Snel en exact rekenen in getaltheorie en computeralgebra door middel van benaderingen

Bas Edixhoven

Universiteit Leiden

2010/10/25, KNAW

Een wanhoopskreet

Van Kampen, afdelingsdag natuurkunde, 27 september 2010, over een voordracht over wiskunde op 31 mei 2010, die hij onbegrijpelijk vond:

> *Voorzitter, is daar dan ècht níets aan te doen?*

Een wanhoopskreet

Van Kampen, afdelingsdag natuurkunde, 27 september 2010, over een voordracht over wiskunde op 31 mei 2010, die hij onbegrijpelijk vond:

> *Voorzitter, is daar dan ècht níets aan te doen?*

Ik zal proberen hier iets aan te doen, door:

- definities te geven van de objecten waarover het gaat,
- resultaten en methoden zo eenvoudig mogelijk te beschrijven,
- te eindigen met een toegankelijke toepassing.

Een wanhoopskreet

Van Kampen, afdelingsdag natuurkunde, 27 september 2010, over een voordracht over wiskunde op 31 mei 2010, die hij onbegrijpelijk vond:

> *Voorzitter, is daar dan ècht níets aan te doen?*

Ik zal proberen hier iets aan te doen, door:

- definities te geven van de objecten waarover het gaat,
- resultaten en methoden zo eenvoudig mogelijk te beschrijven,
- te eindigen met een toegankelijke toepassing.

Maar alle verdere details blijven noodzakelijkerwijs in duister gehuld.

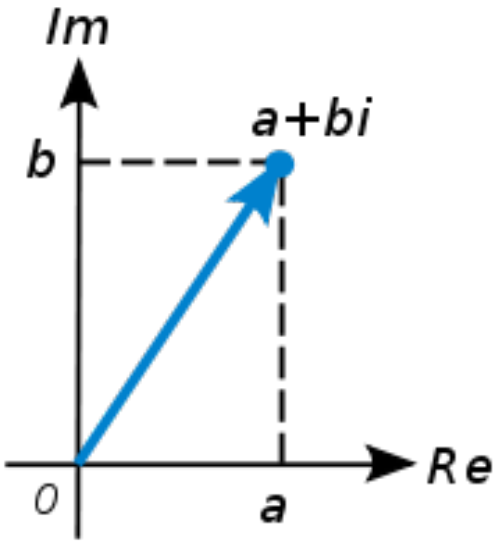
Wàt willen we uitrekenen?

Twee-dimensionale Galoisrepresentaties. Uitleg volgt.

Wàt willen we uitrekenen?

Twee-dimensionale Galoisrepresentaties. Uitleg volgt.

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



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

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

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

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

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

Feiten:

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

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

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);

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

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;

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

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;
- als $\sigma(z) = \sigma(w)$, dan $z = w$;

De bril van de getaltheoreticus

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

- $\sigma(z+w) = \sigma(z) + \sigma(w)$;
- $\sigma(z \cdot w) = \sigma(z) \cdot \sigma(w)$;
- $\sigma(1) = 1$;
- voor iedere z is er een w met $\sigma(w) = z$.

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;
- als $\sigma(z) = \sigma(w)$, dan $z = w$;
- voor alle σ in Aut($\mathbb{C}$) en p/q in $\mathbb{Q}$: $\sigma(p/q) = p/q$.

Galoisgroepen

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

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 Roots(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 Roots(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 Roots(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 Roots(f).

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

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:

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

is een *labelling* van de wortels.

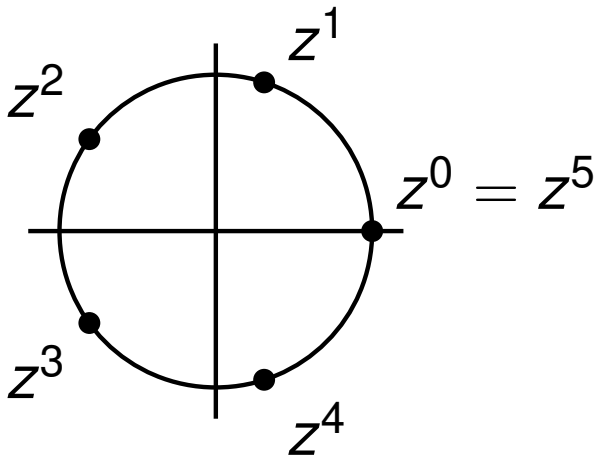
Eenheidswortels

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

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

is een *labelling* van de wortels.

