Snelle algoritmen in de getaltheorie

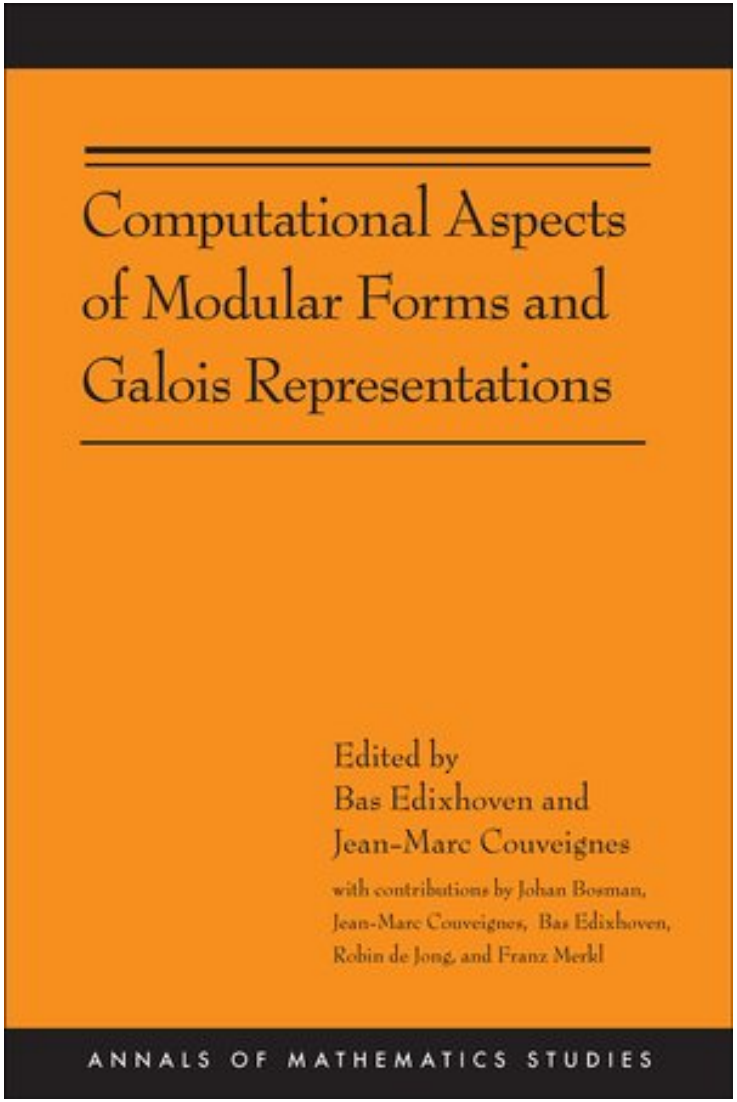
Bas Edixhoven

Universiteit Leiden

vacantiecursus CWI 2011

in samenwerking met Jean-Marc Couveignes, Robin de Jong, Johan Bosman, Franz Merkl, Peter Bruin, Ila Varma

Reclame


Computational Aspects
of Modular Forms and
Galois Representations
Edited by
Bas Edixhoven and
Jean-Marc Couveignes
with contributions by Johan Bosman,
Jean-Marc Couveignes, Bas Edixhoven,
Robin de Jong, and Franz Merkl
ANNALS OF MATHEMATICS STUDIES

Reclame, een citaat van Princeton Univ. Press:

Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices.

Reclame, een citaat van Princeton Univ. Press:

Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices. Their Fourier coefficients, with Ramanujan's tau-function as a typical example, have deep arithmetic significance.

Reclame, een citaat van Princeton Univ. Press:

Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices. Their Fourier coefficients, with Ramanujan's tau-function as a typical example, have deep arithmetic significance.

Prior to this book, the fastest known algorithms for computing these Fourier coefficients took exponential time, except in some special cases.

Reclame, een citaat van Princeton Univ. Press:

Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices. Their Fourier coefficients, with Ramanujan's tau-function as a typical example, have deep arithmetic significance.

Prior to this book, the fastest known algorithms for computing these Fourier coefficients took exponential time, except in some special cases. The case of elliptic curves (Schoof's algorithm) was at the birth of elliptic curve cryptography around 1985.

Reclame, een citaat van Princeton Univ. Press:

Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices. Their Fourier coefficients, with Ramanujan's tau-function as a typical example, have deep arithmetic significance.

Prior to this book, the fastest known algorithms for computing these Fourier coefficients took exponential time, except in some special cases. The case of elliptic curves (Schoof's algorithm) was at the birth of elliptic curve cryptography around 1985.

This book gives an algorithm for computing coefficients of modular forms of level one in polynomial time. For example, Ramanujan's tau of a prime number p can be computed in time bounded by a fixed power of the logarithm of p. . .

Terug naar wiskunde: sommen van kwadraten

Om de vooruitgang die gemaakt is in het boek en Peter Bruin's proefschrift te illutreren bekijken we het probleem om snel, voor d en n in $\mathbb{Z}$:

$$r_d(n) := \#\{x \in \mathbb{Z}^d : x_1^2 + \cdots + x_d^2 = n\}.$$

uit te rekenen.

