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

LEBESGUE

Recherches sur les nombres

Journal de mathématiques pures et appliquées 1re série, tome 3 (1838), p. 113-144.
<http://www.numdam.org/item?id=JMPA_1838_1_3__113_0>

RECHERCHES

SUR LES NOMBRES;

PAR M. LEBESGUE,

Professeur-suppléant à la Faculté des Sciences de Grenoble (*).

§ II. *Sur la résolution de l'équation* $x^p = 1$, *en supposant p premier.*

I.

Calcul de l'équation dont les racines sont les sommes $y_0, y_1, \ldots y_{m-1}$.
(§ 1, page 288 du volume précédent.)

On a rappelé dans le § 1 (page 288) la distribution des $p-1=mh$ racines imaginaires de l'équation $x^p = 1$, en m groupes de h racines chacun, et en représentant par $y_0, y_1, y_2, \ldots y_{m-1}$ la somme des racines de chaque groupe, l'on a indiqué la méthode de M. Libri, pour trouver l'équation du m^e degré ayant ces sommes pour racines; cette équation étant représentée par

$$y^m - A_1 y^{m-1} + A_2 y^{m-2} \ldots \pm A_m = 0. \qquad (43)$$

Cette méthode consiste à déterminer les sommes des puissances des racines de l'équation (43). Or, si l'on représente ces sommes par f_1, f_2, $f_3 \ldots f_m$, la formule (40) qui revient à

$$pN_k = p^k + f_1 + k.mf_2 + \frac{k.k-1}{1.2} m^2 f_3 + \ldots + km^{k-1} f_k + m^k f_{k+1} \qquad (44)$$

(*) Le § I^er^ de ces *Recherches sur les Nombres* a été imprimé dans le volume précédent, *voyez* page 253.

donne, en posant successivement $k = 1, 2, 3 \ldots m-1$, l'équation

$$(45) \qquad f_{k+1} = \frac{p\left[N_k - k\,.\,N_{k-1} + \frac{k.k-1}{1.2} N_{k-2} \ldots \pm k N_1\right] - (p-1)^k}{m^k}.$$

Cette formule qui renferme la solution du problème, quand on a déterminé les valeurs de $N_1, N_2 \ldots N_{m-1}$, prend une forme beaucoup plus simple, et préférable dans le cas où le calcul des nombres N se fait par la substitution effective des valeurs de $x_1, x_2 \ldots x_k$ dans la congruence $1 + x_1^m + x_2^m + \ldots + x_k^m \equiv 0 \pmod{p}$, ce qui est praticable pour de petites valeurs de p.

Cette simplification est fondée sur les propositions suivantes, qui d'ailleurs sont d'une utilité directe dans la théorie des résidus.

Si l'on représente par n_k ce que devient N_k quand on exclut des solutions de la congruence $1 + x_1^m + x_2^m + \ldots + x_k^m \equiv 0$ (ou plus généralement de $x_1^m + x_2^m + \ldots + x_k^m \equiv \rho^a \pmod{p}$) celles où des inconnues sont nulles, on pourra déterminer N_k en fonction de n_k, ou réciproquement, au moyen du théorème suivant.

« Théorème. On a entre les quantités N_k et n_k, les relations suivantes :

$$» \ (46) \qquad N_k = n_k + k\,.\,n_{k-1} + \frac{k.k-1}{1.2} n_{k-2} + \ldots + k n_1,$$

$$» \ (47) \qquad n_k = N_k - k N_{k-1} + \frac{k.k-1}{1.2} N_{k-2} - \ldots \pm k N_1.$$

Démonstration. La formule (46) s'obtient en distribuant par groupes les solutions de la congruence $x_1^m + x_2^m + \ldots + x_k^m \equiv \rho^a \pmod{p}$. Savoir : 1° celui où aucune des inconnues n'est nulle, il renferme n_k solutions; 2° celui où une inconnue seulement est nulle, il renferme k fois n_{k-1} solutions, puisqu'on peut égaler successivement à zéro chacune des k inconnues; 3° celui où deux inconnues seulement sont nulles, il renferme $\frac{k.k-1}{1.2}$ fois n_{k-2} solutions, puisqu'il y a $\frac{k.k-1}{1.2}$ manières de choisir les deux inconnues qu'on égale à zéro, et ainsi de suite, d'où la formule (46).

