45.

SUR LA LOI DE RÉCIPROCITÉ DANS LA THÉORIE DES NOMBRES.

[*Comptes Rendus*, XC. (1880), pp. 1053—1057, 1104—1106.]

Soit $\left(\frac{Q}{P}\right)$ le symbole bien connu de Jacobi, généralisation du symbole $\left(\frac{Q}{p}\right)$ de Legendre. Selon que $\left(\frac{Q}{P}\right) = +1$ ou -1, je dirai que l'aspect quadratique ou simplement l'aspect de Q vers P est positif ou négatif. On accorde que Q et P peuvent l'un et l'autre être ou positifs ou négatifs, avec la convention que $\left(\frac{Q}{-P}\right) = \left(\frac{Q}{P}\right)$ et $\left(\frac{Q}{1}\right) = 1$. Alors il est plus ou moins distinctement reconnu que, Q, P étant tous les deux nombres impairs et relativement premiers, si Q et P ne sont pas tous les deux négatifs, $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = 1$ quand Q et P *ne sont pas*, et $= -1$ quand Q et P *sont*, tous les deux de la forme $4m + 3$.

Mais, si Q et P sont tous les deux négatifs, $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = -1$ quand Q et P *ne sont pas*, et $= 1$ quand Q et P *sont*, tous les deux de la forme $4m + 3$.

Servons-nous du mot *reste quaternaire* pour exprimer le reste minimum absolu d'un nombre impair par rapport au module 4. Ce reste sera ou $+1$ ou -1. Servons-nous aussi, en général, du symbole $\left(\frac{m}{n}\right)$ ou $\left(\frac{n}{m}\right)$ pour signifier un nombre qui est -1 quand m et n sont tous les deux négatifs et $+1$ dans le cas contraire. Soient a, b deux nombres quelconques positifs ou négatifs, impairs et relativement premiers, a' et b' leurs restes quaternaires; alors, en vertu des théorèmes précédents, on aura

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b'}\right),$$

formule qui constitue le véritable théorème de réciprocité et suffit à elle-même comme formule universelle de réduction, sans avoir besoin de supplément (*Ergänzung*) aucun.

Je nomme, en général, *chaîne réductive* une suite de chiffres positifs ou négatifs dont le dernier est l'unité positive ou négative et dont chaque terme intermédiaire est un diviseur de la différence de ses deux termes voisins; une telle suite se nomme *chaîne réductive impaire* quand tous les termes sont impairs. Il est évident qu'on peut toujours former une chaîne réductive impaire dont les deux premiers termes sont des nombres impairs donnés, car dès le second terme on peut trouver des termes continuellement décroissants qui rempliront les conditions imposées.

Or je dis que, pour trouver la valeur de $\left(\frac{b}{a}\right)$, on n'a qu'à former une chaîne réductive impaire commençant avec a, b et une chaîne auxiliaire dont les termes sont les résidus quaternaires des termes de la première; alors, selon que la somme des nombres des permanences des signes *moins* prises dans une suite et dans l'autre est paire ou impaire, l'*aspect* de b vers a sera positif ou négatif.

En voici la preuve. Soient

$$a,\ b,\ c,\ d,\ \ldots,\ h,\ k,\ l,$$
$$a',\ b',\ c',\ d',\ \ldots,\ h',\ k',\ l',$$

la première une suite réductive impaire et la seconde une suite auxiliaire formée avec les restes quaternaires de l'autre. Alors on aura

$$\left(\frac{b}{a}\right) = \left(\frac{b}{a}\right)\left(\frac{b'}{a'}\right)\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)\left(\frac{b'}{a'}\right)\left(\frac{c}{b}\right),$$
$$\left(\frac{c}{b}\right) = \left(\frac{c}{b}\right)\left(\frac{c'}{b'}\right)\left(\frac{b}{c}\right) = \left(\frac{c}{b}\right)\left(\frac{c'}{b'}\right)\left(\frac{d}{c}\right),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\left(\frac{k}{h}\right) = \left(\frac{k}{h}\right)\left(\frac{k'}{h'}\right)\left(\frac{h}{k}\right) = \left(\frac{k}{h}\right)\left(\frac{k'}{h'}\right)\left(\frac{l}{k}\right),$$
$$\left(\frac{l}{k}\right) = \left(\frac{l}{k}\right)\left(\frac{l'}{k'}\right)\left(\frac{k}{l}\right) = \left(\frac{l}{k}\right)\left(\frac{l'}{k'}\right).$$

Donc

$$\left(\frac{b}{a}\right) = \left(\frac{b}{a}\right)\left(\frac{c}{b}\right)\cdots\left(\frac{k}{h}\right)\left(\frac{l}{k}\right) \times \left(\frac{b'}{a'}\right)\left(\frac{c'}{b'}\right)\cdots\left(\frac{k'}{h'}\right)\left(\frac{l'}{k'}\right) = (-1)^{n+n'},$$

n étant le nombre de fois que les successions a, b; b, c; ...; h, k; k, l contiennent deux signes $-$ et n' le nombre correspondant pour a', b'; b', c'; ...; h', k'; k', l'; c'est-à-dire l'aspect de b vers a sera positif ou négatif, selon que $n + n'$ (que je nommerai ν) est pair ou impair, ce qui était à démontrer.