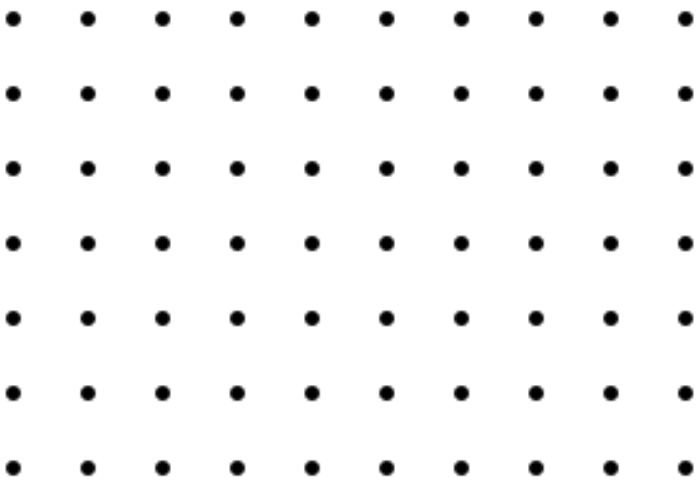
Terug naar wiskunde: sommen van kwadraten

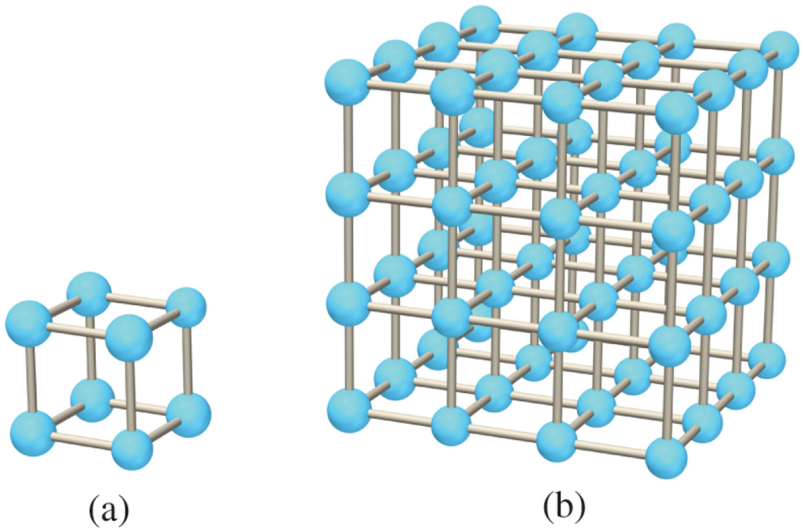
Om de vooruitgang die gemaakt is in het boek en Peter Bruin's proefschrift te illutreren bekijken we het probleem om snel, voor d en n in $\mathbb{Z}$:

$$r_d(n) := \#\{x \in \mathbb{Z}^d : x_1^2 + \cdots + x_d^2 = n\}.$$

uit te rekenen.

Meetkundige interpretatie (Pythagoras): bereken snel het aantal roosterpunten in $\mathbb{Z}^d$ op een gegeven afstand $\sqrt{n}$ van de oorsprong.



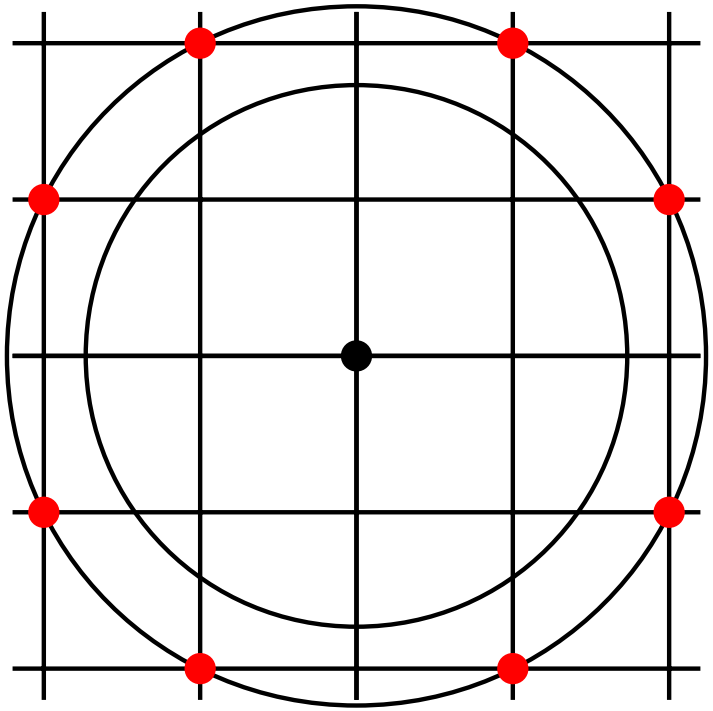


Sommen van kwadraten: een paar voorbeelden

$r_2(3) = 0.$

$r_2(5) = 8$:

$$5 = (\pm 2)^2 + (\pm 1)^2$$
$$5 = (\pm 1)^2 + (\pm 2)^2.$$



Dimensie één

Voor n in $\mathbb{Z}$, gegeven in het tweetallig stelsel, zeg, kan $r_1(n)$ uitgerekend worden in tijd hoogstens een macht van $\log(1 + |n|)$ (ongeveer het aantal cijfers van n).

