JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

V.-A. LEBESGUE

Note sur le Canon arithmeticus de Jacobi

Journal de mathématiques pures et appliquées 1re série, tome 19 (1854), p. 334-336.
<http://www.numdam.org/item?id=JMPA_1854_1_19__334_0>

NOTE

SUR

LE *CANON ARITHMETICUS* DE JACOBI,

PAR M. V.-A. LEBESGUE.

Quand on a trouvé une racine primitive $g < p$ pour le module premier p (calcul susceptible d'abréviation, comme je le montrerai ailleurs), on peut déterminer directement les racines primitives pour le module p^n.

Soit $g' < p^2$ le reste positif de g^p divisé par p^2; faites $h = \frac{g' - g}{p}$: la formule

$$g + px + p^2 y$$

donnera $p^{n-2}(p-1)$ racines primitives, en posant

$$x = 0,\ 1,\ 2,\ h-1,\ h+1,\ \ldots\ldots,\ p-1,$$
$$y = 0,\ 1,\ 2,\ \ldots\ldots\ldots\ldots\ldots,\ p^{n-2}-1,$$

et combinant de toutes les manières possibles les valeurs de x et celles de y.

Comme on peut remplacer g par g^i, $i < p-1$ étant premier à $p-1$, c'est-à-dire susceptible de $\varphi(p-1)$ valeurs, le nombre de racines primitives est donc

$$p^{n-2} \cdot p - 1 \cdot \varphi(p-1) = \varphi(p^{n-1}) \cdot \varphi(p-1) = \varphi(p^{n-1} \cdot p - 1) = \varphi\varphi(p^n),$$

comme on le sait.

L'exclusion de $x = h$ tient à ce que $(g + ph)^{p-1} - 1$ est divisible par p^2.

Jacobi a prouvé que les racines primitives pour le module p^2 le sont aussi pour le module p^n; c'est une conséquence de la règle donnée

plus haut. Il a vérifié que presque toujours les racines pour le module p le sont pour le module p^2.

L'exception tient à ce qu'on peut avoir, mais très-rarement, $h = 0$. Alors g, racine primitive pour le module p, ne l'est pas pour le module p^2.

On peut donc, pour le module p^n, en représentant par a un entier quelconque premier à p^n et plus petit, déterminer un entier α ou ind $a < p^{n-1}(p-1)$, et tel qu'on ait

$$g^{\text{ind } a} \equiv a \,(\text{mod. } p^n).$$

De là les deux Tables du *Canon* :

L'une donnant ind a quand on connaît a;

L'autre donnant a quand on connaît ind a.

Comme les congruences

$$g^{\text{ind } a} \equiv a \,(\text{mod. } p^n), \quad g^{\frac{p^{n-1}(p-1)}{2}} \equiv -1 \,(\text{mod. } p^n)$$

donnent

$$g^{\text{ind } a + \frac{p^{n-1}(p-1)}{2}} \equiv (p-a),$$

on reconnaît de suite que les Tables peuvent être réduites *à moitié*.

L'usage principal du *Canon*, c'est la résolution de la congruence

$$ax^m \equiv b \,(\text{mod. } p^n).$$

En effet, si l'on a

$$acd\ldots e \equiv b \,(\text{mod. } p^n),$$

on a aussi par cela même

$$\text{ind } a + \text{ind } c + \ldots + \text{ind } e \equiv \text{ind } b \,(\text{mod. } p^{n-1}.p-1) :$$

donc de

$$ax^m \equiv b \,(\text{mod. } p^n)$$

on conclut

$$m \,\text{ind } x \equiv \text{ind } b - \text{ind } a \,(\text{mod. } p^{n-1}.p-1).$$

De là directement, ou à l'aide de la Table, on tire ind x, puis x au moyen de la Table. Comme ind x peut avoir plusieurs valeurs, il en est de même de x.

Le module 2^n ne présente aucune difficulté, et si la Table n'était pas très-peu étendue, il serait également facile de la réduire *à moitié*.

Le *Canon arithmeticus* n'est pas seulement utile pour la résolution numérique de

$$ax^m \equiv b \,(\text{mod. } p^n).$$

Ainsi j'ai montré, d'après *Eisenstein*, comment le *Canon* fait connaître les coefficients entiers a_0, a_1, etc., de l'équation

$$p = f(\rho) \cdot f(\rho^{-1}),$$

où

$$\rho^m = 1, \quad p = m\varpi + 1, \quad m > 2,$$
$$f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{m-1}\rho^{m-1}.$$

Comme on en tire

$$\mathrm{F}(\rho) = [f(\rho)]^k = \mathrm{A}_0 + \mathrm{A}_1\rho + \ldots + \mathrm{A}_{m-1}\rho^{m-1}, \quad p^k = \mathrm{F}(\rho) \cdot \mathrm{F}(\rho^{-1}),$$

si, dans la décomposition de $2p$ en m carrés, on change a en A, on aura une décomposition correspondante de $2p^k$ en m carrés.

Le *Canon arithmeticus* a été publié *impensis Academiæ litterarum regiæ Borussicæ*; il est très-correct, *cura et benevolentia virorum clarissimorum, Professorum Dirichlet, Dove, Steiner; Doctorum Wolfers, Bremiker, Galle*, sans oublier surtout le célèbre astronome *Encke*, car Jacobi finit son Introduction par ces mots : *Maximas autem gratias ago illustrissimo* Encke *qui et his emendatricibus curis præsidere et summo studio ac benevolentia me egregiis consiliis in adornando opere adjuvare voluit.*

Pourrait-on publier en France, et d'une manière analogue, des Tables d'exponentielles et de logarithmes modulaires (les mêmes sous un autre nom), ces Tables étant modifiées, surtout comme on l'a vu plus haut?

C'est là une question à laquelle je ne saurais trop que répondre.