Counting quickly the vectors with integer coordinates and with a given length

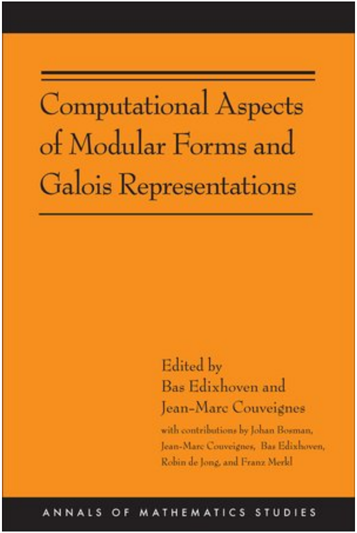
Bas Edixhoven

Universiteit Leiden

2011/07/14

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

The commercial



The commercial, continued

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

The commercial, continued

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.

The commercial, continued

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 commercial, continued

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.

The commercial, continued

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...

Back to mathematics: sums of squares

To illustrate the progress made in the book and Peter Bruin's PhD thesis, we consider the problem of computing quickly, for d and n in $\mathbb{Z}$:

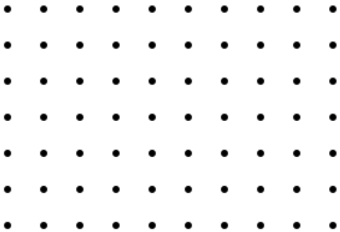
$$r_d(n) := \#\{x \in \mathbb{Z}^d : x_1^2 + \cdots + x_d^2 = n\}.$$

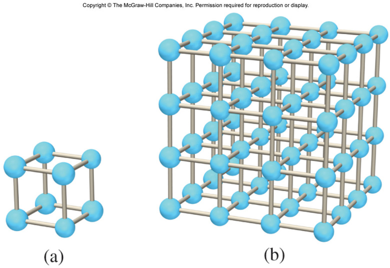
Back to mathematics: sums of squares

To illustrate the progress made in the book and Peter Bruin's PhD thesis, we consider the problem of computing quickly, for d and n in $\mathbb{Z}$:

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

Geometric interpretation (Pythagoras): count the number of lattice points in $\mathbb{Z}^d$ at a given distance $\sqrt{n}$ from the origin.



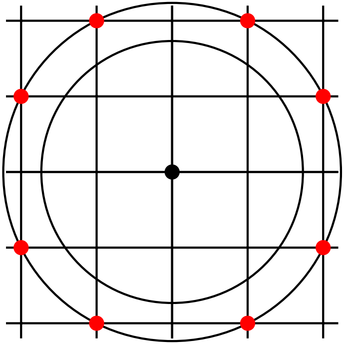


Sums of squares: some examples

$r_2(3) = 0.$

$r_2(5) = 8:$

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



Dimension one

For n in $\mathbb{Z}$, given in binary notation, say, one can compute $r_1(n)$ in time at most a power of $\log(1 + |n|)$ (approximately the number of digits of n).

Dimension one

For n in $\mathbb{Z}$, given in binary notation, say, one can compute $r_1(n)$ in time at most a power of $\log(1+|n|)$ (approximately the number of digits of n).

If $n < 0$ then $r_1(n) = 0$.

Dimension one

For n in $\mathbb{Z}$, given in binary notation, say, one can compute $r_1(n)$ in time at most a power of $\log(1+|n|)$ (approximately the number of digits of n).

If $n < 0$ then $r_1(n) = 0$.

If $n = 0$ then $r_1(n) = 1$.

Dimension one

For n in $\mathbb{Z}$, given in binary notation, say, one can compute $r_1(n)$ in time at most a power of $\log(1+|n|)$ (approximately the number of digits of n).

If $n < 0$ then $r_1(n) = 0$.

If $n = 0$ then $r_1(n) = 1$.

If $n > 0$ and n is a square, then $r_1(n) = 2$, and otherwise $r_1(n) = 0$. Use the method of bisection of intervals for approximating $\sqrt{n}$, starting with $[0, n]$.

Dimension one

For n in $\mathbb{Z}$, given in binary notation, say, one can compute $r_1(n)$ in time at most a power of $\log(1 + |n|)$ (approximately the number of digits of n).