Je ferai l'application de cette méthode de calculer le symbole $\left(\frac{b}{a}\right)$ à des exemples tirés du Traité (*Zahlentheorie*) de Lejeune-Dirichlet. Pour trouver $(\frac{195}{1901})$, on forme la chaîne réductive

$$\begin{matrix} + & + & - & - \\ 1901 & 195 & 49 & 1, \end{matrix}$$

qui donne la chaîne auxiliaire

$$\begin{matrix} + & - & - & - \\ 1 & 1 & 1 & 1. \end{matrix}$$

On a donc $n = 1$, $n' = 2$, $\nu = n + n' = 3$; conséquemment $(\frac{195}{1901}) = -1$, et, puisque 1901 est nombre premier, 195 est non-résidu quadratique de ce nombre. Pour trouver $\left(\frac{74}{101}\right) = \left(\frac{-27}{101}\right)$, on obtient les deux chaînes (omettant dans la seconde le chiffre constant 1)

$$\begin{matrix} + & - & - & + \\ 101, & 27, & 7, & 1; \\ + & + & + & + \end{matrix}$$

$\nu = 1 + 0 = 1$, et, comme auparavant, 74 est non-résidu au nombre premier 101.

Si $b > a$, les suites prendront la forme

$$\begin{matrix} a, & b, & a, & d, \ldots, & l, \\ a', & b', & a', & d', \ldots, & l', \end{matrix}$$

et, puisque la somme des permanences négatives dans aba et $a'b'a'$ est évidemment 0, 2 ou 4, on peut faire abstraction de ces parties de la chaîne double dans le calcul. Ainsi, par exemple, on aura pour $(\frac{27}{103})$

$$\begin{matrix} + & + & - & - & + \\ 103, & 27, & 5, & 3, & 1, \\ - & - & - & + & + \end{matrix}$$

et pour $(\frac{103}{27})$

$$\begin{matrix} + & - & - & + \\ 27, & 5, & 3, & 1. \\ - & - & + & + \end{matrix}$$

Comme dernier exemple, je trouverai la valeur générale de $\left(\frac{2}{k}\right)$, c'est-à-dire de $\left(\frac{2-k}{k}\right)$. Si l'on donne à n les valeurs 1, 3, 5, 7, on obtient les chaînes doubles

$$\begin{matrix} + & + - & + - - & + - - + \\ 1; & 3, 1; & 5, 3, 1; & 7, 5, 3, 1; \\ + & - - & + + - & - - + + \end{matrix}$$

et, en général, pour $n = 2i + 1$, 3, 5, 7, on trouvera très facilement que les valeurs des quatre chaînes doubles de signes qui y correspondent seront

$$\begin{pmatrix} + - - + \\ + + - - \end{pmatrix}^i +; \quad \begin{pmatrix} + - - + \\ - - + + \end{pmatrix}^i + -;$$

$$\begin{pmatrix} + - - + \\ + + - - \end{pmatrix}^i + - -; \quad \begin{pmatrix} + - - + \\ - - + + \end{pmatrix}^i + - - +,$$

où l'indice supérieur i signifie que les signes contenus dans les parenthèses doivent être i fois répétés. Il est à remarquer que dans ces suites répétées de quatre signes il n'arrive jamais que le premier et le dernier signe sont tous les deux négatifs; de sorte qu'on n'obtiendra aucune permanence négative à la jonction de deux de ces suites.

On aura donc la somme des permanences négatives pour ces quatre cas égale à

$$2i,\ 2i+1,\ 2i+1,\ 2i+2,$$

respectivement: de sorte que l'aspect de 2 vers $8i+1$, 7 est positif et vers $8i+3$, 5 négatif: résultat qu'on a ainsi déduit avec l'aide de la seule formule de réduction pour les nombres impairs.

Il est digne de remarque que, puisque $\left(\frac{b}{a}\right) = \left(\frac{b}{-a}\right)$, il s'ensuit que, si, dans une série réductive impaire quelconque et la série de ses restes quaternaires, on change simultanément le signe des termes alternés en commençant avec le premier terme en chacune, la somme des permanences des signes négatifs sera augmentée ou diminuée par un nombre pair.