Voor $n = 5$:



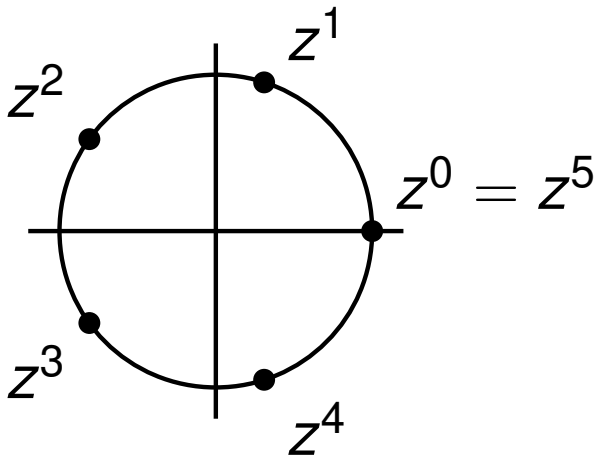
Eenheidswortels

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

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

is een *labelling* van de wortels.

Voor $n = 5$:



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

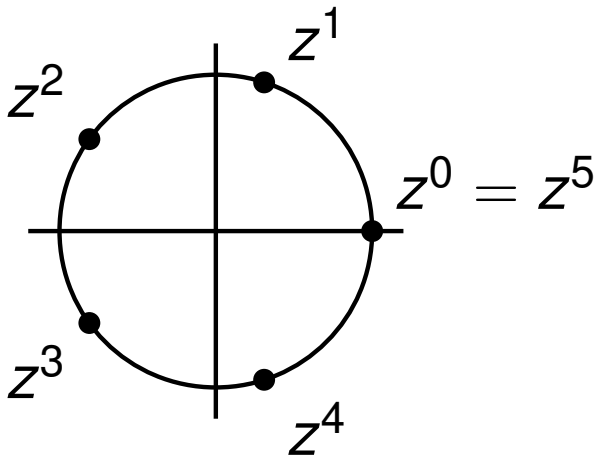
Eenheidswortels

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

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

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 Roots(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 Roots(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 Roots(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 Roots(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?

Computeralgebra? Nee.

Het Langlandsprogramma geeft (nogal impliciet) systemen polynoomvergelijkingen voor de coëfficiënten a_i van f's, met coëfficiënten in $\mathbb{Q}$:

$$\begin{cases} F_1(x_1, \ldots, x_{n^2}) = 0, \\ F_2(x_1, \ldots, x_{n^2}) = 0, \\ \vdots \\ F_r(x_1, \ldots, x_{n^2}) = 0. \end{cases}$$

Computeralgebra? Nee.

Het Langlandsprogramma geeft (nogal impliciet) systemen polynoomvergelijkingen voor de coëfficiënten a_i van f's, met coëfficiënten in $\mathbb{Q}$:

$$\begin{cases} F_1(x_1, \ldots, x_{n^2}) = 0, \\ F_2(x_1, \ldots, x_{n^2}) = 0, \\ \vdots \\ F_r(x_1, \ldots, x_{n^2}) = 0. \end{cases}$$

Men kan proberen dit soort systemen te berekenen, en vervolgens met computeralgebra op te lossen.

Computeralgebra? Nee.

Het Langlandsprogramma geeft (nogal impliciet) systemen polynoomvergelijkingen voor de coëfficiënten a_i van f's, met coëfficiënten in $\mathbb{Q}$:

$$\begin{cases} F_1(x_1, \ldots, x_{n^2}) = 0, \\ F_2(x_1, \ldots, x_{n^2}) = 0, \\ \vdots \\ F_r(x_1, \ldots, x_{n^2}) = 0. \end{cases}$$

Men kan proberen dit soort systemen te berekenen, en vervolgens met computeralgebra op te lossen. Helaas leidt dat tot een rekentijd die exponentieel groeit in n. (De F_i zijn niet lineair.)