Il faut remarquer d'abord qu'on a omis l'accent de N et de n qui doit être le même, et que si le second membre de la congruence était zéro au lieu d'être ρ^a, il faudrait augmenter le 2e membre de l'équation (46) de $N_0 = 1$.

Par de simples éliminations, la formule (46) donne la formule (47), dont le second membre devra aussi être augmenté de $\pm n_0 = \pm 1$; pour le cas de la congruence $x_1^m + x_2^m + \ldots + x_k^m \equiv 0 \ldots\ldots\ldots$ (mod. $p = hm + 1$).

« Théorème. Le nombre de solutions de la congruence..... » $r_1 + r_2 + \ldots + r_k \equiv \rho^a \pmod{p}$, où $r_1, r_2 \ldots r_k$ sont des résidus » de m^e puissance, étant représenté par $R_k^{(a)}$, on aura,

$$m^k . R_k^{(a)} = n_?^{(a)}. \tag{48}$$

Démonstration. Cela suit immédiatement de ce qu'il y a m valeurs de x_1 donnant $x_1^m \equiv r_1 \pmod{p}$, autant donnant $x_2^m \equiv r_2 \pmod{p}$ et ainsi de suite, de sorte qu'une seule solution de la congruence $r_1 + r_2 + \ldots + r_k \equiv \rho^a \pmod{p}$, en donne, par la combinaison des valeurs de $x_1, x_2 \ldots x_k$, un nombre égal à m^k pour la congruence $x_1^m + x_2^m + \ldots + x_k^m \equiv \rho^a \pmod{p}$.

Si l'on remarque maintenant que le nombre de solutions de la congruence

$$x_1^m + x_2^m + \ldots + x_k^m + 1 \equiv 0 \pmod{p = hm + 1},$$

que M. Libri représente par N_k, est représenté par le même symbole, d'après les conventions du § 1, si h est pair, ou — 1 résidu de m^e puissance, et par celui-ci $N_k^{\left(\frac{m}{2}\right)}$, si h est impair ou — 1 non résidu de $\left(\frac{m}{2}\right)^e$ classe, on aura dans le premier cas

$$N_k - k . N_{k-1} + \frac{k\,k-1}{1.2} N_{k-2} \ldots \pm k N_1 = m^k R_k,$$

et dans le second (en conservant la notation de M. Libri),

$$N_k - k . N_{k-1} + \frac{k . k-1}{1.2} N_{k-2} \ldots \pm k N_1 = m^k R_k^{\left(\frac{m}{2}\right)},$$

de sorte que, si, pour n'avoir qu'un seul cas à considérer, on représente par S_k le nombre de solutions de la congruence

$$r_1 + r_2 + \ldots + r_k + 1 \equiv 0 \pmod{p},$$

on aura toujours

$$N_k - k.N_{k-1} + \frac{k.k-1}{1.2} N_{k-2} - \ldots \pm kN_1 = m^k S_k,$$

ce qui réduit la formule (45) à celle-ci :

$$f_{k+1} = pS_k - h^k. \tag{49}$$

De là se tire la règle suivante, pour le calcul de l'équation (43).

« Cherchez les résidus de m^e puissance où les restes différents des » puissances 1^m, 2^m, $3^m \ldots (p-1)^m$ et faites toutes les permutations » possibles de ces h restes $r_1, r_2, \ldots r_k$, sans exclure la répétition d'un » même résidu. Représentez par S_k combien il y a de ces permutations » où la somme des termes augmentée de 1 soit multiple de p, et la » somme des n^{es} puissances des racines de l'équation (43) sera égale à » $pS_{n-1} - h^{n-1}$. »