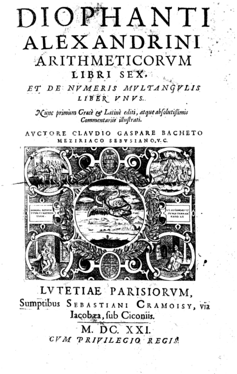
If $n < 0$ then $r_1(n) = 0$.

If $n = 0$ then $r_1(n) = 1$.

If $n > 0$ and n is a square, then $r_1(n) = 2$, and otherwise $r_1(n) = 0$. Use the method of bisection of intervals for approximating $\sqrt{n}$, starting with $[0, n]$.

Do *not* use the factorisation of n into primes, because we do not know how to to that fast enough.

Dimension two: Diophantus



Diophantus of Alexandria ($\approx$ 3rd century):

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

Dimension two: Fermat

Pierre de Fermat (lawyer, Toulouse, 17th century), for $n \geq 1$: $r_2(n) \neq 0$ if and only if every prime factor of n that is 3 modulo 4, occurs an even number of times in the factorisation of n.

Dimensions 2 and 3: Legendre, Gauss

Adrien-Marie Legendre (1798) gave a formula for $r_2(2^a m^2)$.

Dimensions 2 and 3: Legendre, Gauss

Adrien-Marie Legendre (1798) gave a formula for $r_2(2^a m^2)$.

Carl Friedrich Gauss (1801) gave a general formula for $r_2(n)$, and a formula for $r_3(n)$ that shows that the $r_d(n)$ for odd d are more complicated (involve class numbers).

Higher even dimensions: Jacobi

Carl Gustav Jacob Jacobi (1829) proved for $n > 1$:

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

Higher even dimensions: Jacobi

Carl Gustav Jacob Jacobi (1829) proved for $n > 1$:

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

and:

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

Eisenstein, Smith

It follows from work of Jacobi, Ferdinand Eisenstein and Henry Smith that:

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

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

Dimension 10: Liouville

For $d = 10$ Joseph Liouville (1865) found a formula in terms of the Gaussian integers $d = a + bi$ with a and b in $\mathbb{Z}$:

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

Dimension 12: Glaisher, Ramanujan

James Whitbread Lee Glaisher, reinterpreted by Srinivasa Ramanujan in 1916, proved that:

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

Dimension 12: Glaisher, Ramanujan

James Whitbread Lee Glaisher, reinterpreted by Srinivasa Ramanujan in 1916, proved that:

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

where:

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

Dimension 12: Glaisher, Ramanujan

James Whitbread Lee Glaisher, reinterpreted by Srinivasa Ramanujan in 1916, proved that:

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

where:

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

Note: unlike for $d \leq 10$, this formula does *not* lead to computation of $r_{12}(n)$ in time polynomial in $\log n$, if n is given with its factorisation into primes.

$r_d(n)$ for all even d

Negative. Ila Varma (masters thesis, Leiden, June 2010): there is no even $d > 10$ for which there is an “elementary” formula for $r_d(n)$.

$r_d(n)$ for all even d

Negative. Ila Varma (masters thesis, Leiden, June 2010): there is no even $d > 10$ for which there is an “elementary” formula for $r_d(n)$.

Positive (book and Peter Bruin’s PhD thesis). For every even d one can compute $r_d(n)$ in time polynomial in $\log n$, if $n \in \mathbb{N}$ is given with its factorisation into primes.

$r_d(n)$ for all even d

Negative. Ila Varma (masters thesis, Leiden, June 2010): there is no even $d > 10$ for which there is an "elementary" formula for $r_d(n)$.

Positive (book and Peter Bruin's PhD thesis). For every even d one can compute $r_d(n)$ in time polynomial in $\log n$, if $n \in \mathbb{N}$ is given with its factorisation into primes.

Note: for $n = pq$ with p and q distinct odd primes:

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

$r_d(n)$ for all even d

Negative. Ila Varma (masters thesis, Leiden, June 2010): there is no even $d > 10$ for which there is an “elementary” formula for $r_d(n)$.

Positive (book and Peter Bruin’s PhD thesis). For every even d one can compute $r_d(n)$ in time polynomial in $\log n$, if $n \in \mathbb{N}$ is given with its factorisation into primes.