Dimensie één

Voor n in $\mathbb{Z}$, gegeven in het tweetallig stelsel, zeg, kan $r_1(n)$ uitgerekend worden in tijd hoogstens een macht van $\log(1 + |n|)$ (ongeveer het aantal cijfers van n).

Als $n < 0$ dan $r_1(n) = 0$.

Dimensie één

Voor n in $\mathbb{Z}$, gegeven in het tweetallig stelsel, zeg, kan $r_1(n)$ uitgerekend worden in tijd hoogstens een macht van $\log(1 + |n|)$ (ongeveer het aantal cijfers van n).

Als $n < 0$ dan $r_1(n) = 0$.

Als $n = 0$ dan $r_1(n) = 1$.

Dimensie één

Voor n in $\mathbb{Z}$, gegeven in het tweetallig stelsel, zeg, kan $r_1(n)$ uitgerekend worden in tijd hoogstens een macht van $\log(1 + |n|)$ (ongeveer het aantal cijfers van n).

Als $n < 0$ dan $r_1(n) = 0$.

Als $n = 0$ dan $r_1(n) = 1$.

Als $n > 0$ en n is een kwadraat, dan $r_1(n) = 2$, en anders $r_1(n) = 0$. Gebruik de methode van bisectie van intervallen om $\sqrt{n}$ te benaderen, beginnend met $[0, n]$.

Dimensie één

Voor n in $\mathbb{Z}$, gegeven in het tweetallig stelsel, zeg, kan $r_1(n)$ uitgerekend worden in tijd hoogstens een macht van $\log(1 + |n|)$ (ongeveer het aantal cijfers van n).

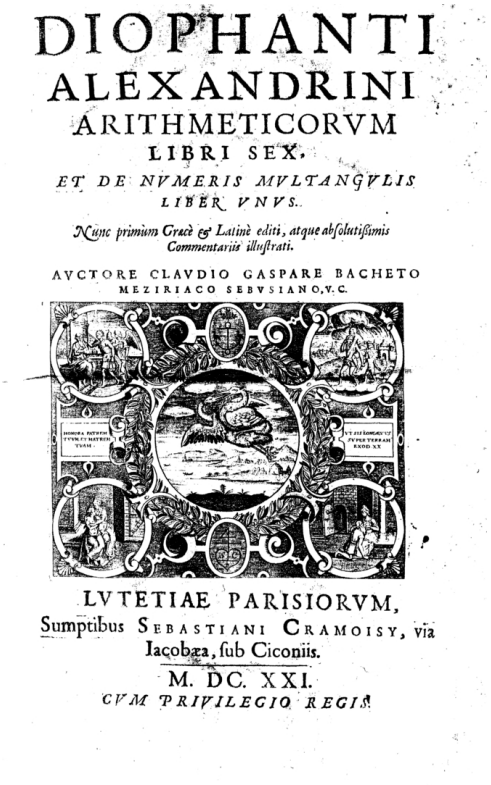
Als $n < 0$ dan $r_1(n) = 0$.

Als $n = 0$ dan $r_1(n) = 1$.

Als $n > 0$ en n is een kwadraat, dan $r_1(n) = 2$, en anders $r_1(n) = 0$. Gebruik de methode van bisectie van intervallen om $\sqrt{n}$ te benaderen, beginnend met $[0, n]$.

Gebruik *niet* de ontbinding van n in priemgetallen, want we weten niet hoe we die snel genoeg kunnen berekenen.

Dimensie twee: Diophantus



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.

AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V. C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diophantus van Alexandrië ($\approx$ 3rd eeuw):

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Dimensie twee: Fermat

Pierre de Fermat (jurist, Toulouse, 17e eeuw), voor $n \geq 1$: $r_2(n) \neq 0$ precies dan als iedere priemfactor van n die 3 modulo 4 is, een even aantal keer voorkomt in de factorisatie van n.

Dimensies 2 en 3: Legendre, Gauss

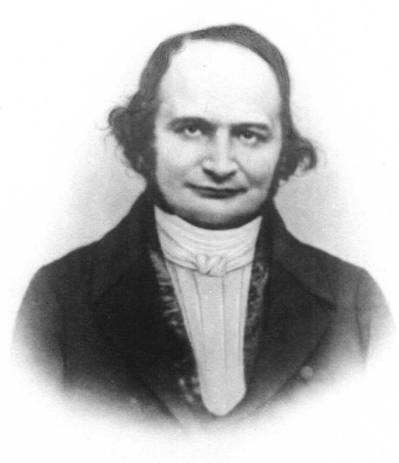
Adrien-Marie Legendre (1798) gaf een formule voor $r_2(2^a m^2)$.

Dimensies 2 en 3: Legendre, Gauss

Adrien-Marie Legendre (1798) gaf een formule voor $r_2(2^a m^2)$.

Carl Friedrich Gauss (1801) gaf een algemene formule voor $r_2(n)$, en een formule voor $r_3(n)$ die laat zien dat de $r_d(n)$ voor oneven d ingewikkelder zijn (in $r_3(n)$ komen “klassegetallen” voor).

