v.p. dit goed begrijpen. Dit verschijnsel, en deze formule komen steeds terug.)
**Opmerking.** Ga na dat het punt $\mathcal{Z}(Z) \cap C$ niet een singulier punt is op $C \subset \mathbb{P}^2_K$.
**Waarschuwing.** In bovenstaande opgave wordt er niets (van te voren) verteld over de karakteristiek van $K$; die kan gelijk aan 2 zijn.

**(3.6) Opmerking / Toelichting.*** We hebben voor de meest zuinige definitie voor een elliptische kromme gekozen. Hier volgt de algemene opzet (die we niet gebruiken in dit project). Voor elke algebraïsche kromme $C$ kunnen we de definitie geven van het *geslacht* $g = g(C)$. Daarin is $g(\mathbb{P}^1) = 0$. Elke elliptische kromme (zoals boven gedefinieerd) heeft geslacht gelijk aan 1. We kunnen een elliptische kromme definiëren als: een projectieve, niet-singuliere kromme $E \subset \mathbb{P}^m_K$ over een lichaam $K$ met $g(E) = 1$ en een punt $0 \in E(K)$. Om dit schijnbaar algemenere begrip goed te hanteren moeten we allerlei definities en feiten algemeen invoeren; we proberen dit te omzeilen zoals dat gebeurt in (3.1).

Dan geldt: elke elliptische kromme als in deze opmerking gedefinieerd kan overgevoerd worden in een die voldoet aan (3.1), en omgekeerd.

Een kromme van geslacht 1 die (*niet een $K$-rationaal punt heeft noemen we niet een elliptische kromme.* Er bestaan krommen van geslacht één over een lichaam $K$, die niet een $K$-rationaal punt hebben; zie (17.10).

**(3.7) Vergelijkingen.** (Hier gebruiken we $\mathrm{char}(K) \neq 2, \neq 3$.) We zullen het volgende taalgebruik hanteren (en dat wordt vaak zo gedaan in de literatuur). We zeggen "de elliptische kromme gedefinieerd door $Y^2 = X^3 + AX + B$" met $A, B \in K$. Daarmee bedoelen we het volgende; bekijk het polynoom $f = -Y^2 + X^3 + AX + B$; maak het homogeen: $f^h = g = -Y^2Z + X^3 + AXZ^2 + BZ^3$. Geef $E := \mathcal{Z}(g) \subset \mathbb{P}^2_K$. We zien dat het punt $0 = [x = 0 : y = 1 : z = 0] \in E(K)$ een buigpunt is met als raaklijn $\mathcal{Z}(Z) \subset \mathbb{P}^2_K$.

We zagen in (3.5) dat voor $16(-4A^3 - 27B^2) \neq 0$ deze kromme niet-singulier is en dat er dan inderdaad een elliptische kromme komt zoals in (3.1).

Merk op dat voor elk lichaam $K \subset L$ we hebben:

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

Voor vergelijkingen zie (W1) – (W7) in § 14. Een vergelijking in een van de eerste drie vormen wordt een *Weierstrass vergelijking* of een *Weierstrass normaal vorm* genoemd.

**(3.8) Lemma.** *Zij $E'$ een elliptische kromme over een lichaam $K$, zoals gedefinieerd in* (3.1). *Dan bestaat er een lineaire, projectieve transformatie die de vergelijking voor $E'$ overvoert in een Weierstrass vergelijking* (W2).

*Als de karakteristiek van $K$ bovendien niet gelijk aan* 3 *is dan kunnen we zo de vergelijking* (W3) *verkrijgen.*

*Als de karakteristiek van $K$ niet gelijk is aan* 3 *en niet gelijk is aan* 2 *dan kunnen we zo de vergelijking* (W1) *verkrijgen.*
Een bewijs wordt op college gegeven. □

**(3.9) Constructie van de groepswet.** *Voor een elliptische kromme $E \subset \mathbb{P}^2_K$ en voor punten $P, Q \in E(L)$, met $K \subset L$ gaan we $P + Q$ definiëren.*
We schrijven $P * Q$ voor het punt zo dat de lijn die $P$ met $Q$ verbindt als snijpunten met $E$ precies $\{P, Q, P * Q\}$ heeft; als $P = Q$ dan kiezen we voor die lijn de raaklijn in dat punt. Ga na dat in alle gevallen $P * Q$ goed gedefinieerd is. Merk op: als $P$ een buigpunt is, dan is $P * P = P$.
Neem $0 \in E(K) \subset E(L)$ het buigpunt dat gegeven is op $E$.

(Merk op: als $E$ door een Weierstrass normaal vorm gegeven is, dan nemen we $0 = [0 : 1 : 0]$.).
We schrijven $P + Q := (P * Q) * 0$. We schrijven $-P := P * 0$ (teken zelf plaatjes).

(Merk op: als $E$ door de Weierstrass normaal vorm (W2) gegeven is, en $R = (x, y) = [x : y : 1]$ dan is $R * 0 = (x, -y)$.)
Vanaf nu zullen we de groepswet schrijven als $P+Q$; pas op: $(x, y)+(x', y')$ is niet de optelling van vectoren in $\mathbb{A}^2$.
Merk op: als $E$ door de Weierstrass normaal vorm (W2) gegeven is, dan is $(x, y) + (x, y) = 0$ desda de raaklijn in dat punt verticaal loopt. We zullen zien dat bovendien $(x, y) + (x, y) + (x, y) = 0$ desda dit punt een buigpunt is.

We zien: $P + Q$ is goed gedefinieerd; $P + Q = Q + P$; verder: $P + 0 = P$ en $P + (-P) = 0$.

Ga dit allemaal na.

**Stelling / Feit.**$^*$ *Voor elke elliptische kromme $E$ en voor elke $L$ is $E(L)$ met de bovenstaande bewerkingen een commutatieve groep.*
Alle eigenschappen behalve de associatieve wet zijn eenvoudig in te zien. Een bewijs voor de associatieve wet kost meer werk. Ik geef toelichting, maar niet een volledig bewijs op het college. Of, zie elk van de boeken over elliptische krommen voor een bewijs (er zijn er vele verschillende). □

**(3.10) Opgave.** Als een elliptische kromme wordt gegeven door $Y^2 = X^3 + aX^2 + bX + c$ (over een lichaam $K$ van karakteristiek niet gelijk aan 2), en $P = (x, y) \in E(K)$ dan is $-P = (x, -y)$; bewijs dit.

Een elliptische kromme wordt gegeven door $Y^2 + Y = X^3 + aX^2 + bX + c$, en $Q = (x, y) \in E(K)$; bepaal in dit geval $-Q$.
N.B. in al deze gevallen wordt het punt $0 = [0 : 1 : 0]$ als nulpunt van de groepswet gekozen.

De groepswet wordt gekarakteriseerd door de keuze van 0 en door de eigenschap

$$P + Q + R = 0 \quad \Longleftrightarrow \quad P, Q, R \quad \text{liggen op een rechte lijn.}$$

**(3.11) Opmerking.** Op een singuliere kubische kromme $C$ gegeven door een Weierstrass normaal vorm is er precies één singulier punt; noem dat $S$. Zie (3.3), (3.4). Bovendien geeft de constructie hierboven een groepswet op $E(L) - \{S\}$, en het bewijs dat dit een groepswet geeft is in zulke gevallen niet zo moeilijk. Zie (15.2). – We zullen deze situatie tegenkomen. Bij voorbeeld $Y^2 = X(X^2 - 9)$ geeft een niet-singuliere kromme over $\mathbb{Q}$ maar een singuliere kromme over $\mathbb{F}_3$, en een studie van "reductie modulo 3" geeft nuttige informatie; daarover later veel meer.

**(3.12)** We zeggen dat elliptische krommen $E_1$ en $E_2$ over $K$, zoals in (3.1) *isomorf* zijn als er een projectieve, lineaire transformatie over $K$ bestaat die de vergelijking van $E_1$ overvoert in die van $E_2$ en die $0 \in E_1$ overvoert in $0 \in E_2$.
**Opmerking.** We kunnen ook zeggen "isomorf over $K$" als verwarring mogelijk zou zijn. Echter we zullen de notatie $E$ gebruiken over $K$ en $E \otimes L$ gebruiken voor de kromme die door de vergelijking van $E$ gegeven wordt over $L \supset K$,
**Voorbeeld.** De vergelijking $Y^2 = X^3 + AX + B$ wordt door $U = t^2X, \;\; V = t^3Y$ met $t \neq 0$ na vermenigvuldigen met de constante $t^6$ overgevoerd in $V^2 = U^3 + t^4AU + t^6B$. We zien dat de elliptische krommen gegeven door $Y^2 = X^3 + 1$ en door $Y^2 = X^3 + t^6$ met $t \in \mathbb{Q}^*$ isomorf zijn over $\mathbb{Q}$.

**(3.13)**$^*$ Eigenlijk hebben we we een veel algemener begrip van "morfisme", "isomorfisme" en "endomorfisme" nodig.
**Voorbeeld.** Gegeven is een elliptische kromme $E$ door $Y^2 = X^3 + AX + B$ en $P = (a, b) \in E(K)$. Schrijf uit in coördinaten de afbeelding $Q = (x, y) = [x : y : 1] \mapsto Q + P$, "translatie op $E$ met het punt $P$". In het algemeen is dat niet een lineaire transformatie, maar zulke afbeeldingen willen we wel graag beschouwen als "morfisme van een kromme"; merk echter op dat "translatie op $E$ met het punt $P$" voor $P \neq 0$ niet het punt 0 in 0 overvoert; het is daarom niet een isomorfisme van elliptische krommen (het respecteert de groepswet niet).
**Voorbeeld.** Schrijf uit $Q \mapsto Q + Q$ op $E$. We krijgen "verdubbelingsformules". Schrijf zulke formules uit. Ook die willen we in een algemener kader onderbrengen.

Ad hoc definitie. We zeggen dat we een morfisme hebben van de algebraïsche krommen $E_1$ naar $E_2$ als er homogene polynomen van dezelfde graag zijn $\mathcal{U}(X, Y, Z), \mathcal{V}(X, Y, Z), \mathcal{W}(X, Y, Z)$ die een vergelijking in $X, Y, Z$ overvoert (op vermenigvuldigen met een constante na) in een vergelijking in $U, V, W$. In het kader van de algebraïsche meetkunde zijn betere definities te geven. We zien aan bovenstaande voorbeelden dat zulke polynomen knap ingewikkeld kunnen zijn. We spreken bovendien van een *endomorfisme* $E \to E$ als de afbeelding ook de groepswet respecteert; de ring van endomorfismen $\mathrm{End}(E)$ van een elliptische kromme $E$ over een lichaam $K$ kunnen (en zullen) we bestuderen (in speciale gevallen).

**(3.14)**$^*$ Voor een elliptische kromme $E$ over een lichaam $K$ geven we een getal $j(E) \in K$; voor de definitie van $j(E)$ zie § 14. Het is een nogal ad hoc definitie. We zullen er niet zoveel mee doen. Pas in de theorie van "moduli" wordt het belang duidelijk. Gemakkelijk te bewijzen: als $E_1$ en $E_2$ isomorf zijn, dan is $j(E_1) = j(E_2)$. Ook waar, maar iets moeilijker om te bewijzen: als $j(E_1) = j(E_2)$ dan zijn $E_1 \otimes k$ en $E_2 \otimes k$ isomorf; opmerking: we schrijven $k$ voor een algebraïsch afgesloten lichaam. De curieuze formules die $j(-)$ geven worden pas duidelijk in een veel algemenere theorie. (De notatie $E \otimes k$ betekent: neem de kromme $E$ over $K$ en beschouw die nu als kromme over $k$.)

# 4 Elliptische krommen, over $\mathbb{C}$ $^*$

Deze paragraaf behoort niet tot de stof van het college. Echter, voor een goed begrip van elliptische krommen is het nuttig om meetkundig inzicht in elliptische krommen over $\mathbb{C}$ te hebben. Vraagstukken uit deze paragraaf kunnen gemaakt worden met behulp van de "black box" (4.4).

In deze paragraaf beschrijven we een klassieke methode: uniformisatie van elliptische krommen over $\mathbb{C}$ met behulp van *transcendente functies*. We zullen niet veel bewijzen. Het is goed om de uitspraken van deze paragraaf te begrijpen, als motivatie en achtergrond bij het hanteren van elliptische krommen. Methoden uit deze paragraaf zijn klassiek, en ook modern te bewijzen.

**(4.1) Opmerking.** Analytische methoden geven veel informatie en meetkundig inzicht. Echter, in arithmetische situaties is die informatie op sommige aspecten onvoldoende.
**Voorbeeld/Vraagstuk.** Neem $a, b \in \mathbb{Q}$ met $a \neq 0$ en $b \neq 0$. Geef $E$ over $\mathbb{Q}$ met behulp van $Y^2 = X^3 + a$ en geef $E'$ over $\mathbb{Q}$ met behulp van $Y^2 = X^3 + b$. Zie ook (6.2).
**(1)** Laat zien dat $E$ en $E'$ elliptische krommen zijn.
**(2)** Laat zien dat er een transformatie is over $\mathbb{C}$ die een isomorfisme tussen deze beide elliptische krommen over $\mathbb{C}$ geeft.
**(3)** Neem $a = 1$ en $b$ niet een derde-macht in $\mathbb{Q}$. Laat zien dat $E$ en $E'$ als elliptische krommen over $\mathbb{Q}$ niet isomorf zijn.

**(4.2) Opmerking.** Een elliptische kromme over $\mathbb{C}$ kan gegeven worden door middel van een vergelijking, zie (14.4):

$$Y^2 = 4X^3 - g_2X - g_3; \qquad (W3)$$

$$j(E) = 1728 \cdot \frac{g_2^3}{\Delta}; \quad \Delta = \Delta(E) = g_2^3 - 27g_3^2 \neq 0.$$

**(4.3) Definitie.** Onderstel gegeven $\omega_1, \omega_2 \in \mathbb{C}$ zodanig dat $\{\omega_1, \omega_2\}$ een $\mathbb{R}$-lineair onafhankelijk stelsel is. De groep

$$\mathbb{Z}\cdot\omega_1 \times \mathbb{Z}\cdot\omega_2 =: \Lambda_{\omega_1,\omega_2} = \Lambda \subset \mathbb{C}$$

wordt een *rooster* in $\mathbb{C}$ genoemd.
**Equivalente definitie.** De additieve groep $\Lambda \subset \mathbb{C}$ bevat een stelsel $\mathbb{R}$-voortbrengers voor de $\mathbb{R}$-vectorruimte $\mathbb{C}$ en $\Lambda \subset \mathbb{C}$ is discreet, d.w.z. er is een $\epsilon \in \mathbb{R}_{>0}$ zodanig dat elke cirkel in $\mathbb{C}$ met straal $\epsilon$ hooguit één punt van $\Lambda$ bevat.

**(4.4) Feit / Stelling**$^*$ (Weierstrass; complexe uniformisatie van een elliptische kromme.)
**(1)** *Zij $E$ een elliptische kromme over $\mathbb{C}$. Veronderstel dat $Y^2 = 4X^3 - g_2X - g_3$ een vergelijking is die $E$ geeft. Dan is er een rooster $\Lambda = \Lambda_{\omega_1,\omega_2} \subset \mathbb{C}$, en er is een meromorfe functie $\wp$ op $\mathbb{C}$, holomorf op $\mathbb{C}$ buiten $\Lambda$, die dubbel-periodiek is:*

$$\wp(z) = \wp(z + a\cdot\omega_1 + b\cdot\omega_2), \qquad \forall a, b \in \mathbb{Z}$$

*die voldoet aan de differentiaal vergelijking*

$$(\wp')^2 = \wp^3 - g_2\wp - g_3.$$

*In dit geval geeft*

$$(\wp, \wp') : \mathbb{C} \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$$

*een surjectieve afbeelding, die een* groeps-isomorfisme

$$\mathbb{C}/\Lambda \quad \xrightarrow{\sim} \quad E(\mathbb{C})$$

*induceert.* Hierin wordt $z \in \Lambda$ afgebeeld op $0 = [0:1:0]$.
**(2)** *Omgekeerd geeft elk rooster $\Lambda = \Lambda_{\omega_1,\omega_2} \subset \mathbb{C}$ een Weierstrass dubbel-periodiek functie, die aan een differentiaal vergelijking voldoet, en die vergelijking definieert een elliptische kromme (zoals hierboven).*
**(3)** Merk op: een $\mathbb{C}$–lineaire afbeelding $\mathbb{C} \to \mathbb{C}$ is niets anders dan het vermenigvuldigen met een complex getal $t \in \mathbb{C}$. *Een afbeelding*

$$\times t : \mathbb{C} \longrightarrow \mathbb{C} \quad \textit{die de eigenschap heeft} \quad t{\cdot}\Lambda \subset \Lambda$$

*induceert een endomorfisme van $E(\mathbb{C})$. Dit geeft een isomorfisme van ringen:*

$$\{t \in \mathbb{C} \mid t{\cdot}\Lambda \subset \Lambda\} \xrightarrow{\sim} \mathrm{End}_{\mathbb{C}}(\mathbb{C}/\Lambda) \cong \mathrm{End}(E).$$

Voor expliciete formules zie o.a. [31], pag. 43. Zie ook [11], Ch. VI; [19], Ch. III; [29], Ch. VI.
Een klassieke beschrijving van de Weierstrass $\wp$–functie vinden we in:
E. Whittaker & G. Watson – A course of modern analysis. Cambridge Univ. Press, 1969. □

**(4.5)**$^*$ Over deze stelling en over het bewijs ervan is veel te vertellen. Laat ik slechts enkele opmerkingen maken. Het klassiek bewijs van deze stelling maakt gebruik van complexe functietheorie. Daarin kunnen we het verband tussen enerzijds de getallen $g_2$ en $g_3$ en anderzijds de perioden $\omega_1$ en $\omega_2$ expliciet (maar niet eenvoudig) geven. Die formules zijn erg mooi, mar niet altijd practisch.

Hier is een voorbeeld. Als $\omega_1/\omega_2$ (imaginair) kwadratisch is over $\mathbb{Q}$ dan is $j(\mathbb{C}/\Lambda)$ een getal dat geheel is over $\mathbb{Z}$. Maar het is niet eenvoudig om dat feit expliciet uit de formules af te leiden.

Een modern bewijs van de stelling maakt gebruik van theorie van complexe Lie groepen; daarin volgt de afbeelding $\mathbb{C} \cong \mathfrak{t}_{E,0} \to E(\mathbb{C})$ als exponentiaal afbeelding; compactheid van $E(\mathbb{C})$ geeft dat de kern van deze afbeelding een rooster is, en daarom voortgebracht over $\mathbb{Z}$ door twee "perioden". Het laatste deel van de stelling past in een algemene theorie, die voor compacte algebraïsche variëteiten een isomorfisme geeft tussen de analytische en de algebraïsche afbeeldingen (een diepe stelling van Chow en van Serre). Beide benaderingen zijn niet elementair.

Deze stelling ligt ten grondslag aan een indrukwekkend apparaat, de benadering van arithmetische problemen via modulaire vormen (geheel buiten het materiaal voor dit project, helaas !).

**(4.6) Vraagstuk.** Zij $\Lambda_\tau := \mathbb{Z}{\cdot}1 + \mathbb{Z}{\cdot}\tau$ met $\tau \in \mathbb{C}$ en $\mathrm{Im}(\tau) > 0$. Stel dat er een $t \in \mathbb{C}$ is met $t \notin \mathbb{R}$ en $t(\Lambda_{1,\tau}) \subset \Lambda_{1,\tau}$. Bewijs dat in dit geval $L := \mathbb{Q}(\tau) \supset \mathbb{Q}$ een imaginair kwadratische uitbreiding is (m.a.w. $\tau$ voldoet aan een kwadratische vergelijking over $\mathbb{Q}$).

**(4.7) Vraagstuk. (1) Karakteristiek nul.** Zij $K$ een lichaam van Karakteristiek nul. Zij $E$ een elliptische kromme over $K$. Laat zien dat $\mathrm{End}(E)$ een commutatieve ring is.
**(2) Over $\mathbb{C}$.** Bewijs dat elke orde in elk imaginair kwadratisch getallen lichaam $L$ kan optreden als een endomorfismen ring van een elliptische kromme over $\mathbb{C}$ (een orde in $L$: een deelring van de ring van gehelen $\mathcal{O}_L$ die bovendien daarin van eindig index is als additieve groep).
**(3) Over een eindig lichaam.** Zij $E$ de elliptische kromme gegeven over $K = \mathbb{F}_4$ door $Y^2 + Y = X^3$. Geef twee automorfismen van $E$ over $K$ die niet commuteren; concludeer dat

in dit geval $\mathrm{End}(E)$ niet commutatief is.
**Opmerking.** Voor elke $p$ is er over $k = \overline{\mathbb{F}_p}$ een eindige verzameling van elliptische krommen (de supersinguliere elliptische krommen) waarvoor de endomorfismen ring niet-commutatief is; in alle andere gevallen is de endomorfismen ring van een elliptische kromme commutatief.

