JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

V.-A. LEBESGUE

Nombre de solutions d'une congruence du premier degré à plusieurs inconnues

Journal de mathématiques pures et appliquées 2e série, tome 4 (1859), p. 366.

<http://www.numdam.org/item?id=JMPA_1859_2_4__366_0>

NOMBRE DE SOLUTIONS
D'UNE CONGRUENCE DU PREMIER DEGRÉ A PLUSIEURS INCONNUES;

Par M. V.-A. LE BESGUE,
Correspondant de l'Institut.

Soit $p = hm + 1$ un nombre premier impair, g une racine primitive de p et $1 + x + x^2 + \ldots + x^{p-1} = 0$ (1). En posant $y_i = \sum x^{g^{km+i}}$, i étant un des nombres $0, 1, \ldots, m-1$ et k prenant les h valeurs $0, 1, 2, \ldots, h-1$, les m quantités $y_0, y_1, \ldots, y_{m-1}$ seront les racines de l'équation auxiliaire de degré m pour la résolution de l'équation (1). Cette auxiliaire se simplifiera si l'on pose $1 + my = z$.

Ceci rappelé, si l'on fait, pour abréger,

$$y_a y_b \ldots y_i + y_{a+1} y_{b+1} \ldots y_{i+1} + \ldots + y_{a+m-1} y_{b+m-1} \ldots y_{i+m-1} = \mathrm{T}(y_a y_b \ldots y_i),$$

on verra par la méthode exposée pages 287 et suivantes du tome II de la 1re série du *Journal de Mathématiques*, que les deux congruences à k inconnues

$$(a)\ g^b x_1^m + g^c x_2^m + \ldots + g^i x_k^m \equiv 0, \quad (b)\ g^a + g^b x_1^m + \ldots + g^i x_k^m \equiv 0 \ (\mathrm{mod.}\ p = hm + 1),$$

ont leur nombre de solutions S_k déterminé respectivement par les équations

$$(a')\ p\mathrm{S}_k = p^k + \frac{p-1}{m}\mathrm{T}(z_b z_c \ldots z_i), \quad (b')\ p\mathrm{S}_k = p^k + \frac{1}{m}[\mathrm{T}(z_a z_b \ldots z_i) - \mathrm{T}(z_b z_c \ldots z_i)],$$

si $x_1, x_2, \ldots, x_k$, nombres positifs inférieurs à p, peuvent être supposés nuls, et par les équations

$$(a'')\ p\mathrm{S}_k = (p-1)^k + \frac{p-1}{m} m^k \mathrm{T}(y_b y_c \ldots y_i), \quad (b'')\ p\mathrm{S}_k = (p-1)^k + m^k \mathrm{T}(y_a y_b \ldots y_i),$$

si $x_1, x_2, \ldots, x_k$ doivent tomber entre 0 et p.

Pour $m = 1$, on a $z_i = 0$, $y_i = -1$ et l'on trouve pour S_k les quatre nombres

$$p^{k-1},\ p^{k-1},\ \frac{1}{p}(p-1)[(p-1)^{k-1} - (-1)^{k-1}],\ \frac{1}{p}[(p-1)^k - (-1)^k].$$

Ces nombres sont indépendants des coefficients des congruences (a), (b), Il serait facile de donner *a priori* la raison de cette indépendance.