Il y a tant d'analogie entre la méthode exposée dans un précédent article et celles qu'on emploie dans les théorèmes de Newton et Fourier sur les racines réelles des équations algébriques, qu'on se sent très porté à soupçonner que le nombre que j'ai nommé ν est la limite supérieure à quelque affection de a, b à laquelle elle reste toujours congrue par rapport au module 2; mais de la nature de cette affection, si toutefois elle existe, je n'ai nulle connaissance.

De même qu'on a trouvé une expression générale pour l'aspect de $2-k$ vers k, on peut, avec l'aide du théorème de la chaîne, construire, d'une infinité de manières, des fonctions algébriques de k, dont on saura d'avance les aspects des unes vers les autres. Ainsi, pour prendre un exemple très simple, formons la série

$$1,\ 2,\ 5,\ 12,\ 29,\ 70,\ 169,\ 408,\ 985,\ 2378,\ \ldots,$$

où $$u_k = 2u_{k-1} + u_{k-2},\quad u_1 = 2,\quad u_0 = 1,$$

et conséquemment

$$u_k = 2^k + (k-1)\,2^{k-2} + \frac{(k-1)(k-3)}{1.2}\,2^{k-4} + \ldots.$$

On peut se demander l'expression générale pour l'*aspect quadratique* de u_{2i-1} vers u_{2i} pour une valeur quelconque de i.

On trouvera sans peine que les suites de signes qui donnent les valeurs de $(\frac{2}{5})$, $(\frac{12}{29})$, $(\frac{70}{169})$, $(\frac{408}{985})$ sont

$$\begin{array}{l} + - -\\ + + -\end{array};\quad \begin{array}{l} + - - + +\\ + - - - +\end{array};\quad \begin{array}{l} + - - + + - -\\ + + - + + + -\end{array},$$

$$\begin{array}{l} + - - + + - - + +\\ + - - - + - - - +\end{array};$$

et, en général, que $\left(\frac{u_{4i+1}}{u_{4i+2}}\right)$ donne naissance à la chaîne double

$$\begin{pmatrix} + & - & - \\ + & + & - \end{pmatrix}\begin{pmatrix} + & + & - & - \\ + & + & + & - \end{pmatrix}^i$$

et $\left(\frac{u_{4i-1}}{u_{4i}}\right)$ à

$$\begin{pmatrix} + \\ + \end{pmatrix}\begin{pmatrix} - & - & + & + \\ - & - & - & + \end{pmatrix}^i.$$

Dans le premier cas, ν est égal à $i+1$, et dans le second à $3i$; ainsi les valeurs successives de ν étant 1, 3, 2, 6, 3, 9, 4, 12, 5, ..., l'aspect de u_{8j+1} à u_{8j+2} et de u_{8j+3} à u_{8j+4} est positif, mais de u_{8j+5} à u_{8j+6} et de u_{8j+7} à u_{8j+8} négatif.

Dans le *Zahlentheorie* de Lejeune-Dirichlet, rédigé par M. Dedekind (3e édition, p. 110; Braunschweig, 1879), on rencontre cette phrase: "Es zeigt sich nun, dass die damals nothwendige Zerlegung in Primzahlfactoren (abgesehen von dem Factor 2) ganz überflüssig geworden." Ce qui précède ici rend évident (il me semble) que cette exclusion du nombre 2 (due probablement à quelque mésintelligence de la part des auditeurs de l'illustre Dirichlet) est elle-même (*überflüssig*) superflue.

Je profite de cette occasion pour corriger la liste que j'ai donnée dans une Note précédente des nombres qu'on démontre, par le moyen des diviseurs de x^3-3x+1, être indécomposables dans une somme de cubes rationnels. Dans cette liste*, $9pq$, $9p_1p_2^2$, $9q_1q_2^2$, $9p^2q^2$ étaient insérés par erreur; la démonstration, en un seul coup, de l'irrésolubilité des seize formes générales qui restent a paru† dans le dernier fascicule de l'*American Journal of Mathematics*.

Post-scriptum.—Dans les exemples très nombreux que j'ai calculés de l'application de mon algorithme pour déterminer l'aspect de Q vers P, j'ai toujours trouvé que la *différence* δ de n et n' (les nombres de permanences négatives dans les deux suites), prise positivement, est une *limite inférieure* au nombre de cas où q est non-résidu de p (q étant un facteur premier quelconque de Q et p de P).

Si cette remarque est démontrée de validité universelle, elle fournira un moyen de mettre à l'épreuve, d'une infinité de manières, si un nombre donné P est un nombre premier. Car, en combinant P avec un nombre premier arbitraire Q, si δ est plus grand que 1, P, devant contenir au moins δ facteurs auxquels Q est non-résidu, sera nécessairement un nombre composé. Au contraire, quand P est nombre premier, δ sera toujours ou 0 ou 1, selon la valeur de Q, ce qui constituerait un théorème nouveau sur le symbole $\left(\frac{q}{p}\right)$ de Legendre.

[* Above, p. 430.] [† Above, p. 347.]