**(4.8) Opmerking.** Zie ook (4.1). Waarom lossen we arithmetische problemen niet op met analytische parametrisaties? Als we een analytische functie $\psi(z)$ hebben, zoals bij voorbeeld $\psi = \wp$, dan is moeilijk om uit getaltheoretische informatie over $z$ getaltheoretisch informatie over $\psi(z)$ te halen, en omgekeerd.
Een voorbeeld. We zullen in het probleem van de congruente getallen (en eigenschap van gehele getallen) krommen van de vorm $E_n : \quad Y^2 = X(X-n)(X+n)$ tegenkomen; zie § 9. Die krommen geven voor gehele getallen $n > 0$ veel verschillende isomorfie-klassen van elliptische krommen over $\mathbb{Q}$ (en de arithmetiek daarvan beheerst het probleem); echter voor $n > 0$ en $m > 0$ zijn $E_n \otimes \mathbb{C}$ en $E_m \otimes \mathbb{C}$ isomorf over $\mathbb{C}$: overgang naar de complexe getallen laat arithemtische informatie verloren gaan.
Een ander voorbeeld. Andrew Wiles gebruikte in zijn bewijs van FLT elliptische krommen over $\mathbb{Q}$ op een essentiële manier; ook daar gaat benodigde aritmetische kennis verloren bij overgang naar $\mathbb{C}$.
Kortom: deze paragraaf, en vooral (4.4) geeft topologische en meetkundige informatie over $E(\mathbb{C})$, maar vaak niet voldoende arithemetische informatie over $E$.

**(4.9) Notatie.** We schrijven $\mathrm{SL}(\mathbb{Z}, 2)$ voor de (multiplicatief geschreven) groep van $2 \times 2$ matrices met elementen uit $\mathbb{Z}$ en determinant gelijk aan 1 (SL = Special Linear group). We schrijven $\Gamma = \mathrm{SL}(\mathbb{Z}, 2)/\{\pm 1\}$. We schrijven $\mathfrak{h}$ voor het "bovenhalfvlak":

$$\mathfrak{h} := \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

We geven een werking van $\Gamma$ op $\mathfrak{h}$ door:

$$\Gamma \times \mathfrak{h} \longrightarrow \mathfrak{h} : \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot z = \frac{Az + B}{CZ + D}.$$

We schrijven $E_\tau$ voor een elliptische kromme met de eigenschap

$$E_\tau(\mathbb{C}) \cong \mathbb{C}/\Lambda_{1,\tau}, \quad \tau \in \mathfrak{h}, \quad \Lambda_{1,\tau} = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau.$$

**(4.10) Opdracht.** (1) Neem $\tau, \rho \in \mathfrak{h}$. Bewijs dat $E_\tau \cong E_\rho$ dan en slechts dan als er een $\gamma \in \Gamma$ is met $\gamma\cdot\tau = \rho$. [Gebruikt mag worden: een dergelijk isomorfisme geeft een lineair isomorfisme op de raakruimtes $\mathfrak{t}_{E_\tau,0} \to \mathfrak{t}_{E_\rho,0}$.]
(2) Laat zien dat de werking van $\Gamma$ op $\mathfrak{h}$ trouw is (d.w.z. alleen $1 \in \Gamma$ geeft de indentieke afbeelding op $\mathfrak{h}$). Schrijf

$$S\cdot z = \frac{-1}{z}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \quad T\cdot z = z + 1, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Bepaal de orde van deze elementen in $\Gamma$. Laat zien dat $\Gamma$ wordt voortgebracht door deze twee elementen. [Aanwijzing: zie bv. [45].] Zie ook:
`http://en.wikipedia.org/wiki/Modular_group`

# 5 Torsie punten

Een element $a \in A$ in een groep $A$ heet een *torsie-element* als het van eindige orde is. Pas op, in een niet-abelse groep kan het voorkomen dat het product van torsie-elementen niet een torsie-element is (kun je een voorbeeld geven ?).

**(5.1) Vraagstuk.** Geef een voorbeeld van een groep $G$, en elementen $S, T \in G$ zodanig dat $S$ en $T$ eindige orde hebben, maar $ST$ niet eindige orde heeft.

**(5.2)** Maar voor een *abelse groep* $A$ geldt dat de verzameling $\mathrm{Tors}(A)$ van alle elementen van eindige orde in $A$ een ondergroep is (geef een bewijs). We zullen hier bekijken wat de structuur is van $\mathrm{Tors}(E(K))$ en van $\mathrm{Tors}(E(k))$ voor een elliptische kromme $E$ over een lichaam $K$ waar $k$ een algebraïsch afgesloten lichaam is dat $K$ bevat.

**Notatie.** Voor een *abelse* groep $A$ en een getal $n \in \mathbb{Z}_{>1}$ schrijven we $A[n]$ voor de ondergroep van elementen $a$ waarvoor de orde van $a$ een deler is van $n$; m.a.w.

$$A[n] \quad = \quad \mathrm{Ker}\,(\times n : A \longrightarrow A)\,.$$

**Opmerking.** *Zij $E$ een elliptische kromme over $K$, en $K \subset K'$.* Merk op dat $E(K) \subset E(K')$, en dus $\mathrm{Tors}(E(K)) \subset \mathrm{Tors}(E(K'))$.

**(5.3) Feit** *Zij $n \in \mathbb{Z}_{>1}$. Zij $k$ een algebraïsch afgesloten lichaam.*
**(1)** *Veronderstel dat de karakteristiek van $k$ niet een deler is van $n$. Dan geldt*

$$E(k)[n] \quad \cong \quad (\mathbb{Z}/n)^2\,.$$

**(2)** *Zij $p > 0$ de karakteristiek van $k$ en $i \in \mathbb{Z}_{>0}$. Dan geldt*

$$E(k)[p^i] \cong \mathbb{Z}/(p^i) \quad \text{óf} \quad E(k)[p^i] = 0;$$

*bovendien: voor elke karakteristiek $p > 0$ komen beide gevallen voor.* □

**Opmerking.** We zien dat $E(K)[n]$ een ondergroep is van $E(K')[n]$ voor $K \subset K'$. In veel gevallen is het moeilijk om de structuur van $E(K)[n]$ te bepalen, alhoewel we al weten dat het een ondergroep is van een groep $E(k)[n]$ die we goed kennen; zie (5.3).

**Opmerking.** Als $k \subset L$ een inclusie van lichamen, met $k$ algebraïsch afgesloten, en $E$ is een elliptische kromme over $k$ dan is de inclusie $\mathrm{Tors}(E(k)) \subset \mathrm{Tors}(E(L))$ een gelijkheid. (Geef een bewijs.)

**(5.4) Vraagstuk.** Gebruik (4.4). Bewijs (5.3)(1) voor elke elliptische kromme over een lichaam $k$ van karakteristiek nul.

**(5.5) Vraagstuk.** Zij $E$ een elliptische kromme gegeven door door (14.2) = (W2) over een lichaam $K$; in het bijzonder is $\infty = [0 : 1 : 0]$ een buigpunt van $E$, en dat punt is als 0 voor de optelling op $E$ gebruikt. Hoe kunnen we punten van orde precies 2 op $E$ karakteriseren? Bewijs (5.3) voor het geval $n = 2 = 2^1$. (Pas op: in dit vraagstuk is er geen restrictie op de karakteristiek van $K$.)

**(5.6) Vraagstuk.** Zij $E \subset \mathbb{P}^2_{\mathbb{Q}}$ gegeven door $Y^2 + XY = X^3 + 4X^2 + X$ met $K = \mathbb{Q}$ als grondlichaam. Bewijs dat dit een elliptische kromme is. Bepaal $E(K)[2]$.
(Opmerking. We zien een 2-torsie punt met niet-gehele coördinaten.)

**(5.7) Vraagstuk. Karakteristiek $p = 2$.** In deze opgave is $k = \overline{\mathbb{F}_2}$.
**(1)** Zij $E$ de kromme over $\mathbb{F}_2$ gegeven door $E := \mathcal{Z}(Y^2+Y+X^3)$. Bewijs dat $E$ een elliptische kromme is. Is er een element van orde precies gelijk aan 64 in $E(k)$? Bereken $\#(E(\mathbb{F}_{32}))$.
**(2)** Zij $E'$ de kromme over $\mathbb{F}_2$ gegeven door $E' := \mathcal{Z}(Y^2 + XY + X^3 + X)$. Bewijs dat $E'$ een elliptische kromme is. Vind een punt van orde gelijk aan 4 in $E'(k)$

**(5.8) Definitie.** Voor een polynoom $f \in K[X, Y, Z]$ schrijven we

$$\mathrm{Hes}(f) := \begin{pmatrix} f_{XX} & f_{XY} & f_{XZ} \\ f_{YX} & f_{YY} & f_{YZ} \\ f_{ZX} & f_{ZY} & f_{ZZ} \end{pmatrix};$$

dit heet *de Hessiaan* van $f$; we schrijven $f_{XY}$ voor $(d/dY)((d/dX)(f))$, etc. Let wel dit zijn "formele afgeleiden", in de zin dat $(d/dX)(AX^m) := mAX^{m-1}$, waar $A$ niet de variabele $X$ bevat.

Merk op: als $f$ homogeen is van graad $m$, dan is $\mathrm{Hes}(f)$ homogeen van graad $3(m-2)$ of $\mathrm{Hes}(f) = 0$. (Dit kan voorkomen als de karakteristiek kleiner is dan de graad van $f$. Geef een voorbeeld.)

**(5.9) Definitie.** Zij $C \subset \mathbb{P}^2_K$ een vlakke algebraïsche kromme. Een punt $P \in C(k)$ heet een *buigpunt* van die kromme als $P$ niet-singulier is op $C$ en de raaklijn snijdt $C$ in $P$ met multipliciteit precies gelijk aan 3.

Een raaklijn in een niet-singulier punt van een kromme snijdt die kromme met multipliciteit $\geq 2$ en "in het algemeen" snijdt de raaklijn die kromme met multipliciteit 2.

Het kan voorkomen dat de raaklijn met multipliciteit $> 3$ snijdt; we spreken dan van een hyper-buigpunt. Terzijde: de theorie van hyper-buigpunten van krommen van graad 4 is een fascinerend onderwerp.

Enkele voorbeelden. Het punt $P = (0, 0)$ op de affiene kromme $\mathcal{Z}(-Y^2 + X^2(X - 1))$ is niet een buigpunt (het is een singulier punt).

Het punt $P = (0, 0)$ op $\mathcal{Z}(-Y + aX^2 + X^3)$ is een buigpunt dan en slechts dan als $a = 0$.

Zij $K$ een lichaam van karakteristiek 3. Op de kromme $C := \mathcal{Z}(-Y^2 + X^3)$ is $P = (0, 0)$ singulier, en *alle andere punten zijn buigpunten* (laat dat zien: over $k = \overline{K}$ zijn er oneindig veel buigpunten op deze kromme).

**(5.10) Vraagstuk. Punten van orde 3.** Zij $E \subset \mathbb{P}^2_k$ een elliptische kromme waarin een buigpunt als de 0 voor de optelling gekozen is. Bewijs:
**(1)** $P \in E(k)$ is een buigpunt dan en slechts dan als $P \in E(k)[3]$.
**(2)** Als $P, Q \in E(k)$ verschillende buigpunten zijn, dan snijdt de lijn $L$ die door $P$ en door $Q$ gaat nog in een derde punt, en dat punt is ook een buigpunt.

(Pas op: in deze opgave is er geen restrictie op de karakteristiek van $K$.)

**(5.11) Vraagstuk. Punten van orde 3 over $\mathbb{R}$.** Zij $K$ een deellichaam van $\mathbb{R}$. Zij $E \subset \mathbb{P}^2_K$ een elliptische kromme waarin een buigpunt als de 0 voor de optelling gekozen is. Bewijs:

$$\#(E(K)[3]) = 1 \quad \text{of} \quad \#(E(K)[3]) = 3.$$

**Opmerking / algemener.*** Voor een elliptische kromme $E$ gedefinieerd over een lichaam $K$ van karakteristiek nul, en een priemgetal $p$ zodanig dat $E(K)[p] = E(k)[p]$ (d.w.z. alle punten van orde $p$ zijn al over $K$ gedefinieerd) geldt dat $\mathbb{Q}(\zeta_p) \subset K$; hier is $\zeta_n$ een primitieve $n$-de eenheidswortel. Ik ken niet een elementair bewijs voor $p > 3$. Voor $p = 2$ spreekt dit vanzelf: in dat geval is $\mathbb{Q}(\zeta_2) = \mathbb{Q}(-1) = \mathbb{Q}$. Voor $p = 3$ is er een elementair bewijs dat niet alle punten van orde 3 over $K$ gedefinieerd zijn als $K \subset \mathbb{R}$: dat is het vraagstuk.

**(5.12) Vraagstuk. Karakteristiek $p = 3$.** We werken over $k = \overline{\mathbb{F}_3}$.
**(1)** Zij $E := \mathcal{Z}(-Y^2Z + X^3 + XZ^2)$. Bepaal alle buigpunten van $E \subset \mathbb{P}^2_k$.
**(2)** Zij $E := \mathcal{Z}(-Y^2Z + X^3 + X^2Z + Z^3)$. Bepaal alle buigpunten van $E \subset \mathbb{P}^2_k$.
(Opmerking: deze opgave illustreert (5.3)(2).) (Pas op voor "verkeerde informatie" zoals toegelicht in (5.15).)

**(5.13) Vraagstuk. Punten van orde 3.** Zij $K$ een lichaam *van karakteristiek nul*, en zij $E \subset \mathbb{P}^2_K$ een elliptische kromme over $K$ gegeven door een homogeen polynoom $f \in K[X, Y, Z]$ van graad 3. Bewijs dat $P \in E(k)$ een buigpunt is op $E$ dan en slechts dan als $\mathrm{Hes}(f)(P) = 0$.

**(5.14) Opmerking.** Gebruikmakend van het resultaat van deze opgave kunnen we (5.3)(1) bewijzen voor $n = 3$ en $K \supset \mathbb{Q}$: we kunnen inzien dat $\mathrm{Hes}(f)$ transversaal snijdt in een buigpunt, en uit de stelling van Bezout volgt dan dat het aantal buigpunten gelijk is aan $\deg(f).\deg(\mathrm{Hes}(f)) = 3.3 = 9$; daaruit volgt de structuur van $E(k)[3]$.

In de vorige opgave zien we de conditie dat de karakteristiek van $K$ gelijk aan nul is. We kunnen, nog steeds in karakteristiek nul, deze opgave generaliseren (nog steeds in karakteristiek nul): voor een kromme $C = \mathcal{Z}(f)$ en $P \in C(k)$ met $\mathrm{Hes}(f)(P) = 0$ kunnen we concluderen dat $P$ singulier is op $C$ of dat $P$ een (hyper-)flex op $C$ is.

Echter, de conditie dat de karakteristiek gelijk aan nul is is essentiëel zoals blijkt uit de volgende opdracht.

**(5.15) Opdracht.** Zij $k = \overline{\mathbb{F}_2}$. We definiëren $g = XY^2 + YZ^2 + ZX^2$ en $C := \mathcal{Z}(g) \subset \mathbb{P}^2_k$ (het zal blijken een elliptische kromme te zijn). Bewijs:
**(1)** $C$ is niet-singulier.
**(2)** $\mathrm{Hes}(g) = 0$.
**(3)** De snijpunten $\mathcal{Z}(X) \cap C$ en $\mathcal{Z}(Y) \cap C$ en $\mathcal{Z}(Z) \cap C$ zijn niet buigpunten op $C$.
**(4)** Bewijs dat $C$ precies 9 buigpunten heeft. Bepaal over welk eindig lichaam die reeds gedefinieerd zijn.
(We zien dat de Hessiaan "verkeerde informatie" kan geven in positieve karakteristiek.)

**(5.16)** Algemeen geldt: Zij $g \in k[X, Y, Z]$ homogeen van graad $d \geq 2$, en $\mathrm{char}(k) = 0$ of $\mathrm{char}(k) > d$. Schrijf $C = \mathcal{Z}(g)$. Neem aan dat $P \in C(K)$ een niet-singulier punt is. Dan

geldt: óf een component van $C$ is bevat in $\mathcal{Z}(H)$, óf

$$i(C, \mathfrak{t}_{C,P}; P) = r \quad \Longleftrightarrow \quad i(C, \mathcal{Z}(\mathrm{Hes}(g)); P) = r - 2.$$

**(5.17)*Opmerking.** Welke groepen komen voor als de torsie-groep van een elliptische kromme over $\mathbb{Q}$? Dit is een lastig probleem. Het is volledig opgelost voor Mazur: er zijn precies 15 groepen $G$ zodanig dat er een $E$ over $\mathbb{Q}$ is met $G \cong \mathrm{Tors}(E(\mathbb{Q}))$. Zie [17], [11], p. 133. Een bewijs van deze stelling is een onderwerp dat (helaas !) te moeilijk is voor dit college; ook heb ik het gevoel dat ik die stelling van Mazur niet begrijp; het resultaat ken ik, het bewijs kan ik volgen, maar "waarom" is dit zo?

# 6 Elliptische krommen over een getallenlichaam

**(6.1)** Omdat we elliptische krommen willen gebruiken in getaltheorie is het nodig om elliptische krommen over lichamen te beschouwen die niet noodzakelijk algebraïsch afgesloten zijn (zoals getallen lichamen en eindige lichamen). Ook zullen we elliptische krommen over ringen gaan beschouwen. Bij voorbeeld zullen we informatie over de krommen gegeven door $Y^2 = X^3 + X$ gegeven over $\mathbb{Z}$, gaan vergelijken met einformatie over $\mathbb{Q}$, over $\mathbb{C}$, en over een eindig lichaam.

**(6.2) Opmerking.** Het komt voor dat twee vergelijkingen krommen over een lichaam $K$ geven, die niet isomorf zijn over $K$, maar die over over een uitbreiding $K \subset L$ wel isomorf zijn.
**Voorbeeld.** We geven $E_1$ over $\mathbb{Q}$ door $Y^2 = X^3 + 1$ en $E_2$ over $\mathbb{Q}$ door $2Y^2 = X^3 + 1$. Er is niet een coördinaten transformatie die een isomorfisme geeft tussen $E_1$ en $E_2$ over $\mathbb{Q}$. We zien bij voorbeeld dat $x = 0$ de punten $(0, +1) = [0 : 1 : 1]$, en $(0, -1) = [0 : -1 : 1]$ en $[0 : 1 : 0]$ geeft, en die punten zijn buigpunten van $E_1 \subset \mathbb{P}^2_{\mathbb{Q}}$, en de andere buigpunten zijn niet rationaal over $\mathbb{Q}$. Maar de kromme $E_2$ heeft behalve $[0 : 1 : 0]$ geen buigpunten rationaal over $\mathbb{Q}$. Beschouw $\mathbb{Q} \subset L := \mathbb{Q}(\sqrt{2})$. De substitutie $\eta = \sqrt{2} \cdot Y$ voert de vergelijking voor $E_2$ over $L$ over in die voor $E_1$. (In plaats van die coëfficiënt 2 kunnen we elk kwadraatvrij getal in $\mathbb{Z}_{>0}$ nemen, en het voorbeeld werkt ook).

**Voorbeeld.** We geven $E_1$ over $\mathbb{Q}$ door $Y^2 = X^3 + 1$ en $E_2$ over $\mathbb{Q}$ door $2Y^2 = X^3 - 1$. Laat zien dat $E_1$ en $E_2$ over $\mathbb{Q}$ niet isomorf zijn, maar over een geschikt gekozen uitbreiding van $\mathbb{Q}$ wel.

Voor elke $a \in \mathbb{Q} - \{0\}$ zijn de krommen gegeven door $Y^2 = X^3 + 1$, respectievelijk $Y^2 = X^3 + a$ isomorf over een geschikt gekozen uitbreidingslichaam van $\mathbb{Q}$.

Terzijde*. Als $E_1$ en $E_2$ elliptische krommen zijn over $K$ die isomorf zijn over $L \supset K$ dan zeggen we dat $E_2$ een $L/K$-vorm is van $E_1$. Voor algemene theorie, en een beschrijving van $L/K$-vormen zie bij voorbeeld [58], III.1.3.

**(6.3)** We "kennen" alle torsie-punten op een elliptische kromme over $\mathbb{C}$. Maar deze kennis is onvoldoende om te beslissen welke torsie-groepen kunnen optreden als we alle elliptische krommen over een gegeven lichaam beschouwen; dit is opgelost voor $K = \mathbb{Q}$ (Mazur), een diep en moeilijk te bewijzen resultaat; zie (5.17). Ook voor de volgende stelling is er niet een bewijs bekend dat alleen gebruik maakt van analytische methoden.

