La notion de « module d'entiers » appliquée à la démonstration du théorème de Gauss sous sa forme générale

Dans un récent *Bulletin* (n° 174, décembre 1955) j'ai montré que le théorème suivant :

« *Si un nombre premier $p > 1$ divise un produit ab sans diviser a, alors il divise b* »

pouvait se déduire de la notion de « module d'entiers ». Il en est de même du théorème plus général :

« *Si un nombre $m > 1$ divise un produit ab et s'il est premier avec a, il divise b.* »

Je renvoie à l'article du n° 174 pour la définition et la propriété (existence d'une base) d'un module d'entiers ; il en résulte la démonstration suivante du théorème cité.

L'ensemble E des entiers x quelconques (positifs, négatifs ou nul) tels que :

$$ax \equiv 0 \pmod{m}$$

admet visiblement pour sous-ensemble l'ensemble E' des entiers y, tels que

$$y \equiv 0 \pmod{m}$$

et est un module d'entiers.

Si d ($d > 0$) est la base de ce module on a :

$$x \equiv 0 \pmod{d} \qquad \text{pour tout } x \in \text{E}.$$

Comme $m \in \text{E}' \subset \text{E}$ on a donc :

$$(1) \quad m \equiv o \pmod{d}.$$

De plus, par définition d E d'où

$$(2) \quad ad \equiv 0 \pmod{m}.$$

D'après (1) et (2) il existe deux entiers ordinaires k et k' tels que :

$$m = k.d,$$
$$ad = k'.m,$$

de ces deux égalités résulte

$$a = k.k',$$

k diviseur commun à d et a ne peut être d'après l'hypothèse que 1 ; par suite

$$d = m \qquad \text{et}$$

$$x \equiv 0 \pmod{m} \text{ pour tout } x \in E.$$

Or $b \in E$, car par hypothèse $ab \equiv 0 \pmod{m}$ d'où

$$b \equiv 0 \pmod{m} \qquad \text{(C.Q.F.D.)}.$$

Le théorème se trouve ainsi démontré sans la théorie du P.G.C.D. et sans faire intervenir les nombres premiers absolus. On peut évidemment exposer le raisonnement sans la notation des congruences.

Jacques LEGRAND (*Lycée de Biarritz*).