Lemme de Gauss

Samuel Rochetin

Vendredi 21 décembre 2018

Résumé

Le but de ce document est de présenter quatre preuves de ce théorème d'arithmétique, la quatrième n'étant qu'une amélioration formelle de la troisième.

1 Énoncé du théorème

Théorème (Carl Friedrich Gauss, 1801)**.** *Soient a, b et c trois entiers relatifs.*

$$a \mid bc \text{ et } a \wedge b = 1 \implies a \mid c$$

2 Preuves

2.1 Preuve par le PGCD

Démonstration. $a \mid ac$ et $a \mid bc$ donc $a \mid ac \wedge bc$. Et $ac \wedge bc = c(a \wedge b) = c$. □

2.2 Preuve par le théorème de Bachet-Bézout

Démonstration. $a \mid bc$ donc $\exists k \in \mathbb{Z}, bc = ka$. En outre, $a \wedge b = 1$ donc d'après le théorème de Bachet-Bézout, $\exists (u, v) \in \mathbb{Z}^2, au + bv = 1$. En multipliant par c, il vient $acu + bcv = c$, c'est-à-dire $(cu + kv)a = c$. □

2.3 Preuve par la décomposition canonique

Démonstration. On peut supposer que $a > 1$ et $b > 1$, le contraire ($a = 1$ ou $b = 1$) étant évident à traiter. Ainsi, a, b admettent des diviseurs premiers. En décomposant a et b en produit de facteurs premiers, l'égalité $bc = ka$ s'écrit $p_{b_1}^{\beta_1} \times \cdots \times p_{b_m}^{\beta_m} \times c = k \times p_{a_1}^{\alpha_1} \times \ldots p_{a_n}^{\alpha_n}$. Aucun des facteurs $p_{a_i}^{\alpha_i}$ n'apparaît dans la décomposition de b puisque a et b sont premiers entre eux. Or, la décomposition canonique est unique donc chacun de ces facteurs doit apparaître dans le membre de gauche, c'est-à-dire dans la décomposition canonique de c. Donc $a \mid c$. □

2.4 Preuve par la valuation

Démonstration. $a \mid bc$ donc $\exists k \in \mathbb{Z}, bc = ka$. Par unicité de la décomposition canonique en produit de facteurs premiers, pour tout nombre premier p, $v_p(bc) = v_p(ka) \iff v_p(b) + v_p(c) = v_p(k) + v_p(a)$. Si $a = 1$, alors le théorème est vrai. Sinon, a admet au moins un diviseur premier. Or, $a \wedge b = 1$ donc pour tout diviseur premier p de a, $v_p(b) = 0$. Donc $v_p(c) = v_p(k) + v_p(a) \geq v_p(a)$. Donc $a \mid c$. □