Peter Scholze awarded the Fields medal

Ulrich Görtz

Bonn, October 1, 2018

Most important research prize in mathematics

John Charles Fields

Since 1936,

59 medals awarded.

Age limit: 40 years

Most important research prize in mathematics

Der 30-jährige Peter Scholze darf sich über 10.000 Euro Preisgeld freuen.
(Foto: picture alliance/dpa)

Mittwoch, 01. August 2018

"Nobelpreis der Mathematik"

Peter Scholze gewinnt Fields-Medaille

Der Bonner Peter Scholze ist mit einem der höchsten Preise der Mathematik geehrt

Most important research prize in mathematics

SPIEGEL ONLINE

Fields-Medaille

Peter Scholze bekommt weltweit höchste Auszeichnung für Mathematiker

Peter Scholze bekommt als erster Deutscher seit 32 Jahren eine Fields-Medaille. Die Auszeichnung gilt als Nobelpreis für Mathematik.

Aus Rio de Janeiro berichtet Holger Dambeck

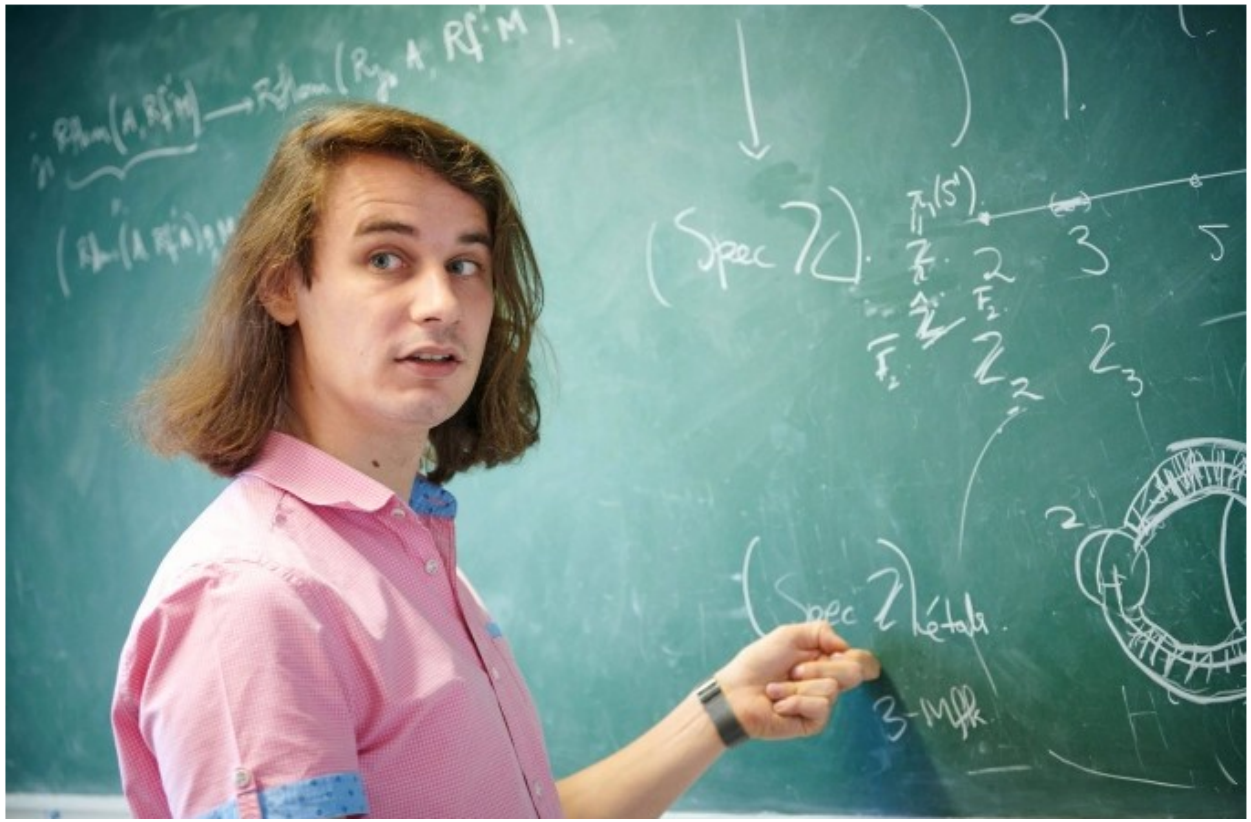
Most important research prize in mathematics

Frankfurter Allgemeine
Computer & Mathematik

MATHEMATIKER PETER SCHOLZE

Räume, die vor ihm niemand sah

VON ULF VON RAUCHHAUPT - AKTUALISIERT AM 06.08.2018 - 08:27



Goal of this talk

Some impression of the area, provide context for non-experts.

Urbano Monte's map of the earth, 1587

Goal of this talk

Some impression of the area, provide context for non-experts.

Urbano Monte's map of the earth, 1587

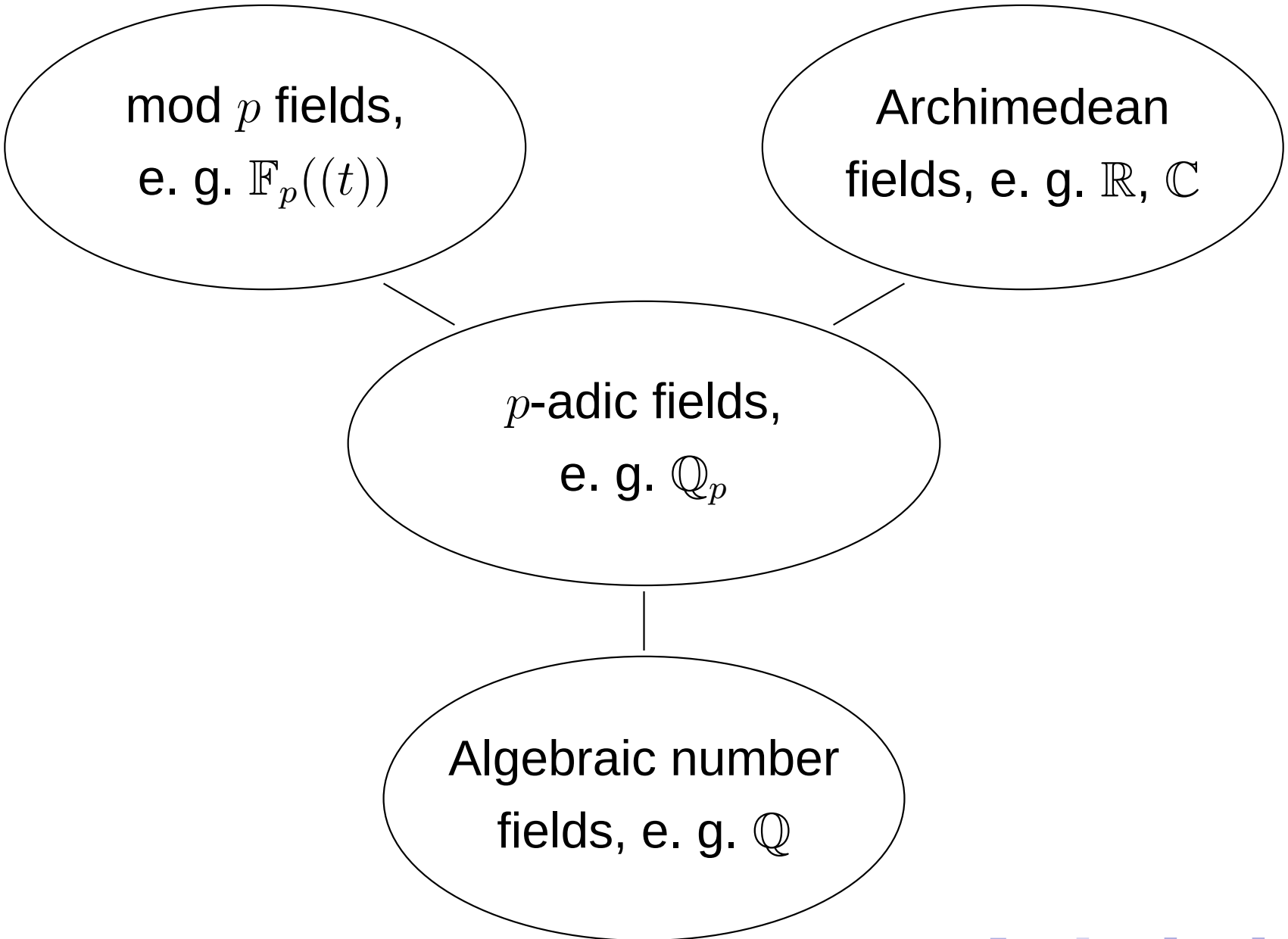
Goal of this talk

Some impression of the area, provide context for non-experts.

Urbano Monte's map of the earth, 1587

David Rumsey Map Collection CC-BY-NC-SA 3.0

Goal of this talk



Solving equations

Important problem in mathematics:

Understand set of solutions of an equation.

Solving equations

Important problem in mathematics:

Understand set of solutions of an equation.

- Do solutions exist?
- Are there only finitely many solutions? Can we count them? Can we write them down explicitly?
- If there are infinitely many solutions, does the set of solutions have a (geometric) structure?

Where are we looking for solutions?

Natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Integers *(add negative numbers)*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Where are we looking for solutions?

Natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Integers *(add negative numbers)*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Rational numbers *(add fractions* $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, *...)*

$$\mathbb{Q}$$

Where are we looking for solutions?

Natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Integers *(add negative numbers)*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Rational numbers *(add fractions* $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, *...)*

$$\mathbb{Q} = \left\{ \frac{a}{b};\ a, b \in \mathbb{Z}, b \neq 0 \right\}$$

Where are we looking for solutions?

Natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Integers *(add negative numbers)*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Rational numbers *(add fractions* $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, *...)*

$$\mathbb{Q} = \left\{ \frac{a}{b};\ a, b \in \mathbb{Z}, b \neq 0 \right\}$$

Real numbers *(add all decimal numbers)*

$$-1,\ -0.5,\ 0,\ 0.333\dots,\ 1,\ 2,\ 3.14159265\dots \in \mathbb{R}$$

Can we detect cases without solutions?

This is often a very hard problem, for instance:

Theorem ("Fermat's Last Theorem", A. Wiles)

Let $n > 2$ be an integer. Then the equation

$$x^n + y^n = z^n$$

has no solutions with integers $x, y, z \geq 1$.

Can we detect cases without solutions?

This is often a very hard problem, for instance:

Theorem ("Fermat's Last Theorem", A. Wiles)

Let $n > 2$ be an integer. Then the equation

$$x^n + y^n = z^n$$

has no solutions with integers $x, y, z \geq 1$.

For certain equations, however, it is easy to show that there are no solutions in the integers.

Understand set of solutions in real numbers

Trivially: If no solutions in $\mathbb{R}$, then no solutions in $\mathbb{Z}$.

Sometimes: Good understanding of solutions in real numbers

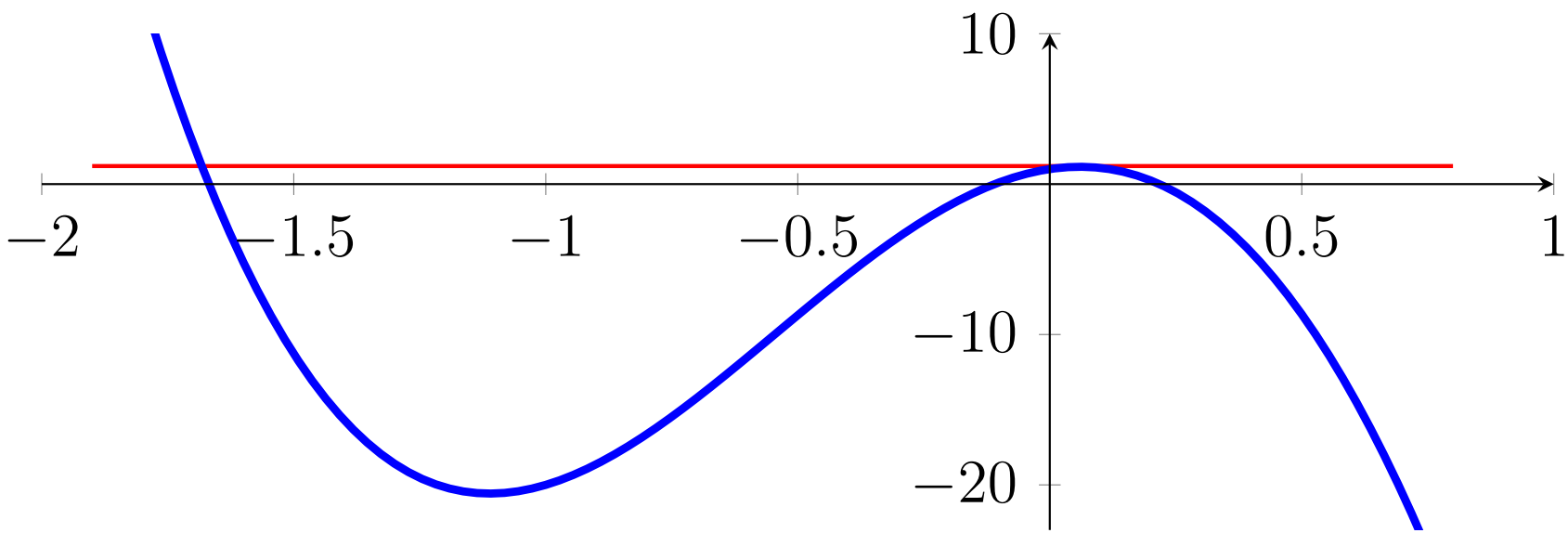
$\rightsquigarrow$ understand solutions in integers.

Understand set of solutions in real numbers

Trivially: If no solutions in $\mathbb{R}$, then no solutions in $\mathbb{Z}$.

Sometimes: Good understanding of solutions in real numbers $\rightsquigarrow$ understand solutions in integers.

Over $\mathbb{R}$, can use analytic methods (Differential calculus, derivatives, …)



Looking at the final digit …

We see that the equation

$$x^4 + 17 = 4y^2$$

has no solutions with integers $x, y \in \mathbb{Z}$,

Looking at the final digit …

We see that the equation

$$x^4 + 17 = 4y^2$$

has no solutions with integers $x, y \in \mathbb{Z}$,

because the final digit can only be

left hand side $x^4 + 17$:
2, 3, 7 or 8,

right hand side $4y^2$:
0, 4, or 6.

Looking at the final digit …

We see that the equation

$$x^4 + 17 = 4y^2$$

has no solutions with integers $x, y \in \mathbb{Z}$,

because the final digit can only be

left hand side $x^4 + 17$:	right hand side $4y^2$:
2, 3, 7 or 8,	0, 4, or 6.

More powerful: Look at more final digits.

Looking at the final digit …

We see that the equation

$$x^4 + 17 = 4y^2$$

has no solutions with integers $x, y \in \mathbb{Z}$,

because the final digit can only be

left hand side $x^4 + 17$:	right hand side $4y^2$:
2, 3, 7 or 8,	0, 4, or 6.

More powerful: Look at more final digits.

In other words: division with remainder by 10, 100, 1000, …, 10^i.

Looking at the final digit, refined version

Could also do division with remainder by other numbers $n = 2, 3, 4, \ldots$.

For instance consider the equation

$$x^4 - 17 = 7y^2$$

This is “solvable mod 10” (both sides can have final digit 3, for instance).

Looking at the final digit, refined version

Could also do division with remainder by other numbers $n = 2, 3, 4, \ldots$.

For instance consider the equation

$$x^4 - 17 = 7y^2$$

This is "solvable mod 10" (both sides can have final digit 3, for instance).

But division with remainder by 7 gives remainder 1, 3, 4, or 5 on the left, and 0 on the right.

Division with remainder = n-adic final digit

Division with remainder = n-adic final digit

Binary expression:

$$23$$

Division with remainder = n-adic final digit

Binary expression:

$$23 = 16 + 4 + 2 + 1$$

Division with remainder = n-adic final digit

Binary expression:

$$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0$$

Division with remainder = n-adic final digit

Binary expression:

$$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0 = 10111_2.$$

Division with remainder = n-adic final digit

Binary expression:

$$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0 = 10111_2.$$

$23 \equiv 1 \mod 2$,

$23 \equiv 11_2 = 3 \mod 4$,

$23 \equiv 111_2 = 7 \mod 16$.

Division with remainder = n-adic final digit

Binary expression:

$$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0 = 10111_2.$$

$23 \equiv 1 \mod 2$,

$23 \equiv 11_2 = 3 \mod 4$,

$23 \equiv 111_2 = 7 \mod 16$.

7-adic expression:

$$23 = 21 + 2 = 3 \cdot 7^1 + 2 \cdot 7^0 = 32_7.$$

$23 \equiv 2 \mod 7$.

Analytic methods

Key point: passing to limit.

A sequence of real numbers “coming arbitrarily close to each other” converges to a limit in $\mathbb{R}$.

Analytic methods

Key point: passing to limit.

A sequence of real numbers “coming arbitrarily close to each other” converges to a limit in $\mathbb{R}$.

- …not interesting in $\mathbb{Z}$,
- …does not work in $\mathbb{Q}$: We can approximate $\sqrt{2}$ by rational numbers, but it is not rational itself.

Analytic methods

Key point: passing to limit.

A sequence of real numbers “coming arbitrarily close to each other” converges to a limit in $\mathbb{R}$.

Two real numbers are close to each other if the differences lie far to the right of the decimal point:

123.12345 is much closer to 123.12346 than to 123.22345

Analytic methods

Key point: passing to limit.

A sequence of real numbers “coming arbitrarily close to each other” converges to a limit in $\mathbb{R}$.

Two real numbers are close to each other if the differences lie far to the right of the decimal point:

123.12345 is much closer to 123.12346 than to 123.22345

A limit always exists because, naively speaking, we allow infinitely many digits to the right of the decimal point.

Setting up an analogy

“Solving” an equation so that the final 5 digits match is more difficult than having only the final digits match.

Having more digits match is a “better approximation” of the solution from this point of view.

Setting up an analogy

"Solving" an equation so that the final 5 digits match is more difficult than having only the final digits match.

Having more digits match is a "better approximation" of the solution from this point of view.