Note: for $n = pq$ with p and q distinct odd primes:

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

Conclusion. From an algorithmic perspective this classical problem is now solved for *all* even d. The question for *formulas* has a negative answer, but for *computing* that negative answer does not matter and we now have a *positive* answer.

Explanation: generating series

It is more than time to explain what is going on behind all these formulas. Generating series:

$$\theta_d := \sum_{x \in \mathbb{Z}^d} q^{x_1^2 + \cdots + x_d^2} = \sum_{n \geq 0} r_d(n) q^n \quad \text{in } \mathbb{Z}[[q]].$$

Explanation: generating series

It is more than time to explain what is going on behind all these formulas. Generating series:

$$\theta_d := \sum_{x\in\mathbb{Z}^d} q^{x_1^2+\cdots+x_d^2} = \sum_{n\geq 0} r_d(n)q^n \quad \text{in } \mathbb{Z}[[q]].$$

Let $\theta := \theta_1$ (Jacobi theta function at $z = 0$). Then:

$$\theta^d = \left(\sum_{x_1\in\mathbb{Z}} q^{x_1^2}\right)\cdots\left(\sum_{x_d\in\mathbb{Z}} q^{x_d^2}\right) = \theta_d.$$

Explanation: generating series

It is more than time to explain what is going on behind all these formulas. Generating series:

$$\theta_d := \sum_{x\in\mathbb{Z}^d} q^{x_1^2+\cdots+x_d^2} = \sum_{n\geq 0} r_d(n)q^n \quad \text{in } \mathbb{Z}[[q]].$$

Let $\theta := \theta_1$ (Jacobi theta function at $z = 0$). Then:

$$\theta^d = \left(\sum_{x_1\in\mathbb{Z}} q^{x_1^2}\right)\cdots\left(\sum_{x_d\in\mathbb{Z}} q^{x_d^2}\right) = \theta_d.$$

Compute θ^d in $\mathbb{Z}[[q]]/(q^{n+1})$: gives $r_d(n)$ but takes time at least linear in nd.

Theta functions are modular forms

Key idea: $q\colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Theta functions are modular forms

Key idea: $q\colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Then $\theta_d\colon \mathbb{H} \to \mathbb{C}$, and for $z \in \mathbb{H}$: $\theta_d(z+1) = \theta_d(z)$, and Jacobi proved (Poisson summation formula):

$$\theta_d(-1/4z) = (2z/i)^{d/2}\theta_d(z).$$

Theta functions are modular forms

Key idea: $q\colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Then $\theta_d\colon \mathbb{H} \to \mathbb{C}$, and for $z \in \mathbb{H}$: $\theta_d(z+1) = \theta_d(z)$, and Jacobi proved (Poisson summation formula):

$$\theta_d(-1/4z) = (2z/i)^{d/2}\theta_d(z).$$

This implies: θ_d is in the $\mathbb{C}$-vector space $M_{d/2}(\Gamma_1(4))$ of modular forms of weight $d/2$ on the subgroup $\Gamma_1(4)$ of $\mathrm{SL}_2(\mathbb{Z})$. Assume from now on that d is even. Then $k = d/2$ is in $\mathbb{Z}$.

Theta functions are modular forms

Key idea: $q\colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Then $\theta_d\colon \mathbb{H} \to \mathbb{C}$, and for $z \in \mathbb{H}$: $\theta_d(z+1) = \theta_d(z)$, and Jacobi proved (Poisson summation formula):

$$\theta_d(-1/4z) = (2z/i)^{d/2}\theta_d(z).$$

This implies: θ_d is in the $\mathbb{C}$-vector space $M_{d/2}(\Gamma_1(4))$ of modular forms of weight $d/2$ on the subgroup $\Gamma_1(4)$ of $\mathrm{SL}_2(\mathbb{Z})$. Assume from now on that d is even. Then $k = d/2$ is in $\mathbb{Z}$.

The $M_k(\Gamma_1(4))$ are finite dimensional.

Theta functions are modular forms

Key idea: $q\colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Then $\theta_d\colon \mathbb{H} \to \mathbb{C}$, and for $z \in \mathbb{H}$: $\theta_d(z+1) = \theta_d(z)$, and Jacobi proved (Poisson summation formula):

$$\theta_d(-1/4z) = (2z/i)^{d/2}\theta_d(z).$$

This implies: θ_d is in the $\mathbb{C}$-vector space $M_{d/2}(\Gamma_1(4))$ of modular forms of weight $d/2$ on the subgroup $\Gamma_1(4)$ of $\mathrm{SL}_2(\mathbb{Z})$. Assume from now on that d is even. Then $k = d/2$ is in $\mathbb{Z}$.