Computeralgebra? Nee.

Het Langlandsprogramma geeft (nogal impliciet) systemen polynoomvergelijkingen voor de coëfficiënten a_i van f's, met coëfficiënten in $\mathbb{Q}$:

$$\begin{cases} F_1(x_1, \ldots, x_{n^2}) = 0, \\ F_2(x_1, \ldots, x_{n^2}) = 0, \\ \vdots \\ F_r(x_1, \ldots, x_{n^2}) = 0. \end{cases}$$

Men kan proberen dit soort systemen te berekenen, en vervolgens met computeralgebra op te lossen. Helaas leidt dat tot een rekentijd die exponentieel groeit in n. (De F_i zijn niet lineair.)

Curse of dimensionality: het aantal monomen in $x_1, \ldots, x_n$ van graad hoogstens n is minstens 2^n.

Benaderingen, numerieke analyse: ja.

Doorbraak: men kan de f's zoals boven toch berekenen in een rekentijd die hoogstens als een vaste macht van n groeit.

Benaderingen, numerieke analyse: ja.

Doorbraak: men kan de f's zoals boven toch berekenen in een rekentijd die hoogstens als een vaste macht van n groeit.

Werk met Couveignes (Toulouse), Merkel (München), de Jong, Bosman, te verschijnen als boek in Annals of Mathematics Studies, Princeton University Press, en Peter Bruin's proefschrift.

Benaderingen, numerieke analyse: ja.

Doorbraak: men kan de f's zoals boven toch berekenen in een rekentijd die hoogstens als een vaste macht van n groeit.

Werk met Couveignes (Toulouse), Merkel (München), de Jong, Bosman, te verschijnen als boek in Annals of Mathematics Studies, Princeton University Press, en Peter Bruin's proefschrift.

Methode: de exacte oplossing kan berekend worden uit een benadering met voldoend grote precisie.

Benaderingen, numerieke analyse: ja.

Doorbraak: men kan de f's zoals boven toch berekenen in een rekentijd die hoogstens als een vaste macht van n groeit.

Werk met Couveignes (Toulouse), Merkel (München), de Jong, Bosman, te verschijnen als boek in Annals of Mathematics Studies, Princeton University Press, en Peter Bruin's proefschrift.

Methode: de exacte oplossing kan berekend worden uit een benadering met voldoend grote precisie.

Als $p/q \neq p'/q'$ en $|p|$, $|q|$, $|p'|$ en $|q'|$ hoogstens M, dan:

$$\left|\frac{p}{q} - \frac{p'}{q'}\right| = \left|\frac{pq' - qp'}{qq'}\right| \geq \frac{1}{|qq'|} \geq \frac{1}{M^2}.$$

Benaderingen, numerieke analyse: ja.

Doorbraak: men kan de f's zoals boven toch berekenen in een rekentijd die hoogstens als een vaste macht van n groeit.

Werk met Couveignes (Toulouse), Merkel (München), de Jong, Bosman, te verschijnen als boek in Annals of Mathematics Studies, Princeton University Press, en Peter Bruin's proefschrift.

Methode: de exacte oplossing kan berekend worden uit een benadering met voldoend grote precisie.

Als $p/q \neq p'/q'$ en $|p|$, $|q|$, $|p'|$ en $|q'|$ hoogstens M, dan:

$$\left|\frac{p}{q} - \frac{p'}{q'}\right| = \left|\frac{pq' - qp'}{qq'}\right| \geq \frac{1}{|qq'|} \geq \frac{1}{M^2}.$$

Het vereiste aantal cijfers nauwkeurigheid groeit hoogstens als een vaste macht van n.

Voorbeeld. Het polynoom:

$$\begin{aligned} f = x^{24} &+ 9x^{23} + 46x^{22} + 115x^{21} - 138x^{20} - 1886x^{19} \\ &+ 1058x^{18} + 59639x^{17} + 255599x^{16} + 308798x^{15} \\ &- 1208328x^{14} - 6156732x^{13} - 10740931x^{12} \\ &+ 2669403x^{11} + 52203054x^{10} + 106722024x^{9} \\ &+ 60172945x^{8} - 158103380x^{7} - 397878081x^{6} \\ &- 357303183x^{5} + 41851168x^{4} + 438371490x^{3} \\ &+ 484510019x^{2} + 252536071x + 55431347 \end{aligned}$$

heeft Galoisgroep $\mathrm{PGL}_2(\mathbb{Z}/23\mathbb{Z})$, en (gereduceerde) discriminant 23^{37}.