**(6.4) Stelling = Feit** (Mordell – Weil)*. *Zij $[K:\mathbb{Q}] < \infty$ en zij $E$ een elliptische kromme over $K$. Dan is $E(K)$ een eindig voortgebrachte abelse groep.*
Dit impliceert: $\mathrm{Tors}(E(K))$ is een eindige groep, en er is een getal $n \in \mathbb{Z}_{\geq 0}$ en een isomorfisme

$$E(K) \quad \cong \quad \mathbb{Z}^n \times \mathrm{Tors}(E(K)).$$

□

Op het college zal ik niet een bewijs geven. Deze stelling werd eerst dor Mordell bewezen met $K = \mathbb{Q}$; zie (17.5). André Weil generaliseerde dit (in zijn proefschrift) voor abelse variëteiten over een getallenlichaam.

Het getal $n$ zoals hier boven wordt de *rang* van $E$ over $K$ genoemd.

# 7 Elliptische krommen over een ring

**(7.1)** We werken over een ring $R$ (commutatief, met $1 \in R$). We beschouwen de projectieve ruimte $\mathbb{P}^2_R$ over $R$ (op college wordt uitgelegd wat we hier precies mee bedoelen). Beschouw een vergelijking in de vorm (14.2). Beschouw $\mathcal{E} \subset \mathbb{P}^2_R$. In het bijzonder is voor elk ringhomomorfisme $\varphi : R \to K$ de kromme $\mathcal{E}_K$ over $K$ gegeven door die vergelijking nadat $\varphi$ toegepast is op de coëfficiënten.

**(7.2) Belangrijke opmerking / voorbeeld.** We werken over een ring $R$, denk bv. aan $R = \mathbb{Z}$, en een lichaam $K$ dat $R$ bevat, denk bv. aan $K = \mathbb{Q}$. Algemener: een domein $R$ (commutatieve ring met 1 zonder nuldelers) en het breukenlichaam $K = \mathrm{Frac}(R)$. Veronderstel dat $\mathcal{E}^0$ gegeven wordt door een (affiene) vergelijking zoals gegeven in § 14. Veronderstel dat de discriminant van die vergelijking niet nul is. Dan geeft die vergelijking over $K$ een elliptische kromme $E^0 \subset E$. Echter (!!) de notatie $E^0(R)$ is in het algemeen niet zinvol.

Hier is een eenvoudig voorbeeld, $R = \mathbb{Z}$, en $K = \mathbb{Q}$. De vergelijkingen $Y^2 + Y = X^3 - X$ en $V^2 + 8V = U^3 - 16{\cdot}U$ zijn verschillend en niet in elkaar over te voeren met een inverteerbare transformatie over $\mathbb{Z}$ (want reductie modulo 2 geeft verschillende vergelijkingen, waarvan de ene een singuliere en de andere een niet-singuliere kromme definieert); we krijgen $\mathcal{E}^0_1$ en $\mathcal{E}^0_2$. De vergelijkingen geven over $\mathbb{Q}$ isomorfe krommen onder de transformatie $U = 4X$ en $V = 8Y$ (ga na); noem die affiene kromme $E^0$. We zien dat $(1/4, -5/8) \in E^0(\mathbb{Q})$. Is de schrijfwijze $E(\mathbb{Z})$ zinvol? NEE, want $(u = 1, v = -5) \in \mathcal{E}_2(\mathbb{Z})$ aan de ene kant, maar aan de andere kant correspondeert dit punt niet met een keuze $(x, y) \in \mathbb{Z}^2$ die een punt in $\mathcal{E}_1(\mathbb{Z})$ geeft. In dit voorbeeld zien we:

$$\mathcal{E}^0_1(\mathbb{Z}) \subsetneqq \mathcal{E}^0_2(\mathbb{Z}) \subset E^0(\mathbb{Q}).$$

Ga na: als we een elliptische kromme $E$ hebben over $\mathbb{Q}$ dan is er voor elk punt $P = (x, y) \in E^0(\mathbb{Q})$ een vergelijking voor $E^0$ met coëfficienten in $\mathbb{Z}$ zodanig dat die vergelijking $\mathcal{E}^0$ definieert, zodanig dat het punt $P$ komt van een punt in $\mathcal{E}^0(\mathbb{Z})$ (maar voor een ander punt hebben we misschien wel weer een andere vergelijking nodig).

Dit verschijnsel treedt op voor elke kromme $E$ over $\mathbb{Q}$ met positieve rang (want een dergelijke kromme heeft voor elke vergelijking die de kromme definieert punten waarvan de coördinaten niet geheel zijn). Kun je dat inzien/bewijzen? We zien:

$$E^0(\mathbb{Q}) = \cup_{\mathcal{E}}\ \mathcal{E}^0(\mathbb{Z}),$$

de vereniging genomen over alle vergelijkingen die deze kromme $E^0$ over $\mathbb{Q}$ definiëren.

**(7.3) Stelling** (Nagell-Lutz). *Zij $K = \mathbb{Q}$ en zij $E$ een elliptische kromme gegeven door $Y^2 = X^3 + AX + B$ met $A, B \in \mathbb{Z}$.* We schrijven $D := -4A^3 - 27B^2$ (de discriminant van $X^3 + AX + B$). *Zij $P = (x, y) \in \mathrm{Tors}(E(\mathbb{Q}))$. Dan geldt:*
**(a)** *$x, y \in \mathbb{Z}$. Bovendien:*
**(b)** *óf $y = 0$ (een 2-torsiepunt) óf $y^2$ deelt $D$.*
Zie [11], Th. 5.1; [29], Coroll. 7.2; [31], II.5. □
De naam Nagell wordt ook wel als Nagel gespeld.
In deze stelling gebruiken we $K = \mathbb{Q}$, en gebruiken we dat de kromme door de vergelijking (14.1) gegeven wordt. Beide condities zijn nodig.
**Waarschuwing.** De vergelijking die $E$ geeft in de stelling speelt een rol in de formulering. In (5.6) zien we een 2-torsiepunt met niet gehele coördinaten op een kromme gegeven door een vergelijking van de vorm (14.2).
**Waarschuwing.** In deze stelling zien we dat het feit dat $P$ een torsie-punt is impliceert dat de coördinaten, onder de goede voorwaarden, geheel zijn. Maar de omkering geldt niet; er zijn veel voorbeelden van een $P \in \mathcal{E}(\mathbb{Q})$ met gehele coördinaten, terwijl $P$ niet eindige orde heeft. Zoek zelf veel voorbeelden.

**(7.4) Vraagstuk.** (Hierin mag (7.3) gebruikt worden.) Bepaal $\mathrm{Tors}(E(\mathbb{Q}))$ waar $E$ gegeven is door $Y^2 = X^3 - X$.

**(7.5) Vraagstuk.** Geef $E$ over $\mathbb{Q}$ door middel van de vergelijking $Y^2 + Y = X^3 - X$. We zien dat $P := (0, 0) \in E(\mathbb{Q})$.
**(1)** Bepaal $\mathrm{Tors}(E(\mathbb{Q}))$.
**(2)** Bepaal $iP$ voor alle $1 < i \leq 8$. Bepaal de orde van $P$ (en bewijs de juistheid van het antwoord).
**(3)** Bepaal $p$ zodanig dat $Y^2 + Y = X^3 - X$ een singuliere kromme geeft over $\mathbb{F}_p$.

**(7.6) Vraagstuk.** Geef $E$ over $\mathbb{Q}$ door

$$Y^2 = 4X^3 - 4X + 1.$$

We zien $P := (0, 1) \in E(\mathbb{Q})$. Bepaal $iP$ voor alle $1 < i \leq 8$ Bepaal de orde van $P$ (en bewijs de juistheid van het antwoord).

Een ander lichaam dan $\mathbb{Q}$ zien we in de volgende twee vraagstukken.

**(7.7) Vraagstuk.** Zij $E$ over $\mathbb{Q}$, en $\mathcal{E}$ over $\mathbb{Z}$, gegeven door $Y^2 = X^3 + 1$. Bepaal een lichaam $K \supset \mathbb{Q}$ zodanig dat $E(K)$ alle buigpunten van $E$ bevat. Laat zien dat die buigpunten coördinaten hebben in $\mathcal{O}_K$ (de ring van gehelen van $K$).

**(7.8) Vraagstuk.** Zij $E$ over $\mathbb{Q}$, en $\mathcal{E}$ over $\mathbb{Z}$, gegeven door $Y^2 = X^3 + X$. Bewijs dat er een $K$ bestaat met $[K : \mathbb{Q}] < \infty$ zodanig dat $E(K)$ alle buigpunten van $E$ bevat. Bewijs dat voor een dergelijke keuze er een buigpunt $P = (x, y) \in E(K)$ bestaat waar $x \notin \mathcal{O}_K$.

**(7.9) Opmerking.** Het verschil in gedrag van 3-torsie t.a.v. het al of niet geheel zijn van coördinaten in de vorige twee vraagstukken kan begrepen en verklaard worden met behulp van "reductie modulo $p$, in dit geval $p = 3$". Merk op dat $Y^2 = X^3 + 1$ over een lichaam

van karakteristiek 3 een singuliere kromme geeft, en $Y^2 = X^3 + X$ over een lichaam van karakteristiek 3 een niet-singuliere kromme geeft.

**(7.10) Opmerking.** We kunnen bewijzen: voor elke $[K : \mathbb{Q}] < \infty$ en elke elliptische kromme $E$ over $K$ gegeven door een verglijking (14.1) met $A$ en $B$ in de ring van gehelen van $K$, dan bestaat er een priemgetal $p$ en een uitbreiding $[L : K] < \infty$ zodanig dat er een $p$-torsie punt in $E(L)$ is waarvan de coördinaten niet gelegen zijn in $\mathcal{O}_L$. (M.a.w. de eis $K = L = \mathbb{Q}$ in (7.3) is essentieel.)

**(7.11) Opmerking.** Voor elke elliptische kromme $E$ over $\mathbb{Q}$ is het berekenen van $\mathrm{Tors}(E(\mathbb{Q}))$ effectief: breng door middel van een coördinaten-transformatie een vergelijking voor de kromme in de vorm (W1), en pas (7.3) toe. Maak voorbeelden.

**(7.12) Definitie.** Zij $R$ een ring, en $a, b \in R$. We definiëren een *Frey kromme* als:

$$E_{a,b}: \quad Y^2 = X(X - a)(X + b).$$

Deze krommen werden geïntroduceerd door Gerhard Frey. Deze definitie was van belang voor FLT-Ribet-Wiles. Zie [8].

**(7.13) Vraagstuk. (1)** Bewijs dat elke elliptische kromme over $\mathbb{C}$ isomorf is met een Frey kromme.
**(2)** Zij een elliptische kromme $E$ gegeven over $\mathbb{Q}$ door de vergelijking $Y^2 = X(X-(1/5))(X-5^2)$. Is $E$ over $\mathbb{Q}$ isomorf met een Frey kromme? (N.B. met $a, b \in \mathbb{Z}$.)

We gaan nu de opmerking (7.2) beschouwen voor projectieve krommen. We werken over de basis-ring $R = \mathbb{Z}$, met breukenlichaam $K = \mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$. Deze resultaten kunnen we eenvoudig generaliseren onder de conditie dat in het domein $R$ eenduidige factor-ontbinding heerst.

**(7.14) Lemma/ Notatie.** *Zij $E$ een elliptische kromme over $\mathbb{Q}$ gegeven door een van de vergelijkingen in § 14. Schrijf $g$ voor het homogene polynoom in de variabelen $X, Y, Z$, verkregen door de vergelijking homogeen van graad 3 te maken. We schrijven $\mathcal{E} \subset \mathbb{P}^2_{\mathbb{Z}}$ voor de nulpunten van dit polynoom. Zij $P \in E(\mathbb{Q})$. Dan is er een unieke schrijfwijze $P = [x : y : z]$ met $x, y, z \in \mathbb{Z}$, en $\gcd(x, y, z) = 1$ en $[x : y : z] \in \mathcal{E}(\mathbb{Z})$. Als $P = [x' : y' : z']$ met dezelfde eigenschappen dan is $x' = \epsilon x$, $y' = \epsilon y$ en $z' = \epsilon z$ met $\epsilon = \pm 1$.* □

**(7.15) Opmerking / waarschuwing.** Bij een gegeven vergelijking voor $E$ (lees: bij een keuze van het coördinaten-systeem) en bij een keuze van een priemgetal $p$, en daardoor een ring homomorfisme $\mathbb{Z} \to \mathbb{Z}/p = \mathbb{F}_p$ krijgen we een afbeelding

$$\rho : E(\mathbb{Q}) \longrightarrow (\mathcal{E} \bmod p)(\mathbb{F}_p).$$

In die constructie gebruiken weer de vergelijking die $\mathcal{E}$ definieert. We laten zien dat het eindresultaat in het algemeen van die keuze afhangt: $E$ over $\mathbb{Q}$ gegeven door $Y^2 = X^3 + 1$ en $P_1 = (2, 3) \in E(\mathbb{Q})$; die vergelijking definieert $\mathcal{E}_1$. De transformatie $U = 4X$, $V = 8Y$ voert $V^2 = U^3 + 64$ na delen door 64 over in de eerste vergelijking; die tweede vergelijking definieert $\mathcal{E}_2$; het punt $P_2 = (u = 8, v = 24) \in \mathcal{E}_2(\mathbb{Q})$ correspondeert onder die transformatie

met $P_1 \in \mathcal{E}_1$. Reductie van $\mathcal{E}_1$ modulo twee geeft het punt $\rho(P_1) = (0,1) = [0:1:1]$ op de kromme over $\mathbb{F}_2$ gegeven door $Y^2 = X^3 + 1$. Reductie van $\mathcal{E}_2$ modulo twee geeft het punt $\rho(P_2) = (0,0) = [0:0:1]$ op de kromme over $\mathbb{F}_2$ gegeven door $V^2 = U^3$. We zien dat $\rho(-)$ in dit geval afhangt van de keuze van het model $\mathcal{E}_?$.

**(7.16) Stelling / Feit.**$^*$ *Zij $E$ over $\mathbb{Q}$ en $\mathcal{E}$ over $\mathbb{Z}$ gegeven door een vergelijking $g = 0$ met coëfficienten in $\mathbb{Z}$ zoals in* (14.2). *Zij $p$ een priemgetal zodanig dat de vergelijking $(g \bmod p) = 0$ een elliptische kromme $E_0$ definieert over $\mathbb{F}_p$. Schrijf*

$$\rho_p = \rho : E(\mathbb{Q}) \longrightarrow E_0(\mathbb{F}_p)$$

*voor de reductie-modulo-$p$ afbeelding. Veronderstel $p > 2$. Dan is de afbeelding*

$$\rho : \mathrm{Tors}(E(\mathbb{Q})) \hookrightarrow \mathcal{E}_0(\mathbb{F}_p)$$

*een injectief homomorfisme.*
Zie [31], page 123; [11], Th. 5.1 op pag. 130, en Prop. 5.6 op pag. 137; [29], prop. 3.1 op pag. 176. □

**(7.17) Opmerkingen.** De condities "$E_0$ is een elliptische kromme" en "$p > 2$ " en "beperken tot torsie" zijn essentieel.

Als $E(\mathbb{Q})$ niet eindig is, d.w.z. de rang van $E/\mathbb{Q}$ is positief, dan is $\rho : E(\mathbb{Q}) \to \mathcal{E}_0(\mathbb{F}_p)$ niet injectief (allicht niet). Maak voorbeelden.
**Voorbeeld.** Stel $\mathcal{E}$ is gegeven door $Y^2 = X^3 - 9X$. De kromme ($\mathcal{E}$ mod 3) is singulier en de reductie afbeelding op $E(\mathbb{Q})[2] \to \mathcal{E}(\mathbb{F}_3)$ is niet injectief. Maak zelf nog veel meer voorbeelden.
**Voorbeeld.** De afbeelding "reductie modulo 5" is *wel injectief* op $E(\mathbb{Q})[5] \cong \mathbb{Z}/5$ voor $E$ gegeven door $Y^2 + Y = X^3 - X^2$ (ga na !).
**Voorbeeld.** Zie Vraagstuk (5.6). Zij $E$ gegeven door $Y^2 + XY = X^3 + 4X^2 + X$ over $\mathbb{Z} \subset \mathbb{Q}$. Neem $p = 2$. Bewijs dat $E_0 := \mathcal{E} \bmod 2$ niet-singulier is, maar dat de afbeelding $\rho_2 : E(\mathbb{Q}) \to E_0(\mathbb{F}_2)$ niet injectief is.

**(7.18) Opmerking.** Kunnen we $p = 2$, en kunnen we basis-ringen anders dan $\mathbb{Z}$ ook in de beschouwingen betrekken? Hier is een algemenere situatie:

$$\kappa \xleftarrow{\varphi} R \subset K,$$

waar $R$ een domein is met eenduidige factor-ontbinding, en een $\mathcal{E}$ over $R$ gegeven is zodat $E_0 := (\mathcal{E} \bmod \varphi)$ een elliptische kromme is (en daarom ook $E := (\mathcal{E} \otimes K)$ een elliptische kromme). Zij $p$ de karakteristiek van $\kappa$. Dan is

$$\rho_\varphi = \rho : \mathrm{Tors}(E(K))^{(p)} \hookrightarrow E_0(\kappa)$$

injectief. Hier is $\mathrm{Tors}(E(K))^{(p)}$ de priem-met-$p$ torsie; dat is de grootste ondergroep van $\mathrm{Tors}(E(K))$ waarvan de orde niet deelbaar is door $p$. (Merk op dat in een abelse groep $A$ de deelverzameling $A^{(p)}$ van elementen met eindige orde die niet deelbaar is door $p$ een ondergroep is.) Voor elke $p$ kunnen we voorbeelden maken waar een dergelijke $\rho_\varphi$ niet injectief is op $\mathrm{Tors}(E(K))$.

**(7.19) Vraagstuk.** Geef $E$ over $K = \mathbb{Q}$ en $\mathcal{E}$ over $\mathbb{Z}$ door $Y^2 = X^3 + X$. Bepaal de structuur van $\mathcal{E}(\mathbb{F}_3)$, van $\mathcal{E}(\mathbb{F}_5)$ en geef een volledige beschrijving van $\mathrm{Tors}(E(\mathbb{Q}))$. Hier mag (7.16) gebruikt worden.

**(7.20) Opmerking.** Stelling (7.16), en de variant (7.18) daarvan, is van groot nut. We kunnen torsie op een elliptische kromme $E$ over $\mathbb{Q}$ begrenzen, en daardoor vaak effectief uitrekenen, door een goede reductie $E_0$ over een eindig lichaam $\mathbb{F}_p$ te beschouwen en $E_0(\mathbb{F}_p)$ te berekenen, of door $\#(E_0(\mathbb{F}_p))$ te begrenzen. Hier zijn **voorbeelden** (in alle voorbeelden geldt $R = \mathbb{Z} \subset K = \mathbb{Q}$):
**(1)** $E$ gegeven door $Y^2 + Y = X^3 - X$; dan is en $\mathrm{Tors}(E(\mathbb{Q})) = 0$.

Gebruik eerst reductie bij $p = 3$; omdat $\#(\mathcal{E}(\mathbb{F}_3)) = 7$ en $p = 3$ een priem van goede reductie is zien we dat $\#(\mathrm{Tors}(E(\mathbb{Q})))$ een deler van 7 is, en dus oneven is. Merk op dat $p = 2$ een priem van goede reductie is en dat $\#(\mathcal{E}(\mathbb{F}_2)) = 5$. Uit (7.18) volgt $\mathrm{Tors}(E(\mathbb{Q})) = 0$. Zie [32], p. 202.
**(2)** Voor elke kwadraatvrije $N \in \mathbb{Z}_{>0}$ geven we $E = E_N$ door $Y^2 = X(X^2 - N^2)$. Dan geldt $\mathrm{Tors}(E(\mathbb{Q})) = (\mathbb{Z}/2)^2$ voor elke $N$, zie (9.5). Zie [12], I.9, Prop. 17 op pag. 44 voor een bewijs, waar reductie modulo priemgetallen gebruikt wordt. Dit speelt een belangrijke rol bij het probleem van de congruente getallen. Zie ook (7.4), (16.4) .
**(3)** Zie [31], pag. 124:
**(3a)**

$$Y^2 = X^3 + 3, \quad p = 5,\ p = 7: \quad \mathrm{Tors}(E(\mathbb{Q})) = 0;$$

**(3b)**

$$Y^2 = X^3 + X; \quad \text{zie (7.19)};$$

**(3c)**

$$Y^2 = X^3 - 43X + 166;$$

gebruik (7.3), vind een punt $P$ in $E(\mathbb{Q})$; vind andere punten door verdubbeling; bepaal wat de orde van $P$ is; bepaal de structuur van $\mathcal{E}(\mathbb{F}_3)$; bepaal de structuur van $\mathrm{Tors}(E(\mathbb{Q}))$. Zie ook (15.5).
**(4)** Zie [11], Ch. V voor veel voorbeelden.
**(5)** Zie [29], pp. 176 – 178. (Vind een drukfout op pag. 178.)