The $M_k(\Gamma_1(4))$ are finite dimensional.

For $0 \le k \le 4$, $M_k(\Gamma_1(4))$ is generated by Eisenstein series, hence the formulas for $r_d(n)$ for $d \le 8$.

Theta functions are modular forms

Key idea: $q\colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Then $\theta_d\colon \mathbb{H} \to \mathbb{C}$, and for $z \in \mathbb{H}$: $\theta_d(z+1) = \theta_d(z)$, and Jacobi proved (Poisson summation formula):

$$\theta_d(-1/4z) = (2z/i)^{d/2}\theta_d(z).$$

This implies: θ_d is in the $\mathbb{C}$-vector space $M_{d/2}(\Gamma_1(4))$ of modular forms of weight $d/2$ on the subgroup $\Gamma_1(4)$ of $\mathrm{SL}_2(\mathbb{Z})$. Assume from now on that d is even. Then $k = d/2$ is in $\mathbb{Z}$.

The $M_k(\Gamma_1(4))$ are finite dimensional.

For $0 \leq k \leq 4$, $M_k(\Gamma_1(4))$ is generated by Eisenstein series, hence the formulas for $r_d(n)$ for $d \leq 8$. For $d = 10$: also a Hecke character.

Theta functions are modular forms

Key idea: $q \colon \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\} \to \mathbb{C}, \quad z \mapsto e^{2\pi i z}$.

Then $\theta_d \colon \mathbb{H} \to \mathbb{C}$, and for $z \in \mathbb{H}$: $\theta_d(z+1) = \theta_d(z)$, and Jacobi proved (Poisson summation formula):

$$\theta_d(-1/4z) = (2z/i)^{d/2}\theta_d(z).$$

This implies: θ_d is in the $\mathbb{C}$-vector space $M_{d/2}(\Gamma_1(4))$ of modular forms of weight $d/2$ on the subgroup $\Gamma_1(4)$ of $\mathrm{SL}_2(\mathbb{Z})$. Assume from now on that d is even. Then $k = d/2$ is in $\mathbb{Z}$.

The $M_k(\Gamma_1(4))$ are finite dimensional.

For $0 \leq k \leq 4$, $M_k(\Gamma_1(4))$ is generated by Eisenstein series, hence the formulas for $r_d(n)$ for $d \leq 8$. For $d = 10$: also a Hecke character. Ila Varma: for $d > 10$ θ_d is not linear combination of Eisenstein and Hecke.

Complex analytic geometry

To get further ($\mathrm{SL}_2(\mathbb{Z})$ does not suffice, we need Galois symmetry), interpret $M_k(\Gamma)$ in terms of de Rham cohomology of the quotient E^{k-2} of $\mathbb{C}^{k-2} \times \mathbb{H}$ by an action of $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$:

$$(x, z) \mapsto \left(x + n_1 + n_2 z, \frac{az + b}{cz + d}\right)$$

Complex analytic geometry

To get further ($SL_2(\mathbb{Z})$ does not suffice, we need Galois symmetry), interpret $M_k(\Gamma)$ in terms of de Rham cohomology of the quotient E^{k-2} of $\mathbb{C}^{k-2} \times \mathbb{H}$ by an action of $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$:

$$(x, z) \mapsto \left(x + n_1 + n_2 z, \frac{az + b}{cz + d}\right)$$

For $f \in M_k(\Gamma)$, $f\, dx_1 \cdots dx_{k-2} dz$ is a $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$-invariant and closed holomorphic $(k-1)$-form.

Complex analytic geometry

To get further ($\mathrm{SL}_2(\mathbb{Z})$ does not suffice, we need Galois symmetry), interpret $M_k(\Gamma)$ in terms of de Rham cohomology of the quotient E^{k-2} of $\mathbb{C}^{k-2} \times \mathbb{H}$ by an action of $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$:

$$(x, z) \mapsto \left(x + n_1 + n_2 z, \frac{az + b}{cz + d}\right)$$

For $f \in M_k(\Gamma)$, $f\,dx_1 \cdots dx_{k-2} dz$ is a $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$-invariant and closed holomorphic $(k-1)$-form.