Hogere even dimensies: Jacobi



Carl Gustav Jacob Jacobi (1829) bewees voor $n > 1$:

$$r_2(n) = 4 \sum_{d|n} \chi(d), \quad \text{met} \quad \chi(d) = \begin{cases} 0 \text{ als } d \text{ is even}, \\ 1 \text{ als } d = 4r+1, \\ -1 \text{ als } d = 4r+3, \end{cases}$$

Hogere even dimensies: Jacobi

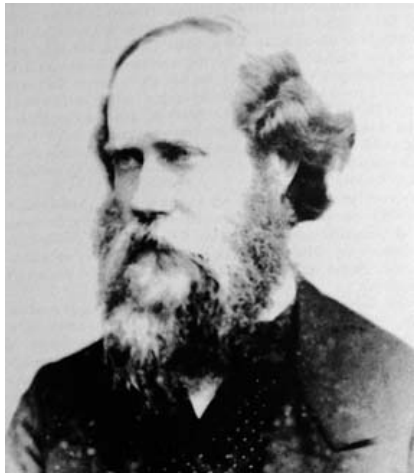
Carl Gustav Jacob Jacobi (1829) bewees voor $n > 1$:

$$r_2(n) = 4\sum_{d|n} \chi(d), \quad \text{met} \quad \chi(d) = \begin{cases} 0 \text{ als } d \text{ is even}, \\ 1 \text{ als } d = 4r+1, \\ -1 \text{ als } d = 4r+3, \end{cases}$$

en:

$$r_4(n) = 8\sum_{2\nmid d|n} d + 16 \sum_{2\nmid d|(n/2)} d.$$

Eisenstein, Smith



Het volgt uit werk van Jacobi, Ferdinand Eisenstein en Henry Smith dat:

$$r_6(n) = 16 \sum_{d|n} \chi(n/d) d^2 - 4 \sum_{d|n} \chi(d) d^2,$$

$$r_8(n) = 16 \sum_{d|n} d^3 - 32 \sum_{d|(n/2)} d^3 + 256 \sum_{d|(n/4)} d^3.$$

Dimensie 10: Liouville

Voor $d = 10$ vond Joseph Liouville (1865) een formule in termen van de gehele getallen $d = a + bi$ van Gauss met a en b in $\mathbb{Z}$:

$$r_{10}(n) = \frac{4}{5}\sum_{d|n}\chi(d)d^4 + \frac{64}{5}\sum_{d|n}\chi(n/d)d^4 + \frac{8}{5}\sum_{d\in\mathbb{Z}[i],\,|d|^2=n} d^4.$$

Dimensie 12: Glaisher, Ramanujan

James Whitbread Lee Glaisher, geïnterpreteerd door Srinivasa Ramanujan in 1916, bewees dat:

$$r_{12}(n) = 8 \sum_{d|n} d^5 - 512 \sum_{d|(n/4)} d^5 + 16 a_n$$

Dimensie 12: Glaisher, Ramanujan

James Whitbread Lee Glaisher, geïnterpreteerd door Srinivasa Ramanujan in 1916, bewees dat:

$$r_{12}(n) = 8 \sum_{d|n} d^5 - 512 \sum_{d|(n/4)} d^5 + 16 a_n$$

waar:

$$\sum_{n \geq 1} a_n q^n = q \prod_{m \geq 1} (1 - q^{2m})^{12} \quad \text{in } \mathbb{Z}[[q]].$$

Dimensie 12: Glaisher, Ramanujan

James Whitbread Lee Glaisher, geïnterpreteerd door Srinivasa Ramanujan in 1916, bewees dat:

$$r_{12}(n) = 8\sum_{d|n} d^5 - 512 \sum_{d|(n/4)} d^5 + 16a_n$$

waar:

$$\sum_{n\geq 1} a_n q^n = q\prod_{m\geq 1}(1-q^{2m})^{12} \quad \text{in } \mathbb{Z}[[q]].$$

Merk op: in tegenstelling tot de gevallen met $d \leq 10$, leidt deze formule *niet* tot berekening van $r_{12}(n)$ in tijd polynomiaal in $\log n$, als n is gegeven met zijn factorisatie in priemgetallen.

$r_d(n)$ voor alle even d

Negatief. Ila Varma (masterscriptie, Leiden, Juni 2010): voor geen enkele even $d > 10$ is er een "elementaire" formule voor $r_d(n)$.

$r_d(n)$ voor alle even d

Negatief. Ila Varma (masterscriptie, Leiden, Juni 2010): voor geen enkele even $d > 10$ is er een "elementaire" formule voor $r_d(n)$.

Positief (boek en Peter Bruin's proefschrift). Voor iedere even d kan $r_d(n)$ berekend worden in tijd polynomiaal in $\log n$, als $n \in \mathbb{N}$ is gegeven met zijn priemfactorisatie.

$r_d(n)$ voor alle even d

Negatief. Ila Varma (masterscriptie, Leiden, Juni 2010): voor geen enkele even $d > 10$ is er een "elementaire" formule voor $r_d(n)$.

Positief (boek en Peter Bruin's proefschrift). Voor iedere even d kan $r_d(n)$ berekend worden in tijd polynomiaal in $\log n$, als $n \in \mathbb{N}$ is gegeven met zijn priemfactorisatie.

