NOUVELLES ANNALES DE MATHÉMATIQUES

LEBESGUE

Note sur les congruences

Nouvelles annales de mathématiques 1re série, tome 9 (1850), p. 436-439

<http://www.numdam.org/item?id=NAM_1850_1_9__436_1>

NOTE SUR LES CONGRUENCES;

Par M. LEBESGUE,
Professeur à la Faculté de Bordeaux.

On emploie quelquefois les expressions

$$\frac{a}{b} \equiv c \pmod{p}, \quad \frac{a}{b} \equiv \frac{c}{d} \pmod{p},$$

sans bien les définir ; ce qui laisse quelque obscurité.

Une fraction $\frac{a}{b}$, dont le dénominateur est premier à p, est dite *congrue* au nombre c pour le module p, quand on peut poser $\frac{a+pk}{b}=c$, le nombre k étant entier. Comme il suit de là que l'on a

$$bc-a=pk \quad \text{ou} \quad bc\equiv a \ (\text{mod. } p),$$

on dira qu'un nombre et une fraction sont congrus, suivant le module p, quand leur différence a un numérateur divisible par p; ou bien encore, quand, en réduisant l'entier et la fraction au même dénominateur, on trouve des expressions fractionnaires dont les numérateurs sont congrus suivant le module donné.

Cette définition s'étendra à deux fractions $\frac{a}{b}, \frac{c}{d}$, dont les dénominateurs b, d sont premiers à p; elles seront congrues suivant le module p, si les fractions $\frac{ad}{bd}, \frac{bc}{bd}$ sont telles, que l'on ait

$$ad\equiv bc \ (\text{mod. } p) \quad \text{ou} \quad ad-bc\equiv 0 \ (\text{mod. } p).$$

Cela posé, voici quelques théorèmes très-simples :

Théorème I. *Les fractions équivalentes* $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}, \ldots,$ *ayant pour expression réduite (irréductible)* $\frac{\alpha}{\beta}$, *sont congrues, suivant le module p (premier à* β*), à un même nombre* ξ.

Soit

$$\frac{\alpha+pv}{\beta}=\xi \quad \text{ou} \quad \alpha=\beta\xi-pv;$$

cette équation fera connaître les entiers ξ et v, et l'on aura

$$\frac{\alpha}{\beta}\equiv\xi \ (\text{mod. } p).$$

Comme

$$\frac{a}{b} = \frac{\alpha}{\beta},$$

il en résultera

$$a = k\alpha, \quad b = k\beta,$$

k étant entier ; de là

$$k\alpha = k\beta\xi - pkv \quad \text{ou} \quad a = b\xi - p(kv),$$

ce qui donne

$$\frac{a}{b} \equiv \xi \pmod{p}.$$

On trouverait de même

$$\frac{c}{d} \equiv \xi, \quad \frac{e}{f} \equiv \xi, \ldots \pmod{p}.$$

Théorème II. *Si les fractions $\frac{a}{b}$, $\frac{c}{d}$ sont congrues suivant le module p premier à b et à d, elles seront congrues à un même nombre suivant le module p.*

L'expression

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{p},$$

revenant à

$$ad \equiv bc \pmod{p},$$

on a

$$ad - bc \equiv 0 \pmod{p};$$

on transformera la congruence par l'addition de

$$-bd\xi + bd\xi = 0.$$

On a ainsi

$$d(a - b\xi) - b(c - d\xi) \equiv 0 \pmod{p}.$$

Si l'on détermine ξ, de sorte que l'on ait

$$a \equiv b\xi \pmod{p},$$

ou encore

$$\frac{a}{b} \equiv \xi \ (\text{mod. } p),$$

puisque $a - b\xi$ est divisible par p, $c - d\xi$ le sera aussi ; donc

$$c \equiv d\xi \ (\text{mod. } p),$$

ou bien

$$\frac{c}{d} \equiv \xi \ (\text{mod. } p).$$

Ainsi les deux fractions sont congrues au même nombre ξ.

On voit que, dans ces deux théorèmes, il serait désavantageux de remplacer les mots *congruence, congrue* par *équivalence, équivalent*. Peut-être vaut-il mieux, dans tous les cas, s'en tenir aux expressions employées par M. Gauss.