Via de Rham's comparison theorem, interpret $M_k(\Gamma)$ as a piece of $H^{k-1}(E^{k-2}, \mathbb{C})$ (Betti cohomology, defined topologically).

Complex analytic geometry

To get further ($\mathrm{SL}_2(\mathbb{Z})$ does not suffice, we need Galois symmetry), interpret $M_k(\Gamma)$ in terms of de Rham cohomology of the quotient E^{k-2} of $\mathbb{C}^{k-2} \times \mathbb{H}$ by an action of $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$:

$$(x, z) \mapsto \left(x + n_1 + n_2 z, \frac{az + b}{cz + d}\right)$$

For $f \in M_k(\Gamma)$, $f\, dx_1 \cdots dx_{k-2} dz$ is a $\mathbb{Z}^{2(k-2)} \rtimes \Gamma$-invariant and closed holomorphic $(k-1)$-form.

Via de Rham's comparison theorem, interpret $M_k(\Gamma)$ as a piece of $H^{k-1}(E^{k-2}, \mathbb{C})$ (Betti cohomology, defined topologically).

The coefficients $a_n(f)$ of the modular forms $f = \sum_{n \geq 0} a_n(f) q^n$ are closely related to Hecke operators T_n coming from the $\mathrm{GL}_2(\mathbb{Q})^+$-action on $\mathbb{H}$.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Some facts about $\mathrm{Aut}(\mathbb{C})$, the group of automorphisms of the field $\mathbb{C}$.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Some facts about $\mathrm{Aut}(\mathbb{C})$, the group of automorphisms of the field $\mathbb{C}$.

- $\mathrm{Aut}(\mathbb{C})$ is big, and $\mathrm{Aut}(\mathbb{R})$ is trivial.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Some facts about $\mathrm{Aut}(\mathbb{C})$, the group of automorphisms of the field $\mathbb{C}$.

- $\mathrm{Aut}(\mathbb{C})$ is big, and $\mathrm{Aut}(\mathbb{R})$ is trivial.
- We only know identity and complex conjugation (the continuous ones).

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Some facts about $\mathrm{Aut}(\mathbb{C})$, the group of automorphisms of the field $\mathbb{C}$.

- $\mathrm{Aut}(\mathbb{C})$ is big, and $\mathrm{Aut}(\mathbb{R})$ is trivial.
- We only know identity and complex conjugation (the continuous ones).
- We know: $\exists \sigma \in \mathrm{Aut}(\mathbb{C})$, $\sigma(\pi) = e$.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Some facts about $\mathrm{Aut}(\mathbb{C})$, the group of automorphisms of the field $\mathbb{C}$.

- $\mathrm{Aut}(\mathbb{C})$ is big, and $\mathrm{Aut}(\mathbb{R})$ is trivial.
- We only know identity and complex conjugation (the continuous ones).
- We know: $\exists \sigma \in \mathrm{Aut}(\mathbb{C})$, $\sigma(\pi) = e$.
- We know: $\exists \sigma \in \mathrm{Aut}(\mathbb{C})$, $\sigma(e) = \pi$.

Algebraic geometry

In fact, E^{k-2} is an algebraic variety, defined over $\mathbb{Q}$.

Grothendieck: $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ is defined algebraically, as étale cohomology, hence $\mathrm{Aut}(\mathbb{C})$ acts on it.

Some facts about $\mathrm{Aut}(\mathbb{C})$, the group of automorphisms of the field $\mathbb{C}$.

- $\mathrm{Aut}(\mathbb{C})$ is big, and $\mathrm{Aut}(\mathbb{R})$ is trivial.
- We only know identity and complex conjugation (the continuous ones).
- We know: $\exists \sigma \in \mathrm{Aut}(\mathbb{C}), \sigma(\pi) = e$.
- We know: $\exists \sigma \in \mathrm{Aut}(\mathbb{C}), \sigma(e) = \pi$.
- We do *not* know (yet?): $\exists \sigma \in \mathrm{Aut}(\mathbb{C}), \sigma(\pi) = e$ *and* $\sigma(e) = \pi$.