Example (Lind-Reichardt equation: $x^4 - 17 = 2y^2$)

- $x = 5$, $y = 8$: 608 versus 128
- $x = 85$, $y = 548$: 52 200 608 versus 600 608

Setting up an analogy

"Solving" an equation so that the final 5 digits match is more difficult than having only the final digits match.

Having more digits match is a "better approximation" of the solution from this point of view.

Example (Lind-Reichardt equation: $x^4 - 17 = 2y^2$)

- $x = 5$, $y = 8$: 608 versus 128
- $x = 85$, $y = 548$: 52 200 608 versus 600 608

10-adic numbers $\mathbb{Z}_{10}$:
Allow infinitely many digits, extending to the left.

Computing with 10-adic numbers

$$\mathbb{Z}_{10} = \{\ldots a_2 a_1 a_0;\ a_i \in \{0, 1, \ldots, 9\}\}.$$

All natural numbers are 10-adic numbers.

Computing with 10-adic numbers

$$\mathbb{Z}_{10} = \{\ldots a_2 a_1 a_0;\ a_i \in \{0, 1, \ldots, 9\}\}.$$

All natural numbers are 10-adic numbers. We can add and multiply 10-adic numbers.

Computing with 10-adic numbers

$\mathbb{Z}_{10} = \{\ldots a_2 a_1 a_0;\ a_i \in \{0, 1, \ldots, 9\}\}$.

All natural numbers are 10-adic numbers. We can add and multiply 10-adic numbers.

Surprising things may happen:

$$\ldots 999 + 1 = 0, \quad \text{hence } \ldots 999 = -1.$$

Computing with 10-adic numbers

$\mathbb{Z}_{10} = \{\ldots a_2 a_1 a_0;\ a_i \in \{0, 1, \ldots, 9\}\}$.

All natural numbers are 10-adic numbers. We can add and multiply 10-adic numbers.

Properties

- all integers are 10-adic numbers,
- $\mathbb{Z}_{10}$ has operations $+$, $-$, $\cdot$.
- Even some fractions are 10-adic: $\ldots 6667 \cdot 3 = 1$.

Variant: p-adic numbers

Although we can compute in the set $\mathbb{Z}_{10}$ of 10-adic numbers, it has some less nice features:

$$\ldots 8212890625 \cdot \ldots 1787109376 = 0.$$

Variant: p-adic numbers

Although we can compute in the set $\mathbb{Z}_{10}$ of 10-adic numbers, it has some less nice features:

$$\ldots 8212890625 \cdot \ldots 1787109376 = 0.$$

Better: p-adic numbers $\mathbb{Z}_p$ for a prime number p.
That means: use p-adic expression, and allow it to extend infinitely to the left.

Variant: p-adic numbers

Although we can compute in the set $\mathbb{Z}_{10}$ of 10-adic numbers, it has some less nice features:

$$\ldots 8212890625 \cdot \ldots 1787109376 = 0.$$

Better: p-adic numbers $\mathbb{Z}_p$ for a prime number p.
That means: use p-adic expression, and allow it to extend infinitely to the left.

$$\mathbb{Z}_2 = \{\ldots a_2 a_1 a_0;\ a_i \in \{0, 1\}\}$$
$$\mathbb{Z}_7 = \{\ldots a_2 a_1 a_0;\ a_i \in \{0, 1, \ldots, 6\}\}$$

Geometry of the p-adic numbers

Absolute value on $\mathbb{Z}_p$

$$|x|_p = \frac{1}{p^n},$$

where n is the number of zeros at the end of p-adic expression

Geometry of the p-adic numbers

Absolute value on $\mathbb{Z}_p$

$$|x|_p = \frac{1}{p^n},$$

where n is the number of zeros at the end of p-adic expression

Example

- $|48|_2 = |110000_2|_2 = 1/2^4 = 1/16,$
- $|23|_7 = |32_7|_7 = 1.$

Geometry of the p-adic numbers

Absolute value on $\mathbb{Z}_p$

$$|x|_p = \frac{1}{p^n},$$

where n is the number of zeros at the end of p-adic expression

We regard x close to y, if $|x - y|$ small.

Some unusual features:

- Every triangle is isosceles.
- Any two circles are disjoint or concentric.

The field of p-adic numbers

The field $\mathbb{Q}_p$: Enlarge $\mathbb{Z}_p$ by allowing finitely many digits after decimal point.

The field of p-adic numbers

The field $\mathbb{Q}_p$: Enlarge $\mathbb{Z}_p$ by allowing finitely many digits after decimal point.

Example ($p = 2$)

$0.1_2 = 1/2, \quad 0.01_2 = 1/4,$

The field of p-adic numbers

The field $\mathbb{Q}_p$: Enlarge $\mathbb{Z}_p$ by allowing finitely many digits after decimal point.

Example ($p = 2$)

$0.1_2 = 1/2, \quad 0.01_2 = 1/4, \qquad \ldots 111.1_2 = -1/2.$

The field of p-adic numbers

The field $\mathbb{Q}_p$: Enlarge $\mathbb{Z}_p$ by allowing finitely many digits after decimal point.

Example ($p = 2$)

$0.1_2 = 1/2, \quad 0.01_2 = 1/4, \qquad \ldots 111.1_2 = -1/2.$

$\mathbb{Q}_p$ a *field*: have $+$, $-$, $\cdot$, $/$.

Über eine neue Begründung der Theorie der algebraischen Zahlen.

Von **K. Hensel** in Berlin.

Die Analogie zwischen den Resultaten der Theorie der algebraischen Functionen einer Variabeln und der der algebraischen Zahlen hat mir schon seit mehreren Jahren den Gedanken nahe ge-

The field of p-adic numbers

The field $\mathbb{Q}_p$: Enlarge $\mathbb{Z}_p$ by allowing finitely many digits after decimal point.

Example ($p = 2$)

$0.1_2 = 1/2, \quad 0.01_2 = 1/4, \qquad \ldots 111.1_2 = -1/2.$

$\mathbb{Q}_p$ a *field*: have $+$, $-$, $\cdot$, $/$.

Im allgemeinen schreiten alle diese Entwickelungen nach Potenzen von p mit ganzzahligen Exponenten fort, d. h. sie können folgendermafsen geschrieben werden:

$$(1) \qquad X = \frac{A_{-h}}{p^h} + \cdots + \frac{A_{-1}}{p} + A_0 + A_1 p + \cdots;$$

für diese Zahlen erhält man also genau dieselben Entwickelungen wie für eine algebraische Function in der Umgebung einer regulären Stelle.

The field of p-adic numbers

The field $\mathbb{Q}_p$: Enlarge $\mathbb{Z}_p$ by allowing finitely many digits after decimal point.

Example ($p = 2$)

$0.1_2 = 1/2, \quad 0.01_2 = 1/4, \qquad \ldots 111.1_2 = -1/2.$

$\mathbb{Q}_p$ a *field*: have $+$, $-$, $\cdot$, $/$.

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i; \quad a_i \in \{0, 1, \ldots, p-1\} \right\},$$

$$\mathbb{Q}_p = \left\{ \sum_{i=i_0}^{\infty} a_i p^i; \quad i_0 \in \mathbb{Z}, \quad a_i \in \{0, 1, \ldots, p-1\} \right\}.$$

p-adic geometry

Tate (around 1962): Rigid analytic spaces

...

Huber (around 1990): Adic spaces

$\rightsquigarrow$ reasonable notion of p-adic manifold/space.

p-adic geometry

Tate (around 1962): Rigid analytic spaces

...

Huber (around 1990): Adic spaces

$\rightsquigarrow$ reasonable notion of p-adic manifold/space.

> *Peter Scholze has revolutionized the field of p-adic geometry.*
>
> *M. Rapoport, Laudatio for P. Scholze, ICM 2018*

p-adic and complex geometry are similar

Theorem (Scholze)

Let $C/\mathbb{Q}_p$ be complete and algebraically closed. Let X be a smooth proper rigid analytic space over C. For all $i \geq 0$, we have

$$\sum_{j=0}^{i} \dim_C H^{i-j}(X, \Omega_X^j) = \dim_C H^i_{dR}(X/C) = \dim_{\mathbb{Q}_p} H^i_{et}(X, \mathbb{Q}_p)$$

The local-global principle

Theorem (Hasse-Minkowski)

Let $n \geq 1$ and let $a_i \in \mathbb{Q}$, $1 \leq i \leq n$. Then the equation

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = 1$$

has a solution $x_i \in \mathbb{Q}$, if and only if it has a solution in $\mathbb{R}$ and in every field $\mathbb{Q}_p$.

The local-global principle

Theorem (Hasse-Minkowski)

Let $n \geq 1$ and let $a_i \in \mathbb{Q}$, $1 \leq i \leq n$. Then the equation

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = 1$$

has a solution $x_i \in \mathbb{Q}$, if and only if it has a solution in $\mathbb{R}$ and in every field $\mathbb{Q}_p$.

Example (Hasse-Minkowski for $n = 1$)

$ax^2 = 1$ solvable in $\mathbb{Q} \Leftrightarrow a$ is a square $\neq 0 \Leftrightarrow a > 0$ and every prime p occurs with even exponent in factorization of a

When solutions exist …

…can we write them down?

Linear: $2x - 6 = 0, \qquad x = \frac{6}{2} = 3.$

When solutions exist …

…can we write them down?

