Preuve et calcul, des rapports intimes

Gilles Dowek

Démontrer la correction d’un algorithme

Une activité récente ? ou ancienne ?

Un exemple : l'algorithme d'Euclide

Calculer le plus grand diviseur commun (pgcd) de ceux nombres

Qu'est-ce que le pgcd de deux nombres ?

Un algorithme pour calculer le pgcd

La définition

364 :

42 :

Un algorithme pour calculer le pgcd

La définition

$364 : 1, 2, 4, 7, 13, 14, 26, 28, 52, 91, 182, 364$

$42 :$

Un algorithme pour calculer le pgcd

La définition

$364 : 1, 2, 4, 7, 13, 14, 26, 28, 52, 91, 182, 364$

$42 : 1, 2, 3, 6, 7, 14, 21, 42$

Un algorithme pour calculer le pgcd

La définition

$364 : 1, 2, 4, 7, 13, 14, 26, 28, 52, 91, 182, 364$

$42 : 1, 2, 3, 6, 7, 14, 21, 42$

Un algorithme pour calculer le pgcd

La définition

$364 : 1, 2, 4, 7, 13, 14, 26, 28, 52, 91, 182, 364$

$42 : 1, 2, 3, 6, 7, 14, 21, 42$

14

Un autre algorithme pour calculer le pgcd : l'algorithme d'Euclide

$364, 42$

364	42
28	8

$364, 42 \longrightarrow 42, 28$

Un autre algorithme pour calculer le pgcd : l'algorithme d'Euclide

$364, 42$

$364, 42 \longrightarrow 42, 28$

Un autre algorithme pour calculer le pgcd : l'algorithme d'Euclide

$364, 42$

$364, 42 \longrightarrow 42, 28 \longrightarrow 28, 14$

Un autre algorithme pour calculer le pgcd : l'algorithme d'Euclide

$364, 42$

$364, 42 \longrightarrow 42, 28 \longrightarrow 28, 14 \longrightarrow 14$

Un même résultat ?

L'algorithme d'Euclide est correct

parce que

(1) si r reste de la div. de a par b alors $pgcd(a, b) = pgcd(b, r)$

(2) si a multiple de b, alors $pgcd(a, b) = b$

(3) pas de suites infinies décroissantes

Un même résultat ?

L'algorithme d'Euclide est correct

parce que

(1) si r reste de la div. de a par b alors $pgcd(a, b) = pgcd(b, r)$

(2) si a multiple de b, alors $pgcd(a, b) = b$

(3) pas de suites infinies décroissantes

Ces trois propositions doivent être démontrées : la démonstration de correction de l'algorithme d'Euclide

Démontrer la correction de l'algorithme d'Euclide aujourd'hui

Première déf. du pgcd : la spécification (algo. ou non, simple)

Seconde définition : l'algorithme

Dém. d'équivalence : démonstration de correction de l'algo.

Démontrer la correction de l'algorithme d'Euclide aujourd'hui

Première déf. du pgcd : la spécification (algo. ou non, simple)

Seconde définition : l'algorithme

Dém. d'équivalence : démonstration de correction de l'algo.

Souvent faciles mais grosses (parlent d'un gros objet)

La dém. de correction de l'algorithme d'Euclide est-elle correcte ?

Vérification de sa correction avec un logiciel de vérification de démonstrations (Coq, PVS, HOL, Isabelle, ...)

À quoi ça sert ?