Ces sommes ainsi trouvées, les équations

$$\begin{aligned} f_1 - A_1 &= 0, \\ f_2 - A_1 f_1 + 2A_2 &= 0, \\ f_3 - A_1 f_2 + A_2 f_1 - 3A_3 &= 0, \\ f_4 - A_1 f_3 + A_2 f_2 - A_3 f_1 + 4A_4 &= 0, \\ &\vdots \end{aligned} \tag{50}$$

qui conduisent aux suivantes :

$$\begin{aligned} A_1 &= f_1, \\ 2A_2 &= f_1^2 - f_2, \\ 2.3A_3 &= f_1^3 - 3f_1 f_2 + 2f_3, \\ 2.3.4A_4 &= f_1^4 - 6f_1^2 f_2 + 8f_1 f_3 + 3f_2^2 - 6f_4 \\ &\vdots \end{aligned} \tag{51}$$

donnent les valeurs des coefficients A_1, A_2, A_3, A_4, etc.

Voici les résultats pour $p = 2h + 1$, $p = 3h + 1$ et $p = 4h + 1$. Ils serviront pour la suite de ces recherches.

« Pour $m = 2$ ou $p = 2h + 1$, l'équation en y est

» (52) $$y^2 + y + \frac{1 \mp p}{4} = 0.$$

» selon que p est de forme $4q + 1$ ou $4q - 1$. »

Cela résulte de ce que l'on a $S_1 = 1$ pour le premier cas, et $S_1 = 0$ pour le second.

« L'équation en y, pour le cas de $m = 3$ ou de $p = 3h + 1$, est en » posant $4p = L^2 + 27M^2$, et en déterminant le signe de L de sorte » qu'on ait $L = 1 + 3l$,

» (53) $$y^3 + y^2 + \left(\frac{1 - p}{3}\right) y + \frac{1}{27}(1 - 3p - pL) = 0,$$

» ou bien en posant $y + \frac{1}{3} = \frac{z}{3}$,

(54) $$z^3 - 3pz - pL = 0. »$$

Cela résulte de ce que l'on a pour ce cas

$$S_1 = 1,\ S_2 = \frac{n_2}{9} = \frac{N_2 - 2N_1}{9},\ N_1 = 3 \text{ et } N_2 = A = C' - 3 = p + 1 + L - 3$$

(*Voy.* § I, page 279 du volume précédent.)

Les valeurs de $f_1 = -1$, $f_2 = pS_1 - h$, $f_3 = pS_2 - h^2$ substituées dans les formules (51) donnent l'équation (53), qui devient (54) en y faisant $y + \frac{1}{3} = \frac{z}{3}$.

« L'équation en y pour $m = 4$ ou $p = 4h + 1$, est en posant » $p = (1 + 4u)^2 + 4v^2$ et $h = 2h' + r$ (r étant 0 ou 1),

(55) $$y^4 + y^3 + \frac{1}{2}(pr - 3h)y^2 + \frac{1}{4}(2pu + pr - h)y + \frac{1}{16}[(pr - h)^2 - 4pu^2] = 0,$$

» qui se décompose en deux facteurs, ainsi qu'il suit :

(56) $$\left[y^2 + \frac{1}{2}(1 - \sqrt{p})y + \frac{1}{4}(pr - h + 2u\sqrt{p})\right]\left[y^2 + \frac{1}{2}(1 + \sqrt{p})y + \frac{1}{4}(pr - h - 2u\sqrt{p})\right] = 0.$$

La valeur de N_3 (notation de M. Libri) calculée, tome II de ce Journal, page 284, pour le cas de $r=0$ ou $h=2h'$, et tome II, page 286, pour le cas de $r=1$, ou $h=2h'+1$, et celle de N_2 qui, pour le premier cas, n'est autre que A, et pour le second que C'', conduiront à l'équation (55), et par suite à l'équation (56).

N. B. La valeur de N_3, donnée à la page 286, au lieu d'être $p^2-7p+10+56u+64u^2$, doit être $p^2-7p+6u+4u^2$, comme le montre la substitution indiquée ; et c'est seulement par le changement de u en $1+4u$, qu'elle devient $p^2-7p+10+56u+64u^2$, valeur qu'il faut employer ici, afin d'avoir dans les deux cas l'équation $p=(1+4n)^2+4v^2$.

