Abstract nonsense in Number Theory: replacing integers by polynomials

Antoine Leudière

PIMS PDF summit

April 28th, 2025

Introduction

From integers to elliptic curves

From elliptic curves to Drinfeld modules

About me

- PhD thesis: INRIA Nancy (France), with P.-J. Spaenlehauer and E. Thomé.
- PIMS PDF: University of Calgary, with R. Scheidler.
- Thank you PIMS and Kristine!
- Research interests: algorithmic number theory, Drinfeld modules, applications to information (cryptography, codes).

What is Number Theory?

Integer solutions of in/equations with integer coefficients (Diophantine equations).

Much harder than finding real solutions!

Examples:

- *Integer Linear Programming* (very practical problem with lots of applications) is NP-complete.
- Matiyasevich's theorem (see after).

Heuristics:

- Cannot approximate integers.
- No practical geometry on prime numbers.

What is Number Theory?

Integer solutions of in/equations with integer coefficients (Diophantine equations).

Much harder than finding real solutions!

Examples:

- *Integer Linear Programming* (very practical problem with lots of applications) is NP-complete.
- Matiyasevich's theorem (see after).

Heuristics:

- Cannot approximate integers.
- No practical geometry on prime numbers.

What is Number Theory?

Integer solutions of in/equations with integer coefficients (Diophantine equations).

Much harder than finding real solutions!

Examples:

- *Integer Linear Programming* (very practical problem with lots of applications) is NP-complete.
- Matiyasevich's theorem (see after).

Heuristics:

- Cannot approximate integers.
- No practical geometry on prime numbers.

Classical tools in Number Theory

Tools from classical arithmetics:

- Gauß's lemma: Let a, b, c be three integers such that a divides bc. If $\gcd(a, c) = 1$, then a divides b.
- Fermat's little theorem: Let a be an integer and p be a prime number. If p is not a factor of a, then p divides $a^{p-1} - 1$.
- Bézout's theorem: for any two integers a, b, there exist integers x, y such that $ax + by = \gcd(a, b)$.
- Gauß's Quadratic reciprocity law.

Classical tools in Number Theory

Tools from analytic number theory:

- Adamard and de la Vallée Poussin's prime number theorem: asymptotically, the number of prime numbers less than x is $x/\ln(x)$.
- Dirichlet's theorem on arithmetic progressions: for any two integers a, b such that $\gcd(a, b) = 1$, there are infinitely many primes of the form $a + xb$.

It's hard

Hilbert's 10th problem

Is there an algorithm that can tell if, for any input Diophantine equation, it has an integer solution?

Matiyasevich's theorem (1970)

No.

In other words, there are Diophantine equations that have no solutions but cannot be proven to have no solutions.

Because of this: number theorists look at **geometric problems**.

It’s hard

Hilbert’s 10th problem

Is there an algorithm that can tell if, for any input Diophantine equation, it has an integer solution?

Matiyasevich’s theorem (1970)

No.

In other words, there are Diophantine equations that have no solutions but cannot be proven to have no solutions.

Because of this: number theorists look at **geometric problems**.

It’s hard

Hilbert’s 10th problem

Is there an algorithm that can tell if, for any input Diophantine equation, it has an integer solution?

Matiyasevich’s theorem (1970)

No.

In other words, there are Diophantine equations that have no solutions but cannot be proven to have no solutions.

Because of this: number theorists look at **geometric problems**.

Introduction

From integers to elliptic curves

From elliptic curves to Drinfeld modules

Geometric problems

The solutions in $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ of a Diophantine equation form an *algebraic variety*.

Elliptic curves

Special kind of algebraic variety defined by

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Important theorem

Elliptic curves form a **group**.

Geometric problems

The solutions in $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ of a Diophantine equation form an *algebraic variety*.

Elliptic curves

Special kind of algebraic variety defined by

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Important theorem

Elliptic curves form a **group**.

Geometric problems

The solutions in $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ of a Diophantine equation form an *algebraic variety*.