Just the case Δ

For p prime, the action of T_p on $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ can be computed from the Galois action, as the trace of a Frobenius element at p.

Just the case Δ

For p prime, the action of T_p on $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ can be computed from the Galois action, as the trace of a Frobenius element at p.

To simplify, consider $M_{12}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}{\cdot}E_{12} \oplus \mathbb{C}{\cdot}\Delta$, where

$$E_{12} = 1 + \frac{65520}{691} \sum_{n \geq 1} \left(\sum_{d|n} d^{11} \right) q^n,$$

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n.$$

Just the case Δ

For p prime, the action of T_p on $H^{k-1}(E^{k-2}, \mathbb{Z}/m\mathbb{Z})$ can be computed from the Galois action, as the trace of a Frobenius element at p.

To simplify, consider $M_{12}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}{\cdot}E_{12} \oplus \mathbb{C}{\cdot}\Delta$, where

$$E_{12} = 1 + \frac{65520}{691} \sum_{n \geq 1} \left(\sum_{d|n} d^{11} \right) q^n,$$

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n.$$

Deligne: for every integer $m > 0$ there is $\rho_m \colon \mathrm{Aut}(\mathbb{C}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, such that for every prime $p \nmid m$, $\tau(p) = \mathrm{trace}(\mathrm{Frob}_p)$ in $\mathbb{Z}/m\mathbb{Z}$.

The book and two theses

The *book* explains, in about 400 pages, that one can compute, for ℓ prime, ρ_ℓ in time polynomial in ℓ, and then $\tau(p)$ in time polynomial in $\log p$. More generally: for $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

The book and two theses

The *book* explains, in about 400 pages, that one can compute, for ℓ prime, ρ_ℓ in time polynomial in ℓ, and then $\tau(p)$ in time polynomial in $\log p$. More generally: for $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

Johan Bosman: did real computations.

The book and two theses

The *book* explains, in about 400 pages, that one can compute, for ℓ prime, ρ_ℓ in time polynomial in ℓ, and then $\tau(p)$ in time polynomial in $\log p$. More generally: for $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

Johan Bosman: did real computations.

Peter Bruin's PhD thesis: generalises the theory to $M_k(\Gamma_1(N))$.

Galois groups

Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be in $\mathbb{Q}[x]$.

Galois groups

Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be in $\mathbb{Q}[x]$.

Then $f(z) = 0$ has exactly n solutions in $\mathbb{C}$, counted with multiplicity.

Galois groups

Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be in $\mathbb{Q}[x]$.

Then $f(z) = 0$ has exactly n solutions in $\mathbb{C}$, counted with multiplicity.

For σ in $\mathrm{Aut}(\mathbb{C})$ and z in $\mathrm{Roots}(f)$:

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

hence $\sigma(z)$ is in $\mathrm{Roots}(f)$.

Galois groups

Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be in $\mathbb{Q}[x]$.

Then $f(z) = 0$ has exactly n solutions in $\mathbb{C}$, counted with multiplicity.

For σ in $\mathrm{Aut}(\mathbb{C})$ and z in $\mathrm{Roots}(f)$:

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

hence $\sigma(z)$ is in $\mathrm{Roots}(f)$.

$\mathrm{Gal}(f)$ is the group of permutations of $\mathrm{Roots}(f)$ given by elements of $\mathrm{Aut}(\mathbb{C})$.

Example: roots of unity

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

Example: roots of unity

Example: $f = x^n - 1$. Let $z = e^{2\pi i/n}$.

Example: roots of unity

Example: $f = x^n - 1$. Let $z = e^{2\pi i/n}$. Then:

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Roots}(f), \quad a \mapsto z^a$$

is a *labelling* of the roots.

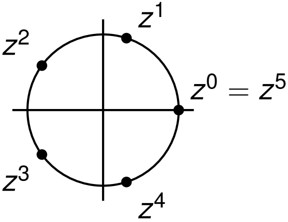
Example: roots of unity

Example: $f = x^n - 1$. Let $z = e^{2\pi i/n}$. Then:

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Roots}(f), \quad a \mapsto z^a$$

is a *labelling* of the roots.