Merk op: voor $n = pq$ met p en q verschillende oneven priemen:

$$r_4(n) = 8(1 + p + q + n).$$

$r_d(n)$ voor alle even d

Negatief. Ila Varma (masterscriptie, Leiden, Juni 2010): voor geen enkele even $d > 10$ is er een "elementaire" formule voor $r_d(n)$.

Positief (boek en Peter Bruin's proefschrift). Voor iedere even d kan $r_d(n)$ berekend worden in tijd polynomiaal in $\log n$, als $n \in \mathbb{N}$ is gegeven met zijn priemfactorisatie.

Merk op: voor $n = pq$ met p en q verschillende oneven priemen:

$$r_4(n) = 8(1 + p + q + n).$$

Conclusie. Vanuit algoritmisch perspectief is dit klassieke probleem nu opgelost voor *alle* even d. De vraag naar *formules* heeft een negatief antwoord, maar voor *berekenen* maakt dat niet uit en hebben we nu een *positief* antwoord.

Verklaring in een notedop, in onbegrijpelijke termen.

De $r_d(n)$ zijn coëfficiënten van modulaire vormen.

Verklaring in een notedop, in onbegrijpelijke termen.

De $r_d(n)$ zijn coëfficiënten van modulaire vormen.

Die coëfficiënten kunnen snel worden uitgerekend door middel van Galoisrepresentaties.

Verklaring in een notedop, in onbegrijpelijke termen.

De $r_d(n)$ zijn coëfficiënten van modulaire vormen.

Die coëfficiënten kunnen snel worden uitgerekend door middel van Galoisrepresentaties.

Galoisgroepen vormen de symmetrieën in de getaltheorie.

Verklaring in een notedop, in onbegrijpelijke termen.

De $r_d(n)$ zijn coëfficiënten van modulaire vormen.

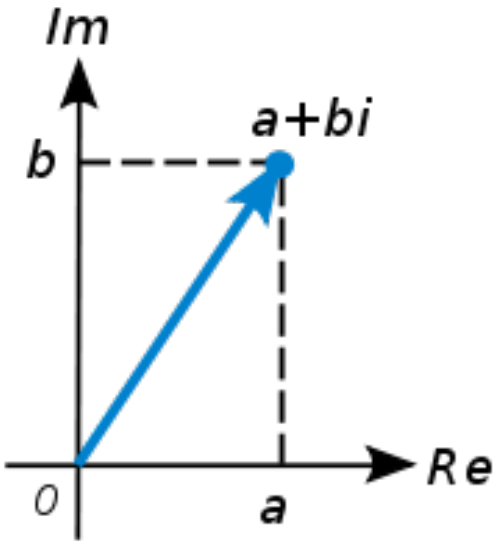
Die coëfficiënten kunnen snel worden uitgerekend door middel van Galoisrepresentaties.

Galoisgroepen vormen de symmetrieën in de getaltheorie.

Dat laatste gaan we toelichten.

Complexe getallen

Complexe getallen: $\mathbb{C} = \{a + bi \mid \text{met } a \text{ en } b \text{ in } \mathbb{R}\}$, met $i^2 = -1$.



$$(a+bi)+(c+di) = (a+c)+(b+d)i$$
$$(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$$
$$|a+bi| = \sqrt{a^2+b^2}$$
$$|z\cdot w| = |z|\cdot|w|$$
$$r\cdot e^{i\phi} = r\cos(\phi) + ir\sin(\phi)$$
$$1/(a+bi) = (a-bi)/(a^2+b^2)$$

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Voorbeeld. Complexe conjugatie: $\sigma(a+bi) = a - bi$.

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Voorbeeld. Complexe conjugatie: $\sigma(a+bi) = a - bi$.

Feiten:

- Aut($\mathbb{C}$) (de verzameling van deze σ) is heel groot;

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Voorbeeld. Complexe conjugatie: $\sigma(a+bi) = a - bi$.

Feiten:

- Aut($\mathbb{C}$) (de verzameling van deze σ) is heel groot;
- Aut($\mathbb{R}$) is heel klein (opgave);

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Voorbeeld. Complexe conjugatie: $\sigma(a+bi) = a - bi$.

Feiten:

- Aut($\mathbb{C}$) (de verzameling van deze σ) is heel groot;
- Aut($\mathbb{R}$) is heel klein (opgave);
- Aut($\mathbb{C}$) is gesloten onder samenstellen;

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Voorbeeld. Complexe conjugatie: $\sigma(a+bi) = a - bi$.

Feiten:

- Aut($\mathbb{C}$) (de verzameling van deze σ) is heel groot;
- Aut($\mathbb{R}$) is heel klein (opgave);
- Aut($\mathbb{C}$) is gesloten onder samenstellen;
- voor alle σ in Aut($\mathbb{C}$) en p/q in $\mathbb{Q}$: $\sigma(p/q) = p/q$.

Symmetrieën in de getaltheorie

Automorfismen van $\mathbb{C}$ zijn afbeeldingen $\sigma\colon \mathbb{C} \to \mathbb{C}$ die voldoen aan:

- $\sigma(z+w) = \sigma(z) + \sigma(w)$,
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$,
- σ heeft een inverse afbeelding.

