THÉORÈMES DE BASE EN ARITHMÉTIQUE

Maurice MIGNOTTE

1.— Introduction

Ce papier correspond à un exposé donné à l'IREM de Niamey en février 1989. Le but est de montrer que plusieurs théorèmes de base de l'arithmétique élémentaire (celle qui était jadis enseignée dans les lycées) sont en fait équivalents. On donne ici neuf énoncés, numérotés de 1 à 9, et on montre les implications

$$(\mathbf{1}) \Longrightarrow (\mathbf{2}),\ (\mathbf{2}) \Longrightarrow (\mathbf{3}),\ \ldots\ ,(\mathbf{8}) \Longrightarrow (\mathbf{9}),\ (\mathbf{9}) \Longrightarrow (\mathbf{1}).$$

En raison de ce souci d'économie, certaines de ces démonstrations sont assez artificielles, voire laborieuses. Le tout constitue un ensemble qu'il est hors de question de présenter aux élèves, il est particulièrement anti-pédagogique! Il s'agit d'un texte destiné au maître, qui montre la grande liberté que peut avoir l'enseignant dans l'ordre de présentation de ces résultats et qui prouve qu'aucun de ces théorèmes n'est plus "*fondamental*" qu'un autre.

Voici deux manières possibles de présenter ces théorèmes. De manière classique, on peut partir du théorème d'EUCLIDE-GAUSS (appelé aussi théorème fondamental de l'arithmétique) : soient a, b et c des entiers non nuls, si a divise bc et si a est premier avec b alors il divise c; en déduire ensuite l'unicité de la décomposition en facteurs premiers, puis l'existence du p.g.c.d., la relation de BÉZOUT ... De manière plus algébrique, on peut d'abord étudier les sous-groupes de $\mathbb{Z}$ (en utilisant la division euclidienne, on montre aussitôt qu'un tel sous-groupe est de la forme $d\mathbb{Z}$), puis en déduire l'existence du p.g.c.d. et la relation de BÉZOUT.

Il reste le point de vue algorithmique. Dans cette optique, on doit présenter l'algorithme d'EUCLIDE (dans sa version qui fournit aussi les coefficients de la relation de BÉZOUT); on peut parler un peu des tests de primalité, de la factorisation; il est bien sûr intéressant de donner quelques informations sur le coût de ces différents algorithmes. Une conséquence de la comparaison de ces différents coûts est que la présentation du p.g.c.d. via l'unicité de la factorisation est inadaptée aux calculs effectifs (sauf pour des entiers très petits).

2.— Enoncés

Dans toute la suite la lettre p désigne un nombre premier. Nous admettrons le résultat suivant

(0). *Pour tout entier n il existe p premier qui divise n.*

Nous aurons aussi besoin de l'asssertion ci-dessous.

(0'). *Tout entier positif n est un produit de facteurs premiers.*

Il est clair que **0'** implique **0**. Réciproquement, en raisonnant par récurrence sur n, on voit facilement que **0** implique **0'**. Ainsi, les assertions **0** et **0'** sont équivalentes.

(1). (EUCLIDE - GAUSS) *Si a divise bc et si a et b sont premiers entre eux alors a divise c.*

(2). *Si d'une part a et b sont premiers entre eux et si d'autre part a et c sont aussi premiers entre eux alors a et bc sont premiers entre eux.*

(3). *L'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est intègre.*

(4). *Si x est un entier non divisible par p alors il existe un entier positif k tel que l'on ait*

$$x^k \equiv 1 (\text{mod } p).$$

(5). *L'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps.*

(6). (BÉZOUT) *Si a et b sont deux entiers premiers entre eux alors il existe des entiers u et v tels que l'on ait*

$$ua + vb = 1.$$

(7). (Théorème chinois) *Si m et n sont deux entiers premiers entre eux alors pour tout couple d'entiers a et b il existe un entier x qui vérifie simultanément*

$$x \equiv a (\text{mod } m) \text{ et } x \equiv b (\text{mod } n).$$

(8). *Si b et c sont deux entiers premiers entre eux et si b divise a et c divise a alors le produit bc divise aussi a.*

(9). *Tout entier positif est égal à un produit de facteurs premiers et ceci de manière unique, à l'ordre près des facteurs.*

3.— Démonstration

Nous utiliserons la notation $(a, b) = 1$ qui signifie : a et b sont premiers entre eux.
(1) $\Longrightarrow$ **(2)**
Supposons que **(1)** soit vrai et que a, b et c soient tels que $(a, b) = (a, c) = 1$. Si **(2)** est faux (d'après **(0)**), il existe un nombre premier p qui divise bc et a; d'après **(1)**, puisque a et b sont premiers entre eux, ce nombre p divise c. Le fait que p divise à la fois a et c contredit l'hypothèse $(a, c) = 1$.

(2) $\Longrightarrow$ **(3)**
Si a et b sont premiers avec p, l'assertion **(2)** montre que leur produit est encore premier avec p. D'où l'implication.