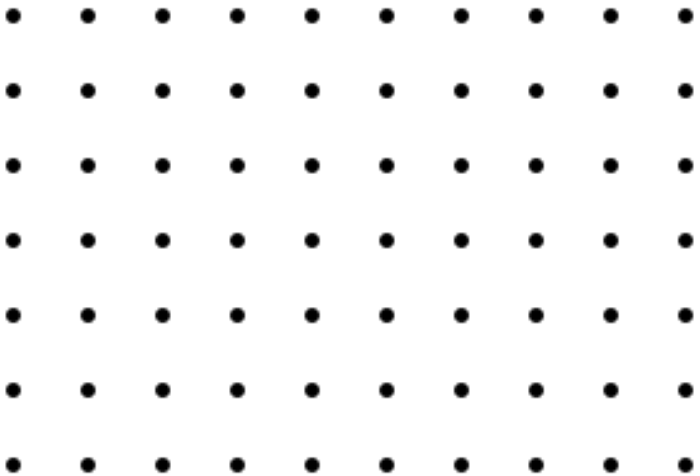
Toepassingen

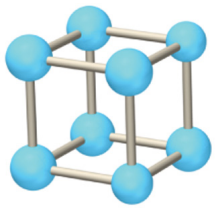
Toepassing: snel uitrekenen van coëfficiënten van modulaire vormen. Deze zijn van groot belang in getaltheorie, algebraïsche meetkunde, combinatoriek en roosters.

Toepassingen

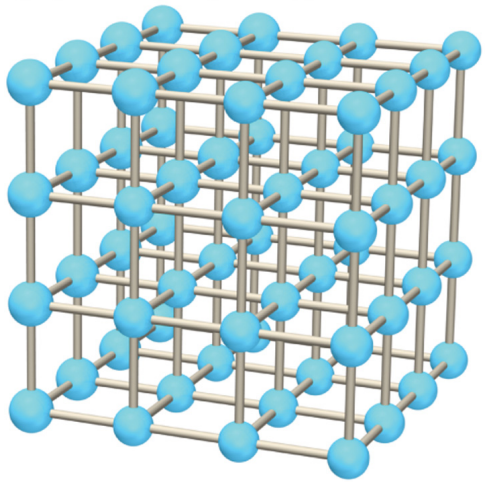
Toepassing: snel uitrekenen van coëfficiënten van modulaire vormen. Deze zijn van groot belang in getaltheorie, algebraïsche meetkunde, combinatoriek en roosters.

Nu: de standaardroosters $\mathbb{Z}^k$ in $\mathbb{R}^k$.





(a)