Voorbeeld. Complexe conjugatie: $\sigma(a+bi) = a - bi$.

Feiten:

- Aut($\mathbb{C}$) (de verzameling van deze σ) is heel groot;
- Aut($\mathbb{R}$) is heel klein (opgave);
- Aut($\mathbb{C}$) is gesloten onder samenstellen;
- voor alle σ in Aut($\mathbb{C}$) en p/q in $\mathbb{Q}$: $\sigma(p/q) = p/q$.

Open probleem: is er een σ in Aut($\mathbb{C}$) met $\sigma(e) = \pi$ èn $\sigma(\pi) = e$?

Galoisgroepen

Laat $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ een veelterm zijn met alle a_i in $\mathbb{Q}$.

Galoisgroepen

Laat $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ een veelterm zijn met alle a_i in $\mathbb{Q}$.

Dan heeft $f(z) = 0$ precies n oplossingen in $\mathbb{C}$, met multipliciteit geteld.

Galoisgroepen

Laat $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ een veelterm zijn met alle a_i in $\mathbb{Q}$.

Dan heeft $f(z) = 0$ precies n oplossingen in $\mathbb{C}$, met multipliciteit geteld.

Voor σ in Aut($\mathbb{C}$) en z in Wortels(f):

$$\begin{aligned} 0 = \sigma(0) = \sigma(f(z)) &= \sigma(z^n + \cdots + a_1 z + a_0) \\ &= \sigma(z^n) + \cdots \sigma(a_1 z) + \sigma(a_0) \\ &= \sigma(z)^n + \cdots + \sigma(a_1)\sigma(z) + \sigma(a_0) \\ &= \sigma(z)^n + \cdots + a_1\sigma(z) + a_0 = f(\sigma(z)), \end{aligned}$$

dus $\sigma(z)$ is in Wortels(f).

Galoisgroepen

Laat $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ een veelterm zijn met alle a_i in $\mathbb{Q}$.

Dan heeft $f(z) = 0$ precies n oplossingen in $\mathbb{C}$, met multipliciteit geteld.

Voor σ in Aut($\mathbb{C}$) en z in Wortels(f):

$$\begin{aligned} 0 = \sigma(0) = \sigma(f(z)) &= \sigma(z^n + \cdots + a_1 z + a_0) \\ &= \sigma(z^n) + \cdots \sigma(a_1 z) + \sigma(a_0) \\ &= \sigma(z)^n + \cdots + \sigma(a_1)\sigma(z) + \sigma(a_0) \\ &= \sigma(z)^n + \cdots + a_1\sigma(z) + a_0 = f(\sigma(z)), \end{aligned}$$

dus $\sigma(z)$ is in Wortels(f).

Gal(f) is de groep van permutaties van Wortels(f) gegeven door elementen van Aut($\mathbb{C}$).

Voorbeelden van Galoisgroepen

Voorbeeld: $f = x^2 + 1$, dan Wortels$(f) = \{i, -i\}$, en Gal(f) bestaat uit de permutaties gegeven door de identiteit ($i \mapsto i$, $-i \mapsto -i$), en door de complexe conjugatie ($i \mapsto -i$, $-i \mapsto i$).

Voorbeelden van Galoisgroepen

Voorbeeld: $f = x^2 + 1$, dan Wortels$(f) = \{i, -i\}$, en Gal(f) bestaat uit de permutaties gegeven door de identiteit ($i \mapsto i$, $-i \mapsto -i$), en door de complexe conjugatie ($i \mapsto -i$, $-i \mapsto i$).

Voorbeeld: $f = x^2 - 2$, dan Wortels$(f) = \{\sqrt{2}, -\sqrt{2}\}$, en Gal$(f)$ bestaat uit de twee permutaties die de twee wortels vastlaten of verwisselen.

Voorbeelden van Galoisgroepen

Voorbeeld: $f = x^2 + 1$, dan Wortels$(f) = \{i, -i\}$, en Gal(f) bestaat uit de permutaties gegeven door de identiteit ($i \mapsto i$, $-i \mapsto -i$), en door de complexe conjugatie ($i \mapsto -i$, $-i \mapsto i$).

Voorbeeld: $f = x^2 - 2$, dan Wortels$(f) = \{\sqrt{2}, -\sqrt{2}\}$, en Gal$(f)$ bestaat uit de twee permutaties die de twee wortels vastlaten of verwisselen.

Laat $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, deelverzameling van $\mathbb{C}$, gesloten onder optelling en vermenigvuldiging.
Het is makkelijk na te rekenen dat de afbeelding $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ optelling en vermenigvuldiging behoudt. Uitbreiden naar $\mathbb{C}$ is slechts een kwestie van techniek.

Voorbeelden van Galoisgroepen

Voorbeeld: $f = x^2 + 1$, dan Wortels$(f) = \{i, -i\}$, en Gal(f) bestaat uit de permutaties gegeven door de identiteit ($i \mapsto i$, $-i \mapsto -i$), en door de complexe conjugatie ($i \mapsto -i$, $-i \mapsto i$).

