BROUILLON - UNE PREUVE RIGOUREUSE (?) DE L'IRRATIONALITÉ DE LA RACINE CARRÉE D'UN NOMBRE PREMIER

CHRISTOPHE BAL

Document, avec son source LATEX, disponible sur la page
https://github.com/bc-writing/drafts.

Mentions « légales »

Table des matières

1. Où allons-nous ?

Ce modeste document va partir d'un fait classique que l'on va chercher à démontrer très rigoureusement. Nous commencerons par des preuves à la rédaction volontairement cavalière avec des phrases du type *« on voit bien que ... »* ou aussi *« c'est immédiat que ... »*. Chaque preuve sera ensuite suivie de blocs **Non Prouvé** indiquant des faits nécessitant d'être démontrés, chose qui sera faite par la suite.

L'idée, un peu folle, de ce document va être de dérouler des arguments de plus en plus fins et rigoureux. Nous allons voir que le chemin, bien que long, est très intéressant !

2. Notations

Notation 2.1. $\mathbb{P}$ *désignera l'ensemble des nombres premiers, c'est à dire l'ensemble des naturels* p *qui ont exactement deux diviseurs à savoir* 1 *et* $p \neq 1$.

Notation 2.2. *Pour* $(a\,;b) \in \mathbb{Z}^2$, $[\![a\,;b]\!]$ *désignera l'ensemble des entiers* k *tels que* $a \leq k \leq b$.

Date: 4 Avril 2019 - 4 Mai 2019.

3. $\sqrt{p}$ n'est pas rationnel, une preuve très classique

Fait 3.1. $\forall p \in \mathbb{P}, \sqrt{p} \notin \mathbb{Q}$.

Démonstration. Soit $p \in \mathbb{P}$ quelconque mais fixé. L'irrationalité de $\sqrt{p}$ peut se démontrer très classiquement comme suit.

- Regardons ce qu'il se passe si nous supposons l'existence de $(r\,;s) \in \mathbb{Q} \times \mathbb{Q}^*$ tel que $\sqrt{p} = \dfrac{r}{s}$. On peut supposer que $(r\,;s) \in \mathbb{Q}_+ \times \mathbb{Q}_+^*$ mais nous n'aurons pas besoin de supposer que $\operatorname{pgcd}(r\,;s) = 1$.
- $\sqrt{p} = \dfrac{r}{s} \Leftrightarrow p \times s^2 = r^2$ car $r \geq 0$ et $s > 0$.
- Nous pouvons écrire les naturels $s = \displaystyle\prod_{j=1}^{n} p_j$ et $r = \displaystyle\prod_{i=1}^{m} q_i$ sous forme de produits de nombres premiers. Après simplification dans $p \times s^2 = r^2$ des nombres premiers communs entre les p_j et les q_i de part et d'autre, il restera un nombre impair de facteurs premiers égaux à p à gauche, et un nombre pair à droite, éventuellement nul. Ceci n'est clairement pas possible.
- Comme nous obtenons quelque chose d'impossible, il ne peut pas exister $(r\,;s) \in \mathbb{Q} \times \mathbb{Q}^*$ tel que $\sqrt{p} = \dfrac{r}{s}$.

□

Non Prouvé 3.1. *Une première chose que nous avons admise très cavalièrement c'est la possibilité d'écrire un naturel comme un produit de facteurs premiers.*

→ *Voir le fait 4.1.*

Non Prouvé 3.2. *Un autre fait a été présenté comme immédiat à savoir l'impossibilité d'avoir une égalité entre deux produits de facteurs premiers dont l'un possède un nombre impair de facteurs premiers égaux à p, et l'autre en a un nombre pair éventuellement nul.*

Ceci équivaut à l'impossibilité d'avoir $p \times a = b$ où soit $b = 1$, soit $b \neq 1$ s'écrit comme un produit de facteurs premiers tous différents de p (pour se ramener à ce cas, il suffit de simplifier de part et d'autre des p tant que c'est possible).

→ *Voir le fait 4.2.*

4. Décompositions en produit de facteurs premiers

Fait 4.1. $\forall a \in \mathbb{N} - \{0\,;1\}$, *il existe au moins une suite finie de nombres premiers $(p_j)_{1 \leq j \leq n}$ telle que $a = \displaystyle\prod_{j=1}^{n} p_j$.*

Démonstration. Considérons $a \in \mathbb{N} - \{0\,;1\}$.