Linear: $2x - 6 = 0, \qquad x = \frac{6}{2} = 3.$

$ax - b = 0,\ a \neq 0, \qquad x = \frac{b}{a} \in \mathbb{Q}.$

When solutions exist …

…can we write them down?

Linear: $2x - 6 = 0, \qquad x = \frac{6}{2} = 3.$

$ax - b = 0,\ a \neq 0, \qquad x = \frac{b}{a} \in \mathbb{Q}.$

Quadratic:

$$ax^2 + bx + c = 0,\ a \neq 0,$$

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ or } x = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \in \mathbb{R}.$$

Formulas for degrees 3, 4

(del Ferro, Tartaglia, Cardano, Ferrari $\approx$ 1500)

Formulas for degrees 3, 4

(del Ferro, Tartaglia, Cardano, Ferrari $\approx$ 1500)

Galois: No formula for higher degree! ($\approx$ 1830)

Formulas for degrees 3, 4

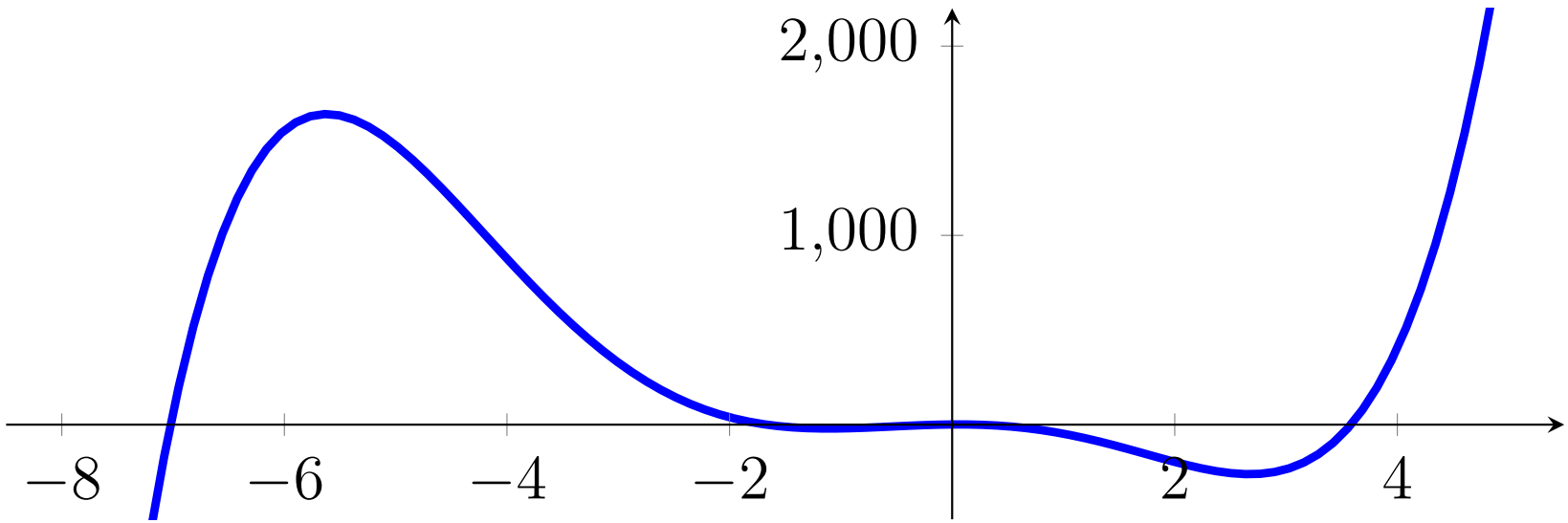
(del Ferro, Tartaglia, Cardano, Ferrari $\approx$ 1500)

Galois: No formula for higher degree! ($\approx$ 1830)

Even worse: For example, the zeros of the polynomial

$x^5 + 5x^4 - 20x^3 - 40x^2 + 5x + 1$

cannot be expressed in terms of $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{-}$.



Formulas for degrees 3, 4

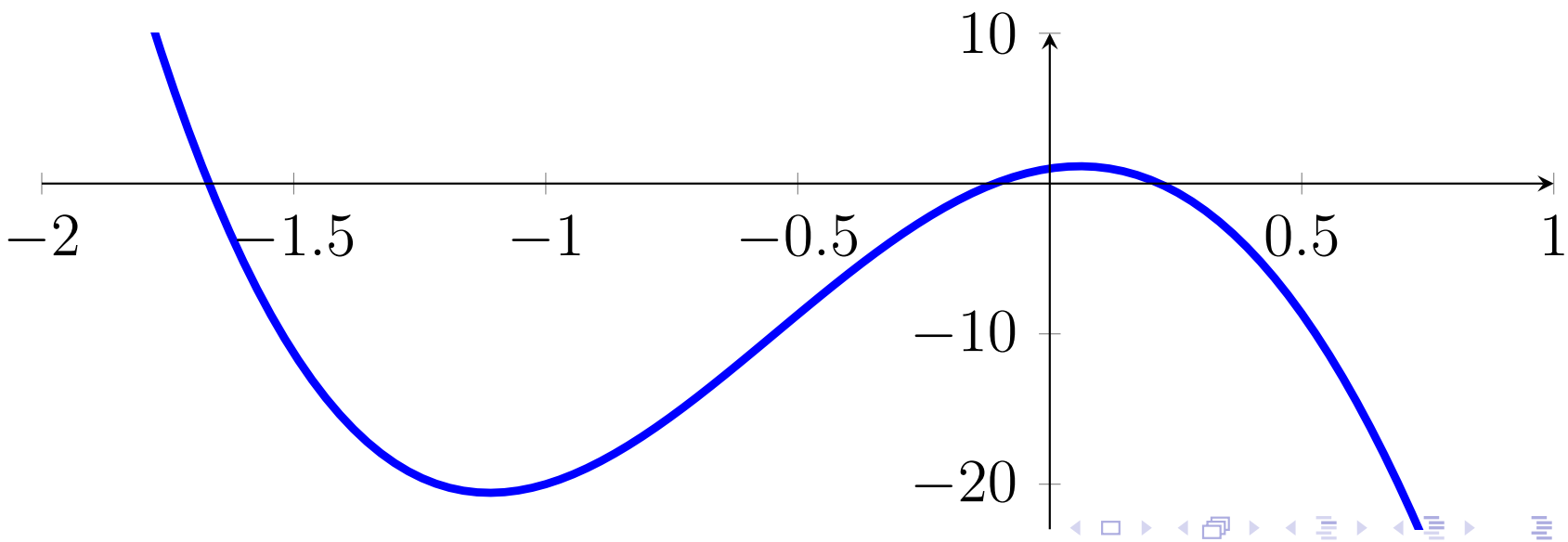
(del Ferro, Tartaglia, Cardano, Ferrari $\approx$ 1500)

Galois: No formula for higher degree! ($\approx$ 1830)

Even worse: For example, the zeros of the polynomial

$x^5 + 5x^4 - 20x^3 - 40x^2 + 5x + 1$

cannot be expressed in terms of $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{-}$.



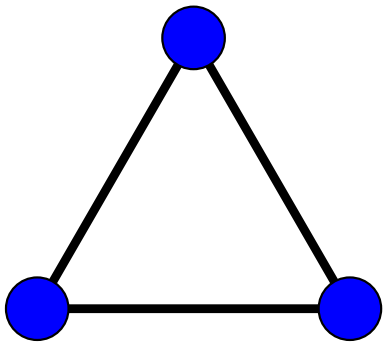
Why no formula?

…understand symmetries of set of solutions

Why no formula?

…understand symmetries of set of solutions

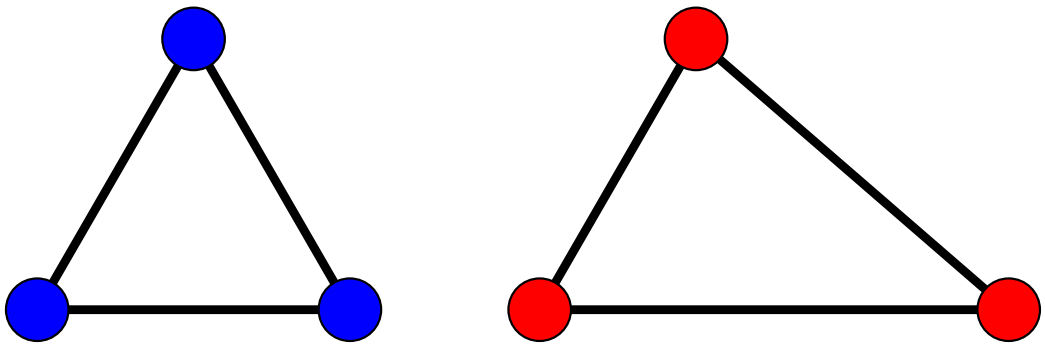
Distinguish geometric objects by their “symmetry group”



Why no formula?