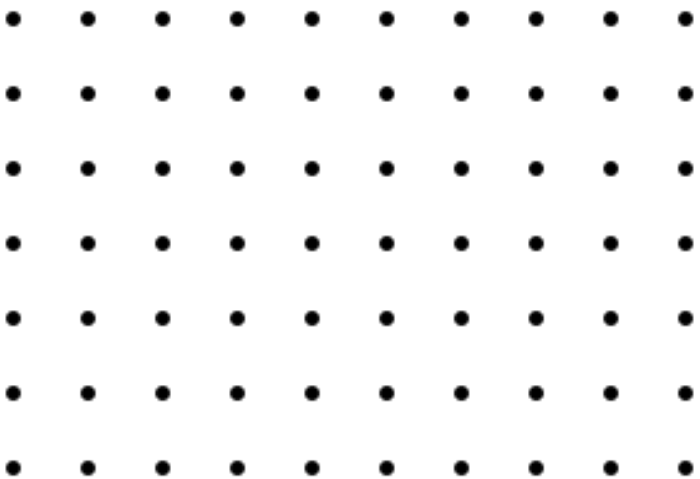


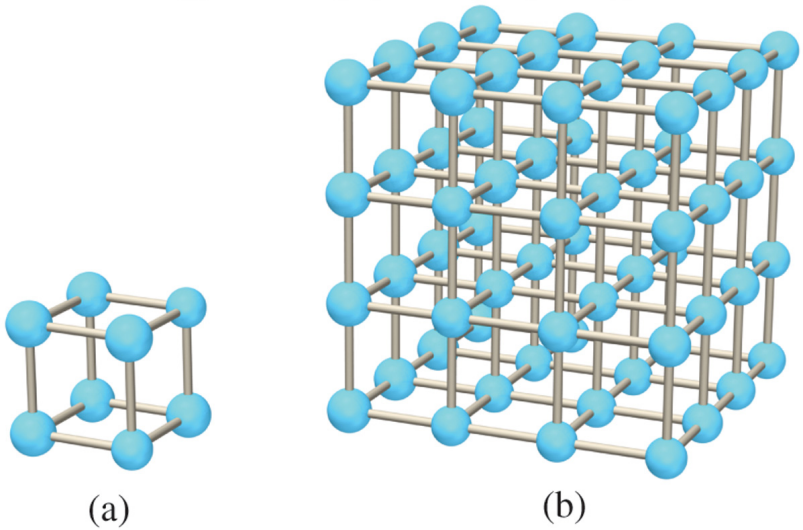
(b)

Toepassingen

Toepassing: snel uitrekenen van coëfficiënten van modulaire vormen. Deze zijn van groot belang in getaltheorie, algebraïsche meetkunde, combinatoriek en roosters.

Nu: de standaardroosters $\mathbb{Z}^k$ in $\mathbb{R}^k$.





(a) (b)

Probleem: tel het aantal roosterpunten met een gegeven afstand tot de oorsprong.

Sommen van kwadraten

Definitie: $r_k(n)$ is het aantal $(x_1, \ldots, x_k)$ in $\mathbb{Z}^k$ met $x_1^2 + \cdots + x_k^2 = n$.
Pythagoras: $r_k(n)$ is het aantal elementen van $\mathbb{Z}^k$ met afstand $\sqrt{n}$ tot de oorsprong.

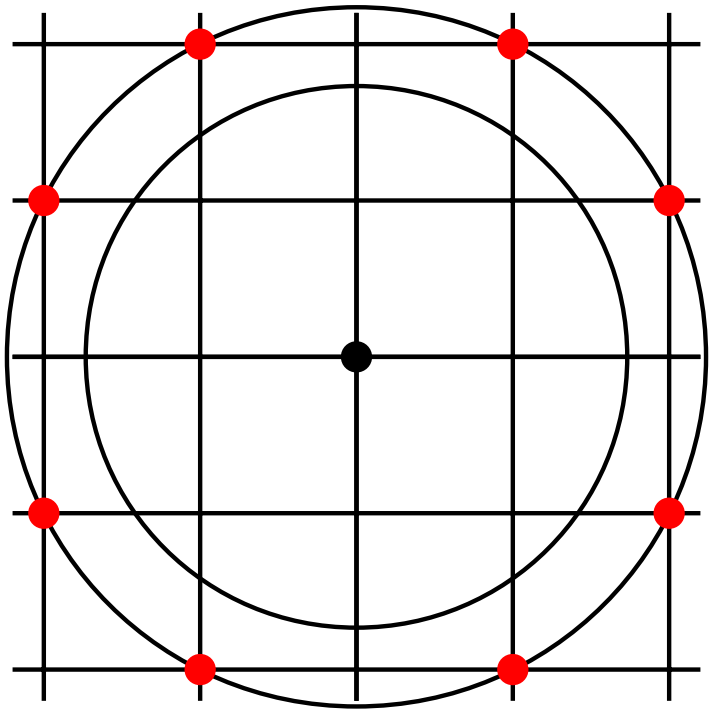
Sommen van kwadraten

Definitie: $r_k(n)$ is het aantal $(x_1, \ldots, x_k)$ in $\mathbb{Z}^k$ met $x_1^2 + \cdots + x_k^2 = n$.
Pythagoras: $r_k(n)$ is het aantal elementen van $\mathbb{Z}^k$ met afstand $\sqrt{n}$ tot de oorsprong.