II.

Calcul direct de l'équation en y.

Dans ses Recherches arithmétiques, M. Gauss a donné l'équation en y pour les cas généraux de $p=2h+1$, et $p=3h+1$. La solution pour ce second cas, introduit dans le calcul les symboles (KK), (KK'), (KK''), etc., qui ne sont autres que les nombres de solutions de certaines congruences; le n° 358 qui renferme cette solution, finit par ces mots « quoique le problème que nous venons de résoudre soit assez » compliqué, nous n'avons pas voulu le supprimer, tant à cause de l'é- » légance de la solution, que parce que les artifices qu'il nous a » donné occasion d'employer, peuvent être d'une très grande utilité » dans d'autres problèmes. »

On donnera donc ici le calcul direct des coefficients de l'équation en y, d'où résultera la règle suivante pour le cas général de $p=mh+1$.

« Soient r_1, r_2, r_3, ... r_h la série des résidus de m^e puissance

et $\left.\begin{array}{l} r'_1,\ r'_2,\ r'_3,\ \ldots\ r'_h \\ r''_1,\ r''_2,\ r''_3,\ \ldots\ r''_h \\ \vdots \\ r_1^{(n-1)},\ r_2^{(n-1)},\ \ldots\ r_h^{(n-1)} \end{array}\right\}$ les $n-1$ séries de non-résidus de m^e puissance (*).

(*) Comme l'ordre des classes de non-résidus est ici indifférent, si l'on n'a

» Combinez de toutes les manières possibles ces nombres 1 à 1, 2 à 2, » 3 à 3... k à k en ayant soin de ne jamais prendre deux nombres » dans une même série, et représentez par σ_1, σ_2, σ_3... σ_k, le nombre » des combinaisons où la somme des termes est divisible par p; alors » l'équation en y, multipliée par $p-1$, prendra la forme

» (57) $$p(y^m - \sigma_1 y^{m-1} + \sigma_2 y^{m-2} - \sigma_3 y^{m-3} + \ldots \pm \sigma_m) - (y-h)^m = 0$$

» d'où la congruence

» 58) $$(y-h)^m \equiv 0 \pmod{p = hm+1}.$$

» déjà démontrée par M. Poinsot (*Mémoire sur l'application de l'Al-* » *gèbre à la théorie des nombres*).»

Pour démontrer le théorème, d'où dérive la règle précédente, on emploiera les notations suivantes.

Le nombre de solutions de la congruence

$$\rho^a x_1^m + \rho^b x_2^m + \ldots + \rho^g x_l^m \equiv 0, \text{ ou } \equiv \rho^t \pmod{p},$$

où les nombres ρ^a, ρ^b... ρ^g sont de classes différentes, ce qui suppose ρ racine primitive, et a, b,... g incongrus suivant le module m, sera représenté par $n_l^0(a, b, \ldots g)$ si le 2e membre de la congruence est 0, et par $n_l^{(t)}(a, b, \ldots g)$, si le 2e membre de la congruence est ρ^t, ces nombres de solutions s'obtenant, non par la substitution des nombres 1, 2,... $p-1$ au lieu de x_1, x_2,... x_m, mais par la substitution des résidus r_1, r_2,... r_n, au lieu de x_1^m, x_2^m,... x_k^m.

Comme les nombres a, b,... g sont inégaux, on pourra, quand il n'en résultera pas d'ambiguité, remplacer $n_l^0(a, b, \ldots g)$ par $n^0(k)$,

---

point de racine primitive, on pourra les former de la manière suivante, comme le fait M. Libri dans une Recherche analogue. 1°. Cherchez les restes des puissances 1^m, 2^m,.....$(p-1)^m$, vous aurez les résidus. 2°. Prenez dans la série 1, 2....$p-1$ un non-résidu, multipliez-le successivement par les résidus, et les restes des produits divisés par p, composeront une classe de non-résidus. 3°. Au moyen d'un non-résidu qui n'appartienne pas à cette classe vous formerez semblablement une seconde classe de non-résidus, et ainsi de suite.

et la somme σ_k de la règle précédente ne sera autre que $\Sigma n^o(k)$, somme qui s'étend à toutes les combinaisons k à k des nombres 0, 1, 2,...$m-1$.