For $n = 5$:



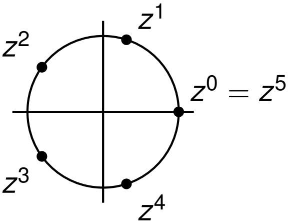
Example: roots of unity

Example: $f = x^n - 1$. Let $z = e^{2\pi i/n}$. Then:

$$\mathbb{Z}/n\mathbb{Z} \to \text{Roots}(f), \quad a \mapsto z^a$$

is a *labelling* of the roots.

For $n = 5$:



$$\text{Gal}(x^n - 1) = \{a \mapsto ka \mod n : k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$$

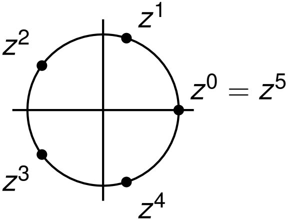
Example: roots of unity

Example: $f = x^n - 1$. Let $z = e^{2\pi i/n}$. Then:

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Roots}(f), \quad a \mapsto z^a$$

is a *labelling* of the roots.

For $n = 5$:



$\mathrm{Gal}(x^n - 1) = \{a \mapsto ka \mod n : k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$

Conclusion: in terms of the labelling Gal(f) is given by elements of $\mathrm{GL}_1(\mathbb{Z}/n\mathbb{Z})$.

Two-dimensional Galois representations

A 2-dimensional Galois representation mod n is a polynomial $f = x^{n^2} + \cdots + a_1 x + a_0$ in $\mathbb{Q}[x]$ of degree n^2, with a bijection $\mathbb{Z}/n\mathbb{Z}^2 \to \mathrm{Roots}(f)$, such that each element of $\mathrm{Gal}(f)$ acts as multiplication by an element of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Two-dimensional Galois representations

A 2-dimensional Galois representation mod n is a polynomial $f = x^{n^2} + \cdots + a_1 x + a_0$ in $\mathbb{Q}[x]$ of degree n^2, with a bijection $\mathbb{Z}/n\mathbb{Z}^2 \to \mathrm{Roots}(f)$, such that each element of $\mathrm{Gal}(f)$ acts as multiplication by an element of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

These objects play the most important role in Andrew Wiles's proof of Fermat's Last Theorem (1993-1994).

Two-dimensional Galois representations

A 2-dimensional Galois representation mod n is a polynomial $f = x^{n^2} + \cdots + a_1 x + a_0$ in $\mathbb{Q}[x]$ of degree n^2, with a bijection $\mathbb{Z}/n\mathbb{Z}^2 \to \mathrm{Roots}(f)$, such that each element of $\mathrm{Gal}(f)$ acts as multiplication by an element of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

These objects play the most important role in Andrew Wiles's proof of Fermat's Last Theorem (1993-1994).

40 years ago the Langlands program started, relating Galois representations and automorphic forms.

Two-dimensional Galois representations

A 2-dimensional Galois representation mod n is a polynomial $f = x^{n^2} + \cdots + a_1 x + a_0$ in $\mathbb{Q}[x]$ of degree n^2, with a bijection $\mathbb{Z}/n\mathbb{Z}^2 \to \mathrm{Roots}(f)$, such that each element of $\mathrm{Gal}(f)$ acts as multiplication by an element of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

These objects play the most important role in Andrew Wiles's proof of Fermat's Last Theorem (1993-1994).

40 years ago the Langlands program started, relating Galois representations and automorphic forms.

Question: can one efficiently compute the Galois representations whose existence is guaranteed by the Langlands program?

Two-dimensional Galois representations

A 2-dimensional Galois representation mod n is a polynomial $f = x^{n^2} + \cdots + a_1 x + a_0$ in $\mathbb{Q}[x]$ of degree n^2, with a bijection $\mathbb{Z}/n\mathbb{Z}^2 \to \mathrm{Roots}(f)$, such that each element of $\mathrm{Gal}(f)$ acts as multiplication by an element of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

These objects play the most important role in Andrew Wiles's proof of Fermat's Last Theorem (1993-1994).

40 years ago the Langlands program started, relating Galois representations and automorphic forms.

Question: can one efficiently compute the Galois representations whose existence is guaranteed by the Langlands program?

It looks as if the answer will be 'yes'.

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.

The commercial, end

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

The commercial, end

…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.

The commercial, end

...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.

The commercial, end

…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.

The commercial, end

. . . 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. . .

The end

Thank you for your attention!

Questions?

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

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