**(7.21) Voorbeeld / Opdracht.** Zij $\mathcal{E}$ over $\mathbb{Z} \subset \mathbb{Q}$ gegeven door

$$Y^2 - 7XY - 36Y = X^3 - 18X^2.$$

**(1)** Bewijs dat voor $p = 5$ de kromme ($\mathcal{E}$ mod 5) niet singulier is.
**(2)** Bepaal de orde van en de structuur van de groep $\mathcal{E}(\mathbb{F}_5)$.
**(3)** Merk op: $P = (0, 0) \in E(\mathbb{Q})$. Geef de coördinaten van alle punten in $\mathrm{Tors}(E(\mathbb{Q}))$ en bepaal de structuur van deze groep.

**(7.22)*Goede en slechte reductie.** Zie ook (15.10). Beschouw de situatie:

$$\kappa \xleftarrow{\varphi} R \subset \mathrm{Frac}(R) = K.$$

Denk b.v. aan $R = \mathbb{Z}$ en $\kappa = \mathbb{Z}/p$. Zij $E$ een elliptische kromme over $K$. We zeggen dat $E$ *goede reductie* heeft bij $\varphi$ als er een Weierstrass vergelijking is over $R$ die $\mathcal{E}$ over $R$, die over $K$ de kromme $E$ geeft zodanig dat $\mathcal{E} \otimes \varphi$ een niet-singuliere (elliptische) kromme definieert.

Merk op dat er meerdere vergelijkingen over $K$ bestaan voor dezelfde elliptische kromme $E$, waarvan het voor kan komen dat de ene wel en de andere niet een goede reductie bij $\varphi$ geeft.

We zeggen dat $E$ *slechte reductie* heeft bij $\varphi$ als het niet goede reductie heeft bij $\varphi$. We zeggen bovendien dat $E$ *erg slechte reductie* heeft bij $\varphi$ als elke Weierstrass vergelijking over $R$, die over $K$ de kromme $E$ geeft, de reductie bij $\varphi$ een singuliere kromme definieert die niet een dubbelpunt heeft (maar en keerpunt).

**Voorbeeld.** Zij $p > 2$, met $\kappa = \mathbb{Z}/p = \mathbb{F}_p$, en laat $E$ over $\mathbb{Q}$ gegeven zijn door $Y^2 = X^3 - p^m X$. Merk op: als $m$ deelbaar is door 4 dan heeft $E$ goede reductie bij $p$. We kunnen laten zien dat in alle andere gevallen de reductie erg slecht is. We kunnen eenvoudig laten zien dat er een eindige uitbreiding $K = \mathbb{Q} \subset L$ en een priem $v$ die $p$ deelt, zodat $E \otimes L$ goede reductie heeft bij $v$. We zeggen in dit geval dat $E/\mathbb{Q}$ "potentieel goede reductie bij $p$ heeft".

Het onderwerp van goede/slechte reductie is prachtig! maar valt grotendeels buiten ons kader.

# 8 Elliptische krommen, over een eindig lichaam

Allicht: voor een elliptische kromme $E$ over een eindig lichaam $\kappa = \mathbb{F}_q$ is de groep $E(\kappa)$ een eindige groep. Ook is het gemakkelijk om een (veel te slordige) afschatting van de orde van die groep te geven: omdat $E(\kappa) \subset \mathbb{P}^2(\kappa)$ krijgen we $\#(E(\kappa)) \leq q^2 + q + 1$ (allicht). Is er een betere grens? Wat is de structuur van die groep?

We kunnen natuurlijk die grens verbeteren: er is een $2:1$ overdekking $E \to \mathbb{P}^1$, en we zien dat $\#(E(\kappa)) < 2(q+1)$. Dat kunnen we nog verder verbeteren, zie (8.4).

Een mooi/lastig probleem dat veelvuldig bestudeerd is: geef een Weierstrass vergelijking over $\mathbb{Z}$; wat is de structuur van $\mathcal{E}$ mod $p$ voor elke $p$ die de discriminant niet deelt? Kun je daar iets over zeggen in die algemeenheid? Of in bijzondere gevallen?

We brengen in herinnering (alhoewel we dat niet bewezen hebben): als $q = p^n$ en $m \in \mathbb{Z}_{>1}$ niet deelbaar door $p$, dan is $E(\mathbb{F})[m] \cong (\mathbb{Z}/m)^2$, zie (5.3); hier is $\mathbb{F} := \overline{\mathbb{F}_p}$. Fascinerend (opgelost) probleem: bepaal hoeveel $j$-waarden er zijn voor een gegeven $p$ van elliptische krommen $E$ met $E(\mathbb{F})[p] = 0$ ("supersinguliere elliptische krommen").

Een feit: voor een elliptische kromme $E$ over $\kappa \supset \mathbb{F}_p$ geldt óf $E(\kappa)[p] \cong \mathbb{Z}/p$ óf $E(\kappa)[p] = 0$. Zie (5.3). Beide gevallen komen voor in elke karakteristiek.

**(8.1) Opmerking.** Zie (15.12). We kunnen vrij eenvoudig inzien: als de karakteristiek van het grondlichaam gelijk aan 2 is, dan geldt:

$$E(k)[2] = 0 \iff j(E) = 0.$$

In dit geval kan $E \otimes \overline{\mathbb{F}_2}$ gegeven worden door $Y^2 + Y = X^3$.

**(8.2) Een voorbeeld.** Is er een elliptische kromme $E$ over $k := \overline{\mathbb{F}_3}$ met $E(k)[3] = \{0\}$? We beweren dat de kromme gegeven door $Y^2 = X^3 - X$ deze eigenschap heeft: *er zijn geen punten op $E$ van precies orde gelijk aan* 3. We laten dit zien;

$$(\partial/\partial X)(-Y^2 + X^3 - X) = -1$$

(want we werken in karakteristiek 3) en we zien dat deze kromme niet-singulier is. Uit (5.3) weten we dat óf $E(k)[3] = \{0\}$ óf $E(k)[3] = \mathbb{Z}/3$; we nemen aan dat er torsie-punten van orde drie zouden zijn, en we gaan komen tot een tegenspraak.

Zij $\beta \in k := \overline{\mathbb{F}_3}$ met $\beta^2 = -1$ (ik noem dat niet $i$, want $i$ is een complex getal en $3i \neq 0$) (terzijde: $\mathbb{F}_2(\beta) \cong \mathbb{F}_9$). We geven een automorfisme $\varphi$ van $E(k)$ door:

$$x \mapsto -x, \quad y \mapsto \beta{\cdot}y; \quad \varphi^2 \neq \mathrm{id.}, \quad \varphi^4 = \mathrm{id.}$$

(ga na dat dit goed gedefinieerd is; merk op dat $\varphi^2(P) = -P$ voor alle $P$). Als zou gelden $E(k)[3] = \mathbb{Z}/3$, dan werkt $< \varphi >= \mathbb{Z}/4$ op $\mathbb{Z}/3 - \{0\}$, een verzameling met twee elementen; dus is de werking van $\varphi^2$ op deze punten triviaal; conclusie: als er een punt van precies orde drie is, dan is het een dekpunt van $\varphi^2$. Echter we zien dat de dekpunten van $\varphi^2$ precies die punten in $E[2]$. Tegenspraak. Conclusie: in dit geval zijn er geen punten van precies orde drie.

Terzijde: voor $p = 3$ is elke kromme die geen punten van orde drie heeft, over $k$ isomorf met de bovengegeven kromme. Voor meer informatie over "supersinguliere kromme" zie bijvoorbeeld [53], IV.4.

**(8.3) Vraagstuk.** Laat zien dat $p := 149$ een priemgetal is. We schrijven $K = \mathbb{F}_{149}$ en $k = \overline{\mathbb{F}_{149}}$. Over $K$ geven we $E$ door $Y^2 = X^3 - 1$. Bewijs dat $E$ een elliptische kromme is. Bewijs dat $E(k)[149] = 0$. [Feiten in deze syllabus gegeven kunnen gebruikt woden.]

**(8.4) Feit / Stelling**$^*$ (Hasse). Voor een elliptische kromme $E$ over een eindig lichaam $\kappa = \mathbb{F}_q$ geldt:

$$| \,\#\,(E(\mathbb{F}_q)) - q - 1\, | \leq 2\sqrt{q}.$$

De grens in deze stelling wordt wel de Hasse – Weil grens genoemd. Lees vooral pp. 107 – 110 van [31]. Zie b.v. [29], V.1, Th. 1.1. □

Dit is een (klein) onderdeel van de Weil vermoedens (een prachtig onderwerp, ver buiten het bereik van deze activiteit).

Grenzen voor $\#\,(C(\mathbb{F}_q))$ voor een kromme van hoger geslacht zijn interessant voor cryptografie. Daar is er veel werk verricht.

# 9 Congruente getallen.

Voor verwijzingen, definities en voorbeelden zie: [36], [37]. Bekend verondersteld: de definitie van een Pythagoreïsche drietal, de classificatie daarvan, en de bijbehorende bewijzen. Lees vooral over dit klassieke, elementaire en fascinerende materiaal.

**(9.1) Definitie.** Een getal $N \in \mathbb{Z}_{>0}$ heet een *congruent getal* (afgekort CG) als er $\alpha, \beta, \gamma \in \mathbb{Q}$ bestaan zodanig dat:

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

In woorden: als er een rechthoekige driehoek bestaat, waarvan de zijden een rationale lengte hebben en de oppervlakte gelijk is aan $N$.

**(9.2) Vraagstuk.** Bewijs dat deze definitie equivalent is met:
Een getal $N \in \mathbb{Z}_{>0}$ is een *congruent getal* dan en slechts dan als er een $\delta \in \mathbb{Q}$ bestaat zodanig dat

$$\delta^2 - N, \quad \delta^2, \quad \delta^2 + N$$

kwadraten in $\mathbb{Q}$ zijn.

**(9.3) Een voorbeeld.**

$$N = 5, \quad \alpha = \frac{9}{6}, \quad \beta = \frac{40}{6}, \quad \gamma = \frac{41}{6}, \quad \delta = \frac{41}{12}.$$

Laat zien dat deze getallen voldoen aan beide definities.

**(9.4) Definitie.** Een getal $N \in \mathbb{Z}_{>0}$ heet *kwadraatvrij* als er niet een $d \in \mathbb{Z}_{>1}$ bestaat zo dat $d^2$ een deler is van $N$. Equivalent: voor elk priemgetal $p$ is $p^2$ niet een deler van $N$.

**(9.5) Feit.*** Zij $N$ een kwadraatvrij getal. Over $K = \mathbb{Q}$ geven we $E_N$ door $Y^2 = X(X - N)(X + N)$. Dan geldt:

$$\mathrm{Tors}(E(\mathbb{Q})) = \{\infty, (0,0), (N,0), (-N,0)\} \cong (\mathbb{Z}/2)^2.$$

Een bewijs is te vinden: [12], I.9, Prop.17 op pag. 44. Voor $N = 1$ zie (7.4). Een speciaal geval, $N$ is een priemgetal, bewijzen we in (16.4).

# 10 Het Poncelet probleem

In 1822 publiceerde J.-V. Poncelet een stelling, die nog steeds in het centrum van de belangstelling staat. Voor een historische inleiding, een bewijs, en nog veel meer zie [1]; zie ook vele verwijzingen in dat artikel. Zie ook [6]. We geven hier wat notaties, en een moderne formulering van de stelling.

N.B. In deze paragraaf werken we over $K = k = \mathbb{C}$, tenzij anders vermeld

**(10.1)** Een *kwadriek* is de nulpuntenverzameling $\mathcal{Z}(g) \subset \mathbb{P}^n_K$ van een homogeen polynoom van de graad 2. Voor het geval $n = 2$, een vlakke kwadriek, spreken we van een *kegelsnede*. Een singuliere kegelsnede heet een "ontaarde kegelsnede". Over $k$ zijn kegelsneden gemakkelijk te classificeren.
(1) Als $C_1, C_2 \subset \mathbb{P}^2_k$ kegelsneden zijn die beide niet ontaard zijn, dan is er een projectieve transformatie van $\mathbb{P}^2_k$ die $C_1$ in $C_2$ overvoert.
(2) Ontaarde kegelsneden kunnen van de volgende vorm zijn:
(2.1) Het kan voorkomen dat in $k[X, Y, Z]$ geldt dat $g = h^2$, waar $h$ een lineair polynoom is; we spreken dan van een "dubbele lijn".
(2.2) Als het voorgaande niet het geval is, en $C = \mathcal{Z}(g)$ is wel ontaard, dan is er precies één singulier punt en $C$ bestaat uit twee elkaar snijdende lijnen.
Laat zien dat bovenstaande indeling een volledige classificatie geeft van kegelsneden over $k$

**(10.2) Opmerking.** Over een lichaam $K$ dat niet algebraïsch afgesloten is, is de classificatie gecompliceerder. Het kan voorkomen dat voor een kegelsnede $C \subset \mathbb{P}^2_K$ de verzameling van rationale punten leeg is: $C(K) = \emptyset$; bij voorbeeld, het polynoom $g = X^2 + Y^2 + Z^2$ geeft $C = \mathcal{Z}(g)$ over $K = \mathbb{R}$ met deze eigenschap.

Het kan voorkomen dat $C \otimes k$ reducibel is, maar dat $C$ irreducibel is; bij voorbeeld $\mathcal{Z}(X^2 + Y^2)$ over een lichaam waarin $-1$ niet een kwadraat is.

**(10.3) De duale van een kegelsnede.** Zij $D \subset \mathbb{P}^2_K$ een niet-ontaarde kegelsnede. We schrijven $D^*$ voor de verzameling van alle raaklijnen aan $D$. Precieser: voor elke $P \in D(k)$ is $\mathfrak{t}_{D_k,P}$ een element van $D^*(k)$.

**(10.4) Terzijde** (karakteristiek 2). Laat zien dat als $K \supset \mathbb{F}_2$ en $D = \mathcal{Z}(X^2 + YZ)$ alle raaklijnen aan $D$ door het punt $[1 : 0 : 0]$ gaan.

**(10.5)** We kunnen $(\mathbb{P}^2_K)^*$ definiëren als de verzameling van alle lijnen in $(\mathbb{P}^2_K)$. We kunnen inzien dat $(\mathbb{P}^2_K)^* \cong \mathbb{P}^2_K$ door aan de lijn $\mathcal{Z}(aX + bY + cZ) \in (\mathbb{P}^2_K)^*$ het punt $[a : b : c] \in \mathbb{P}^2_K$ toe te voegen. Laat zien dat op deze manier, over een lichaam van karakteristiek $\neq 2$ elke niet-ontaarde kegelsnede $D$ een niet-ontaarde kegelsnede $D^* \subset (\mathbb{P}^2_K)^* \cong \mathbb{P}^2_K$ geeft. We zullen dit niet gebruiken, maar het is goed om deze structuur te begrijpen.

**(10.6)** We beschouwen twee kegelsneden $C, D \subset \mathbb{P}^2$, beide niet-ontaard, zodanig dat $C$ en $D$ elkaar nergens raken; dat wil zeggen:

$$\text{voor elk punt } P \in C \cap D \text{ geldt } \mathfrak{t}_{C,P} \neq \mathfrak{t}_{D,P}.$$

**Belangrijke eigenschap.** Dan geldt:

$$\#(C \cap D) = 4.$$

Dit volgt uit de stelling van Bezout. Zie ook (16.5).

**(10.7) De Poncelet constructie.** Werk over $k = \mathbb{C}$. Beschouw twee kegelsneden $C, D \subset \mathbb{P}^2$, beide niet-ontaard, zodanig dat $C$ en $D$ elkaar nergens raken. Neem $P \in C$ en $L \in D^*$ met $P \in L$; we noemen een dergelijk paar $(P, L)$ een Poncelet-paar. Uitgaande van een Poncelet-paar $(P_0, L_0)$ construeren we een volgend Poncelet-paar $(P_1, L_1)$: de lijn $L_0$ snijdt $C$ in de punten $P_0, P_1$:

$$C \cap L_0 = \{P_0, P_1\};$$

merk op dat het kan voorkomen dat $L_0$ raakt aan $C$, en in dat geval is $P_0 = P_1$ (geef een voorbeeld); we construeren $L_1$ als de "tweede raaklijn aan $D$ die door $P_1$ gaat";

$$L_0, L_1 \in D^*, \quad P_1 \in L_0 \cap L_1.$$

Ga na dat, uitgaande van een Poncelet-paar $(P_0, L_0)$ het Poncelet-paar $(P_1, L_1)$ goed gedefinieerd is. We kunnen dit proces recursief herhalen, en we krijgen een Poncelet-rij $(P_0, L_0), (P_1, L_1), \cdots, (P_i, L_i), \cdots$ .

**(10.8) De sluitingsstelling van Poncelet.** *Werk over $k = \mathbb{C}$. Beschouw twee kegelsneden $C, D \subset \mathbb{P}^2$, beide niet-ontaard, zodanig dat $C$ en $D$ elkaar nergens raken. Veronderstel dat er een Poncelet-paar $(P_0, L_0) \in C \times D^*$ en een $n \in \mathbb{Z}_{>0}$ bestaan zodanig dat in de Poncelet-rij de gelijkheid $(P_0, L_0) = (P_n, L_n)$ geldt.* (We zeggen wel, "de Poncelet-constructie sluit na $n$ stappen".) *Dan geldt voor elk Poncelet-paar $(Q_0, M_0)$ dat de Poncelet-constructie sluit na $n$ stappen: $(Q_0, M_0) = (Q_n, M_n)$.*

**(10.9) Opmerking / Vraagstuk.** Maak een situatie met $C, D \subset \mathbb{P}^2$ als boven, een Poncelet-paar $(P_0, L_0)$ en een $n \in \mathbb{Z}_{>0}$ zodanig dat de Poncelet-constructie een Poncelet-rij geeft waarin $(P_n, L_n)$ met $P_0 = P_n$ terwijl er een ander Poncelet-paar $(Q_0, M_0)$ is met $Q_0 \neq Q_n$. Merk op het subtiele verschil in de formulering hier en in (10.8).

# 11 De discriminant van een polynoom

We geven hier de definitie en verwijzingen voor de discrimimant van een polynoom.
**Waarschuwing.** Ook voor een eindige lichaamsuitbreiding $K \subset L$ en voor een polynoom dat een elliptische kromme definieert zullen we een discriminant zien; die begrippen zijn wel verwant aan het onderwerp van deze paragraaf, maar niet hetzelfde.

**(11.1)** Als $f \in R[T]$ een polynoom is met coëfficiënten in een ring $R$, dan definieren we de afgeleide (de "formele afgeleide"):

$$\text{voor} \quad f = \sum_{i=0}^{n} a_i T^{n-i} \in R[T] \quad \text{is} \qquad f' := \sum_{i=1}^{n} (n-i) \cdot a_i T^{n-i-1}.$$

**Opmerking over notatie.** Als $R$ is een ring, als altijd met $1 \in R$, dan is er één en precies één ringhomomorfisme $\iota : \mathbb{Z} \to R$. Als $m \in \mathbb{Z}$ en $a \in R$ dan schrijven we $ma$, of $m \cdot a$ voor de som in $R$ van $m$ keer het element $a$. We hadden ook kunnen schrijven $\iota(m) \cdot a$; die notatie was correcter geweest, maar die is te omslachtig.

**(11.2)** Zij $f \in K[T]$. We zeggen dat $f$ een *meervoudig nulpunt* heeft, als er een lichaamsuitbreiding $K \subset L$ en een element $b \in L$ zodanig dat $(T-b)^2$ een deler is van $f \in L[T]$. Hierbij zien we $K[T]$ als een deelring van $L[T]$.

Een polynoom $f = \sum_{i=0}^{n} a_i T^{n-i}$ heet *monisch* van graad $n$ als ($a_i = 0$ voor $i > n$ en $i < 0$) en $a_0 = 1$.

**(11.3) Vraagstuk.** **(a)** Zij $f \in K[T]$. Bewijs: *$f$ heeft een meervoudig nulpunt dan en slechts dan als $f$ en $f'$ een nulpunt gemeen hebben (in een lichaam dat $K$ bevat).*
**(b)** *Zij $f = T^3 + AT + B$. Vind een polynoom in $A$ en $B$ dat nul is dan en slechts dan als $f$ een meervoudig nulpunt heeft.*
**(c)** *Zij $f = T^p - a$. Zelfde vraag als in (b). Geef een uitleg van de oplossing.*
N.B. De karakteristiek van het grondlichaam is willekeurig in bovenstaande opgaven en vraagstukken. Merk op dat de uitdrukking die in (b) en in (c) gevraagd wordt niet eenduidig is.