- Si a premier il suffit de choisir $n = 1$ et $p_1 = a$.
- Dans le cas contraire, $a = b\,c$ où $(b\,;c) \in [\![2\,;a-1]\!]$ par définition d'un nombre premier. Il suffit alors de reprendre le même type de raisonnement à partir de b et c car l'on obtiendra de proche en proche des naturels de plus en plus petits et donc forcément il arrivera un moment où la décomposition en produit de deux naturels du type $b\,c$ ne sera plus possible.

□

Non Prouvé 4.1. *Nous avons été bien cavaliers avec l'argument* « on obtiendra des naturels de plus en plus petits et donc forcément il arrivera un moment où... ». *Ce type d'argument se rédige proprement à l'aide du raisonnement par récurrence.*

→ *Voir le fait 5.1 et la preuve dans la section 5.2.*

Fait 4.2. *Si $p \in \mathbb{P}$ alors il n'existe pas $(a\,;b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $p\,a = b$ avec $b = 1$ ou $b \neq 1$ s'écrivant comme un produit de facteurs premiers tous différents de p.*

Démonstration. Ceci découle directement du fait suivant plus facile à retenir. □

Fait 4.3. *Soit $(a\,;b) \in \mathbb{N}^* \times \mathbb{N}^*$. Si $p \in \mathbb{P}$ vérifie $p\,a = b$ alors $b \neq 1$ et p apparait dans toute décomposition en facteurs premiers de b.*

Démonstration. $b \neq 1$ découle de $a \geq 1$ et $p \geq 2$. Supposons avoir au moins une suite $(q_i)_{1 \leq i \leq m}$ de nombres premiers tous distincts de p tels que $b = \prod_{i=1}^{m} q_i$. Nous raisonnons alors comme suit.

- Posant $q = q_1$ et $c = \prod_{i=2}^{m} q_i$ si $m \neq 1$ ou $c = 1$ sinon, nous avons l'identité $p\,a = q\,c$ avec p et q deux nombres premiers distincts.
- Par définition des nombres premiers, p et q ont juste 1 comme diviseur commun donc leur PGCD est 1.
- Si $c \neq 1$, démontrons que p divise c, autrement dit qu'il existe $k \in \mathbb{N}^*$ tel que $p\,k = c$. L'algorithme d'Euclide nous donne par remontée des calculs l'existence de $(u\,;v) \in \mathbb{Z}^2$ tel que $p\,u + q\,v = 1$. Ce résultat est appelé le théorème de Bachet-Bézout [1].

  Nous avons alors sans effort :

  $c = c(p\,u + q\,v)$

  $c = p\,c\,u + q\,c\,v$

  $c = p\,c\,u + p\,a\,v$ via $p\,a = q\,c$

  $c = p(c\,u + a\,v)$

  Donc $k = c\,u + a\,v$ convient.
- En répétant autant de fois que nécessaire ce qui précède, c'est à dire en isolant à chaque fois un facteur premier à droite, nous avons l'existence de $\widetilde{k} \in \mathbb{N}^*$ tel que $p\,\widetilde{k} = \widetilde{q}$ avec $\widetilde{q}$ un nombre premier distinct de p.
- Comme $\widetilde{q} \in \mathbb{P}$, ses seuls diviseurs sont 1 et lui-même. De $p\,\widetilde{k} = \widetilde{q}$ nous déduisons alors que p est un diviseur de $\widetilde{q}$. Comme $p \neq 1$, nous avons alors $p = \widetilde{q}$ ce qui n'est pas possible car par construction $\widetilde{q} \neq p$.

□

Non Prouvé 4.2. *L'algorithme d'Euclide, le théorème de Bachet-Bézout et l'existence d'une relation du type $p\,\widetilde{k} = \widetilde{q}$ ne peuvent être démontrés proprement que via un raisonnement par récurrence.*

→ *Voir les faits 5.3 et 5.4 ainsi que la section 5.4.*

Remarque 4.1. *Le fait 4.3 est une forme faible du lemme de divisibilité d'Euclide qui dit que si un nombre premier p divise le produit de deux nombres entiers b et c alors p divise b ou c* (il suffit de considérer des décompositions en facteurs premiers de b et c en s'inspirant de la preuve précédente).

1. À ne pas confondre avec une célèbre insulte du capitaine Haddock.

Notons au passage que le fait 4.3 implique l'unicité de la décomposition en facteurs premiers qui est indiquée dans le fait suivant.

