Théorème de Bachet-Bézout

Samuel Rochetin

Mercredi 5 décembre 2018

Résumé

Le but de ce document est de présenter quatre preuves de ce théorème d'arithmétique.

1 Énoncé du théorème

Théorème 1 (Claude-Gaspard Bachet de Méziriac, 1624)**.** *Soient a et b deux entiers relatifs.*

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$$

2 Preuve du sens indirect

La preuve du sens indirect ne présente aucune difficulté ; seul le sens direct constitue véritablement le théorème.

Démonstration. Supposons que $\exists (u, v) \in \mathbb{Z}^2, au + bv = 1$. Tout diviseur de a et b, en particulier $a \wedge b$, divise toute combinaison linéaire de a et b, en particulier $au + bv$. Donc $|a \wedge b| \leq 1$. Or, $1 \leq a \wedge b$ donc $a \wedge b = 1$. □

3 Preuve du sens direct

Le cas où $b = 0$ et le cas où $|b| = 1$ sont triviaux. Dans toutes les preuves ci-dessous, nous supposons que $|b| \geq 2$.

3.1 Preuve par la division euclidienne

Démonstration. Posons $E \coloneqq \left\{au + bv \in \mathbb{N}^*, (u, v) \in \mathbb{Z}^2\right\}$. Si $b > 0$, alors $b = a \times 0 + b \times 1 \in E$; si $b < 0$, alors $-b = a \times 0 + b \times (-1) \in E$. Ainsi, E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément n_0, non nul par définition de E. Autrement dit, $\exists (u, v) \in \mathbb{Z}^2, au + bv = n_0$. La division euclidienne de b par n_0 donne : $\exists ! (q, r) \in \mathbb{Z} \times \mathbb{N}, b = n_0 q + r, 0 \leq r < n_0$. Il vient : $r = a \times (-uq) + b \times (1 - vq)$. Si $0 < r$, alors $r \in E$. Or, $r < n_0$. Contradiction. Donc $r = 0$ et $n_0 \mid b$. Nous montrons de même que $n_0 \mid a$. Or, $a \wedge b = 1$, donc $n_0 \leq 1$. Or, $1 \leq n_0$ donc $n_0 = 1$. □

3.2 Preuves par les congruences

Quitte à changer b en $-b$ et v en $-v$, supposons que b est positif dans les preuves de cette section.

3.2.1 Système complet de résidus

Démonstration. Montrons que l'ensemble $R \coloneqq \{r \in [\![0, b-1]\!], ak \equiv r \pmod{b}, k \in [\![0, b-1]\!]\}$ est un système complet de résidus modulo b. Il suffit de montrer que les éléments de R sont distincts. Supposons qu'il existe deux termes distincts de la suite finie $(ak)_{k\in[\![0,b-1]\!]}$ ayant le même reste modulo b. Notons-les ai et aj, avec $i < j$. Ainsi :

$$\begin{aligned} & aj \equiv ai \pmod{b} & \\ \iff & a(j-i) \equiv 0 \pmod{b} & \\ \iff & j - i \equiv 0 \pmod{b} & \text{théorème de Gauss} \end{aligned}$$

Ainsi, $b \mid j - i$ donc $b \leq j - i \leq b - 1$. Contradiction. R contient donc b éléments distincts. En particulier, R contient 1 donc $\exists u \in [\![0, b-1]\!], au \equiv 1 \pmod{b}$. D'où $\exists v \in \mathbb{Z}, au + bv = 1$. □

Remarque 1. *D'un point de vue algorithmique, cette preuve donne une méthode pour déterminer un couple (u, v) : pour k allant de 1 à $b - 1$, il suffit de vérifier si ak est congru à 1 modulo b ; lorsque c'est le cas, le couple $(u, v) \coloneqq \left(k, \dfrac{1 - ak}{b}\right)$ convient.*

3.2.2 Puissances successives

Nous utilisons la proposition bien connue suivante.