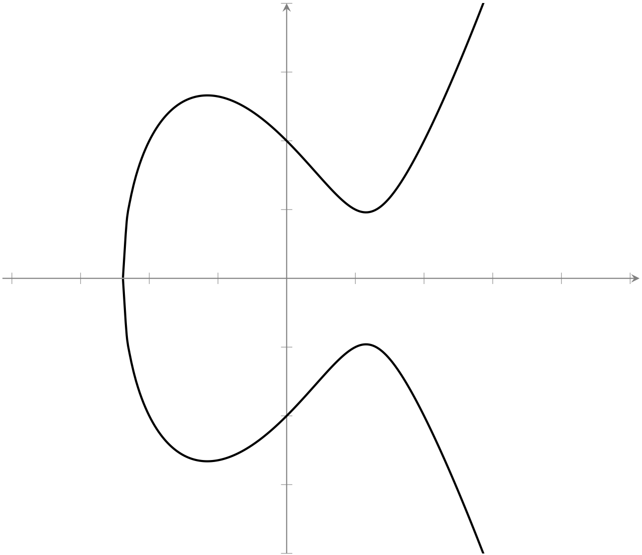
Elliptic curves

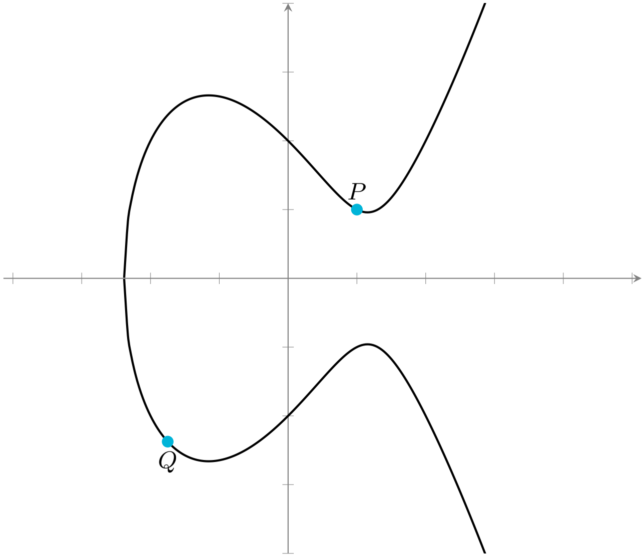
Special kind of algebraic variety defined by

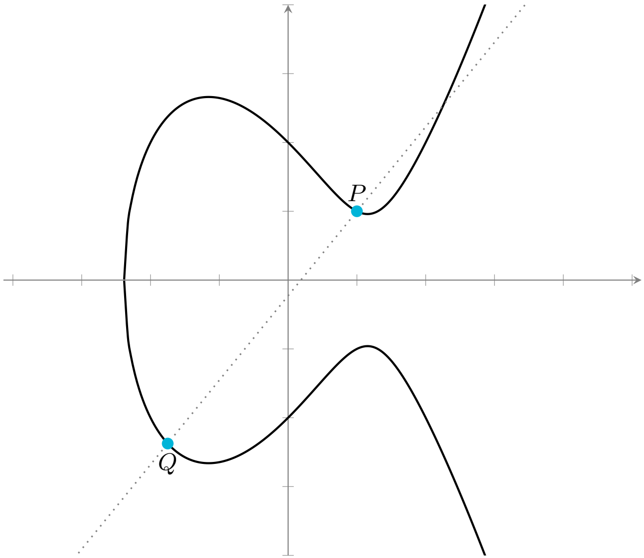
$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

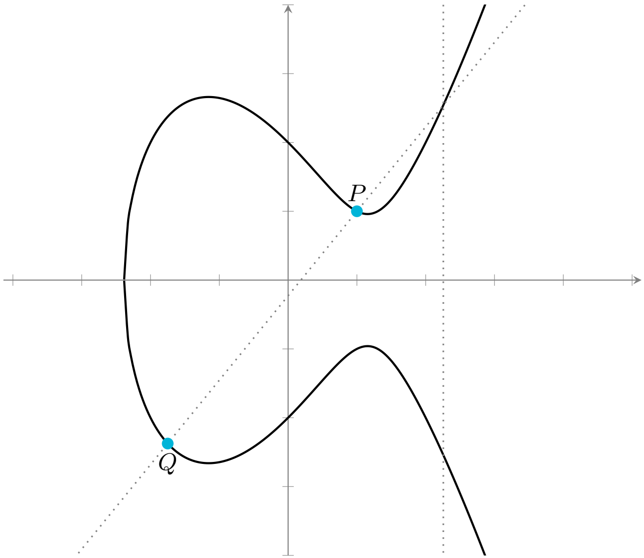
Important theorem

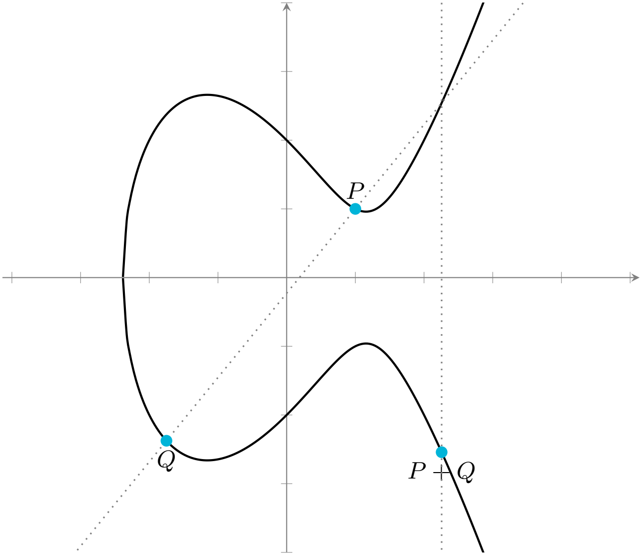
Elliptic curves form a **group**.