Pour faciliter le calcul des coefficients de l'équation en y, on pourra distribuer les combinaisons k à k, des m nombres différents 0, 1, 2... $m-1$ par périodes de la manière suivante.

Soit $a, b, \ldots g$ une combinaison déterminée : si l'on augmente chacun des nombres $a, b, \ldots g$ qui la forment de 1, 2, 3...$m-1$ unités, on aura une période qui se reproduirait, si l'on continuait à augmenter également les nombres $a, b, \ldots g$; car on convient de retrancher m des sommes surpassant ce nombre. De cette convention résultent les deux théorèmes qui suivent :

« Théorème. Les combinaisons k à k des m nombres 0, 1, 2...$m-1$, » et généralement de m nombres différents, peuvent se distribuer en » périodes, dont le nombre des termes est m, ou un diviseur de m.»

Démonstration. Cela suit de ce que l'ensemble des combinaisons $a, b \ldots g$; $a+1, b+1, \ldots g+1$; ... $a+m-1, b+m-1, \ldots g+m-1$; se reproduit périodiquement, et doit être conséquemment formé de plusieurs périodes, dont le nombre des termes ne peut être qu'un diviseur de m, qui peut être l'unité ou m lui-même.

» Théorème. Si m et k sont premiers entre eux, toutes les périodes » formées avec les combinaisons k à k des nombres 0, 1, 2... $m-1$, » auront m termes. Mais si m et k ont pour plus grand commun diviseur δ, et qu'on ait $m = m'\delta$, $k = i\delta$, le nombre de termes des périodes sera m' ou un multiple de m'. »

Démonstration. Soit $a_1, a_2, \ldots a_g, a_{g+1}, \ldots a_{g+i} = a_k$ la combinaison initiale de la période, et telle qu'on ait $a_1 < a_2 < a_3 \ldots < a_k$. Soit de plus n le nombre des termes de la période, de sorte que la combinaison suivante

$$a_1 + n,\ a_2 + n, \ldots a_g + n,\ a_{g+1} + n, \ldots\ a_{g+i} + n$$

revienne à la première quand on aura soustrait m des sommes qui surpassent ce nombre, comme par suite de l'hypothèse $a_1 < a_2 < a_3 \ldots$ les sommes $a_1 + n$, $a_2 + n, \ldots$ vont en croissant, si $a_{g+1} + n$ est la première qui surpasse m, il en sera de même des suivantes, et les sommes $a_{g+1} + n - m$, $a_{g+2} + n - m \ldots a_{g+i} + n - m$ toutes plus petites que m iront en croissant. D'ailleurs on a $a_{g+i} + n - m$ ou

$a_k + n - m < a_1 + n$, puisque cette inégalité revient à $a_k < a_1 + m$; donc si l'on range les termes de la combinaison $a_1 + n$, $a_2 + n$, $a_3 + n$..... par ordre de grandeur, on aura $a_{g+1} + n - m$, $a_{g+2} + n - m \ldots a_k + n - m$, $a_1 + n$, $a_2 + n \ldots a_g + n$, qui devra coïncider avec a_1, $a_2 \ldots a_g$, $a_{g+1} \ldots a_k$. Si donc on égale les sommes des termes de ces deux combinaisons, on aura $kn - im = 0$, qui peut s'écrire $\frac{k}{i} = \frac{m}{n}$ ou $\frac{n}{i} = \frac{m}{k}$. Comme n est diviseur de m, on pourra donc poser $m = n\mathrm{D}$, $k = i\mathrm{D}$: or D est un diviseur de δ ; n sera donc un multiple de m'. L'équation $\frac{n}{i} = \frac{m}{k}$ montre d'ailleurs que si m et k sont premiers entre eux, on doit avoir nécessairement $n = m$, puisque n ne peut surpasser m.