…understand symmetries of set of solutions

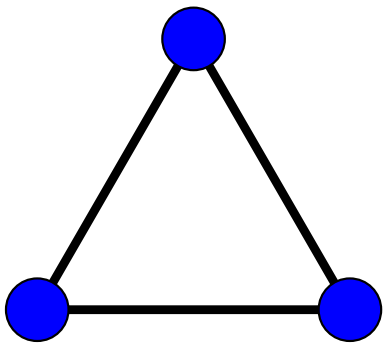
Distinguish geometric objects by their “symmetry group”

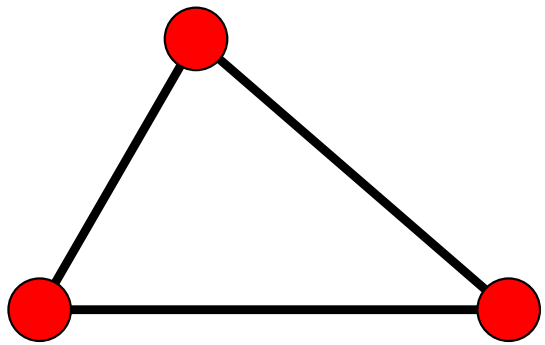


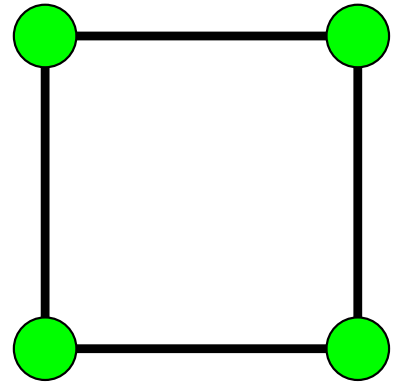
Why no formula?

…understand symmetries of set of solutions

Distinguish geometric objects by their “symmetry group”







Galois groups

Distinguish kind of solution of polynomial by their symmetry group

Definition (informal)

The Galois group of a polynomial is the group of permutations of the zeros of the polynomial that are compatible with $+$, $-$, $\cdot$.

Galois groups

Distinguish kind of solution of polynomial by their symmetry group

Definition (informal)

The Galois group of a polynomial is the group of permutations of the zeros of the polynomial that are compatible with $+$, $-$, $\cdot$.

Definition

Let f be a polynomial with coefficients in a field K. Let L be the smallest field containing K and all zeros of f (in some algebraically closed extension field).
The Galois group of f is the group of field automorphisms $L \to L$ which fix all elements of K.

Solvability in terms of Galois groups

Theorem

If f is a polynomial over $\mathbb{Q}$ whose solutions can be expressed in terms of $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{-}$ starting from rational numbers, then the Galois group of f is solvable.

Example

The Galois group of the polynomial

$$x^5 + 5x^4 - 20x^3 - 40x^2 + 5x + 1$$

is the symmetric group S_5 which is not solvable.

Can we understand Galois groups?

Definition (Absolute Galois group)

Let K be a field, and let $\overline{K}$ be a separable closure of K. We call $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K.

Can we understand Galois groups?

Definition (Absolute Galois group)

Let K be a field, and let $\overline{K}$ be a separable closure of K. We call $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K.

Example ($K = \mathbb{Q}$)

$G_{\mathbb{Q}}$ is highly mysterious.

Understanding it properly is one of the principal goals of number theory.

Can we understand Galois groups?

Definition (Absolute Galois group)

Let K be a field, and let $\overline{K}$ be a separable closure of K. We call $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K.

Example ($K = \mathbb{Q}$)

$G_{\mathbb{Q}}$ is highly mysterious.

Understanding it properly is one of the principal goals of number theory.

Example ($K = \mathbb{Q}_p$)

$G_{\mathbb{Q}_p}$ is somewhat easier to understand, but still complicated.

The absolute Galois group of a finite field

Definition (Finite field with p elements)

Let p be a prime number. We let

$$\mathbb{F}_p := \{0, 1, \ldots, p-1\}$$

with addition and multiplication "modulo p".

In particular: $\underbrace{1 + \cdots + 1}_{p \text{ summands}} = 0$ in $\mathbb{F}_p$. ("Characteristic p")

The absolute Galois group of a finite field

Definition (Finite field with p elements)

Let p be a prime number. We let

$$\mathbb{F}_p := \{0, 1, \ldots, p-1\}$$

with addition and multiplication "modulo p".

In particular: $\underbrace{1 + \cdots + 1}_{p \text{ summands}} = 0$ in $\mathbb{F}_p$. ("Characteristic p")

Remark

Let K be a field of characteristic p. Then

$$(x+y)^p = x^p + y^p \quad \text{for all } x, y \in K.$$

Remark

Let K be a field of characteristic p. Then

$$(x+y)^p = x^p + y^p \quad \text{for all } x, y \in K.$$

In other words: The map $x \mapsto x^p$ is a field homomorphism, the *Frobenius homomorphism*.

Remark

Let K be a field of characteristic p. Then

$$(x+y)^p = x^p + y^p \quad \text{for all } x, y \in K.$$

In other words: The map $x \mapsto x^p$ is a field homomorphism, the *Frobenius homomorphism*.

Consequence

The absolute Galois group $G_{\mathbb{F}_p}$ is isomorphic to $\widehat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$. It is topologically generated by the Frobenius automorphism.

How far apart are characteristic 0 and p?

Compare

$$\mathbb{Q}_p = \left\{ \sum_{i=i_0}^{\infty} a_i p^i;\ i_0 \in \mathbb{Z},\ a_i \in \{0, 1, \ldots, p-1\} \right\}.$$

versus

$$\mathbb{F}_p((t)) = \left\{ \sum_{i=i_0}^{\infty} a_i t^i;\ i_0 \in \mathbb{Z},\ a_i \in \{0, 1, \ldots, p-1\} \right\}.$$

These descriptions look similar, but addition is very different!

Perfectoid fields and tilting

Definition (Scholze)

A *perfectoid field* is a field K, complete with respect to a non-discrete non-archimedean valuation, with residue characteristic $p > 0$ with ring of integers $\mathcal{O}_K = \{x \in K;\ |x| \leq 1\}$, such that the map

$$\mathcal{O}_K/p \to \mathcal{O}_K/p, \quad x \mapsto x^p,$$

is surjective.

Example

$\mathbb{Q}_p(p^{1/p^\infty})^\wedge$, $\mathbb{Q}_p(\mu_{p^\infty})^\wedge$, $\mathbb{F}_p((t))(t^{1/p^\infty})^\wedge$.

Tilting: Switch from char. 0 to positive characteristic

Every perfectoid field K has a tilt $K^\flat$.

$$K^\flat = \text{Frac}(\varprojlim_{x \mapsto x^p} \mathcal{O}_K/p).$$

The tilt $K^\flat$ has characteristic p: $1 + \cdots + 1 = 0$ in $K^\flat$.

Theorem (Fontaine, Wintenberger)

$$G_K \cong G_{K^\flat}.$$

Perfectoid spaces

Definition (Scholze)

Let K be a perfectoid field. A perfectoid space over K is an adic space which is locally isomorphic to an affinoid adic space, i.e., an adic space of the form $Spa(R, R^+)$ where R is a perfectoid K-algebra.

Perfectoid spaces

Definition (Scholze)

Let K be a perfectoid field. A perfectoid space over K is an adic space which is locally isomorphic to an affinoid adic space, i.e., an adic space of the form $Spa(R, R^+)$ where R is a perfectoid K-algebra.

Tilting for perfectoid spaces

Every perfectoid space X has a tilt $X^\flat$, and both have "the same étale covers":

Theorem (Scholze)

$$\pi_1(X) \cong \pi_1(X^\flat)$$

The Langlands program

The Langlands program

Theorem (Quadratic Reciprocity Law, Gauß)

Let $p \neq q$ *be prime numbers* > 2, $p \equiv 1 \mod 4$. *The equation*

$$x^2 \equiv q \mod p \quad \textit{has a solution}$$

if and only if the equation

$$x^2 \equiv p \mod q \quad \textit{has a solution.}$$

The Langlands program

Theorem (Quadratic Reciprocity Law, Gauß)

Let $p \neq q$ be prime numbers > 2, $p \equiv 1 \mod 4$. The equation

$$x^2 \equiv q \mod p \quad \textit{has a solution}$$

if and only if the equation

$$x^2 \equiv p \mod q \quad \textit{has a solution.}$$

Example ($p = 5$, $q = 67$)

The equation $x^2 \equiv 67 \equiv 2 \mod 5$ has no solution.

Hence $x^2 \equiv 5 \mod 67$ has no solution.

Class field theory

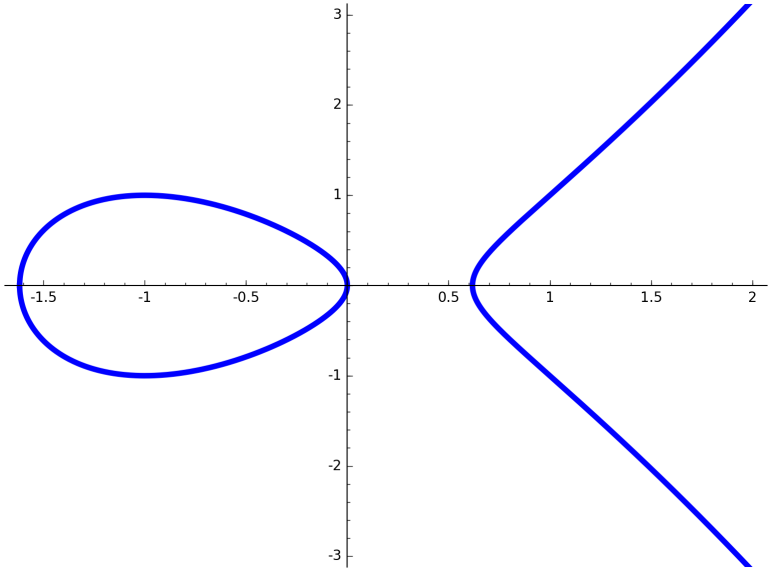
Describe the maximal abelian quotients $G_{\mathbb{Q}}^{\mathrm{ab}}$ and $G_{\mathbb{Q}_p}^{\mathrm{ab}}$.

