Présentation du projet Papiée

Emmanuel Beffara, Martin Bodin, Nathan Coquerel

LIG, Inria

14 Avril 2026

Un TP de preuve

- Un TP qui s'insère dans un cours déjà existant en maths.
- Première utilisation d'un assistant à la preuve.

Objectif

- Aider à comprendre ce qu'est une preuve.
- Améliorer les productions écrites des élèves.

Non-objectifs

Apprendre à utiliser un assistant à la preuve.

Une interface qui ressemble le plus possible à un cours

- Notations mathématiques usuelles
- Varier les registres.
  - Possibilité d'ajouter des diagrammes, des tableaux, etc.

$\Rightarrow$ Un « Jupyter notebook » qui alterne Markdown et démonstrations interactives.

- Utilisation de langage naturel au lieu de tactiques.
  - Besoin d'autocomplétion.
  - Implicites de structure de preuve.

Structure de preuve

On pose $A_n = n(2n+1)(7n+1)$.
Montrons que $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, A_n = 3k$.
Soit $n \in \mathbb{N}$.
On distingue les cas suivants.

- Si $n \bmod 3 = 0$.
  Il existe alors k tel que $n = 3k$.
  Alors $A_n = 3(k(2n+1)(7n+1))$.
- Si $n \bmod 3 = 1$.
  Il existe alors k tel que $n = 3k+1$.
  Alors $2n+1 = 3(2k+1)$.
  Alors $A_n = 3(n(2k+1)(7n+1))$.
- Si $n \bmod 3 = 2$.
  Il existe alors k tel que $n = 3k+2$.
  Alors $7n+1 = 3(7k+5)$.
  Alors $A_n = 3(n(2n+1)(7k+5))$.

Structure de preuve

On pose $A_n = n(2n+1)(7n+1)$.
Montrons que $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, A_n = 3k$.
Soit $n \in \mathbb{N}$.
On distingue les cas suivants.

- Si $n \bmod 3 = 0$.
  Il existe alors k tel que $n = 3k$.
  Alors $A_n = 3(k(2n+1)(7n+1))$.
- Si $n \bmod 3 = 1$.
  Il existe alors k tel que $n = 3k+1$.
  Alors $2n+1 = 3(2k+1)$.
  Alors $A_n = 3(n(2k+1)(7n+1))$.
- Si $n \bmod 3 = 2$.
  Il existe alors k tel que $n = 3k+2$.
  Alors $7n+1 = 3(7k+5)$.
  Alors $A_n = 3(n(2n+1)(7k+5))$.

- Possibilité de réordonner les cas.
- Pouvoir continuer en cas d'erreur.
- Faire des vérifications en fin de cas.

Structure de preuve

On pose $A_n = n(2n+1)(7n+1)$.
Montrons que $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, A_n = 3k$.
Soit $n \in \mathbb{N}$.
On distingue les cas suivants.

- Si $n \bmod 3 = 0$.
  Il existe alors k tel que $n = 3k$.
  Alors $A_n = 3(k(2n+1)(7n+1))$.
- Si $n \bmod 3 = 1$.
  Il existe alors k tel que $n = 3k+1$.
  Alors $2n+1 = 3(2k+1)$.
  Alors $A_n = 3(n(2k+1)(7n+1))$.
- Si $n \bmod 3 = 2$.
  Il existe alors k tel que $n = 3k+2$.
  Alors $7n+1 = 3(7k+5)$.
  Alors $A_n = 3(n(2n+1)(7k+5))$.

```
1  \toBeProven{forall n, ...}
2  \letIn{n}{\mathbb{N}}.
3  \caseBegin{}.
4    \caseItem{n mod 3 = 0}.
5      \introExists{k}{n = 3 * k}.
6      \therefore{A_ n = 3 * ...}.
7      \caseItemEnd{}.
8    \caseItem{n mod 3 = 1}.
9      \introExists{k}{n = 3 * k + 1}
10     \therefore{2 * n + 1 = ...}.
11     \therefore{A_ n = 3 * ...}.
12     \caseItemEnd{}.
13   \caseItem{n mod 3 = 2}.
14     \introExists{k}{n = 3 * k + 2}
15     \therefore{7 * n + 1 = ...}.
16     \therefore{A_ n = 3 * ...}.
17     \caseItemEnd{}.
18 \caseEnd{}.
```

Structure de preuve

```
n : nat
__prop : n \in \mathbb{N}
__prop0 : n mod 3 = 2
__private1 : n mod 3 = 0 -> exists a ...
__private0 : n mod 3 = 1 -> exists a ...
__private : case_item_prop_lists
              [[n mod 3 = 1; n mod 3 = 0]]
```

```
\toBeProven{forall n, ...}
athbb{N}}.
.
n mod 3 = 0}.
ists{k}{n = 3 * k}.
re{A_ n = 3 * ...}.
mEnd{}.
n mod 3 = 1}.
ists{k}{n = 3 * k + 1}
re{2 * n + 1 = ...}.
  \therefore{A_ n = 3 * ...}.
  \caseItemEnd{}.
\caseItem{n mod 3 = 2}.
  \introExists{k}{n = 3 * k + 2}
  \therefore{7 * n + 1 = ...}.
  \therefore{A_ n = 3 * ...}.
  \caseItemEnd{}.
\caseEnd{}.
```

Variables :

$n \in \mathbb{N}$

Hypothèses :

$n \bmod 3 = 2$

Démonstration en construction

On pose $A_n = n(2n+1)(7n+1)$.
Montrons que $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, A_n = 3k$.
Soit $n \in \mathbb{N}$.
On distingue les cas suivants.

- Si $n \bmod 3 = 0$.
  $A_n = 3(k(2n+1)(7n+1))$.
- Si $n \bmod 3 = 1$.
  Il faut montrer que $A_n = 3(k(2n+1)(7n+1))$.

Styles de démonstrations

Raisonnement (in)équationnel

$$\begin{aligned} A_n &= n(2n+1)(7n+1) \\ &= 3(k(2n+1)(7n+1)) \end{aligned}$$

Analyse/synthèse

On cherche x tel que $P(x)$.
Nécessairement $Q(x)$.
Nécessairement $x = \ldots$.
Vérifions que $P(\ldots)$.

Grammaire contextuelle

- Une pile d'états de preuve
  - Raisonnement linéaire,
  - Raisonnement équationnel,
  - Analyse,
  - Synthèse.
- Chaque tactique indique un préfixe de pile et comment elle la modifie.

Grammaire contextuelle

```
const LET_IN = createTactic(
  "reasoning", "reasoning",
  "Soit $|identifier| \\in |inset|$.",
  ({ value }) =>
    `\\letIn{${value.identifier}}{${value.inset}}.`
);

const QED = createTactic(
  "reasoning", "end",
  "Ce qu'il fallait démontrer.",
  ({ value }) => `\\closeGoal{}.`
);
```

Grammaire contextuelle

```
const CASE_ANALYSIS = createTactic(
  "reasoning", "reasoning case>",
  "On distingue les cas suivants.",
  ({ value }) => `\\caseBegin{}.`
);

const CASE_ITEM = createTactic(
  "case", "case reasoning",
  "- Si $|property|$.",
  ({ value }) => `\\caseItem{(${value.property})}.`
);

const CASE_ITEM_END = createTactic(
  "case end", "case",
  "",
  ({ value }) => `\\caseItemEnd{}.`
);
```

Démo

`https://github.com/Wyrdix/Papiee`