Les k équations qu'on obtiendra en égalant terme à terme les deux combinaisons seront

$$a_1 + n = a_{i+1}, \quad a_2 + n = a_{i+2} \ldots\ldots \quad a_{g+1} + n = a_{i+g} = a_k$$
$$a_{g+1} + n - m = a_1, \quad a_{g+2} + n - m = a_2 \ldots \quad a_{g+i} + n - m = a_i ;$$

celles de la première ligne se réduiront à

$a_{i+1} = a_1 + n$	$a_{2i+1} = a_1 + 2n$	$\ldots a_{(\mathrm{D}-1)i+1} = a_1 + (\mathrm{D}-1)n$
$a_{i+2} = a_2 + n$	$a_{2i+2} = a_2 + 2n$	$a_{(\mathrm{D}-1)i+2} = a_2 + (\mathrm{D}-1)n$
⋮	⋮	⋮
$a_{2i} = a_i + n$	$a_{3i} = a_i + 2n$	$a_{\mathrm{D}i} = a_k = a_i + (\mathrm{D}-1)n$

en posant $g + i = k = i\mathrm{D}$, d'où $g = (\mathrm{D}-1)i$.

Quant aux équations de la seconde ligne, elles rentrent dans celles de la première, puisque l'on a $m - n = (\mathrm{D}-1)n$.

Une conséquence des équations précédentes, c'est qu'on doit avoir $a_1, a_2, \ldots a_i$ tous plus petits que n, ce qui est toujours possible, puisque l'équation $\frac{n}{i} = \frac{m}{k}$ montre que i ne surpasse jamais n: il suffira donc de combiner i à i les nombres 0, 1, 2, ... $n-1$, et par le moyen de ces combinaisons prises pour $a_1, a_2, \ldots a_i$, on obtiendra les combinaisons

$$a_1, a_2, \ldots a_i, \quad a_1 + n \ldots a_i + n, \quad a_1 + 2n, \ldots, a_{i+2n} \ldots a_i + (\mathrm{D}-1)n \ldots a_{i+(\mathrm{D}-1)n}$$

donnant naissance à des périodes de n termes.

Voici quelques exemples :

1°. m impair et $k=2$. Ici les périodes seront de m termes, puisque m et k sont premiers entre eux. Ainsi, pour $m=7$, il y a $\frac{7.6}{1.2}=7.3$ combinaisons formant les 3 périodes suivantes : 0,1 : 1,2 : 2,3 : 3,4 : 4,5 : 5,6 : 6,0 — 0,2 : 1,3 : 2,4 : 3,5 : 4,6 : 5,0 : 6,1 — 0,3 : 1,4 : 2,5 : 3,6 : 4,0 : 5,1 : 6,2.

2°. m pair et $k=2$. Ici, on peut faire $D=2$, $i=1$: il y a donc outre les périodes de m termes, une période de $\frac{m}{2}$ termes, savoir pour $m=8$, par exemple, 0,4 : 1,5 : 2,6 : 3,7. De plus, il y a 3 périodes de 8 termes qui ont pour combinaisons initiales 0, 1 ; 0, 2 ; 0, 3 ; ce qui forme le nombre total des combinaisons $\frac{8.7}{1.2}=28=24+4$.

Au moyen de tout ce qui précède l'équation en y pourra se déterminer par le théorème suivant :

» Théorème. Si l'on pose pour abréger $\Sigma n^{o}(k)=\sigma_k$ et.....