**(11.4) Definitie van $D(f)$.** Voor elk lichaam $K$ en elk polynoom $f \in K[T]$, monisch van graad $n$, en een lichaamsuitbreiding $K \subset L$ zodanig dat $f \in L[T]$ in lineaire factoren uiteenvalt schrijven we:

$$f = a_0(T - t_1) \times \cdots \times (T - t_n), \quad t_i \in L,$$

en

$$D(f) := \left( \prod_{1 \le i < j \le n} (t_i - t_j) \right)^2 .$$

Merk op:

$$f \text{ heeft een meervoudig nulpunt} \iff D(f) = 0.$$

Uit de constructie volgt dat $D(f) \in L$, maar we zullen zien dat $D(f) \in K$.

**(11.5) Constructie / Stelling.** *Voor elke $n \in \mathbb{Z}_{\ge 2}$ is er een polynoom*

$$\delta_n \in \mathbb{Z}[A_0, A_1, A_2, \cdots, A_n]$$

*met de volgende eigenschappen.*
**(a)** *De graad van dit polynoom is $2n - 2$.*
**(b)** *Voor elk lichaam $K$ en elk polynoom $f \in K[T]$, monisch van graad $n$, verkrijgen we $D(f) \in K$ door de coëfficiënten van $f$ te substitueren in $\delta_n$.*
Een bewijs is te vinden in [39], Deel 1, §§ 33 - 35; zie [38], IV 6 – 8. □

**(11.6)** Formules voor een discriminant.
**(2)**

$$D(AX^2 + BX + C) = B^2 - 4AC;$$

**(3)**

$$D(X^3 + AX + B) = -4A^3 - 27B^2;$$

$$D(X^3 + aX^2 + bX + c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Er zijn allerlei manieren om bij gegeven $f$ de discriminant $D(f)$ uit te rekenen. Zie [31], II.3; zie [39], 5 Kap., § 34. In deze laatste verwijzing wordt $D(f)$ uitgerekend als $D(f) = R(f, f')$, de "resultante" van $f$ en $f' = (d/dX)(f)$. Als je hierin oefenen wilt, bewijs dan bovenstaande formules op deze manier.

In een bewijs komen de volgende belangrijke algebraïsche begrippen voor: *elementair symmetrische functies*, en *de resultante van twee polynomen*, hulpmiddelen die elke wiskundige hoort te kennen.

**Voorbeeld.** Zij $f = T^3 - 1 \in \mathbb{Q}$. In een uitbreidingslichaam kunnen we kiezen $1, \omega, \omega^2$ met $\omega^3 = 1$ en $1 + \omega + \omega^2 = 0$. Bereken $((1 - \omega)(\omega - \omega^2)(\omega^2 - 1))^2$.

**(11.7) Opdracht.** Laat zien dat $f \in k[T]$ een meervoudig nulpunt heeft desda als $f$ en $f'$ een nulpunt gemeen hebben. Beschrijf de resultante van twee polynomen $f, g \in k[T]$. Beschrijf een manier om de discrimimant van een polynoom uit te rekenen. Doe die berekening voor polynomen van graad 2, 3 en 4.

**(11.8)** Onderstel we hebben een lichaam $K$, en variabelen $T_1, \cdots, T_m$. De symmetrische groep $S_m$ werkt op de polynoomring $K[T_1, \cdots, T_m]$ en op de lichaamsuitbreiding $K \subset K(T_1, \cdots, T_m)$ (zuiver transcendent van transcendentie graad $m$); deze werking wordt gegeven door een $\sigma \in S_m$ te laten werken op de indices van de variabelen: $\sigma{\cdot}T_i = T_{\sigma(i)}$, en dit wordt voortgezet in een werking van $\sigma$ op een polynoom $f \in K[T_1, \cdots, T_m]$. We schrijven

$$K[T_1, \cdots, T_m]^{S_m} := \{f \in K[T_1, \cdots, T_m] \mid \sigma{\cdot}f = f\}$$

voor de ring van invarianten onder deze werking.

We schrijven $s_1, \cdots, s_m$ voor de elementair symmetrische polynomen:

$$s_1 = T_1 + \cdots + T_m, \cdots, s_u = \sum_{i_1 < \cdots < i_u} (T_{i_1} \times \cdots \times T_{i_u}), \cdots, s_m = T_1 \times \cdots \times T_m$$

Het is duidelijk dat $\sigma{\cdot}s_u = s_u$; dus $K[s_1, \cdots, s_m] \subset K[T_1, \cdots, T_m]^{S_m}$.

**(11.9) Stelling.**

$$K[T_1, \cdots, T_m]^{S_m} = K[s_1, \cdots, s_m].$$

Zie bv. [38], IV.6 Theorem 6.1. □
**Opmerking.** Dit resultaat geldt ook over $\mathbb{Z}$.

**(11.10)$^{\mathbf{e}}$** (De "e" slaat op "extra".) We zien dat, onder deze natuurlijk werking, $K(T_1, \cdot, T_m)^{S_m}$ weer een zuiver transcendente uitbreiding van transcendentie graad $m$ is.
**Het probleem van Emmy Noether.** *Zij $H \subset S_m$ een ondergroep. Is $K(T_1, \cdots, T_m)^H$ een zuiver transcendente uitbreiding van transcendentie graad $m$?* Zie [65].

Als het antwoord op dit probleem wel bevestigend zou zijn voor elke ondergroep $H \subset S_m$, dan zou het volgende probleem opgelost zijn:

**Het omkeerprobleem van de Galois theorie.** *Gegeven een eindige uitbreiding $\mathbb{Q} \subset K$, en een eindige groep $H$. Bestaat er een Galois uitbreiding $K \subset L$ met* $\mathrm{Gal}(L/K) \cong H$?

Pas in 1969 kwam er een tegenvoorbeeld voor het probleem van Emmy Noether, zie [66]; hierin is $H$ een cyclische groep van orde 47. We zien dat zo het omkeerprobleem in zij algemeenheid niet kan worden opgelost. Later werden er meer voorbeelden gevonden, en tenslotte begrijpen we dit fenomeen nu redelijk goed, zie [63].

Het omkeerprobleem werd in vele speciale gevallen bewezen. We verwachten dat het antwoord bevestigend zal zijn voor elke eindige groep $H$, maar dit is nog niet bewezen (of tegengesproken). Voor een overzicht zie [64]. Een prachtig onderwerp.

# 12 Commutatieve algebra

(Een zeer onvolledig hoofdstuk.)

We gebruiken een generalisatie van het begrip "vectorruimte over een lichaam". We nemen een ring $R$; die is in sommige gevallen niet noodzakelijk commutatief, maar wel associatief en met eenheidselement. We nemen een additief geschreven *abelse* groep $M$, en een afbeelding $R \times M \to M$, een "werking van elementen van $R$ op $M$". Deze werking voldoet aan de

gebruikelijke voorwaarden. In het geval $R$ niet commutatief is, moeten we goed onderscheid maken tussen "werking van links" (dit gebruiken we) en "werking van rechts" (we zullen dat hier niet tegenkomen).

We zullen begrippen als "vrij moduul", "vrij moduul van eindige rang" en "projectief moduul" gebruiken (zie literatuur).

**Voorbeeld.** Zij $R$ een ring, en $M = R^+ = (R, +)$, d.w.z. $M$ is de optelgroep van $R$, met de links-vermenigvuldiging van $R$.

**Voorbeeld.** Zij $A$ een abelse groep. Dan is $A$ op één en precies één manier een moduul voor de ring $R = \mathbb{Z}$.

We zeggen dat een verzameling $S \subset M$ een stelsel voortbrengers is voor $M$ over $R$ als elk element $x$ van $M$ geschreven kan worden als een *eindige som*

$$x = \sum_i a_i \cdot s_i, \quad a_i \in R, \quad s_i \in S.$$

Als we met een vectorruimte over een lichaam werken, dan kunnen we elke verzameling voortbrengers uitdunnen tot een basis. Bovendien is het aantal elementen in twee bases voor een eindig dimensionale vectorruimte gelijk.

Voor modulen gelden veel eigenschappen zoals voor vectorruimten, maar niet elke moduul heeft een basis, en het aantal benodigde voortbrengers hangt af van keuzen.

**Voorbeeld.** We merken op dat het moduul $M = \mathbb{Z}^+ = (\mathbb{Z}, +)$ over de ring $R = \mathbb{Z}$ de verzameling $S = \{2, 3\}$ als stelsel voortbrengers toelaat, maar dat ook $\{1\}$ dit moduul voortbrengt. Voor vectorruimtes over een lichaam is het aantal elementen van twee verschillende bases gelijk; pas op met een equivalent hiervan voor modulen over een ring.

**(12.1) Vraagstuk.** Zij $M = \mathbb{Z}^+$ over de ring $R = \mathbb{Z}$. Geef $S \subset M$ met $\#(S) = 5$, zodanig dat $S$ dit moduul voortbrengt, en zo dat elke $S' \subsetneqq S$ niet een stelsel voortbrengers is.

**(12.2)** Zij $R$ een ring bevat in een lichaam $K$. We zeggen dat $a \in K$ *geheel* is over $R$ als er een monisch polynoom $f \in R[T]$ bestaat met $f(a) = 0$.
**Voorbeelden. (a).** Met $R = \mathbb{Z}$ en $K = \mathbb{Q}$ laat zien: $a \in \mathbb{Q}$ is geheel over $\mathbb{Z}$ dan en slechts dan als $a \in \mathbb{Z}$.
**(b).** Welke elementen in $K = L(T)$ zijn geheel over $R = L[T]$?
**(c).** Laat zien dat $(-1 + \sqrt{-3})/2$ geheel is over $R = \mathbb{Z}$.

**(12.3) Vraagstuk.** Zij $R \subset K$ als boven. Voor een element $a \in K$ schrijven we $R[a]$ voor de kleinste deelring van $K$ die $R$ en $a$ bevat.
**(a).** Bewijs: *het $R$-moduul $R[a]$ is eindig voortgebracht dan en slechts dan als $a$ geheel is over $R$.*
**(b).** *Bewijs dat de verzameling van alle elementen in $K$ die geheel zijn over $R$ een deelring vormen van $K$.*
**(c).** Vind een $f \in \mathbb{Z}[T]$ waarvan $\sqrt{2} + \sqrt{3}$ een nulpunt is.

De ring in (b) hierboven noemen we de gehele afsluiting van $R$ in $K$.
**Commentaar.** Als $a$ en $b$ geheel zijn over $R$ dan zijn $a+b$ en $ab$ geheel over $R$, zoals we gezien hebben. Echter, als polynomen $f, g \in R[T]$ gegeven zijn met $f(a) = 0$ en $g(b) = 0$, dan valt het in het algemeen niet mee om een polynoom te vinden waarvan $a+b$ een nulpunt is, zoals we zagen in (c). De truc bewezen in (a) stelt ons in staat (b) te bewijzen zonder zulke polynomen expliciet aan te geven.

De ring $R[a]$ wordt wel een *algebra van eindig type* over $R$ genoemd. Soms is er een spraakverwarring tussen de terminologie een ring (of een algebra), die eindig voortgebracht is als algebra, en een moduul dat eindig voorgebracht is. Een ring die van eindig type is (eindig voorgebracht als algebra) hoeft niet als moduul eindig voortgebracht te zijn.
**Voorbeeld.** De ring $\mathbb{Z}[1/2]$ bestaat uit alle breuken waarvan de noemer een macht van 2 is. We zeggen dat deze ring als algebra eindig voortgebracht is over $\mathbb{Z}$: de kleinste deelring die $1/2$ bevat is deze ring zelf. Laat zien dat dit als moduul over $\mathbb{Z}$ niet eindig voortgebracht is.
**Notatie.** Zij $[K : \mathbb{Q}] < \infty$; een dergelijk lichaam noemen we een *getallenlichaam*. De ring van elementen in $K$ die geheel zijn over $\mathbb{Z}$ noemen we de ring van gehelen in $K$, notatie: $\mathcal{O}_K$.

**(12.4) Vraagstuk.** Zij $R = \mathbb{Z}$. Bepaal voor elk priemgetal $p$ de ring van gehelen $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ en bepaal de ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-p})}$.

**(12.5) Waarschuwing / Opdracht.** In $\mathbb{Z}$ geldt *eenduidigheid van priemfactorontbinding* (op volgorde van de factoren, en op eenheden na). Kun je een bewijs daarvoor reproduceren? Die eigenschap geldt in sommige gevallen wel in $O_K$, waar $K$ een algebraïsch getallenlichaam is, maar in vele gevallen geldt die eigenschap niet.
**(1).** Ga na wat de priemelementen zijn in $\mathbb{Z}[i]$, waar $i = \sqrt{-1}$. In die ring, die wel de ring van gehelen van Gauss genoemd wordt. Bewijs de eenduidigheid van priemfactorontbinding in deze ring.
**(2).** Laat zien dat in de ring $R = \mathbb{Z}[\sqrt{-5}]$ eenduidigheid van priemfactorontbinding niet geldt: wat zijn de eenheden van deze ring? Kies irreducibele elementen $a, b, c, d \in R$ met $ab = cd$ zo dat $a$ niet een deler is van $c$ en ook niet een deler is van $d$.

**Opmerking.** De ideaaltheorie is uitgevonden om dit euvel te verhelpen en de theorie te stroomlijnen.

# 13 Algebraïsche meetkunde

(Een zeer onvolledig hoofdstuk.)

In de algebraïsche meetkunde zien we o.a. de volgende fases in de historische ontwikkelingen:

Vóór 1900: Riemann, Klein, Max Noether en vele anderen; zowel het begin van de analytische theorie (theorie van Riemann oppervlakken, Weierstrass uniformizatie), als de algebraïsche theorie.

Eerste helft 20-ste eeuw: de Italiaanse school (Severi, Enriques en vele anderen); fantastische meetkundige ideeën; er was wel eens kritiek op hun methoden, omdat die niet altijd precies en foutloos bleken te zijn.

Midden 20-ste eeuw: algebraïsche fundering (Van der Waerden, Weil, Zariski, Chow, Emmy Noether en vele anderen), ook meer toepassingen in de getaltheorie. Steeds meer toepassingen van meetkundige gedachten met een ander lichaam dan $\mathbb{C}$ als grondlichaam, in het bijzonder eindige lichamen. André Weil schrijft in 1946 zijn "Foundations ..."waarmee hij hoopt alles te kunnen beschrijven. Grote rijkdom aan oplossingen en nieuwe problemen. Zie ook uit die periode: [61], [62] , [60], [51], [49]; deze boeken zijn allemaal te lezen zonder iets over schema's te weten.

Methoden uit andere delen van de meetkunde geven een nieuwe impuls, vooral door het baanbrekende werk FAC van J-P. Serre, 1955, zie [59]; lees het vooral, het is glashelder geschreven, en het geeft een prachtig beeld van hoe je wiskunde moet doen en moet opschrijven. Daarna komt Grothendieck, die de "Weil vermoedens" wil bewijzen door een geheel nieuwe theorie op te zetten. De algebraïsche meetkunde kun je nu over een willekeurig ring doen, een prachtig apparaat. De duizenden pp. geschreven door Grothendieck, 1960 – 1970, zijn niet eenvoudig in één keer te verwerken. Maar de theorie van de schema's is wel de "beste manier" om algebraïsche meetkunde te ontwikkelen en te gebruiken. In [53], vooral in de eerste twee hoofdstukken, wordt die theorie prachtig beschreven, vooral wat betreft de eerste technieken die je onder de knie moet hebben om verder te kunnen.

Artikel en boeken waarin de moderne theorie wordt uitgelegd: [59], [53], [55], [50].

Opzet van dit project/college. Je kunt elliptische krommen prima bestuderen door middel van vergelijkingen. Je hebt niet veel geavanceerde theorie nodig om de eerste begrippen te hanteren. Wel is het zo dat het nuttig is voor meer begrip als je meer theorie, of uit de abstracte algebraïsche meetkunde, of uit de theorie van de schema's, tot je beschikking hebt. Ik probeer aan te geven wat de definities zijn waar we van uit gaan. Stellingen die we nodig hebben, maar waarvan een bewijs te ver gaat voor ons voor dit doel, zullen we als een "black box" hanteren. Probeer precies te begrijpen wat de grond is waar je op staat, en wat de uitspraak is die je gebruikt. Als je meer erover wilt weten: in deze korte paragraaf geef ik wat aanwijzingen.

**(13.1) Affiene en projectieve verzamelingen.** We gebruiken de affiene ruimte $\mathbb{A}^n_K$ en de projectieve ruimte $\mathbb{P}^n_K$ van dimensie $n$ over een lichaam $K$; ik zal uitleggen wat we hiermee precies bedoelen. Een affiene variëteit $V \subset \mathbb{A}^n_K$ wordt gedefiniëerd als de nulpunten verzameling van elementen van een ideaal $I \subset K[T_1, \cdots, T_n]$. We schrijven dan $V = \mathcal{Z}(I)$, spreek uit: de nulpuntenverzameling van $I$. Een polynoom $f \in K[T_0, T_1, \cdots, T_n]$ heet homogeen van graad $m$ als alle monomen in het polynoom precies graad $m$ hebben. Een ideaal $J \subset K[T_0, T_1, \cdots, T_n]$ heet homogeen als het voortgebracht wordt door homogene polynomen (mogelijk van verschillende graad). De nulpunten verzameling daarvan noteren we als $\mathcal{Z}(J) \subset \mathbb{P}^n_K$. Uitleg wordt verder op college gegeven. in deze theorie worden begrippen als dimensie, irreducibel, complete variëteit gegeven.

**(13.2) Algebraïsche krommen.** Een absoluut irreducibele variëteit (d.w.z. irreducibel over een algebraïsche afsluiting van het grondlichaam) van dimensie één wordt een *algebraïsche kromme* genoemd. Als $f \in K[X, Y]$ en polynoom is dat irreducibel is in $k[X, Y]$, waar $k$ een algebraïsch afgesloten lichaam is dat $K$ bevat, dan is $\mathcal{Z}(f) \subset \mathbb{A}^2_K$ een affiene algebraïsche kromme. Dit is een manier om sommige krommen te definiëren en te bestuderen.

Elke complete algebraïsche kromme kan ingebed worden in $\mathbb{P}^3_K$, maar niet elke algebraïsche kromme kan ingebed worden in $\mathbb{P}^2_K$; op het college wordt dit verder toegelicht. Echter, dit aspect is niet belangrijk voor het doel dat we voor ogen hebben. (Het begrip "compleet" voor een algebraïsche variëteit heb ik niet gedefinieerd. Over $\mathbb{C}$ is het equivalent met compact in de klassieke topologie. In de algebraïsche meetkunde is een mooie generalisatie gevonden, zonder de klassieke topologie te gebruiken.)

Overigens, voor hogere dimensies liggen deze dingen veel moeilijker. Hironaka construeerde een complete 3-dimensionale variëteit, die niet ingebed kan worden in welke projectieve ruimte dan ook; zie [53], App. B, 3.4.1.

Zie ook voor verdere verwijzingen:
`http://www.math.umn.edu/~roberts/math8203/references.html`

## 14 Vergelijkingen voor elliptische krommen

In de meeste gevallen wordt een elliptische kromme gegeven door een vergelijking; voor een uitleg zie (3.7). We zullen veelvuldig gebruikmaken, verwijzen naar de volgende vergelijking, die vaak *Weierstrass vergelijkingen* worden genoemd. In de §§ 3, 6, 7, 8 leggen we uit in welke situaties, over welke lichamen, over welke ringen, deze vergelijkingen gebruikt kunnen worden. Zie [11], III.2 en VIII.3; [19], II.2; [29], III.1; [30], I.4; [31], I.3 en p. 43.

Elk van de vergelijkingen vermeld in (14.1) – (14.3) wordt een *Weierstrass vergelijking* of een *Weierstrass normaal vorm* genoemd.

**(14.1)**

$$Y^2 = X^3 + AX + B; \qquad \text{(W1)}$$

$$j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2};$$

$\Delta(\mathcal{E}) = -16 \cdot (4A^3 + 27B^2)$;
$D(X^3 + AX + B) = -4A^3 - 27B^2$
$c_4 = -48A$.

**(14.2)**

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6; \qquad \text{(W2)}$$

$b_2 = a_1^2 + 4a_2$,
$b_4 = 2a_4 + a_1a_3$,
$b_6 = a_3^2 + 4a_6$,
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$,
en
$c_4 = b_2^2 - 24b_4$,
$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$,

$\Delta(\mathcal{E}) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$,

$$j(E) = \frac{c_4^3}{\Delta}.$$

**(14.3)**

$$Y^2 = X^3 + aX^2 + bX + c; \qquad \text{(W3)}$$

$D = D(X^3 + aX^2 + bX + c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$,
$\Delta = 16 \cdot D$.