(3) $\Longrightarrow$ **(4)**
Soit x un entier non divisible par p. Considérons les puissances de x modulo p. Comme il n'y a qu'un nombre fini de classes modulo p, il existe deux exposants m et n, $0 \leq m < n$, tels que $x^m \equiv x^n (\text{mod } p)$. Donc, $x^m(x^{n-m} - 1) \equiv 0 (\text{mod } p)$. Si l'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre, on en déduit, par récurrence sur m, la relation $x^{n-m} \equiv 0$ modulo p.

(4) $\Longrightarrow$ **(5)**
C'est immédiat.

(5) $\Longrightarrow$ **(6)**
Soient a et b deux entiers premiers entre eux. Grâce à la propriété **(0')** on peut écrire

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ et } b = q_1^{\beta_1} \dots q_s^{\beta_s},$$

où les nombres $p_1, \dots, p_r, q_1, \dots, q_s$ sont premiers et deux à deux distincts. En appliquant **(5)** on voit que pour tout i et j, $1 \leq i \leq r$ et $1 \leq j \leq s$, il existe des entiers u_{ij} et v_{ij} tels que l'on ait

$$u_{ij}p_i + v_{ij}q_j = 1.$$

On en déduit

$$(u_{ij}p_i + v_{ij}q_j)^{\alpha_i + \beta_j} = 1,$$

d'où l'existence d'entiers U_{ij} et V_{ij} tels que

$$U_{ij}p_i^{\alpha_i} + V_{ij}q_j^{\beta_j} = 1, 1 \leq i \leq r \text{ et } 1 \leq j \leq s.$$

En effectuant le produit sur $j, 1 \leq j \leq s$, des relations précédentes, on constate qu'il existe des entiers U_i et V_i tels que

$$U_i p_i^{\alpha_i} + V_i b = 1, 1 \leq i \leq r.$$

En faisant le produit sur $i, 1 \leq i \leq r$, de ces dernières relations on conclut qu'il existe des entiers u et v tels que

$$ua + vb = 1.$$

(6) $\Longrightarrow$ **(7)**
Si $um + vn = 1$ alors le nombre $x = avn + bum$ est une solution du système

$$x \equiv a (\text{mod } m) \text{ et } x \equiv b (\text{mod } n).$$

(7) $\Longrightarrow$ (8)
Le théorème chinois montre que l'application naturelle $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ qui à un entier x associe le couple (x mod m, x mod n) est surjective. De plus f est un homomorphisme d'anneaux qui est nul sur l'ensemble des multiples du produit mn. D'où, par passage au quotient, une application $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, qui est encore surjective. Mais, comme les ensembles de départ et d'arrivée de φ sont finis et comportent le même nombre d'éléments (à savoir mn éléments), φ est en réalité une bijection. Le fait que φ soit injective montre que tout nombre à la fois divisible par m et par n est divisible par le produit mn.

(8) $\Longrightarrow$ (9)
Supposons que la factorisation ne soit pas unique. Il existe alors un entier positif minimal n tel que

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r} = q_1^{\beta_1} \dots q_s^{\beta_s},$$

où les nombres $p_1, \dots p_r, q_1, \dots q_s$ sont premiers et deux à deux distincts.
Alors p_1 et q_1 divisent n, avec $(p_1, q_1) = 1$. L'assertion (**8**) montre que le produit $p_1 q_1$ divise n. Ainsi, $n = p_1 q_1 n'$. Ecrivons

$$n' = l_1^{\gamma_1} \dots l_r^{\gamma_r}.$$

On a donc

$$p_1 l_1^{\gamma_1} \dots l_r^{\gamma_r} = q_1^{\beta_1 - 1} q_2^{\beta_2} \dots q_s^{\beta_s}.$$

D'après la minimalité de n, p_1 n'admet une décomposition en facteurs premiers qui est unique; ceci impose à p_1 d'être égal à l'un des q_j : contradiction.

(9) $\Longrightarrow$ (1)
Soient a, b et c trois entiers tels que a divise bc et que a et b soient premiers entre eux. On peut supposer $a > 1$, sinon l'assertion (**1**) est triviale.
Grâce à la décomposition unique en facteurs premiers, puisque a divise bc on peut écrire

$$bc = p_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ et } a = p_1^{\beta_1} \dots p_s^{\beta_s},$$

avec $s \leq r$ et $1 \leq \beta_i \leq \alpha_i$ pour $1 \leq i \leq s$.
Puisque a et b sont premiers entre eux, l'entier b est nécessairement de la forme

$$b = p_{s+1}^{\gamma_{s+1}} \dots p_r^{\gamma_r}, 0 \leq \gamma_i \leq \alpha_i \text{ pour } s < i \leq r.$$

On en déduit que a divise c.

4.— Une question

A la suite de cet exposé, M. TRAOURÉ a posé la question suivante : étudier, dans un anneau plus général que $\mathbb{Z}$, les implications qui peuvent exister entre les généralisations des propriétés (**1**) à (**9**).