» $\frac{m.m-1.m-2\ldots m-k+1}{1.2.3\ldots k}=(m\mathrm{C}k)$, on aura

$$\text{» (59)} \qquad mh\mathrm{A}_k=p\sigma_k-(m\mathrm{C}k)h^k,$$

» et par suite, l'équation (57) et la congruence (58) posées plus » haut. »

Démonstration. L'équation en y n'étant autre que le produit

$$\left[y-(\mathrm{R}^{x_1^m}+\mathrm{R}^{x_2^m}+\ldots+\mathrm{R}^{x_h^m})\right]\left[y-(\mathrm{R}^{\rho x_1^m}+\mathrm{R}^{\rho x_2^m}+\ldots\mathrm{R}^{\rho x_h^m})\right]\ldots\left[y-(\mathrm{R}^{\rho^{m-1}x_1^m}+\ldots+\mathrm{R}^{\rho^{m-1}x_h^m})\right],$$

où x_1^m, x_2^m,... x_h^m, doivent être remplacés par les résidus, ρx_1^m, ρx_2^m,... ρx_h^m, par les non-résidus de première classe ; $\rho^2 x_1^m$, $\rho^2 x_2^m$,... $\rho^2 x_h^m$; par les non-résidus de deuxième classe, et ainsi des autres, on aura

1°. $\mathrm{A}_1=\mathrm{R}^1+\mathrm{R}^2+\mathrm{R}^3\ldots+\mathrm{R}^{p-1}=-1$; d'où $mh\mathrm{A}_1=-m.h^1=p\sigma_1-(m\mathrm{C}1)h'$, car $\sigma_1=0$;

2°. $\mathrm{A}_2=\Sigma\mathrm{R}^{\rho^a x_1^m+\rho^b x_2^m}$, où il faudra mettre d'abord pour a et b, toutes les combinaisons 2 à 2 des nombres 0, 1,... $m-1$ et ensuite pour x_1^m et x_2^m, tous les résidus de même puissance. Or, pour une combinaison déterminée a, b l'exposant $\rho^a x_1^m+\rho^b x_2^m$ prend $n_2^o(a, b)$

valeurs congrues à o (mod. p), qui restent en même nombre pour toutes les combinaisons formant la période de a, b puisque la congruence $\rho^a x_1^m + \rho^b x_2^m \equiv 0$, garde évidemment le même nombre de solutions, quand on multiplie son premier membre ρ^i, quel que soit d'ailleurs i. Le même exposant prenant

$$n_2'(a, b),\ n_2''(a, b),\ n_2'''(a, b) \ldots\ n^{(m-2)}(a, b),\ n_2(a, b),$$

valeurs congrues à ρ, ρ^2, $\rho, \ldots\ \rho^{m-1}$, ρ^m, et pareillement à ρ^{m+1}, $\rho^{m+2}, \ldots\ \rho^{2m-1}$, ρ^{2m} ; et généralement à ρ^{fm+1}, $\rho^{fm+2}, \ldots\ \rho^{fm+m-1}$, ρ^{fm+m} ; la partie du coefficient A_s relative à la combinaison a, b sera

$$n_2^0(a,b) + \gamma_0 n_2(a,b) + \gamma_1 n_2'(a,b) + \gamma_2 n_2''(a,b) + \ldots + \gamma_{m-1} n_2^{(m-1)}(a,b) :$$

pour la partie de A_s relative à la combinaison $a+1$, $b+1$, il faudra comme on l'a dit poser $n_2^0(a+1, b+1) = n_2^0(a, b)$ et $n_2^i(a+1, b+1) = n_2^{(i-1)}(a, b)$, puisque la congruence $\rho^a x_1^m + \rho^b x_2^m \equiv \rho^{i-1}$ (mod. p) revient à $\rho^{a+1} x_1^m + \rho^{b+1} x_2^m \equiv \rho^i$; cette partie de A_s deviendra donc

$$n_2^0(a, b) + \gamma_1 n_2(a,b) + \gamma_2 n_2'(a,b) + \ldots + \gamma_{m-1} n_2^{(m-2)}(a,b) + \gamma_0 n_2^{(m-1)}(a,b) :$$

calculant de même les parties de A_s relatives aux autres termes de la période de la combinaison a, b, on trouvera pour toute la période

