IV. L'ORDRE CLASSIQUE (c), (b), (a)

2) L'étude purement multiplicative des diviseurs et multiples peut alors procéder comme dans le 3) du § II. Pour l'identité de Bezout, il semble préférable d'avoir la théorie des congruences.

3) Jusqu'au théorème disant que Z/pZ est un corps lorsque p est premier (exclus), on procède comme dans le 1) du § II. Mais il n'est pas avantageux de démontrer directement ce théorème; en effet on en sait suffisamment pour démontrer un théorème plus fort, à savoir le dernier théorème du § II relatif à l'identité de Bezout. Alors l'énoncé relatif à Z/pZ (p premier) vient en corollaire: en effet un élément non nul de Z/pZ est la classe d'un entier premier à p, et est donc inversible dans Z/pZ d'après l'assertion *b)* du théorème.

IV. L'ordre classique (c), (b), (a)

1) L'exemple de l'ensemble nZ des multiples de n introduit la notion d'*idéal* de Z (et, plus généralement, d'un anneau commutatif quelconque). La division euclidienne permet alors de montrer le:

THÉORÈME. *Tout idéal* I *de* Z *est « principal », c'est-à-dire de la forme* nZ.

C'est clair si I est réduit à 0. Sinon I contient des éléments > 0, donc un plus petit élément > 0, soit n. Par division euclidienne de $x \in I$ par n, soit $x = nq + r$ avec $0 \leqslant r \leqslant n - 1$, on voit que $r \in I$, donc $r = 0$; ainsi $x \in nZ$, et $I = nZ$. C.Q.F.D.

L'existence du *ppcm* de deux entiers a et b est alors immédiate: en effet $Za \cap Zb$ est un idéal de Z, donc est de la forme Zm. Pour le *pgcd* on peut le déduire du ppcm, en vérifiant que l'entier $d = ab/\text{ppcm}\,(a, b)$, d'une part divise a et b, d'autre part est multiple de tout diviseur commun à a et b. Mais il est plus fructueux et plus classique de noter que tout diviseur commun à a et b divise tous les éléments de l'idéal $Za + Zb$ (ensemble des sommes $ua + vb$, où u et v parcourent Z); or cet idéal est de la forme Zd; comme $Za \subset Zd$, on voit que d divise a, et de même d divise b. Ainsi d a les propriétés classiques du pgcd; de plus il s'écrit

$$d = ua + vb \ (u, v \in Z) \qquad (3)$$

N. B. Il sera bon de dire que les mots « plus grand » et « plus petit » (dans « plus grand commun diviseur » et « plus petit commun multiple ») ne se rapportent qu'incidemment à la relation d'ordre usuelle de N,

mais se rapportent de façon essentielle à la relation d'ordre de la *divisibilité* sur N. D'ailleurs la théorie décrite ici s'applique à n'importe quel anneau principal A, et un tel anneau n'admet en général pas d'ordre analogue à l'ordre usuel de Z.

On démontre alors, à la manière classique, les formules du type pgc $(ab, ac) = a$ pgcd (b, c), le lemme d'Euclide, et les propriétés des entiers premiers entre eux. Un professeur soucieux de pureté s'efforcera de ne pas utiliser l'identité de Bezout dans des questions uniquement multiplicatives (comme le lemme d'Euclide), car il s'agit là de propriétés valables dans tout anneau factoriel, et pas seulement dans tout anneau principal.

On termine la partie (c) par l'*identité de Bezout*, qui affirme ici l'équivalence de:

a) a *et* b *sont premiers entre eux*; c) *il existe* u, v $\in$ Z *tels que* au + bv = 1.

La démonstration résulte aussitôt de la formule (3).

2) On passe à l'étude des nombres *premiers*. Pour l'existence de la décomposition en facteurs premiers, on procède comme dans le 2) du § II. Pour l'unicité on démontre le lemme « si p est premier et s'il divise ab, alors il divise a ou b », qui est une conséquence facile du lemme d'Euclide; l'unicité en résulte de façon classique. On introduit la notation (cf. 2) du § II):

$$x = \prod_{p \in P} p^{v_p(x)}$$

où P désigne l'ensemble des nombres premiers, et où les exposants $v_p(x)$ sont nuls à l'exception d'un nombre fini. Comme dans le 3) du § II, on donne la formule $v_p(xy) = v_p(x) + v_p(y)$, la condition de divisibilité « $v_p(x) \leqslant v_p(y)$ pour tout $p \in P''$, et les formules $v_p(\text{pgcd}(x, y)) = \inf(v_p(x), v_p(x))$ et $v_p(\text{ppcm}(x, y)) = \sup(v_p(x), v_p(y))$.

3) Pour la théorie des congruences on procède comme dans le 1) du § II jusqu'au théorème disant que Z/pZ est un corps lorsque p est premier (exclus). Comme dans le 3) du § III, on passe au théorème sur l'identité de Bezout (dernier théorème du § II); ici la démonstration est quasiment faite car, dans le 1), on a démontré l'équivalence des assertions *a)* et *c)*; reste l'assertion *b)* (« la classe $\bar{b}$ de b est inversible dans Z/aZ »), mais ce n'est qu'une traduction de *b)*. On donne en corollaire l'énoncé relatif à Z/pZ pour p premier (cf. le 3) du § III).