> *La théorie du corps de classes a une réputation de difficulté qui est en partie justifiée. Mais il faut faire une distinction: il n'est peut-être pas en effet dans la science de théorie où tout à la fois les démonstrations soient aussi ardues, et les résultats d'une aussi parfaite simplicité et d'une aussi grande puissance.*
>
> *J. Herbrand, 1936*

Particular instance: Modularity

Elliptic curve

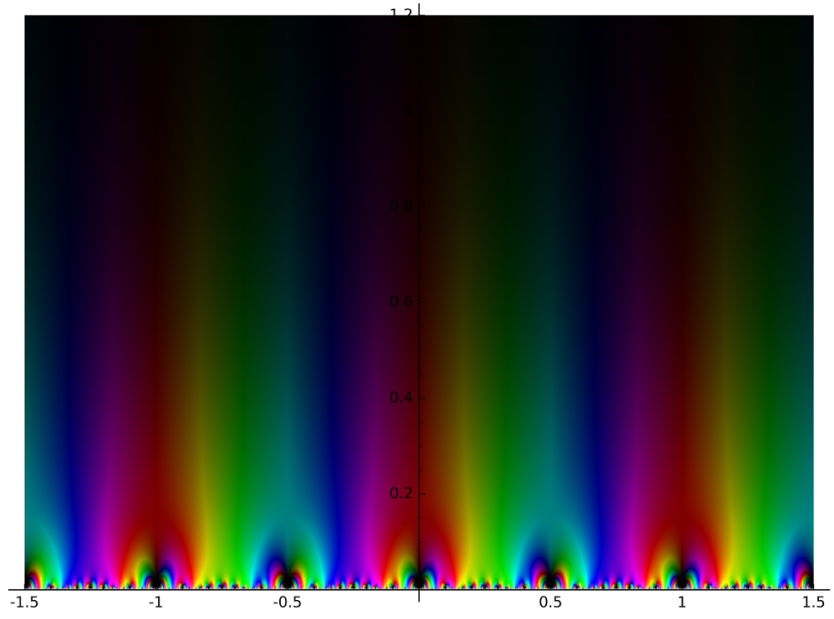
$$y^2 = x^3 + x^2 - x$$



Modular form

$$f : \mathbb{H} \to \mathbb{C}$$

holom., “highly symmetric”



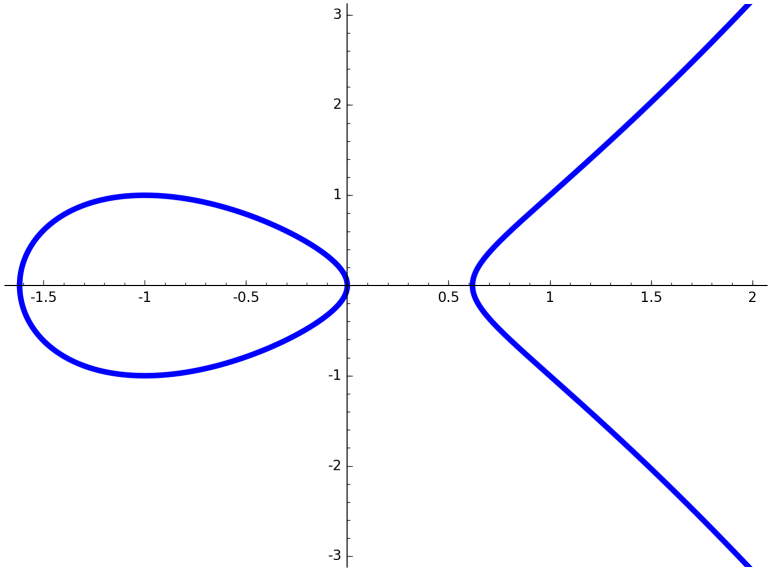
Theorem (Wiles, …)

Every elliptic curve E over $\mathbb{Q}$ is modular.

Particular instance: Modularity

Elliptic curve

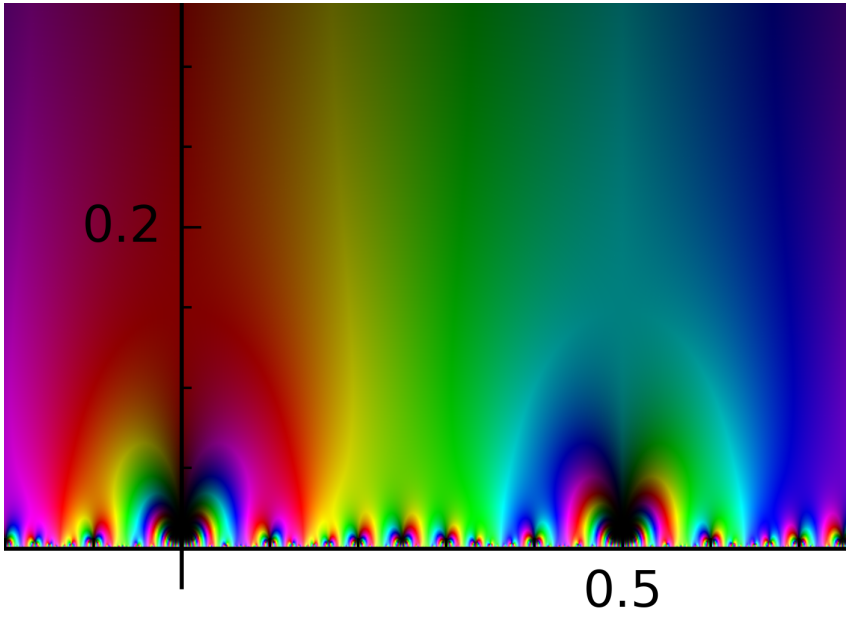
$$y^2 = x^3 + x^2 - x$$



Modular form

$f : \mathbb{H} \to \mathbb{C}$

holom., “highly symmetric”



Theorem (Wiles, …)

Every elliptic curve E over $\mathbb{Q}$ is modular.

Particular instance: Modularity

Elliptic curve

Numbers of solutions mod p,

p a prime number:

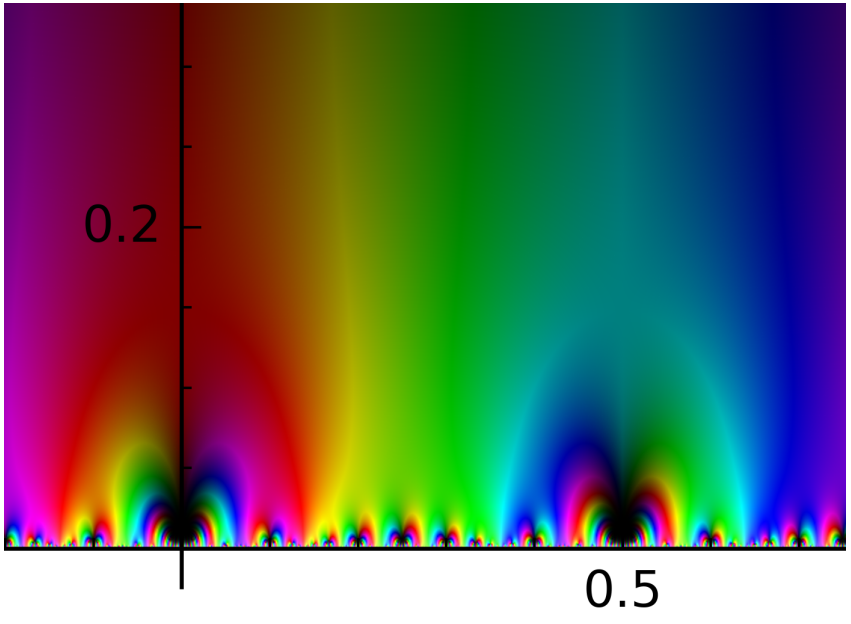
$$\#\{(x,y);\ 0 \le x,y \le p-1,\ y^2 \equiv x^3+x^2-x \bmod p\}$$

$\rightsquigarrow$ L-function $L(E/\mathbb{Q},s)$

Modular form

$f : \mathbb{H} \to \mathbb{C}$

holom., “highly symmetric”



Theorem (Wiles, …)

Every elliptic curve E over $\mathbb{Q}$ is modular.

Particular instance: Modularity

Elliptic curve

Numbers of solutions mod p, p a prime number:

$$\#\{(x,y);\ 0 \le x,y \le p-1,\ y^2 \equiv x^3+x^2-x \bmod p\}$$

$\rightsquigarrow$ L-function $L(E/\mathbb{Q},s)$

Modular form

Fourier expansion, $q = \exp(2\pi i z)$

$$q-2q^3-q^5+2q^7+q^9+2q^{13}+\cdots$$

$\rightsquigarrow$ L-function $L(f,s)$

Theorem (Wiles, ...)