À programmer sans bugs

À permettre de réutiliser l'algorithme d'Euclide dans la construction d'une démonstration ultérieure : rupture avec la méthode axiomatique

Deux types d’algorithmes

Les paraphrases de définitions

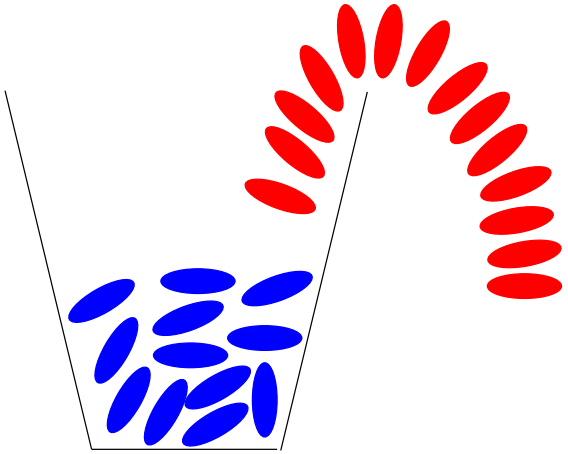
Les autres

Deux types d'algorithmes

Les paraphrases de définitions

Les autres : nécessitent une démonstration

L’addition



$$\begin{array}{r} 12 \\ 14 \\ \hline 26 \end{array}$$

Un peu d'histoire

Des démonstrations depuis 500 av. J.C. (Pythagore, Thalès, ...)

Des algorithmes depuis 2500 av. J.C. (au moins)

2000 ans de mathématiques purement algorithmiques en Mésopotamie, en Égypte, ...

Oui mais ...

Certains de ces algorithmes ne sont pas de simples paraphrases des définitions

Comment a-t-on pu les concevoir sans démonstrations ?

Oui mais ...

Comment a-t-on pu les concevoir sans démonstrations ?

... la découverte de tels procédés de résolution, dont la généralité transparaît sous les applications numériques particulières, n'a pu s'effectuer sans un minimum d'enchaînements logiques (peut-être pas entièrement conscients ...

Bourbaki (*Éléments d'Histoire des Mathématiques*)

Les Mésopotamiens et les Égyptiens

N’écrivaient pas de démonstrations sur les tablettes et papyrus

Mais savaient sans doute faire des démonstrations

En particulier des démonstration de correction d’algorithmes

Un peu de lumière sur le miracle grec ...

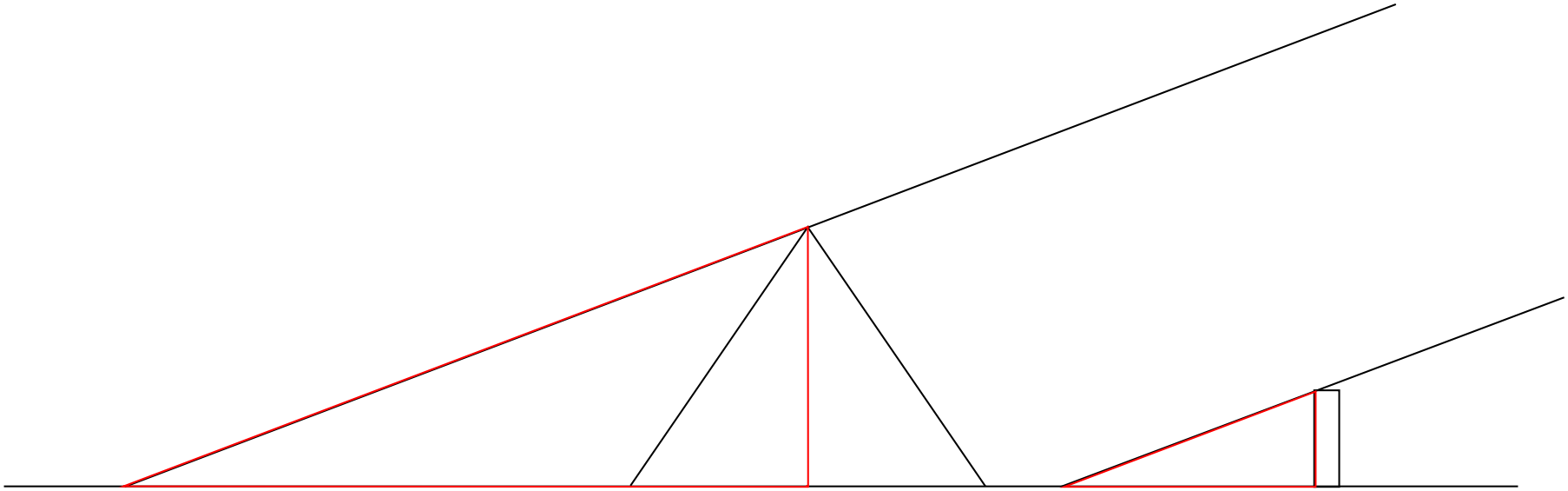
Mais alors, qu’ont apporté les Grecs ?