Proposition 1. *Soient n un entier naturel supérieur ou égal à 2 et a un entier relatif.*

$$a \wedge n = 1 \implies \exists k \in \mathbb{N}^*, a^k \equiv 1 \pmod{n}$$

Démonstration. Il existe n restes possibles modulo n et il existe une infinité de termes de la suite $\left(a^k\right)_{k\in\mathbb{N}^*}$ donc d'après le principe des tiroirs, il existe au moins deux termes distincts de la suite $\left(a^k\right)_{k\in\mathbb{N}^*}$ ayant le même reste modulo n. Notons-les a^i et a^j, avec $i < j$. Ainsi :

$$\begin{aligned} & a^j \equiv a^i \pmod{n} & \\ \iff & a^i \left(a^{j-i} - 1\right) \equiv 0 \pmod{n} & \\ \iff & a^{j-i} - 1 \equiv 0 \pmod{n} & \text{théorème de Gauss} \\ \iff & a^{j-i} \equiv 1 \pmod{n} & \end{aligned}$$

□

Remarque 2. *Détaillons l'application du théorème de Gauss. D'après la décomposition canonique en produit de facteur premiers, les diviseurs premiers de a^i sont les mêmes que ceux de a. Or, a et n n'ont aucun diviseur premier commun donc il en va de même pour a^i et n. Ainsi, $a^i \wedge n = 1$.*

Cette proposition suffit à démontrer le sens direct du théorème de Bachet-Bézout.

Démonstration. La proposition précédente assure que $\exists k \in \mathbb{N}^*, a^k \equiv 1 \pmod{b}$. Ainsi, $\exists v \in \mathbb{Z}, a^k + bv = 1$. Enfin $u \coloneqq a^{k-1} \in \mathbb{Z}$ car $k \geq 1$. □

3.3 Preuve par l'algorithme d'Euclide étendu

Quitte à changer a en $-a$, u en $-u$, b en $-b$ et v en $-v$, supposons que a et b sont positifs.

Démonstration. L'algorithme d'Euclide consiste à écrire les divisions euclidiennes successives $a = bq + r, 0 \leq r < b$ puis $b = rq' + r', 0 \leq r' < r$ et ainsi de suite : d'après le cours, l'algorithme s'arrête lorsque le dernier reste est nul et le dernier reste non nul est $a \wedge b$. Ici, le dernier reste non nul est donc 1.

Intuitivement, $r = a \times 1 + b \times (-q)$ donc r est une combinaison linéaire de a et b; de même, $r' = b - rq' = a \times (-q') + b \times (1 + qq')$ donc r' est également une combinaison linéaire de a et b. Cela laisse penser que le dernier reste non nul 1 est aussi une combinaison linéaire de a et b. Montrons-le par récurrence.

Pour cela, introduisons $(r_n)_{n \in [\![0, N+1]\!]}$, la suite finie des restes successifs de l'algorithme d'Euclide, de sorte que $r_0 = a, r_1 = b, r_2 = r, r_3 = r', r_N = 1$ et $r_{N+1} = 0$. Introduisons aussi $(q_n)_{n \in [\![1, N]\!]}$, la suite finie des quotients successifs de l'algorithme d'Euclide, de sorte que $q_1 = q$ et $q_2 = q'$. Nous avons donc $\forall n \in [\![0, N-1]\!], r_n = r_{n+1}q_{n+1} + r_{n+2}$.

Montrons par récurrence double que $\forall n \in [\![0, N]\!], \exists (u_n, v_n) \in \mathbb{Z}^2, au_n + bv_n = r_n$. Initialisation : $a \times 1 + b \times 0 = r_0$ donc $(u_0, v_0) = (1; 0)$ et $a \times 0 + b \times 1 = r_1$ donc $(u_1, v_1) = (0; 1)$. Supposons que $\exists n \in [\![0, N-2]\!]$ tel que la propriété soit vraie aux rangs n et $n+1$. Montrons qu'elle est vraie au rang $n+2$. Nous avons :

$$\begin{aligned} r_{n+2} &= r_n - r_{n+1}q_{n+1} \\ &= au_n + bv_n - (au_{n+1} + bv_{n+1})q_{n+1} && \text{hypothèse de récurrence} \\ &= a(u_n - q_{n+1}u_{n+1}) + b(v_n - q_{n+1}v_{n+1}) \\ &= au_{n+2} + bv_{n+2} \end{aligned}$$

La propriété est ainsi démontrée $\forall n \in [\![0, N]\!]$, en particulier pour $n = N$, ce qui démontre le sens direct du théorème de Bachet-Bézout. □

Remarque 3. *D'un point de vue algorithmique, cette preuve donne une méthode pour déterminer un couple (u, v) : il suffit d'introduire le couple de suites $(u_n, v_n)_{n \in [\![0, N]\!]}$ défini par $(u_0, v_0) = (1; 0), (u_1, v_1) = (0; 1)$ et $\forall n \in [\![0, N-2]\!], (u_{n+2}, v_{n+2}) = (u_n - q_{n+1}u_{n+1}, v_n - q_{n+1}v_{n+1})$; le couple $(u, v) \coloneqq (u_N, v_N)$ convient.*