Voorbeeld: $f = x^2 - 2$, dan Wortels$(f) = \{\sqrt{2}, -\sqrt{2}\}$, en Gal$(f)$ bestaat uit de twee permutaties die de twee wortels vastlaten of verwisselen.

Laat $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, deelverzameling van $\mathbb{C}$, gesloten onder optelling en vermenigvuldiging.
Het is makkelijk na te rekenen dat de afbeelding $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ optelling en vermenigvuldiging behoudt. Uitbreiden naar $\mathbb{C}$ is slechts een kwestie van techniek.

Nu wat polgalois in pari?

Eenheidswortels

Voorbeeld: $f = x^n - 1$.

Eenheidswortels

Voorbeeld: $f = x^n - 1$. Laat $z = \cos(2\pi/n) + i\sin(2\pi/n)$.

Eenheidswortels

Voorbeeld: $f = x^n - 1$. Laat $z = \cos(2\pi/n) + i\sin(2\pi/n)$. Dan:

$$\{0, 1, \ldots, n-1\} \to \text{Wortels}(f), \quad a \mapsto z^a$$

is een *labelling* van de wortels.

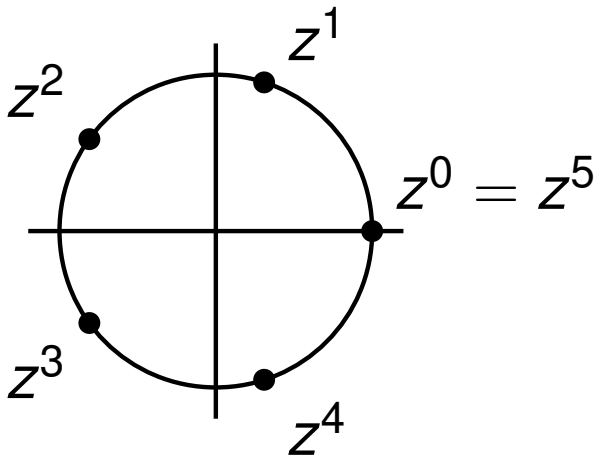
Eenheidswortels

Voorbeeld: $f = x^n - 1$. Laat $z = \cos(2\pi/n) + i\sin(2\pi/n)$. Dan:

$$\{0, 1, \ldots, n-1\} \to \text{Wortels}(f), \quad a \mapsto z^a$$

is een *labelling* van de wortels.

Voor $n = 5$:



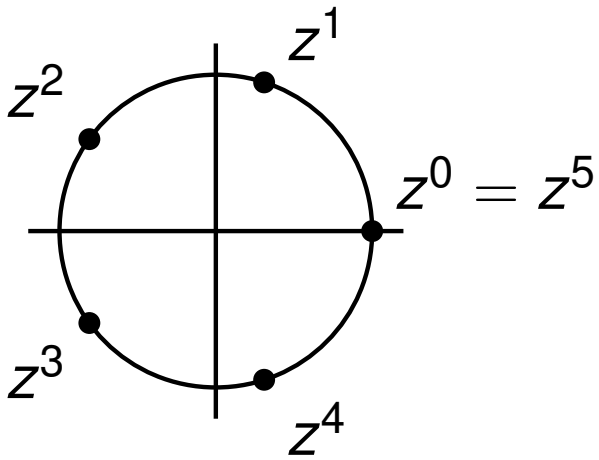
Eenheidswortels

Voorbeeld: $f = x^n - 1$. Laat $z = \cos(2\pi/n) + i\sin(2\pi/n)$. Dan:

$$\{0, 1, \ldots, n-1\} \to \text{Wortels}(f), \quad a \mapsto z^a$$

is een *labelling* van de wortels.

Voor $n = 5$:



$$\text{Gal}(x^n - 1) = \{a \mapsto ka \mod n \mid 0 \le k < n, \text{ggd}(n, k) = 1\}$$

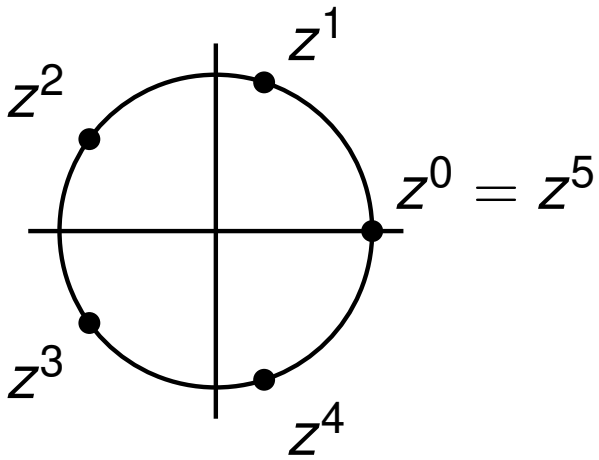
Eenheidswortels

Voorbeeld: $f = x^n - 1$. Laat $z = \cos(2\pi/n) + i\sin(2\pi/n)$. Dan:

$$\{0, 1, \ldots, n-1\} \to \text{Wortels}(f), \quad a \mapsto z^a$$

is een *labelling* van de wortels.