P
Q


P
Q


P
Q



P
Q
$P+Q$

ABC conjecture

ABC conjecture (Masser-Oesterlé)

For every $\varepsilon > 0$, there exist only finitely many integer triples (a, b, c) such that:

- a, b, c are pairwise coprime;
- $a + b = c$;
- $c > \mathrm{rad}(abc)^{1+\varepsilon}$, where $\mathrm{rad}(abc)$ is the product of distinct prime factors of abc.

The ABC conjecture is actually about elliptic curves!

Very strong statement that implies **many** results in Number Theory.

ABC conjecture

ABC conjecture (Masser-Oesterlé)

For every $\varepsilon > 0$, there exist only finitely many integer triples (a, b, c) such that:

- a, b, c are pairwise coprime;
- $a + b = c$;
- $c > \text{rad}(abc)^{1+\varepsilon}$, where $\text{rad}(abc)$ is the product of distinct prime factors of abc.

The ABC conjecture is actually about elliptic curves!

Very strong statement that implies **many** results in Number Theory.

Applications of elliptic curves

- Fermat's last theorem, class field theory, Langlands program.
- Computer algebra (integer factorization, discrete logarithm computation).
- Cryptography (classical and post-quantum).

Introduction

From integers to elliptic curves

From elliptic curves to Drinfeld modules

$\mathbb{Z}$ vs $\mathbb{F}_q[T]$

Notations:

- $\mathbb{F}_q$ is a *finite field* (*i.e.* finite cardinal).
- $\mathbb{F}_q[T]$ is the ring of polynomials with coefficients in $\mathbb{F}_q$.

Theorem

Both $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are *Euclidean*:

$\forall m, n \in \mathbb{Z}, \quad \exists a, b \in \mathbb{Z}$:

$$\begin{cases} m = an + b, \\ |b| < |n|. \end{cases}$$

$\forall P, Q \in \mathbb{F}_q[T], \quad \exists A, B \in \mathbb{F}_q[T]$:

$$\begin{cases} P = AQ + B \\ \deg(B) < \deg(Q). \end{cases}$$

$\mathbb{Z}$ vs $\mathbb{F}_q[T]$

Notations:

- $\mathbb{F}_q$ is a *finite field* (*i.e.* finite cardinal).
- $\mathbb{F}_q[T]$ is the ring of polynomials with coefficients in $\mathbb{F}_q$.

Theorem

Both $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are *Euclidean*:

$\forall m, n \in \mathbb{Z}, \quad \exists a, b \in \mathbb{Z}$:

$$\begin{cases} m = an + b, \\ |b| < |n|. \end{cases}$$

$\forall P, Q \in \mathbb{F}_q[T], \quad \exists A, B \in \mathbb{F}_q[T]$:

$$\begin{cases} P = AQ + B \\ \deg(B) < \deg(Q). \end{cases}$$

Drinfeld modules

Take-home message

Play the role of elliptic curves in the world where integers are polynomials (world of function fields).

Things you can do with Drinfeld modules:

- Solve the Riemann hypothesis for function fields.
- Solve the Langlands program for GL_r of a function field (Lafforgue, 2002 Fields medal).
- State of the art polynomial factorization (Doliskani-Narayanan-Schost).

Broader question

Characteristic 0 vs characteristic p.

Drinfeld modules

Take-home message

Play the role of elliptic curves in the world where integers are polynomials (world of function fields).

Things you can do with Drinfeld modules:

- Solve the Riemann hypothesis for function fields.
- Solve the Langlands program for GL_r of a function field (Lafforgue, 2002 Fields medal).
- State of the art polynomial factorization (Doliskani-Narayanan-Schost).

Broader question

Characteristic 0 vs characteristic p.

Drinfeld modules

Take-home message

Play the role of elliptic curves in the world where integers are polynomials (world of function fields).

Things you can do with Drinfeld modules:

- Solve the Riemann hypothesis for function fields.
- Solve the Langlands program for GL_r of a function field (Lafforgue, 2002 Fields medal).
- State of the art polynomial factorization (Doliskani-Narayanan-Schost).

Broader question

Characteristic 0 vs characteristic p.

My research

Algorithmic aspects of Drinfeld modules:

- With P.-J. Spaenlehauer: efficient computation of a group action from class field theory, and study of applications to cryptography.
- With X. Caruso: efficient computation of isogeny norms and characteristic polynomials of endomorphisms.
- With D. Ayotte, X. Caruso and J. Musleh: Drinfeld modules integration in SageMath.