BULLETIN

DE

L'ACADÉMIE IMPÉRIALE DES SCIENCES

DE

ST.-PÉTERSBOURG.

Nouvelle Série I (XXXIII).

(Avec 3 planches.)

ST.-PÉTERSBOURG, 1890.

Commissionaires de l'Académie Impériale des Sciences:

à ST.-PÉTERSBOURG:	à RIGA:	à LEIPZIG:
MM. Eggers et Cie et J. Glasounof.	M. N. Kymmel.	Voss' Sortiment (G. Haessel).

Prix du volume: 8 Roub. arg. pour la Russie, 7½ marks allemands pour l'étranger.

Sur la loi de réciprocité des résidus quadratiques. Par Edouard Lucas. (Lu le 10 avril 1890.)

On peut déduire immédiatement du criterium de Gauss une démonstration de la loi de réciprocité qui nous paraît la plus simple de toutes celles qui ont été données jusqu'à présent. Soit p un nombre impair et premier, $p = 2h + 1$, et q un entier positif premier à p. Le nombre μ des restes minimums et négatifs des termes

$$q,\ 2q,\ 3q,\ \ldots,\ hq$$

divisés par p, est égal au nombre des restes positifs compris entre $\frac{1}{2}p$ et p. Désignons par λ_n le nombre des termes de la suite (1) qui sont $< \frac{1}{2}np$; on aura évidemment

$$\lambda_n = E\frac{np}{2q},$$

et aussi

$$\mu = -\lambda_1 + \lambda_2 - \lambda_3 + \ldots + \lambda_t,$$

t étant le plus grand nombre pair qui ne surpasse pas q.

Pour $q = p-1$, $q = 2$, $q = 3$, $q = 5$, ..., on trouve immédiatement les propriétés quadratiques des nombres -1, 2, 3, 5. Mais supposons, de plus, q impair et premier; alors $t = q-1$; pour calculer le reste de μ par 2, on peut prendre les termes de μ avec un signe quelconque. Posons

$$np = 2q\,\lambda_n + r,$$
$$(q-n)p = 2q\,\lambda_{q-n} + r',$$

r et r' étant compris entre 0 et $2q$. Par addition

$$pq = (\lambda_n + \lambda_{q-n})\,2q + r + r';$$

donc $r + r'$, impair et divisible par q est égal à q ou à $3q$. Dans le premier cas, r et r' sont tous deux $<q$; dans le second, r et r' sont tous deux $>q$. On a donc

$$\frac{p-1}{2} = \lambda_n + \lambda_{q-n} + (0 \text{ ou } 1).$$

Faisons la somme de ces égalités, en désignant par ν le nombre des 1, on aura

$$\frac{p-1}{2}\frac{q-1}{2} \equiv \mu + \nu. \qquad \text{(mod. 2).}$$

Mais ν est égal au nombre des restes $>q$ de la division de

$$2p,\ 4p,\ \ldots,\ (q-1)p,$$

par $2q$; c'est-à-dire des restes minimums négatifs de

$$p,\ 2p,\ \ldots,\ \frac{q-1}{2}p,$$

divisés par q. Donc ν est ce que devient μ quand on échange les lettres p et q. Par conséquent, avec le symbole de Legendre

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

C. q. f. d.

On peut appliquer cette méthode à la démonstration de la loi de réciprocité généralisée par Jacobi. Mais il faut alors donner au théorème de Fermat généralisé par Euler un énoncé qui est de beaucoup préférable dans l'application: *Six* est premier à un nombre $n = ABC\ldots$, en désignant par $A, B, C, \ldots$ des puissances de nombres premiers différents, et par φ le plus petit multiple commun des indicateurs

$$\varphi(A),\ \varphi(B),\ \varphi(C),\ \ldots,$$

on a la congruence

$$x^{\varphi} \equiv 1, \qquad \text{(mod. } n\text{).}$$

Mais lorsque n est un multiple de 8, on doit remplacer φ par $\frac{1}{2}\varphi$, pour la puissance de 2 correspondante.

Pour adapter le théorème précédent à un nombre quelconque x, premier ou non, au module n, il suffit de multiplier les deux membres de la congruence précédente par x^{σ}, en désignant par σ le plus petit exposant des facteurs premiers contenus dans le module n. D'ailleurs $\varphi + \sigma$ est toujours plus petit que le module.

Les deux améliorations apportées au théorème de Fermat généralisé par Euler permettent de simplifier la théorie des congruences de module quelconque et de généraliser celle des racines primitives.