Voor $n = 5$:



$$\text{Gal}(x^n - 1) = \{a \mapsto ka \mod n \mid 0 \le k < n, \text{ggd}(n, k) = 1\}$$

Conclusie: in termen van de labelling is $\text{Gal}(f)$ gegeven door vermenigvuldingen in het getal systeem $\mathbb{Z}/n\mathbb{Z}$.

Tweedimensionale Galoisrepresentaties

Een 2-dimensionale Galoisrepresentatie mod n is een polynoom $f = x^{n^2} + \cdots + a_1 x + a_0$ van graad n^2, met a_i in $\mathbb{Q}$, zodat een labelling van Wortels(f) met vectoren $v = \binom{v_1}{v_2}$ met v_1 en v_2 in $\mathbb{Z}/n\mathbb{Z}$ bestaat, zodat Gal(f) bestaat uit vermenigvuldingen met matrices:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{pmatrix}.$$

Tweedimensionale Galoisrepresentaties

Een 2-dimensionale Galoisrepresentatie mod n is een polynoom $f = x^{n^2} + \cdots + a_1 x + a_0$ van graad n^2, met a_i in $\mathbb{Q}$, zodat een labelling van Wortels(f) met vectoren $v = \binom{v_1}{v_2}$ met v_1 en v_2 in $\mathbb{Z}/n\mathbb{Z}$ bestaat, zodat Gal(f) bestaat uit vermenigvuldingen met matrices:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{pmatrix}.$$

Deze objecten spelen de hoofdrol in Andrew Wiles's bewijs van Fermat's laatste stelling (1993-1994).

Tweedimensionale Galoisrepresentaties

Een 2-dimensionale Galoisrepresentatie mod n is een polynoom $f = x^{n^2} + \cdots + a_1 x + a_0$ van graad n^2, met a_i in $\mathbb{Q}$, zodat een labelling van Wortels(f) met vectoren $v = \binom{v_1}{v_2}$ met v_1 en v_2 in $\mathbb{Z}/n\mathbb{Z}$ bestaat, zodat Gal(f) bestaat uit vermenigvuldingen met matrices:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{pmatrix}.$$

Deze objecten spelen de hoofdrol in Andrew Wiles's bewijs van Fermat's laatste stelling (1993-1994).

Sinds 40 jaar is er theorie over waar dit soort representaties vandaan komen: modulaire vormen, d.w.z., Langlands programma.

Tweedimensionale Galoisrepresentaties

Een 2-dimensionale Galoisrepresentatie mod n is een polynoom $f = x^{n^2} + \cdots + a_1 x + a_0$ van graad n^2, met a_i in $\mathbb{Q}$, zodat een labelling van Wortels(f) met vectoren $v = \binom{v_1}{v_2}$ met v_1 en v_2 in $\mathbb{Z}/n\mathbb{Z}$ bestaat, zodat Gal(f) bestaat uit vermenigvuldingen met matrices:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{pmatrix}.$$

Deze objecten spelen de hoofdrol in Andrew Wiles's bewijs van Fermat's laatste stelling (1993-1994).

Sinds 40 jaar is er theorie over waar dit soort representaties vandaan komen: modulaire vormen, d.w.z., Langlands programma.

Vraag: kan men ze ook efficiënt uitrekenen? Het lijkt van wel.

An example by Johan Bosman

The polynomial:

$$\begin{aligned} f = x^{24} &- 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19} \\ &+ 9223x^{18} + 121141x^{17} + 1837654x^{16} - 800032x^{15} \\ &+ 9856374x^{14} + 52362168x^{13} - 32040725x^{12} \\ &+ 279370098x^{11} + 1464085056x^{10} + 1129229689x^{9} \\ &+ 3299556862x^{8} + 14586202192x^{7} + 29414918270x^{6} \\ &+ 45332850431x^{5} - 6437110763x^{4} - 111429920358x^{3} \\ &- 12449542097x^{2} + 93960798341x - 31890957224 \end{aligned}$$

has Galois group $\mathrm{PGL}_2(\mathbb{Z}/23\mathbb{Z})$, and (reduced) discriminant 23^{43}; it comes from étale cohomology of degree 21 of a variety of complex dimension 21.

Reclame, eind van citaat van Princeton Univ. Press

. . . The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves.

Reclame, eind van citaat van Princeton Univ. Press

. . . The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves.

The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties.

Reclame, eind van citaat van Princeton Univ. Press

. . . The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves.

The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties.

Exact computations involving systems of polynomial equations in many variables take exponential time.

Reclame, eind van citaat van Princeton Univ. Press

. . . The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves.

The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties.

Exact computations involving systems of polynomial equations in many variables take exponential time.

This is avoided by numerical approximations with a precision that suffices to derive exact results from them.

Reclame, eind van citaat van Princeton Univ. Press

. . . The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves.

The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties.

Exact computations involving systems of polynomial equations in many variables take exponential time.

This is avoided by numerical approximations with a precision that suffices to derive exact results from them.

Bounds for the required precision–in other words, bounds for the height of the rational numbers that describe the Galois representation to be computed–are obtained from Arakelov theory. . .

Eind

Dank u voor uw aandacht!

Vragen?

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Met: Jean-Marc Couveignes (Toulouse), Robin de Jong, Franz Merkl (München), Johan Bosman, Peter Bruin, Ila Varma.