Un peu de lumière sur le miracle grec ...

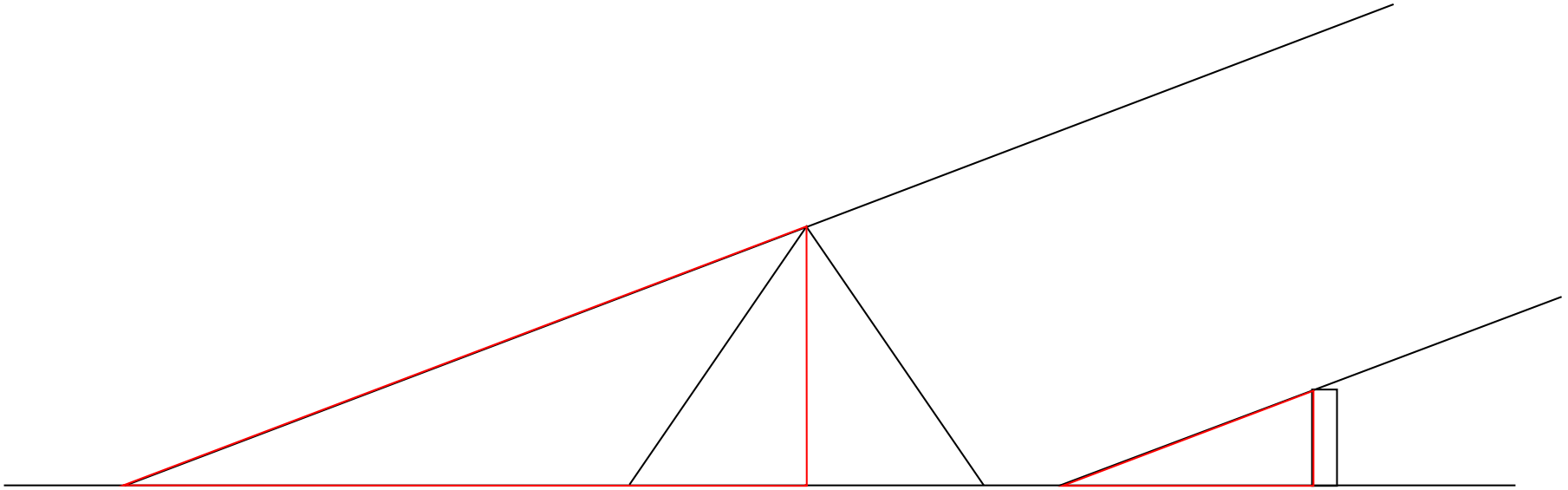
Mais alors, qu'ont apporté les Grecs ?

L'idée de faire des démonstrations qui ne sont pas des démonstrations de correction d'algorithmes

Les premières démonstrations libérées des algorithmes



Les premières démonstrations libérées des algorithmes



Et Pythagore aussi ...

Concevoir un algorithme demande de démontrer des théorèmes

Peut-être l’origine même de la notion de démonstration

Un point de méthode

Peu de sources citées : hypothèses à confronter aux sources

Nombreuses sources sur le caractère algorithmique des mathématiques en Mésopotamie et en Égypte

Mais peu de sources sur le théorème de Thalès et la mesure de la pyramide : Pline, Putarque et Diogène Laërce (brèves, postérieures, enjolivées, plus ou moins cohérentes et attestées)

Analyse des nécessités internes aux mathématiques : outil complémentaire des sources