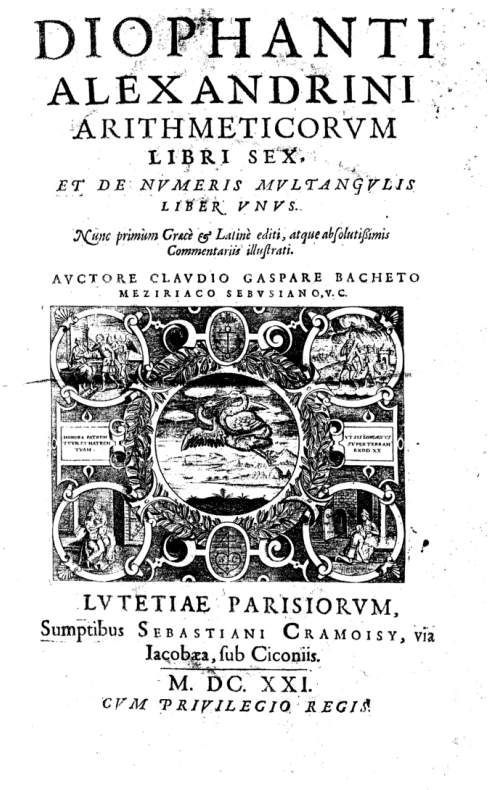
$r_2(3) = 0$.

$r_2(5) = 8$:

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



Diophantus


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primum 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 ($\approx$ 3e eeuw): als

$$n = a^2 + b^2 \quad \text{en} \quad m = c^2 + d^2$$

dan

$$nm = (ac - bd)^2 + (ad + bc)^2.$$

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 in de factorisatie van n voorkomt.

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 $r_k(n)$ voor oneven k gecompliceerder zijn.

Jacobi

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

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

Jacobi

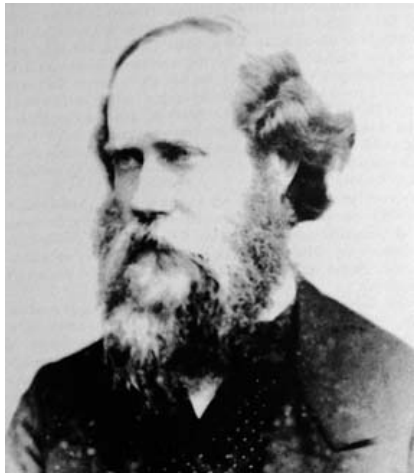
Carl Gustav Jacob Jacobi (1829) bewees voor $n > 1$:

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

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:

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

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

Liouville

Voor $k = 10$ heeft Joseph Liouville (1865) een formule gevonden in termen van de complexe getallen $d = a + bi$ met a en b geheel. Liouville's formule luidt:

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

$r_k(n)$ voor $k > 10$

Negatief. Ila Varma (masters scriptie, Leiden, juni 2010): voor geen enkele even $k > 10$ is er een dergelijke “elementaire” formule voor $r_k(n)$.

$r_k(n)$ voor $k > 10$

Negatief. Ila Varma (masters scriptie, Leiden, juni 2010): voor geen enkele even $k > 10$ is er een dergelijke “elementaire” formule voor $r_k(n)$.

Positief. Voor iedere even k kan $r_k(n)$ worden uitgerekend in een tijd die polynomiaal begrensd is in $\log n$, als n gegeven wordt met zijn priemfactorontbinding.

$r_k(n)$ voor $k > 10$

Negatief. Ila Varma (masters scriptie, Leiden, juni 2010): voor geen enkele even $k > 10$ is er een dergelijke “elementaire” formule voor $r_k(n)$.

Positief. Voor iedere even k kan $r_k(n)$ worden uitgerekend in een tijd die polynomiaal begrensd is in $\log n$, als n gegeven wordt met zijn priemfactorontbinding.

Conclusie. Vanuit algoritmisch standpunt is het klassieke probleem compleet opgelost voor alle even k. De vraag naar *formules* heeft een negatief antwoord, maar voor het *berekenen* maakt dat niet uit en is er nu een *positief* antwoord.

Einde

Dankuwel 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.