Every elliptic curve E over $\mathbb{Q}$ is modular.

Corollary

The L-function $L(E/\mathbb{Q}, s)$ has a holomorphic continuation to $\mathbb{C}$.

Corollary

The L-function $L(E/\mathbb{Q}, s)$ has a holomorphic continuation to $\mathbb{C}$.

Theorem (Allen, Calegari, Caraiani, Gee, Helm, Le Hung, Newton, Scholze, Taylor, Thorne)

Let E be an elliptic curve over a CM field K. Then the L-function of E over K has a meromorphic continuation to $\mathbb{C}$.

Other direction: automorphic $\to$ Galois

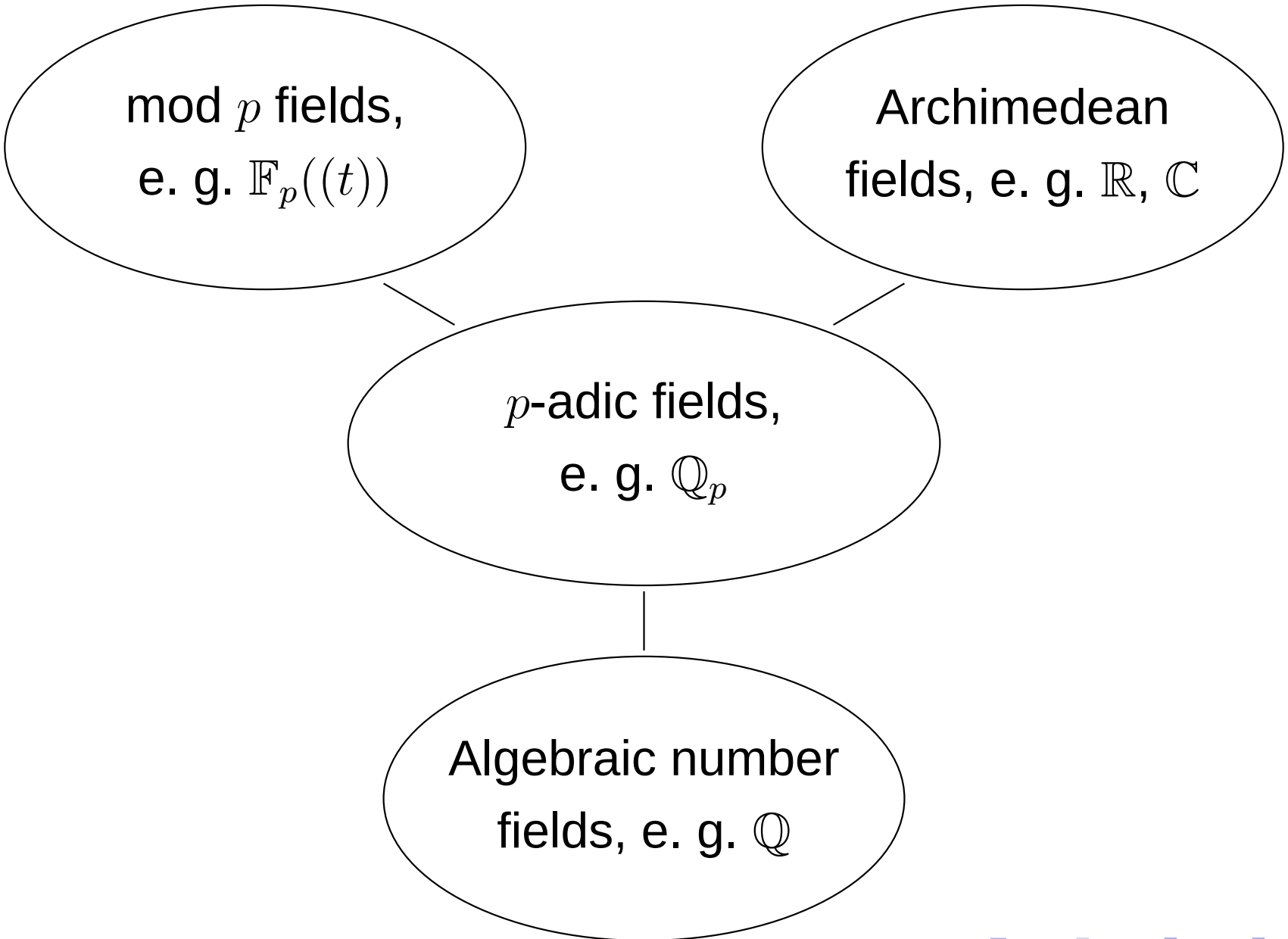
Theorem (Scholze)

Let F be totally real or CM, let $G = \mathrm{Res}_{F/\mathbb{Q}}(GL_n)$, and let X_K be the locally symmetric space attached to G and a compact open subgroup $K \subset G(\mathbb{A}_f)$. For every system of Hecke eigenvalues occurring in the cohomology $H^i(X_K, \overline{\mathbb{F}}_p)$, there exists a continuous Galois representation

$$\rho\colon \mathrm{Gal}(\overline{F}/F) \to GL_n(\overline{\mathbb{F}}_p)$$

such that Hecke eigenvalues and Frobenius eigenvalues match.

Goal of this talk



What is this good for?

Why are we doing this?

Fascinating to

- understand problems that have been studied for more than 2000 years,
- gain conceptual understanding of surprising patterns,
- teach the subject to others.

What is this good for?

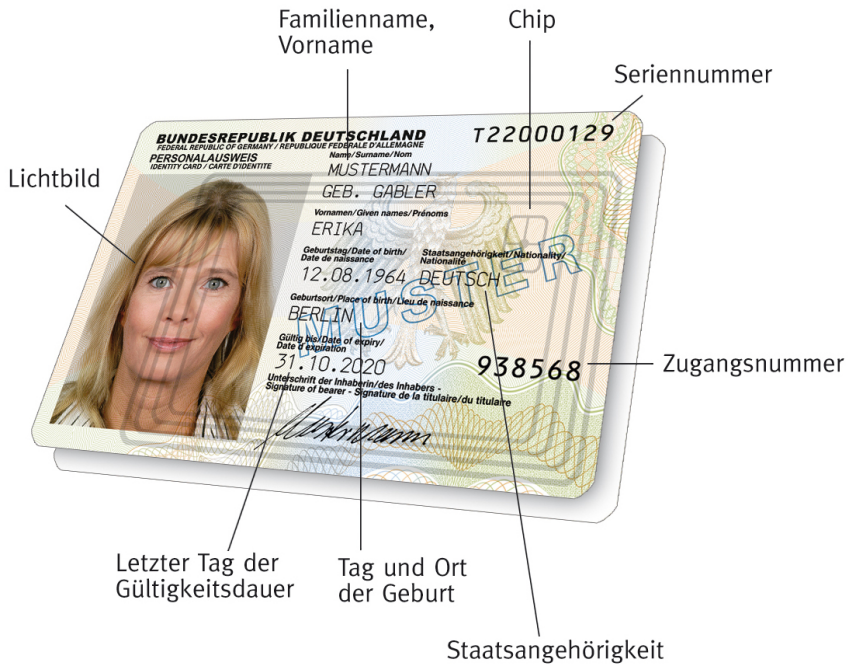
(Polynomial) equations are everywhere:

- Elliptic curve cryptography
- Theoretical physics
- Computer science
- Biochemistry
- …

What is this good for?

(Polynomial) equations are everywhere:

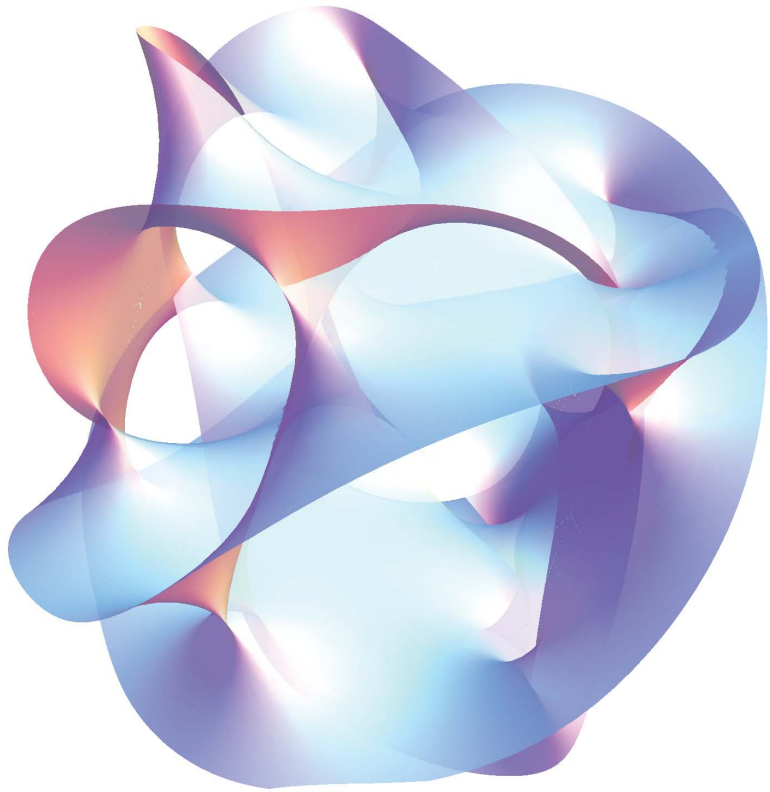
- Elliptic curve cryptography
- Theoretical physics
- Computer science
- Biochemistry
- …



What is this good for?