Fait 4.4. $\forall a \in \mathbb{N} - \{0\,;1\}$, *il existe une et une seule suite finie croissante, non nécessairement strictement, de nombres premiers* $(p_j)_{1 \leq j \leq n}$ *telle que* $a = \prod_{j=1}^{n} p_j$.

Démonstration. L'existence découlant directement du fait 4.1, il nous reste à démontrer l'unicité. Pour cela considérons deux suites finies croissantes de nombres premiers $(p_j)_{1 \leq j \leq n}$ et $(q_i)_{1 \leq i \leq m}$ telles que $\prod_{j=1}^{n} p_j = \prod_{i=1}^{m} q_i$. Nous raisonnons alors comme suit pour prouver que les deux suites sont indentiques.

- Quitte à changer les noms des suites, on peut supposer que $p_1 \leq q_1$.
- D'après le fait 4.3, nous savons qu'il existe i tel que $q_i = p_1$.
- Par croissance de la suite q, nous avons $q_1 \leq q_i$.
- Nous avons alors $p_1 \leq q_1 \leq q_i = p_1$ puis $p_1 = q_1$.
- D'après le point précédent nous pouvons réduire de un les tailles des suites.

On voit alors que l'on pourra ainsi répéter le raisonnement pour obtenir que les deux suites sont de même taille et identiques *(une démonstration par récurrence trouverait sa place ici pour plus de rigueur mais nous ne la ferons pas dans ce document car le fait 4.4 est juste un petit bonus de notre exposé).* □

5. La démonstration par récurrence

5.1. La récurrence, quésako ?

Fait 5.1. *La preuve par récurrence s'exprime comme suit où* $\mathcal{P}(k)$ *désignera n'importe quelle proposition dépendant d'un paramètre naturel* $k \in \mathbb{N}$.

On suppose avoir démontré les deux faits suivants.

- $\mathcal{P}(0)$ *est vraie. On parle d'**initialisation**.*
- *Pour chaque naturel* k *quelconque, mais fixé, si l'on suppose* $\mathcal{P}(k)$ *vraie alors on peut en déduire que* $\mathcal{P}(k+1)$ *sera aussi vraie. On parle d'**hérédité**. Notons qu'ici nous ne savons pas démontrer que* $\mathcal{P}(k)$ *est vraie, nous ne faisons que le supposer.*

Sous ces hypothèses, nous pouvons affirmer que $\forall k \in \mathbb{N}$, $\mathcal{P}(k)$ *est vraie.*

Remarque 5.1. *Nous verrons dans le fait* **??** *que cette méthode de démonstration découle logiquement et rigoureusement d'une propriété simple de l'ensemble des naturels. Pour le moment, nous considérons cette méthode comme un axiome, c'est à dire comme étant une proposition tenue pour vraie sans avoir à être démontrée.*

Fait 5.2. *Soient* $k_0 \in \mathbb{N}$ *et* $\mathcal{P}(k)$ *une proposition dépendant d'un paramètre naturel* $k \in \mathbb{N}$ *tel que* $k \geq k_0$ *. On suppose avoir démontré les deux faits suivants.*

- $\mathcal{P}(k_0)$ *est vraie.*
- *Pour chaque naturel* $k \geq k_0$ *quelconque, mais fixé, si l'on suppose* $\mathcal{P}(k)$ *vraie alors on peut en déduire que* $\mathcal{P}(k+1)$ *sera aussi vraie.*

Sous ces hypothèses, nous pouvons affirmer que $\forall k \in \mathbb{N}$ *tel que* $k \geq k_0$, $\mathcal{P}(k)$ *est vraie.*

Démonstration. Il suffit d'appliquer le raisonnement par récurrence à la propriété $\mathcal{Q}(k)$ définie par « $\mathcal{P}(k+k_0)$ *est vraie* ». □

Remarque 5.2. *On parlera qu'en même d'un raisonnement par récurrence mais sous la condition* $k \geq k_0$.

5.2. **Retour sur l'existence d'une décomposition en facteurs premiers.** Nous pouvons enfin donner une preuve rigoureuse du fait 4.1 qui pour tout naturel $a \in \mathbb{N} - \{0\,;1\}$ affirme l'existence d'au moins une suite finie de nombres premiers $(p_j)_{1 \leq j \leq n}$ telle que $a = \prod_{j=1}^{n} p_j$.