**(14.4)**

$$Y^2 = 4X^3 - g_2X - g_3; \qquad \text{(W4)}$$

$$\Delta = \Delta(\mathcal{E}) = g_2^3 - 27g_3^2; \quad j(E) = 1728 \cdot \frac{g_2^3}{\Delta}.$$

**(14.5)** (J. Tate)

$$Y^2 + XY = X^3 - \frac{36}{t - 1728}X - \frac{1}{t - 1728}; \qquad \text{(W5)}$$

$$\Delta(\mathcal{E}) = t^2/(t - 1728)^3; \qquad j(E) = t;$$

(! bewijs dit !).

**(14.6)** Twee voorbeelden:
($p \neq 3$)

$$j\left(Y^2 + Y = X^3\right) = 0, \quad \Delta = -27;$$

($p \neq 2$)

$$j\left(Y^2 = X^3 + X\right) = 1728, \quad \Delta = -64.$$

**(14.7) Opmerking.** Het is niet zo moeilijk om in te zien dat als $E_1$ en $E_2$ elliptische krommen over een lichaam $K$ zijn met $E_1 \cong E_2$ dan geldt $j(E_1) = j(E_2)$.

**(14.8) Vraagstuk. (1).** Bewijs dat de elliptische krommen over $\mathbb{Q}$ gegeven door $Y^2 = X^3 - 8$, resp. $Y^2 = X^3 - 9$, respectievelijk $Y^2 = X^3 - 10$ onderling over $\mathbb{Q}$ niet isomorf zijn.
**(2).** Gegeven zijn $E_1$ en $E_2$ over $\mathbb{C}$ met $j(E_1) = 0 = j(E_2)$. Bewijs dat $E_1 \cong_{\mathbb{C}} E_2$.
**(3).** (Deuring) Zij $K$ een lichaam. Bewijs dat voor elke $s \in K$ er een elliptische kromme $E$ over $K$ is met $j(E) = s$ (ga alle gevallen na).

**(14.9)** Vraagstuk (14.8)(2) is een bijzonder geval van de volgende stelling: *voor elk algebraïsch afgesloten lichaam $k$ en elliptische kommen $E_1$ en $E_2$ over $k$ met $j(E_1) = j(E_2)$ geldt $E_1 \cong_k E_2$.* In [11], III.3, Prop. 3.7 wordt een bewijs gegeven voor karakteristiek $\neq 2$; de stelling geldt in elke karakteristiek.

Merk op dat het gegeven dat het grondlichaam algebraïsch afgesloten is essentiëel is: zie (14.8)(1) en maak zelf veel andere voorbeelden.

**(14.10) De Legendre normaal vorm.**

$$Y^2 = X(X - 1)(X - \lambda) \qquad \text{(W6)}$$

$$\Delta = \Delta(\mathcal{E}) = -16\lambda^2(1 - \lambda)^2; \qquad j(E) = 2^8 \cdot \frac{(1 - \lambda + \lambda^2)^3}{\lambda^2(1 - \lambda)^2}.$$

**(14.11)**

$$X^3 + Y^3 + Z^3 = 3\mu XYZ \qquad \text{(W7)}$$

$$j(E) = 3^3 . \frac{\mu^3(\mu^3+8)^3}{(\mu^3-1)^3}.$$

Laat zien dat dit een elliptische kromme is desda $\big(\text{char}(K) \neq 3$ en $\mu^3 \neq 1\big)$.

**(14.12) Edwards krommen.** Zie
`http://en.wikipedia.org/wiki/Edwards_curve`
**Vraagstuk.** Neem een lichaam $K$ van karakteristiek ongelijk aan 2. Geef een kromme $C$ door

$$X^2 + Y^2 = 1 + dX^2y^2, \quad d \in K.$$

Voor welke waarde(n) van $d$ is deze affiene kromme niet-singulier?
(Opmerking. De kromme verkregen door projectieve afsluiting in $\mathbb{P}^2$ is singulier. De normalizatie daarvan is een elliptische kromme (als $d \neq 0$ en $C$ niet-singulier). Deze krommen worden gebruikt in de cryptografie.)

# 15 Diverse Vraagstukken

**(15.1) Vraagstuk.** Zij $G$ een groep. Schrijf $\text{Tors}(G)$ voor de *verzameling* van elementen van eindig orde in $G$; zulke elementen heten ook wel torsie-elementen, vandaar de notatie.
**(a).** Als $G$ een abelse groep is, bewijs: $\text{Tors}(G) \subset G$ is een ondergroep. In dit geval geldt $\text{Tors}(G/\text{Tors}(G)) = \{0\}$; bewijs dit.
**(b).** Construeer / kies een commutatieve groep $G$ zodanig dat voor elke $m \in \mathbb{Z}_{>0}$ de groep $G/mG$ eindig voortgebracht is, terwijl $G$ niet eindig voortgebracht is (met bewijs).
**(c).** Construeer / kies een (niet-commutatieve) groep $G$ zodanig dat $\text{Tors}(G) \subset G$ niet een ondergroep is (met bewijs).

**(15.2) Vraagstuk: de groepswet op een singuliere kromme.**
**(a).** Over een lichaam $K$ geven we een vlakke kromme $C \subset \mathbb{P}^2_K$ door $Y^2 = X^2(X-1)$. Merk op dat deze kromme singulier is. Beschouw $C^0 = C - \{(0,0)\}$. Op $C^0$ geven we een optelling net zoals we dat voor een elliptische kromme deden. Bewijs dat voor elke $K \subset L$ er een groeps-isomorfisme

$$C^0(L) \xrightarrow{\sim} L^* := ((L - \{0\}), \times)$$

bestaat; hier is $L^*$ de multiplicatieve groep van het lichaam $L$. Bewijs dat we zo een groepswet op $C^0$ krijgen.
**(b).** Over een lichaam $K$ geven we een vlakke kromme $D \subset \mathbb{P}^2_K$ door $Y^2 = X^3$. Merk op dat deze kromme singulier is. Beschouw $D^0 = D - \{(0,0)\}$. Op $D^0$ geven we een optelling net zoals we dat voor een elliptische kromme deden. Bewijs dat voor elke $K \subset L$ er een groeps-isomorfisme

$$D^0(L) \xrightarrow{\sim} L^+ = (L, +)$$

bestaat; hier is $L^+$ de additieve groep van het lichaam $L$. Bewijs dat we zo een groepswet op $D^0$ krijgen.
(Opmerking. Bovenstaande resultaten kunnen voor een willekeurige, absoluut irreducibele, singuliere kubische kromme bewezen worden; in geval (a) voor een kromme met een dubbelpunt, en in geval (b) voor een kromme met een keerpunt.)

**(15.3) Vraagstuk.** Beschrijf alle $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ zodanig dat $y^2 = x^3 - 4x^2 + 5x - 2$.

**(15.4) Vraagstuk. (1).** We geven $E$ over $\mathbb{Q}$ door $Y^2 = X^3 + 1$. Een feit is dat de rang van deze kromme gelijk is aan 0. Bepaal de structuur van de groep $\mathrm{Tors}(E(\mathbb{Q}))$.
**(2).** We geven $E'$ over $\mathbb{Q}$ door $Y^2 = X^3 - 432$. Een feit is dat de rang van deze kromme gelijk is aan 0. Bepaal de structuur van de groep $\mathrm{Tors}(E'(\mathbb{Q}))$.
**Opmerking.** Zoek op het internet op: het vermoeden van Catalan; dat vermoeden is nu bewezen; leidt een deel het antwoord van onderdeel (1) van dit vraagstuk af uit dat vermoeden: $\{(x, y) \in \mathbb{Z}_{>0} \mid x > 1, \quad y^2 = x^3 + 1\} = \{(2, \pm 3)\}$.

**(15.5) Vraagstuk.** Over $k$ met $\mathrm{char}(k) \neq 2$. Geef $E$ door de vergelijking $Y = X^3 - 43X + 166$. Laat zien dat $P = (3, -8) \in E$. Wat is de orde van dit punt? (Zie ook (7.20), 3c.)

**(15.6) Vraagstuk.** Over $k$ geef $E$ door de vergelijking $Y^2 + Y = X^3 - X$. Bepaal $p$ zodanig dat als $\mathrm{char}(k) = p$ deze kromme singulier is. Wat is de orde van het punt $P = (0, 0) = [0 : 0 : 1]$ als $\mathrm{char}(k) = 0$? Bepaal ook de orde van $P$ voor elk van de waarde $\mathrm{char}(k) = p$ met $2 \leq p \leq 7$.

**(15.7) Vraagstuk.** Zij $C = \mathcal{Z}(Y^2Z - YZ^2 - X^3 + X^2Z) \subset \mathbb{P}^2_k$. Voor welke waarde(n) $\mathrm{char}(k) = p$ is dit een singuliere kromme, en wat is dan het singuliere punt?

**(15.8) Vraagstuk.** Zij $C = \mathcal{Z}(XY^3 + YZ^3 + ZY^3) \subset \mathbb{P}^2_k$. Voor welke waarde(n) $\mathrm{char}(k) = p$ is dit een singuliere kromme, en wat is dan het singuliere punt?

**(15.9) Vraagstuk.** Neem $K = \mathbb{Q}$ en $C = \mathcal{Z}(X^3 + Y^3 + Z^3) \subset \mathbb{P}^2_{\mathbb{Q}}$.
**(1).** Bewijs dat er een punt $0 \in C(\mathbb{Q})$ is dat een buigpunt is op deze kromme. Bewijs dat deze kromme niet-singulier is.
**(2).** Kies een buigpunt in $0 \in C(\mathbb{Q})$ als nul-punt. Bepaal voor de elliptische kromme $(E, 0) = (C, 0)$ zo verkregen de groep $\mathrm{Tors}(E(\mathbb{Q}))$.

**(15.10) Opmerkingen.*** Er bestaat niet een kromme $C$ over $\mathbb{Q}$ van positief geslacht die voor elke $p$ een reductie modulo $p$ een niet-singuliere kromme geeft (een diepe stelling); zie (16.8). De vorige twee vraagstukken illustreren dit: in beide gevallen weten we a priori dat er minstens één $p$ is waar die betreffende kromme modulo $p$ singulier is.

Wel is het gemakkelijk om een elliptische kromme $E$ te geven over een getallenlichaam $K$ zo dat $E$ goede reductie heeft voor alle plaatsen van $K$: neem een elliptische kromme $E'$ over $K' \supset \mathbb{Q}$ waarvan de endomorfismenring $\mathrm{End}(E') \neq \mathbb{Z}$ (een zo genaamde elliptische kromme met complexe vermenigvuldiging). Voor geschikt gekozen $K' \subset K$ heeft kromme $E' \otimes K$ overal goede reductie.

Voor reëel kwadratische lichamen is er veel onderzoek naar de eigenschappen van overal goede reductie gedaan. Zie bv.

urlhttp://www.warwick.ac.uk/staff/J.E.Cremona//ecegr/ecegrqf.html

`http://arxiv.org/abs/1107.4648`

**(15.11) Vraagstuk.** Beschouw het lichaam $K = \mathbb{Q}(\sqrt{41})$. De ring van gehelen in dat lichaam is $\mathcal{O}_K = R = \mathbb{Z}[(1 + \sqrt{41})/2]$. Laat zien dat het element $\varepsilon := 32 + 5\sqrt{41}$ een eenheid is in die ring. Wat is de discriminant van de kromme $\mathcal{E}$ over $R$ gegeven door $Y^2 + XY = X^3 - \varepsilon X$?

**(15.12) Vraagstuk.** In dit vraagstuk is $K$ een lichaam van karakteristiek 2. Zij $E$ een elliptische kromme over $K$; neem aan dat $E$ gegeven is door de formule (W5).
**(a)** Zij $(x, y) = P \in E(K)$. Wat zijn de coördinaten van het punt $-P$? (Merk op: alhoewel in $K$ geldt: $2a = a + a = 0$ geldt in $E(K)$ niet noodzakelijk dezelfde eigenschap).
**(b)** Beschrijf onder welke voorwaarden $2P = 0$.
**(c)** Concludeer dat $E(K) \cong \mathbb{Z}/2$ óf $E(K) = 0$.
**(d)** Zij $K = k$ een algebraïsch afgesloten lichaam. Formuleer de nodig en voldoende voorwaarde in de coëfficiënten van (W2) dat in dit geval (karakteristiek 2) geldt $E[2](k) = 0$.

**(15.13) Vraagstuk.** We geven $E$ over $\mathbb{F}_{13}$ door $Y^2 = X^3 + 3X$. (Notatie: in dit vraagstuk schrijven we voor coëfficiënten en coördinaten zoals $\overline{3}$ of 3 mod 13 het eenvoudiger 3; maar de exponent 3 is natuurlijk echt $3 \in \mathbb{Z}$). Bereken $\#(E(\mathbb{F}_{13}))$. Bepaal de structuur van $E(\mathbb{F}_{13})$.

**(15.14) Vraagstuk.** Zij $\epsilon = \frac{5+\sqrt{29}}{2} \in \mathbb{Q}(\sqrt{29})$. Laat zien dat $\epsilon$ een eenheid is in de ring van gehelen in $\mathbb{Q}(\sqrt{29})$. Geef een elliptische kromme $\mathcal{E}$ over $\mathbb{Z}[\epsilon]$ door:

$$y^2 + xy + \epsilon^2 y = x^3.$$

Is er een priemgetal $p$ zodat $\mathcal{E}_p$ singulier is? (Serre, Tate, Shimura).

**(15.15) Vraagstuk.** gegeven zijn $P_1, \cdots, P_5 \in \mathbb{P}^2_K$ zodanig dat er geen twee punten gelijk zijn, en dat er geen drie op een rechte liggen. Bewijs dat er precies één kegelsnede $C \subset \mathbb{P}^2_K$ is met $P_i \in C$ voor $1 \leq i \leq 5$ en bewijs dat die kegelsnede niet-ontaard is. Vgl. [61], pag. 37.
(Hint. Hoeveel coëfficienten heeft een kwadratisch homogeen polynoom in 3 variabelen? Zij $V_j$ de ruimte van al zulke polynomen met $F(P_i) = 0$ voor $1 \leq i \leq j$; beschrijf $V_j$ voor alle $j \leq 5$.)

**(15.16) Vraagstuk.** We geven een kegelsnede over $K = \mathbb{Q}$ door

$$C = \mathcal{Z}(X^2 + 384XY + 17Y^2 + 35X + 120399Y).$$

Bewijs dat $\#(C(\mathbb{Q})) = \infty$. (Hint: zie (16.5)(a).) Geef tenminste 3 punten met coördinaten in $\mathbb{Q}$ op deze kegelsnede.

# 16 Opdrachten

Zie ook (4.10), (5.15), (7.21), (11.7), (12.5).

**(16.1) Opdracht.** Bewijs de volgende uitspraken.
**(a)** Als $A$ een eindig voortgebrachte, abelse groep is, en $\mathrm{Tors}(A) = 0$, dan is er een $m \in \mathbb{Z}_{\geq 0}$ en een isomorfisme $A \cong \mathbb{Z}^m$.
**(b)** Als $\mathbb{Z}^m \cong \mathbb{Z}^r$ dan is $m = r$.
**(c)** Als $B$ een eindig voortgebrachte, abelse groep is, dan is er een unieke $m \in \mathbb{Z}_{\geq 0}$ en een isomorfisme

$$B \cong \mathrm{Tors}(B) \times \mathbb{Z}^m.$$

**(16.2) Opdracht: topologie.** Alle ruimtes in deze opdracht zijn topologische ruimtes (verkregen door de complexe, of de reële topologie). We schrijven

$$S = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\},$$

de 2-sfeer, het boloppervlak. We schrijven

$$T = \mathbb{R}^2 / \left(\mathbb{Z}\cdot(1,0) + \mathbb{Z}\cdot(0,1)\right)$$

de 2-torus, de ring, de "donut". Bewijs:
**(a)** $\mathbb{P}^1(\mathbb{C}) \approx S$ (homeomorf als toplogische ruimten).
**(b)** Zij $E$ een elliptische kromme over $\mathbb{C}$; dan is $E(\mathbb{C}) \approx T$. (Ga uit van de definitie en gebruik resultaten uit § 4 niet.)

**(16.3) Waarschuwingen.** De topologische ruimtes $\mathbb{P}^2(\mathbb{R})$ en $\mathbb{P}^1(\mathbb{C})$ zijn allebei een compactificatie van $\mathbb{R} \times \mathbb{R} \approx \mathbb{C} \approx \mathbb{A}^2(\mathbb{R}) \approx \mathbb{A}^1(\mathbb{C})$, maar

$$\mathbb{P}^2(\mathbb{R}) \quad \not\approx \quad \mathbb{P}^1(\mathbb{C}).$$

Laat dit zien.

Voor een elliptische kromme $E$ over $\mathbb{C}$ kunnen we beschouwen de *analytische variëteit* $E(\mathbb{C})$. Voor $\tau \in \mathbb{C}$ met $\tau \notin \mathbb{R}$ kunnen we beschouwen de *analytische variëteit* $T_\tau = \mathbb{C}/\left(\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau\right)$. Alleen voor speciale keuzen van $\tau_1, \tau_2$ geldt dat de analytische variëteiten $T_{\tau_1}$ en $T_{\tau_2}$ isomorf zijn; zie (4.9), (4.10). Een dergelijk criterium kan geformuleerd worden met de $j$-invariant, en op vele andere manieren. Voor meer uitleg zie § 4.

**(16.4) Opdracht.** (We bewijzen een speciaal geval van (9.5).) Zij $p$ een priemgetal, en geef $E_p$ door $Y^2 = X(X-N)(X+N)$ over $\mathbb{Q}$. Bewijs:

$$\mathrm{Tors}(E_p(\mathbb{Q})) \cong (\mathbb{Z}/2)^2.$$

(Desgewenst kan de stelling van Nagell-Lutz gebruikt worden.)

**(16.5) Opdracht.** (We bewijzen een speciaal geval van de stelling van Bezout.)
**(a)** (Rationale krommen.) Zij $C \subset \mathbb{P}^2_K$ een niet-ontaarde kegelsneden, met $C(K) \neq \emptyset$. Kies $P \in C(K)$, twee verschillende lijnen $L_1 = \mathcal{Z}(h_1)$, $L_2 = \mathcal{Z}(h_2)$ door $P$. We schrijven $h^{(s,t)} = s\cdot h_1 + t\cdot h_1$ en

$$\mathcal{Z}(h^{(s,t)}) \cap C = \{P, P^{(s:t)}\}.$$

Laat zien dat de coördinaten van $P^{(s:t)}$ kwadratische vormen in $s$ en $t$ zijn. Laat zien dat er zo een bijectieve afbeelding

$$\mathbb{P}^1_K \xrightarrow{\sim} C$$

onstaat.
**Definitie.** Zij $C \subset \mathbb{P}^2_K$ een vlakke kromme van graad $d$ (d.w.z. $C = \mathcal{Z}(g)$, waar $g$ een homogeen polynoom van graad $d$ is). We nemen aan dat $g$ irreducibel is over $k$. We zeggen dat $C$ een *rationale kromme* is als er homogene polynomen $\mathcal{X}(S,T), \mathcal{Y}(S,T), \mathcal{Z}(S,T) \in K[S,T]$ van graad $d$ bestaan zodanig dat voor elke $s, t \in k$ we krijgen:

$$[\mathcal{X}(s,t) : \mathcal{Y}(s,t) : \mathcal{Z}(s,t)] \in C.$$

**(b)** Zij $C \subset \mathbb{P}^2_K$ een vlakke rationale kromme van graad $d$; zij $D \subset \mathbb{P}^2_K$ een vlakke kromme van graad $e$. Gegeven is dat voor elke $P \in (C \cap D)(k)$ dit punt niet-singulier is op $C$ en niet-singulier op $D$ en dat in dat punt de raaklijnen verschillend zijn. Bewijs dat $\#(C \cap D)(k) = d \cdot e$. Bewijs alle details.

**Opmerking.** Met een uitgebreidere definitie van snijpuntsmultipliciteit kunnen we eisen over niet-singularieteit en verschillende raaklijnen laten vallen, en nog hetzelfde resultaat krijgen, maar geteld met multipliciteiten.

**(16.6) Kubische krommen door 8 punten.** We zeggen dat 8 punten $P_1, \cdots, P_8 \in \mathbb{P}^2_K$ in *algemene ligging* zijn als er geen twee gelijk zijn, als er geen 4 op en rechte liggen, en als er geen 6 op een kegelsnede liggen. We schrijven $V_i$ voor de ruimte van homogene kubische vormen $g \in K[X, Y, Z]$ die nul zijn in $P_1, \cdots, P_i$.
**(a)** Bewijs $\dim_K(V_i) = 10 - i$ voor $0 \leq i \leq 8$.
**(b)** Bewijs dat er een niet-singuliere kubische kromme $C \subset \mathbb{P}^2_K$ bestaat die door $P_1, \cdots, P_8$ gaat.

Vergelijk met (15.15).
(Opmerking. Dit is een mooie structuur: bewezen kan worden dat alle kubische krommen die deze 8 punten bevatten alle door een uniek bepaald punt $P_9$ gaan.)