(Polynomial) equations are everywhere:

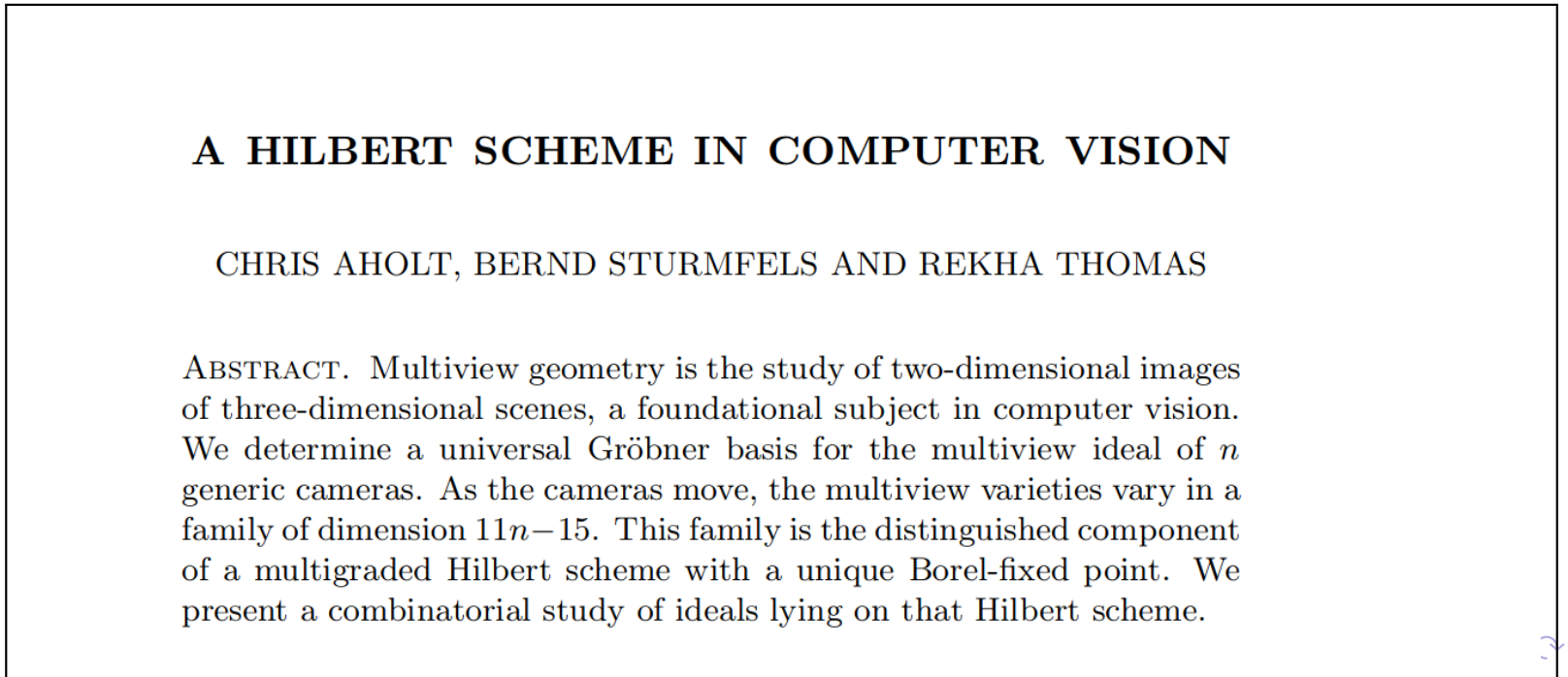
- Elliptic curve cryptography
- Theoretical physics
- Computer science
- Biochemistry
- …



What is this good for?

(Polynomial) equations are everywhere:

- Elliptic curve cryptography
- Theoretical physics
- Computer science
- Biochemistry
- …



A HILBERT SCHEME IN COMPUTER VISION

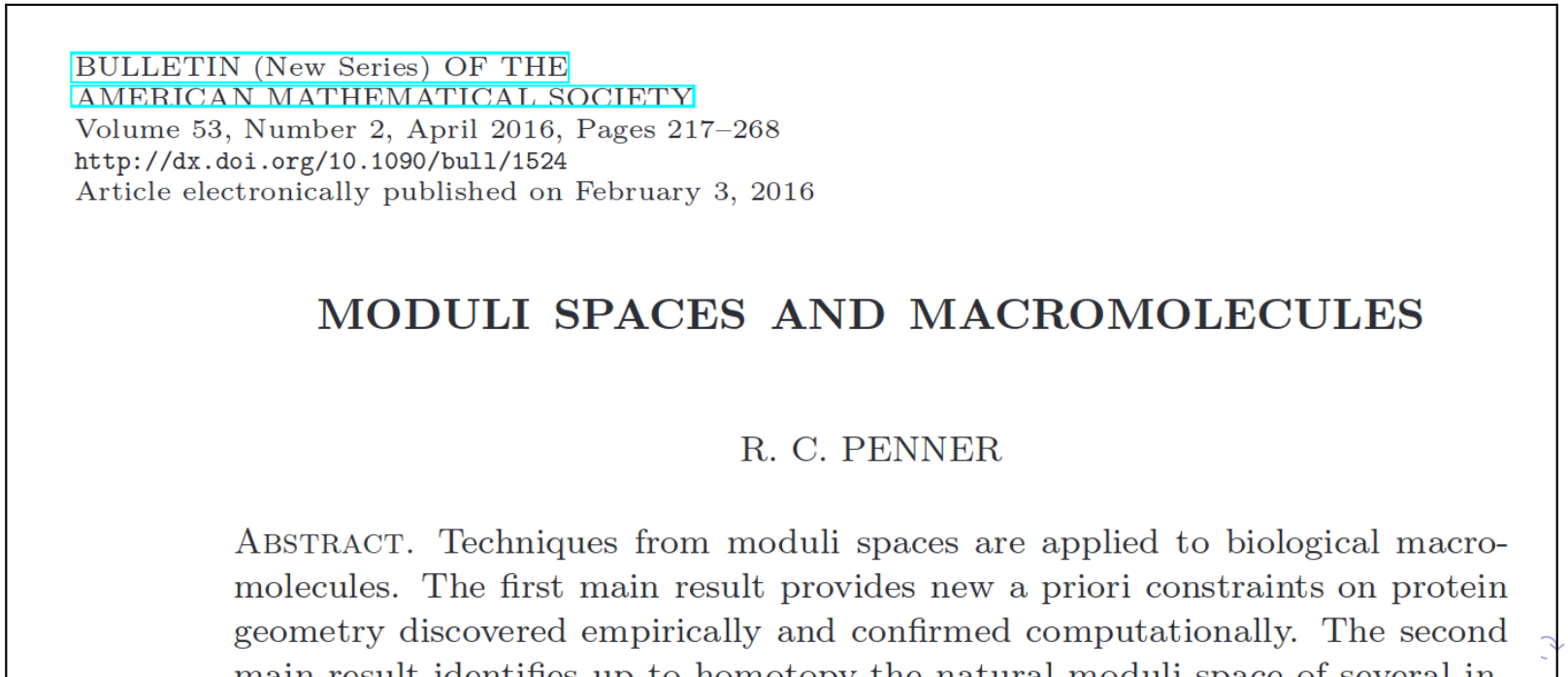
CHRIS AHOLT, BERND STURMFELS AND REKHA THOMAS

ABSTRACT. Multiview geometry is the study of two-dimensional images of three-dimensional scenes, a foundational subject in computer vision. We determine a universal Gröbner basis for the multiview ideal of n generic cameras. As the cameras move, the multiview varieties vary in a family of dimension $11n-15$. This family is the distinguished component of a multigraded Hilbert scheme with a unique Borel-fixed point. We present a combinatorial study of ideals lying on that Hilbert scheme.

What is this good for?

(Polynomial) equations are everywhere:

- Elliptic curve cryptography
- Theoretical physics
- Computer science
- Biochemistry
- …



BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 53, Number 2, April 2016, Pages 217–268
http://dx.doi.org/10.1090/bull/1524
Article electronically published on February 3, 2016

MODULI SPACES AND MACROMOLECULES

R. C. PENNER

ABSTRACT. Techniques from moduli spaces are applied to biological macromolecules. The first main result provides new a priori constraints on protein geometry discovered empirically and confirmed computationally. The second main result identifies up to homotopy the natural moduli space of several in-

Congratulations, Peter!

Seminar: Etale Kohomologie, WS 2007/08

"Programm": Wir haben die ersten drei Kapitel des Artikels von Deligne in SGA 4 1/2 gelesen

Vorträge

1	Treuflacher Abstieg	P. Scholze
2	Grothendieck-Topologien	S. Hähne
3	Etale Morphismen	T. Richarz
4	Die etale Fundamentalgruppe	R. Kucharczyk
5	Henselsche Ringe	A. Müller
6	Etale Garben	P. Hartwig
7	Halme, direktes Bild	A. Ivanov
8	Die Brauer-Gruppe	R. Kucharczyk
9	Der Satz von Tsen	F. Hellmann

Congratulations, Peter!