Démonstration. Pour $k \geq 2$, notons $\mathcal{P}(k)$ la propriété « *Si* $a \in \mathbb{N}$ *vérifie* $1 < a \leq k$ *alors il existe au moins une suite finie de nombres premiers* $(p_j)_{1 \leq j \leq n}$ *telle que* $a = \prod_{j=1}^{n} p_j$ ». Nous allons faire une démonstration par récurrence sous la condition $k \geq 2$.

- **Initialisation :** démontrons que $\mathcal{P}(2)$ est vraie. C'est immédiat car la validité de $\mathcal{P}(2)$ vient de ce que si $a \in \mathbb{N}$ vérifie $1 < a \leq 2$ alors $a = 2$ et aussi de $2 = \prod_{j=1}^{1} p_j$ avec $p_1 = 2$ qui est un nombre premier.
- **Hérédité :** soit un naturel k quelconque, mais fixé, et supposons $\mathcal{P}(k)$ vraie. Nous devons en déduire que ceci implique que $\mathcal{P}(k+1)$ sera aussi vraie. Pour cela, considérons $a \in \mathbb{N}$ tel que $1 < a \leq k+1$. Nous avons alors trois cas possibles.
  - *Cas 1 :* $1 < a \leq k$.

    De la validité supposée de $\mathcal{P}(k)$, nous déduisons que $a = \prod_{j=1}^{n} p_j$ avec $(p_j)_{1 \leq j \leq n}$ une suite finie de nombres premiers.
  - *Cas 2 :* $a = k+1$ *et* a *est premier.*

    Dans ce cas, $a = \prod_{j=1}^{1} p_j$ avec $p_1 = a$ qui est un nombre premier.
  - *Cas 3 :* $a = k+1$ *et* a *n'est pas premier.*

    Ici $a = b\,c$ où $(b\,;c) \in [\![2\,;a-1]\!]$ par définition d'un nombre premier. Comme $[\![2\,;a-1]\!] \subseteq]\!]1\,;k]\!]$, de la validité supposée de $\mathcal{P}(k)$ nous déduisons que $b = \prod_{j=1}^{n} p_j$ et $c = \prod_{i=1}^{m} q_i$ avec $(p_j)_{1 \leq j \leq n}$ et $(q_i)_{1 \leq i \leq m}$ deux suites finies de nombres premiers. Il est alors immédiat d'écrire a comme un produit de nombres premiers.

  D'après les trois cas précédents, $\mathcal{P}(k+1)$ est vraie dès que $\mathcal{P}(k)$ est supposée vraie.
- **Conclusion :** par récurrence sur $k \geq 2$, nous avons prouvé que pour tout naturel $k \in \mathbb{N}$ vérifiant $k \geq 2$, la propriété $\mathcal{P}(k)$ est vraie. De ceci découle que le fait 4.1 est valide.

□

5.3. **L'algorithme d'Euclide et le théorème de Bachet-Bézout.**

Fait 5.3. *???*

Démonstration. ??? □

Fait 5.4. *???*

Démonstration. ??? □

5.4. **Retour sur la forme faible du lemme de divisibilité d'Euclide.** ???

Démonstration. Pour $k \geq 2$, notons $\mathcal{P}(k)$ la propriété « *Si* $a \in \mathbb{N}$ *vérifie* $1 < a \leq k$ *alors il existe au moins une suite finie de nombres premiers* $(p_j)_{1 \leq j \leq n}$ *telle que* $a = \prod_{j=1}^{n} p_j$ ». Nous allons faire une démonstration par récurrence sous la condition $k \geq 2$.

- **Initialisation :** démontrons que $\mathcal{P}(2)$ est vraie. C'est immédiat car la validité de $\mathcal{P}(2)$ vient de ce que si $a \in \mathbb{N}$ vérifie $1 < a \leq 2$ alors $a = 2$ et aussi de $2 = \prod_{j=1}^{1} p_j$ avec $p_1 = 2$ qui est un nombre premier.
- **Hérédité :** soit un naturel k quelconque, mais fixé, et supposons $\mathcal{P}(k)$ vraie.
- **Conclusion :** par récurrence sur $k \geq 2$, nous avons prouvé que pour tout naturel $k \in \mathbb{N}$ vérifiant $k \geq 2$, la propriété $\mathcal{P}(k)$ est vraie. De ceci découle que le fait 4.1 est valide.

□

---

6. AFFAIRE À SUIVRE...