**(16.7) Opdracht: Pythagoreïsche drietallen.** Geef de definitie van een Pythagoreïsch drietal, en formuleer zorgvuldig de stelling die alle PDen classificeert. Schrijf tenminste één bewijs van deze stelling volledig uit.

**(16.8) Opdracht.** Reproduceer en begrijp een bewijs van de stelling (van Tate) dat er niet een $\mathcal{E}$ over $\mathbb{Z}$ bestaat gegeven door een (W2) normaal vorm met $\Delta(\mathcal{E}) = \pm 1$ ("elke elliptische kromme over $\mathbb{Q}$ heeft tenminste een priem van slechte reductie"). Het oorspronkelijke bewijs van Tate staat in [23].

# 17 Onderwerpen voor een voordracht

In de tweede helft van deze activiteit in dit semester houden studenten voordrachten.

Elke week (7/I tot 23/I/2014) geven twee groepen van $\leq$3 studenten in $45 + 30$ minuten voor elke groep een presentatie + vragen. De laatste 15 minuten zijn voor een evaluatie van de voordracht door studenten en docent.

Die wordt in gezamenlijk overleg voorbereid.

Er wordt een manuscript geproduceerd, dat de basis is van de voordrachten.

Vorm van de presentatie en indeling van de tijd mag zelf ingevuld worden.

Let goed op:
– heldere definities, begrijpelijke uitleg;
– precies aangeven wat je wel bewijst, en hoe dan, en wat je niet bewijst;
– in dat laatste geval nauwkeurige formulering en verwijzingen geven.
– Zorg voor instructieve voorbeelden, die goed uitgewerkt zijn, helder geformuleerd, die begrijpelijk zijn, en waarbij je aangeeft wat je van het voorbeeld bewijst. Elke voordracht bevat

tenminste één goed uitgewerkt voorbeeld, en tenminste één goed uitgewerkt bewijs.
– Ga niet over de eindtijd heen. Geef ruimte voor vragen (tijdens of direct na de presentatie).

– Het is goed om literatuur te raadplegen.
– Zoek in de literatuur, zoek op internet naar informatie die erbij past. Raadpleeg internet, Wikipedia, zoekmachines op een woord, om meer informatie en meer literatuur verwijzingen te vinden.
– Eigen initiatief wordt zeer op prijs gesteld.
– Kom met eigen suggesties/onderwerpen als dat mooi en nuttig is.
– Ik heb als algemene regel: *elke wiskundige voordracht moet tenminste één bewijs bevatten* (zo krijgt het gehoor inzicht in methoden, en in de moeilijkheidsgraad).
– Aarzel niet om raad te vragen.
– Maak er wat van dat mooi en interessant is!
Sommige van deze onderwerpen geven veel te veel materiaal voor één voordracht. Kijk hoe je dat systematiseert, hoe je beperkt en snoeit, uitlegt wat het algemene beeld is, wat de algemene stelling is, en geef dan van tenminste één detail een goed bewijst. Kom langs voor overleg als je daar behoefte aan hebt.

**(17.1) Het Poncelet probleem.** Bespreek de Poncelet stuitingsstelling over $\mathbb{C}$. Geef goede definities. Bewijs uitspraken in de constructie. Geef een bewijs van deze stelling. (Beslis zelf over details, over eventueel wel of niet historische feiten, over voorbeelden, over het gedegenereerde geval, etc. Lees literatuur hierover.) Zie § 10.

**(17.2) Congruente getallen en elliptische krommen.** Op mijn homepage
`http://www.staff.science.uu.nl/~oort0109/`
vind je de syllabus [37] over congruente getallen, waar ook veel verwijzingen in staan.

Geef definities, formuleer zorgvuldig vragen over het vinden van CGen. Geef de definitie van een Pythagoreïsch drietal, en formuleer de stelling die alle PDen classificeert. Leg het verband uit tussen CGen en elliptische krommen (zowel in formules als in idee). Leg uit hoe dit tot een vermoeden over CGen leidt. Bepaal zelf wat en hoeveel bewezen kan worden in deze voordracht. Bepaal zelf of iets over de geschiedenis van het onderwerp vermeld wordt. geef voorbeelden. Een keuze: laten zien dat $N = 1$ en dat $N = 2$ niet een CG is ? (Dat werd voor het eerst bewezen door Fermat). Maak veel voorbeelden.
Suggestie: formuleer het vermoeden van Tunnell (1983) dat een (hypothetische, effectieve) beschrijving geeft van alle congruente getallen; zie [12], IV.4, Theorem op pag. 221; zie [37].

**(17.3) Reductie modulo $p$.** Zie [11], Ch. C; zie [12], Ch. I, §9; zie [31], A.5. Formuleer opzet en resultaten. Laat zien wat er met een torsie-punt, en met een niet-torsie-punt gebeurt onder reductie modulo $p$. Geef voorbeelden, zowel waar $\mathcal{E} \bmod p$ singulier is, als waar die niet-singulier is. Formuleer en bewijs [11], V.3, Prop 5.6 (Pas op: de notatie $\mathbb{Z}_p$ bij Knapp staat voor $\mathbb{Z}/p = \mathbb{F}_p$). Geef toepassingen in de stijl van [11], page 131, voorbeelden. Bewijs dat voor $E = E_N$ gegeven door $Y^2 = X(X^2 - N^2)$ we hebben $\mathrm{Tors}(E_N(\mathbb{Q})) = (\mathbb{Z}/2)^2$ (we gebruiken dat in (17.2)).

**(17.4) De stelling van Nagell-Lutz.** Geef een bewijs van deze stelling. Geef vooral ook voorbeelden. Zie [31], II.4 / II.5 voor een iets zwakkere vorm (die ik ook voldoende zou

vinden), met de sterkere vorm in de vraagstukken bij [31]. Zie [11], V,4. – Benadruk dat deze stelling gaat over elliptische krommen over $\mathbb{Q}$ maar dat de gekozen vergelijking een rol speelt.

**(17.5) De stelling van Mordell.** Geef een bewijs van deze stelling. Waarschijnlijk is het materiaal te veel voor één voordracht. Deel goed in. Leg basis-begrippen uit, en vermeld als "black boxes" wat je niet bewijzen kunt. In [31] staat een bewijs van het speciale geval dat $E(\mathbb{Q})[2] \neq 0$. Zie ook [11]. Zie [29], VIII.4.

**Opmerking.** De stelling van Mordell kan gegeneraliseerd worden (Weil) door in plaats van elliptische krommen abelse variëteiten en in plaats van $\mathbb{Q}$ een eindige uitbreiding van $\mathbb{Q}$ te kiezen. Dit onderwerp valt ver buiten het bereik van dit project.

**(17.6) De rang van een elliptische kromme over $\mathbb{Q}$.** Voor een elliptische kromme $E$ over $K = \mathbb{Q}$ weten we (de stelling van Mordell) dat er een geheel getal $r = r(E) \in \mathbb{Z}_{\geq 0}$ bestaat zodanig dat

$$E(\mathbb{Q}) \cong \mathrm{Tors}(E) \times E^r$$

(en het gehele getal $r$ is door $E$ en $K$ eenduidig bepaald); het getal $r$ wordt de *rang* van de elliptische kromme genoemd. Zie (21.4): het is niet bekend of de rang begrensd is. Laat in deze voordracht zien dat er elliptische krommen over $\mathbb{Q}$ bestaan waarvan de rang minstens 9 is (methode van Néron: geen expliciete berekening, "pure thought", een existentie wordt bewezen, maar dit is niet niet een constructief bewijs). Zie [22]; [28], 11.2 – 11.4; [34].

**(17.7) De rang van een elliptische kromme over $\mathbb{Q}$, bis.** In plaats van het vorige onderwerp kan ook het volgende gedaan worden. Bij een gegeven elliptische kromme $E$ over $K = \mathbb{Q}$ kunnen we een bovengrens geven voor $r(E)$ in termen van de plaatsen van slechte reductie. In speciale gevallen is die grens klein. Geef een discussie, bewijzen, en laat zien dat $N = 1$ niet een congruent getal is. Zie [11], IV,7.

**(17.8) De rang van een elliptische kromme over een functie lichaam in karakteristiek $p$.** Er is een analogie tussen enerzijds een ring als $\mathbb{Z}$ of werken over $\mathbb{Q}$, de *arithmetische situatie*, en anderzijds (een orde in) een functie lichaam over een eindig lichaam, de *meetkundige situatie*. In die analogie kunnen we niet zo maar een bewijs in het ene systeem overplanten in het andere, maar we kunnen wel proberen meer gevoel en inzicht te krijgen in de arithmetiek door de meetkundige situatie te beschouwen. In [33], Th. 2 wordt aangetoond dat "the rank may take arbitrarily large values". (Pas op, dat bewijs kan niet overgezet worden op de arithmetische situatie, althans dat hebben velen vaak geprobeerd, en het is tot nu toe niet gelukt.)

**(17.9) De Hasse (-Weil-Serre) grenzen.** Geef een bewijs van (8.4). Zoek literatuur op. Doe dit alleen voor $g = 1$, of ook voor hoger geslacht. Geef motivatie. Geef voorbeelden. Geef zorgvuldige bewijzen.

**(17.10) Voorbeeld van Selmer.** Behandel een voorbeeld van een kromme $C \subset \mathbb{P}^2_{\mathbb{Q}}$ over $\mathbb{Q}$ die over een uitbreidingslichaam van $\mathbb{Q}$ wel een elliptische kromme is, maar over $\mathbb{Q}$ niet een $\mathbb{Q}$ rationaal punt heeft: $\mathcal{Z}(3X^3 + 4Y^3 + 5Z^3) \subset \mathbb{P}^2_{\mathbb{Q}}$. Behandel het feit dat deze kromme een $\mathbb{R}$-rationaal punt heeft, en ook voor elke $m > 1$ een rationaal punt heeft over $\mathbb{Z}/m$. Zeg iets over het Hasse principe. Zie [25].

**(17.11) Elliptic divisibility sequences.** Neem een elliptische kromme $E$ over $\mathbb{Q}$, in Weierstrass normaalvorm. Een punt $T \in E(\mathbb{Q})$ kan geschreven worden als $T = (a/b, d/e)$ met $\text{ggd}(a,b) = 1$ en $\text{ggd}(d,e) = 1$ en $b > 0, e > 0$; bewijs: dan is er een $c \in \mathbb{Z}_{>0}$ met $b = c^2$ en $e = c^3$.

Neem een punt $P \in E(\mathbb{Q})$ van oneindige orde. Voor elke $n \in \mathbb{Z}_{>0}$ kunnen we schrijven

$$nP \quad = \quad (\frac{a_n}{C_n^2}, \ \frac{d_n}{C_n^3}), \quad \text{ggd}(a_n, C_n) = 1, \ \text{ggd}(d_n, C_n).$$

De rij $\{C_n \mid n \in \mathbb{Z}_{>0}\}$ is een EDS (Elliptic divisibility sequence, elliptische deelbaarheids rij); voor een algemenere definitie zie de opgegeven referenties. Beschrijf eigenschappen van zulke rijen, en formuleer vragen. Leg verband met Fibonacci getallen, met Lucas getallen. Zie [35], [5],
R. Shipsey. Elliptic divisibility sequences. PhD thesis, Goldsmith's College (University of London), 2000,
C. Swart. Sequences related to elliptic curves. PhD thesis, Royal Holloway (University of London), 2003.
`http://en.wikipedia.org/wiki/Elliptic_divisibility_sequence`
`http://www.crm.umontreal.ca/Crypto10/pdf/Miller_slides.pdf`
`http://en.wikipedia.org/wiki/Fibonacci_number`
`http://en.wikipedia.org/wiki/Fibonacci_prime`

**(17.12) Factorizatie.** Leg het RSA cryptosysteem uit (in 1977 ontworpen door Ron Rivest, Adi Shamir en Len Adleman). Motiveer hiermee de vraag naar factorizatie van gehele getallen. Leg daarna het factorizatie algoritme uit dat elliptische krommen gebruikt; zie bv. [31], IV.4. Of zie: [13], [14]. Google de namen René Schoof, Hendrik Lenstra.

**(17.13) Het klassegetal $= 1$ probleem.** Dit onderwerp is niet eenvoudig. Maar al het vertellen van een deel, van de geschiedenis, van bijzondere gevallen is prachtig! Fascinerende ontwikkelingen vanaf Gauss tot in de 20-ste eeuw.

Vertel wat een klassegetal is. Vertel (bewijs) dat $h = 1$ hetzelfde is als het bestaan van unieke factorizatie. Geef voorbeelden (al bekend aan Gauss). Bewijs van tenminste één geval dat $h = 1$. Lees [28], Appendix, pp.188 – 199, of [72] voor een overzicht. Litteratuur in [28] en in de literatuurlijst hieronder. Maak een keuze wat binnen het bereik van een voordracht valt.

# 18 Notaties

Voor een abelse groep $A$ en $n \in \mathbb{Z}$ schrijven we $A[n]$ voor de kern van $\times n : A \to A$.
$\square$: einde van een bewijs, of het ontbreken van een bewijs.
desda: dan en slechts dan als.

We schrijven $K$ voor een lichaam, dat in vele gevallen het basis-lichaam is. We denken daar vaak aan: $\mathbb{Q}$, of een eindig lichaam, maar ook aan $\mathbb{R}$, of $\mathbb{C}$. We schrijven $k$ als we te maken hebben met een *algebraïsch afgesloten lichaam*. Soms gebruiken we $\Omega$ voor een algebraïsch afgesloten lichaam. We schrijven $\mathbb{F} := \overline{\mathbb{F}_p}$ als het priemgetal $p$ vastligt.

Voor $n \in \mathbb{Z}_{>0}$ schrijven we $\mathbb{Z}/n$ voor de verzameling van restklassen van gehele getallen modulo $n$. De notatie $\mathbb{Z}/n\mathbb{Z}$ en de notatie $\mathbb{Z}/(n)$ zijn nauwkeuriger, maar ik verkies de verkort schrijfwijze $\mathbb{Z}/n$.

Pas op: sommige auteurs gebruiken $\mathbb{Z}_n$ voor dit begrip, zie bv. [11]. Ook wordt wel $C_n$ gebruikt (C = cyclisch); in dat geval is dit een cyclische groep van orde $n$ met een voortbrenger gemarkeerd . De notatie $\mathbb{Z}_n$, sommige topologen gebruiken dit, is verwarrend: een algebraïcus, of iemand die getaltheorie doet gebruikt $\mathbb{Z}_p$ voor de ring van $p$-adische getallen. (Ik zal een voorval vertellen waar dit tot grote verwarring leidde.)

We schrijven $a \equiv b \pmod{n}$ als $a$, $b$ en $n$ gehele getallen zijn zo dat $a - b$ deelbaar is door $n$. De schrijfwijze $a \equiv b \bmod n$ is niet juist. De notatie $a \bmod n$ wordt gebruikt voor de restklasse van $a$ in $\mathbb{Z}/n$. We zien dat $a \equiv b \pmod{n}$ hetzelfde is als $a \bmod n = b \bmod n$.

Maak goed onderscheid tussen de notatie $E$, gebruikt voor een elliptische kromme over een lichaam, en $\mathcal{E}$, gebruikt voor een kromme over een ring, zie § 7. We zullen uitleggen waarom voor een elliptische kromme $E$ over $\mathbb{Q}$ de notatie $E(\mathbb{Z})$ niet gebruikt mag worden.

Als $R_1 \to R_2$ een ring homomorfisme is, en $\mathcal{E}$ is over $R_1$ gedefinieerd, dan schrijven we $\mathcal{E} \otimes R_2$ voor de kromme gegeven door diezelfde vergelijking, maar nu beschouwd over $R_2$. Gevallen die veel voorkomen: $R_1 = K$ en $R_2 = L$ zijn lichamen; ook: $R = \mathbb{Z}$ en $R = \mathbb{Z} \to \mathbb{Z}/p = \mathbb{F}_p = R_2$.

Als we werken over een lichaam van karakteristiek $p > 0$ en we schrijven b.v. $5X^2$ dan bedoelen we $(5 \bmod p) \cdot X^2$, d.w.z. de coëfficient 5 bedoelen we modulo $p$, maar de exponent is het gehele getal 2. Een schrijfwijze als $\overline{5}X^2$ zou zuiverder zijn.

## 19 Checklist

Hieronder een opsomming van een paar onderwerpen. Van studenten die dit project volgen wordt verwacht dat ze vóór begin januari 2014 deze onderwerpen kennen: in staat zijn definities, stellingen, constructies en bewijzen zelfstandig te kunnen reproduceren. Deze activiteit is pas echt zinvol als je deze onderwerpen in alle details beheerst.

- De stelling die zegt dat een positief geheel getal op één manier te schrijven is als product van priemgetallen, eenduidig op volgorde van die factoren; het is van belang dat je die stelling en een bewijs ervan kunt reproduceren; dat je ook weet dat er in andere getal systemen (in andere ringen) een equivalent van die stelling niet geldt.
- Definitie van de discriminant van een polynoom in één variabele; methode om van een gegeven polynoom van willekeurige graad de discriminant te berekenen.
- Definitie van $\mathbb{A}^n_K$, van $\mathbb{P}^n_K$.
- Definitie van een elliptische kromme, en van een constructie van de groepswet op een elliptische kromme.
- Formules voor de raaklijn van een vlakke kromme in een punt, eigenschappen daarvan, definitie van een buigpunt.

- Zien hoe je bij een $P \in E(K)$ het derde snijpunt van $\mathfrak{t}_{E,P}$ met $E$ uitrekent. Voorbeelden uitwerken!
- Begrijp de uitspraken over complexe uniformizatie, §4. Begrijp de topologie van $E(\mathbb{C})$.
- Ken de structuurstellingen over eindige lichamen.
- Formulering van de stelling van Bezout, van de stelling van Poncelet, van de stelling van Nagell-Lutz.
- Begrijp iets van elliptische krommen over eindige lichamen. Ken tenminste één voorbeeld van het ontbreken of het bestaan van punten van orde $p$ over een eindig lichaam van karakteristiek $p$.

## 20 Eindigheidsstellingen*

In deze paragraaf geven we een paar stellingen, die het hart vormen van moderne ontwikkelingen. Dit materiaal valt ver buiten het bereik van dit college. Elk van de onderstaande stellingen is diep; zelfs in heel "eenvoudige gevallen" valt de gevraagde eindigheid niet elementair of gemakkelijk te bewijzen. Elk van de stellingen kan ook geformuleerd worden en is juist over een getallenlichaam.

De stelling (20.4) past bij dit college, maar vormt er geen onderdeel van. Materiaal in deze paragraaf dient om die stelling tegen een algemenere achtergrond te plaatsen. – Verdere toelichting en/of verwijzingen geef ik graag.

**(20.1) Stelling** (Siegel, 1929). *Zij $n \in \mathbb{Z}_{>0}$. Bekijk de ring $\mathbb{Z}[1/n]$. Zij $\mathbb{Z}[1/n]^*$ de groep van eenheden daarin; met andere woorden:*

$$\mathbb{Z}[1/n]^* = \{\lambda = \frac{a}{b} \mid a, b \in \mathbb{Z}, \quad \exists m : a | n^m, \quad b | n^m\};$$

in de noemer en de teller van $\lambda$ komen alleen maar priem-factoren voor die in de priemontbinding van $n$ voorkomen. *De verzameling*

$$\{\lambda \mid \lambda \in \mathbb{Z}[1/n]^*, 1 - \lambda \in \mathbb{Z}[1/n]^*\}$$

*is eindig.* □

**Opmerking.** De verzameling van priemgetallen die $n$ deelt wordt wel met $S$ aangegeven, de stelling wordt wel de stelling van de $S$-eenheden genoemd. Merk op dat $\Gamma := \mathbb{Z}[1/n]^*$ een oneindige groep is, en dat de stelling gaat over de eindigheid van $\Gamma \cap (1 - \Gamma)$. De ring $\mathbb{Z}[1/n]^*$ wordt wel genoteerd als $\mathcal{O}_{\mathbb{Q},S}$.

Voor elke $[K : \mathbb{Q}] < \infty$ en elke eindige verzameling $S$ van discrete valuaties op $K$ geldt de analoge eindigheidsstelling.

**(20.2) Opmerking.** Omdat $n > 1$ is er tenminste één priemgetal dat $n$ deelt. Daarom kunnen we de verzameling $\mathbb{Z}[1/n]^*$ zien als "reguliere functies" op $\mathbb{P}^1 - \{0, \infty, p \mid p \text{ deelt } n\}$. Een dergelijke algebraïsche kromme (een $\mathbb{P}^1$ minus minstens drie punten) wordt wel een hyperbolische kromme genoemd; vanuit dit gezichtspunt valt deze kromme en de arithmetiek daarop onder het "Mordell vermoeden" bewezen door Faltings in 1983. Dat gaf ook een nieuwe bewijs van de stelling van Siegel. Dit plaatst dit (vroeger voor mij mysterieuze) resultaat in een breder kader.

**(20.3) Voorbeeld.** Een bewijs van bovenstaande stelling is lastig, ook in concrete gevallen. Neem $n = 30$, d.w.z. $S = \{2, 3, 5\}$. Merk op dat

$$\lambda = \frac{1}{2},\ \frac{2}{3},\ \frac{3}{4},\ \frac{4}{5},\ \frac{5}{6},\ \frac{8}{9},\ \frac{15}{16},\ \frac{24}{25},\ \frac{80}{81}, \cdots ??$$

voldoen. Er zijn er nog meer, b.v. 2/5, 3/5, 5/8, 25/27 etc. ? Hoe bewijs je eindigheid al in dit concrete geval?

**(20.4) Stelling** (Siegel, 1929). *Zij $f \in \mathbb{Z}[X, Y]$ zodat dit een Weierstrass vergelijking geeft van een elliptische kromme $E$ over $\mathbb{Q}$. Schrijf $\mathcal{E}^0 = \mathcal{Z}(f)$; dit is de affiene kromme over $\mathbb{Z}$ verkregen door $[0 : 1 : 0]$ uit $\mathcal{E}$ te verwijderen. Dan is $\mathcal{E}^0(\mathbb{Z})$ eindig.* □

Zelfde opmerking als in (20.2): een elliptische kromme waaruit we tenminste één punt weglaten is hyperbolisch; ook hier gaf het resultaat van Faltings een nieuw bewijs.

**(20.5) Voorbeeld.** Zij $\mathcal{E}^0$ gegeven door $Y^2 = X^3 + 17$. Dan bestaat $\mathcal{E}^0(\mathbb{Z})$ uit de punten

$$\{(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23), (43, \pm 228), (52, \pm 375), (5234) \pm 378661\}.$$

Het resultaat in dit voorbeeld werd al bewezen door Nagell (1930). Voor de verwijzing, en voor nog meer resultaten, zie [21], § 26; in het bijzonder zie [21], 26.4.
**Opmerkingen.** Voor de elliptische kromme $\mathcal{E}$ gegeven over $\mathbb{Q}$ door $Y^2 = X^3 + 17$ geldt dat $E(\mathbb{Q}) =< (-2, 3), (2, 5) >$, een torsie-vrije groep van rang 2; zie [29], III.2, Exa. 2.4. Het is lastig om zulke resultaten te bewijzen. Omdat de rang positief is zijn er (heel veel) punten in $\mathcal{E}(\mathbb{Q})$ waarvan de coördinaten niet geheel zijn (maak voorbeelden).

De discriminant van $\mathcal{E}$ gegeven door $Y^2 = X^3 + 17$ is gelijk aan $2^4 \cdot 3^3 \cdot 17$.

Elliptische krommen gegeven door $Y^2 = X^3 + k$ met $k \in \mathbb{Z}$ hebben veel aandacht gekregen. Zie ook [31], Exerc. 1.18 op pag. 36; [29], Exa. 7.3 op pag. 268.

Merk op dat dit een stelling is over de kromme $\mathcal{E}^0$, die gegeven wordt door deze expliciete vergelijking, en niet over de kromme $E$. De vergelijking die $\mathcal{E}^0$ geeft (of te wel: het gekozen coördinaten systeem) is van belang. Voor elke ander keuze van een vergelijking die ook $E$ geeft krijgen we weliswaar weer eindigheid, maar mogelijk een heel andere verzameling. (Maak zelf een voorbeeld in dit geval.)

**(20.6) Vraagstuk.** We geven $E$ over $\mathbb{Q}$ door de vergelijking $Y^2 = X^3 + k$, met $k \in \mathbb{Q}$ en $k \neq 0$. We kiezen $P \in E(\mathbb{Q})$ (en merken op dat het best kan gebeuren dat in dit coördinaten-systeem er noemers kunnen optreden). Kies een nieuw coördinaten-systeem (afhankelijk van de keuze van $P$) en daarin een vergelijking die $E$ over $\mathbb{Q}$ definiëert, zodanig dat deze gekozen $P \in E(\mathbb{Q})$ in dat coördinaten-systeem gehele coördinaten heeft.

**(20.7) Vermoeden** (Mordell, 1922) **Stelling** (Faltings, 1983). *Zij $[K : \mathbb{Q}] < \infty$. Zij $C$ een niet-singuliere kromme van geslacht minstens 2 over $K$. Dan is*

$$\#(C(K)) < \infty.$$

□

**Opmerking.** Voor een kromme $\mathcal{C}$ over een ring zoals $R = \mathcal{O}_{K,S}$, met $\mathcal{C} \otimes K$ van geslacht minstens twee, volgt eindigheid van $\mathcal{C}(R)$ uit eindigheid van $C(K)$. Hier hoeven we een formulering over $R$ niet te kiezen in deze stelling.

**(20.8) Voorbeeld.** Zij $n \in \mathbb{Z}_{>3}$. Zij

$$C = \mathcal{Z}(X^n + Y^n - Z^n) \subset \mathbb{P}^2_K.$$

Dan is $\mathrm{g}(C) = (n-1)(n-2)/2 \geq 2$. We zien dat het aantal primitieve oplossingen van elke Fermat vergelijking eindig is; dit was de eerste keer in de geschiedenis dat dit in deze algemeenheid bewezen wordt. Later bewees Wiles (1995) FLT: er zijn geen oplossingen met $xyz \neq 0$.

Voor $n = 3$ valt de kromme niet onder de stelling van Faltings, maar reeds lang geleden bewees Euler dat het Fermat vermoeden waar is in dat geval: we krijgen een elliptische kromme over $\mathbb{Q}$ van rang 0.

**(20.9) Opmerking, g=0;** Stelling (20.1) gaat over de kromme $\mathbb{P}^1_R - \{0, 1, \infty\}$.
**g=1;** Stelling (20.4) gaat over een kromme $\mathcal{E} - \{\infty\}$.
**g $\geq$ 1.** Stelling (20.7) gaat over een kromme $C$ van geslacht minstens twee.

Het blijkt dat *meetkundige informatie*, in alle drie gevallen is de kromme "hyperbolisch", *arithmetische gevolgen* heeft. Deze opmerking plaatst deze drie diepe stelling in een perspectief. Inderdaad zijn de eerste twee stellingen ook te bewijzen met de methodes van Faltings.

**(20.10) Opmerking.** Deze eindigheidsstellingen zijn vaak niet zo handig om alle oplossingen ook echt te vinden. Bij voorbeeld, bij gegeven $C$ over $K$ zoals in (20.7) kan er een bovengrens berekend worden voor $\#(C(K))$. Veel helpt dat niet, want die grens is meestal niet scherp, en er is geen a priori informatie "hoe groot"de oplossingen zijn; we kunnen niet (voor zover bekend) a priori de rekentijd begrenzen nodig om alle oplossingen te vinden. Voor (20.1) zijn er wel effectieve grenzen; zie b.v. [29], IX.5. Deze stellingen, met moeilijke bewijzen, vormen eigenlijk nog een mysterie.

# 21 Open problemen, vragen

Zoek met google theorie, open problemen en nog veel meer op.
Voorbeeld: google <Mordell-Weil> en
`http://en.wikipedia.org/wiki/Mordell%E2%80%93Weil_theorem` komt boven. Etc. In dit gebied zijn er nog heel veel open vragen. Hier formuleer ik een paar daarvan (en deze problemen zijn echt lastig).

**(21.1) Open probleem.** Waar we helaas niet aan toekomen: het ABC vermoeden, het Szpiro vermoeden, en verbanden daar tussen.

**(21.2) Open probleem.** Het is bekend dat elke elliptische kromme over $\mathbb{Q}$ een "sterke Weil kromme" is (d.w.z. een parametrisatie met een modulaire kromme toelaat, Wiles, etc). Dit was de sleutel, bewezen door Andrew Wiles, voor een bewijs van het Fermat vermoeden. Kunnen we een effectieve grens geven op de graad van een dergelijke minimale parametrisatie? Dit lijkt een lastig, open probleem.

**(21.3) Open probleem.** Geef een effectieve methode om te bepalen of een positief geheel getal een congruent getal is; zie § 9.

Toelichting: we kunnen een (oneindige) lijst van álle congruente getallen maken; kunnen we van te voren bepalen wanneer een dergelijk getal voorkomt? Kunnen we van te voren bepalen (als functie van $N$) hoe lang we moeten zoeken om te beslissen of een gegeven getal $N$ congruent is?

**(21.4) Open probleem: is de rang begrensd?** Beschouw de verzameling van alle elliptische krommen over $K = \mathbb{Q}$ en beschouw de verzameling van alle getallen $r$ die als rang kunnen optreden. Is deze verzameling begrensd?

Experimenten en berekeningen hebben al een vrij grote rang laten zien; zie [24]; de literatuur hierover is heel groot.

Het antwoord op deze vraag is niet bekend, en eigenlijk weten we niet wat we verwachten. Soms lijkt het dat we steeds grotere getallen vinden, dan weer geven overwegingen aan dat de rang best eens begrensd zou kunnen zijn. Een intrigerend, moeilijk probleem. Er is veel over geschreven, veel over nagedacht (en eigenlijk weten we niet waar we moeten beginnen). Berekeningen geven krommen met een hoge rang (elke keer gaat die grens weer omhoog; die berekeningen zijn slim en formidabel).

**(21.5) Open probleem.** Zoek op: het vermoeden van Birch en Swinnerton-Dyer (een van de grote open problemen nu, zie de Millenium problemen).
`http://www.claymath.org/millennium/`

## Referenties


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

[2] J. Cassels – *Diophantine equations with special reference to elliptic curves.* Survey article. Journ. London Math. Soc. **41** (1966), 193–291.

[3] L. Candelori – *Modular curves and Mazur's theorem.* PhD-thesis Harvard University, 2008.
`http://www.math.mcgill.ca/candelori/ThesisFinal.pdf`

[4] J. Cassels – *Lectures on elliptic curves.* London Mathematical Society Student Texts, 24. Cambridge University Press, Cambridge, 1991.

[5] G. Everest, A. van der Poorten, I. Shparlinski & T. Ward – *Recurrence sequences.* Mathematical Surveys and Monographs, 104. American Mathematical Society, Providence, RI, 2003.

[6] L. Flatto – *Poncelet's theorem.* AMS, 2009

[7] G. Frey – *Some aspects of the theory of elliptic curves over number fields.* Expos. Math. **4** (1986), 35–66

[8] G. Frey – *Links between stable elliptic curves and certain Diophantine equations.* Ann. Univ. Sarav. Ser. Math. **1** (1986), 1–40. Frey, Gerhard Some aspects of the theory of elliptic curves over number fields. Exposition. Math. **4** (1986), 35–66.

[9] Guide to elliptic curve cryptography (Springer Professional Computing) by Darrel Hankerson, Alfred Menezes, and Scott Vanstone (Dit heb ik niet gezien.)
`http://www.cacr.math.uwaterloo.ca/ecc/`

[10] D. Husemöller – *Elliptic curves.* Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Graduate Texts in Mathematics 111. Springer-Verlag, New York, 2004.

[11] Knapp, A. – *Elliptic curves.* Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[12] N. Koblitz – *Introduction to elliptic curves and modular forms.* Second edition. Graduate Texts in Mathematics 97. Springer-Verlag, New York, 1993.

[13] N. Koblitz – *A course in number theory and cryptography.* Second edition. Graduate Texts in Mathematics 114. Springer-Verlag, New York, 1994.

[14] N. Koblitz & A. Menezes – *A survey of public-key cryptosystems.* SIAM Rev. **46** (2004), no. 4, 599-634 (electronic).

[15] D. S. Kubert – *Universal bounds on the torsion of elliptic curves.* Proc. London Math. Soc. **33** (1976), 193–237.

[16] B. Mazur – *Modular curves and the Eisenstein ideal.* Publ. Math. IHÉS **47** (1977), 33 – 186,

[17] B. Mazur – *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. **44** (1978), 129–162.

[18] B. Mazur & Tate, J. – *Points of order* 13 *on elliptic curves.* Invent. Math. **22** (1973/74), 41–49.

[19] J. Milne – *Elliptic curves.* Kea books. BookSurge Publishers, Charleston, SC, 2006.

[20] L. Mordell – *On the rational solutions of indeterminate equations of the third and the fourth degree.* Proceed. Cambridge Philosoph. Soc. **21**. 1922/1923, 179–192.

[21] L. Mordell – *Diophantine equations.* Pure and Applied Mathematics, Vol. 30 Academic Press, 1969.

[22] A. Néron – *Propriétés arithmétiques de certaines familles de courbes algébriques.* Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, Vol. III, pp. 481-488, Noordhoff N.V., Groningen; North-Holland Publishing Co., Amsterdam, 1956.

[23] A. Ogg – *Abelian curves of* 2*-power conductor.* Proc. Cambridge Philos. Soc. **62** (1966), 143–148.

[24] K. Rubin & A. Silverberg – *Ranks of elliptic curves.* Bull. AMS (New Series) **39** (2002), 455–474.

[25] E. Selmer – *The diophantine equation* $ax^3+by^3+cz^3 = 0$. Acta Math. **85** (1951), 203–362. Zie b.v.
`https//www.math.lsu.edu/~verrill/teaching/math7280/`
of, google <verril teaching>
`selmer_example/selmer_example.pdf`

[26] E. Selmer – *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Completion of the tables.* Acta Math. **92** (1954), 191–197.

[27] J-P. Serre – *Nombre de points des courbes algébriques sur* $\mathbb{F}_q$. Sém. de Théorie des Nombres de Bordeaux , Exp. no. 22. (= Oeuvres III, No. 129, pp. 664-668), (1982/83).

[28] J-P. Serre – *Lectures on the Mordell-Weil theorem.* Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[29] J. Silverman – *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[30] J. Silverman – *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[31] J. Silverman & J. Tate – *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[32] J. Tate – *The arithmetic of elliptic curves.* Invent. Math. **23** (1974), 179–206.

[33] J. Tate & I. Shafarevich – *The rank of elliptic curves.* Soviet Math. Dokl. **8** (1967), 917 – 920. [Dokl. Akad.Nauk **175** (1967).]

[34] J. Top – *Néron's proof of the existence of elliptic curves over* $\mathbb{Q}$ *with rank at least* 11. Utrecht Preprint 476, July 1987.

[35] M. Ward - *Memoir on elliptic divisibility sequences.* Amer. J. Math. **70** (1948), 31–74.

**Literatuur over congruente getallen.**

[36] F. Oort - *Congruent numbers in the tenth and in the twentieth century.* In: Vrolijk, Arnoud & Jan P. Hogendijk (eds.), O ye Gentlemen: Arabic Studies on Science and Literary Culture, in Honour of Remke Kruk. - Leiden [etc.]: Brill, 2007; pp. 77– 97.

[37] F. Oort – *Congruente getallen.* Syllabus bij de Kaleidoscoop voordracht 10-II-2009. `http://www.staff.science.uu.nl/~oort0109/`
Zie voor verdere literatuurverwijzingen daarin.

**Enige literatuur over algebra.**

[38] S. Lang – *Algebra.* Third edition. Addison-Wesley, 1993.

[39] B. L. van der Waarden – *Moderne Algebra.* Eerste uitgave in 1931. Vierde uitgave: Heidelberger Taschenbuch, 2 delen, Springer-Verlag, 1967.

**Enige literatuur over algebraïsche getaltheorie en over commutatieve algebra.**

[40] M. Atiyah & I. Macdonald – *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969

[41] N. Bourbaki – *Algèbre commutative.* Ch. 1 & 2. Act. sc. indust. 1290. Hermann, 1961

[42] D. Eisenbud – *Commutative algebra.* With a view toward algebraic geometry. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[43] S. Lang – *Algebraic number theory.* Grad. Texts Math., Springer-Verlag, 1986.

[44] H. Matsumura – *Commutative algebra.* W. A. Benjamin, Inc., New York 1970 xii+262 pp. paperbound.

[45] J-P. Serre – *Cours d'arithmétique.* Presses Univ. Paris, 1970.

[46] J-P. Serre – *Topics in Galois theory.* Lecture notes prepared by Henri Darmon. With a foreword by Darmon and the author. Research Notes in Mathematics, 1. Jones and Bartlett Publishers, Boston, MA, 1992.

[47] I. Stewart & D. Tall – *Algebraic number theory.* Second edition. Chapman and Hall Mathematics Series. Chapman & Hall, London, 1987.

[48] E. Weiss – *Algebraic number theory.* McGraw-Hill Book Co., Inc., 1963

**Enige literatuur over algebraïsche meetkunde.**

[49] W. Fulton – *Algebraic curves.* An introduction to algebraic geometry. Notes written with the collaboration of Richard Weiss. Reprint of 1969 original. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[50] U. Görtz & T. Wedhorn – *Algebraic Geometry, I.* Schemes, with examples and exercises. Vieweg+Teubner, 2010.

[51] P. Griffiths & J. Harris – *Principles of algebraic geometry.* Reprint of the 1978 original. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1994.

[52] J. Harris – *Algebraic geometry.* A first course. Corrected reprint of the 1992 original. Graduate Texts in Mathematics, 133. Springer-Verlag, New York, 1995.

[53] R. Hartshorne – *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. Meestal geciteerd als HAG.

[54] H. Lange & C. Birkenhake – *Complex abelian varieties.* Second edition. Grundlehren der Mathematischen Wissenschaften, 302. Springer-Verlag, Berlin, 2004.

[55] D. Mumford – *The red book of varieties and schemes.* Second, expanded edition. Includes the Michigan lectures (1974) on curves and their Jacobians. With contributions by Enrico Arbarello. Lect. Notes in Math. 1358. Springer-Verlag, Berlin, 1999.

[56] D. Mumford – *Abelian varieties.* With appendices by C. P. Ramanujam and Yuri Manin. Corrected reprint of the second (1974) edition. Tata Institute of Fundamental Research Studies in Mathematics, 5. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008.

[57] Mumford, D. *Algebraic geometry. I. Complex projective varieties.* Reprint of the 1976 edition. Classics in mathematics. Springer-Verlag, Berlin, 1995.

[58] J-P. Serre – *Cohomologie galoisienne.* Lect. Notes Math. **5**, Springer-Verlag 1964.

[59] J-P. Serre – *Faisceaux algébriques cohérents.* Ann. of Math. **61** (1955). 197-278.

[60] I. Shafarevich – *Basic algebraic geometry. 1.* Varieties in projective space.
I. Shafarevich – *Basic algebraic geometry. 2.* Schemes and complex manifolds. Second edition. Translated from the 1988 Russian edition by Miles Reid. Springer-Verlag, Berlin, 1994.

[61] B. van der Waerden – *Einführung in die algebraische Geometrie.* Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Vol. 51. Berlin, Springer, 1939.

[62] R. Walker – *Algebraic curves.* Dover Publications, Inc., New York 1962. Reprint of the 1950 edition. Springer-Verlag, New York-Heidelberg, 1978.

**Extra: het probleem van Emmy Noether, het omkeerprobleem van de Galois theorie:**

[63] H.W. Lenstra, Jr. – *Rational functions invariant under a finite abelian group.* Invent. Math. **25** (1974), 299–325.

[64] G. Malle & B. H. Matzat – *Inverse Galois theory.* Springer monogr. math. Springer, 1999.

[65] E. Noether – *Gleichungen mit vorgeschriebener Gruppe.* Math. Ann **78** (1918), 221–229.

[66] G. Swan – *Invariant rational functions and a problem of Steenrod.* Invent. Math. **7** (1969), pp. 148–158.

**Enige literatuur over het klassegetal = 1 probleem.**
Zie [28], Appendix, pp.188 – 199.

[67] K. Heegner – *Diophantische Analysis und Modulfunktionen.* Math. Z. **56** (1952). 227 – 253.

[68] H. Stark – *There is no tenth complex quadratic field with class-number one.* Proc. Nat. Acad. Sci.U.S.A. **57** (1967) 216 – 221.

[69] H. Stark – *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. J. **14** (1967), 1 – 27.

[70] H. Stark – *On the problem of unique factorization in complex quadratic fields.* 1967 Number Theory (Proc. Sympos. Pure Math, Vol. XII, Houston, Tex., 1967) pp. 41 – 56 Amer. Math. Soc., Providence, R.I.

[71] D. Goldfeld – *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **3** (1976), 624 – 663.

[72] D. Goldfeld – *Gauss's class number problem for imaginary quadratic fields.* Bull. Amer. Math. Soc. (N.S.) **13** (1985), 23 – 37. Mooi overzicht.

[73] R. Schoof & N. Tzanakis – *Integral points of a modular curve of level 11.* Te verschijnen in Acta Arithmetica. Zie
`http://www.mat.uniroma2.it/%7Eschoof/schoof_tzanakis_5.pdf`

Prof. Dr F. Oort
Mathematisch Instituut, kamer 501
email: f.oort@uu.nl
`http://www.staff.science.uu.nl/~oort0109/`
postadres: Pincetonplein 5
3584 CC Utrecht