$$\begin{array}{l}
n_2^0(a, b) + \gamma_0\ \ n_2(a, b) + \gamma_1 n_2'(a, b) + \ldots + \gamma_{m-1} n_2^{(m-1)}(a, b), \\
n_2^0(a, b) + \gamma_1\ \ n_2(a, b) + \gamma_2 n_2'(a, b) + \quad + \gamma_0\ \ n_2^{(m-1)}(a, b), \\
n_2^0(a, b) + \gamma_2\ \ n_2(a, b) + \gamma_3 n_2'(a, b) + \quad + \gamma_1\ \ n_2^{(m-1)}(a, b), \\
\quad\vdots \\
n_2^0(a, b) + \gamma_{m-1}\ n_2(a, b) + \gamma_0 n_2'(a, b) + \quad + \gamma_{m-2} n_2^{(m-1)}(a, b),
\end{array}$$

dont la somme est égale à

$$m : n_2^0(a,b) + (\gamma_0 + \gamma_1 + \ldots + \gamma_{m-1})[n_2'(a,b) + n_2''(a,b) + \ldots + n_2^{(m-1)}(a,b)] ;$$

or, on voit de suite que l'on a

$$h^s = n_2^0(a, b) + h[n_2'(a, b) + n_2(a, b) + \ldots + n_2^{(m-1)}(a, b)],$$

ce qui se démontre comme la formule (12) du § 1 (t. II, page 269). D'ailleurs $\gamma_0+\gamma_1+\ldots+\gamma_{m-1}=-1$. Si donc, on multiplie la somme précédente par mh, elle se réduira à

$$m^2h.n_2^0(a,b)-m[h^2-n_2^0(a,b)]=p.mn_2^0(a,b)-mh^2=p[n_2^0(a,b)+n_2^0(a+1,b+1)+n_2^0(a+2,b+2)+\ldots+n_2^0(a+m-1,b+m-1)]-mh^2.$$

On suppose ici que la période de a, b ait m termes; mais si elle en avait seulement $m'=\frac{m}{m''}$ il faudrait diviser la quantité précédente par m'', ce qui la réduirait à

$$p[n_2^0(a,b)+n_2^0(a+1,b+1)+\ldots+n_2^0(a+m'-1,b+m'-1)]-m'h^2.$$

Maintenant si l'on pose $\frac{m.m-1}{1.2}=gm+g'm'+g''m''+\ldots.$ en supposant qu'il y ait g périodes de m termes, g' de m' termes, g'' de m'' termes, etc., on trouvera en réunissant toutes les parties de mhA_2 l'équation

$$mhA_2=p\Sigma n_2^0(a,b)-gmh^2-g'm'h'^2-g''m''h''^2-\ldots \text{ ou}$$
$$mhA_2=p\sigma_2-(mC2)h^2.$$

3°. Par un calcul tout-à-fait semblable, on trouvera

$$mhA_k=p\sigma_k-(mCk)h^k,$$

au moyen de la relation

$$h^k=n_k^0(\ )+h[n_k'(\ )+n_k''(\ )+n_k'''(\ )+\ldots n_k(\ )],$$

où les parenthèses ( ) doivent renfermer la même combinaison $a, b, \ldots g$.

Voici quelques remarques pour faciliter le calcul des coefficients A.

1°. L'on a $\Sigma n_2^0(1)=0$, d'où $A_1=-1$;

2°. L'on a $n_2^0(a,b)=0$, si h est pair.

Mais si h est impair, l'on a $n_2^0(a,b)=h$ ou 0, selon que l'on a

$b = a + \frac{m}{2}$, ou que l'on n'a pas $b = a + \frac{m}{2}$; d'où il suit qu'en posant $h = 2h' + r$ (r étant o ou 1), on aura $\Sigma n_2^\circ(a,b) = \frac{rmh}{2}$, d'où $A_2 = \frac{pr - (m-1)h}{2}$.

3°. Pour l'avant-dernier terme, toutes les combinaisons $m-1$ à $m-1$ forment une seule période de m termes, ainsi l'on aura $\Sigma n^\circ(m-1) = mn^\circ(0, 1, 2, \ldots m-2)$.

4°. Pour le dernier terme il n'y a qu'une seule combinaison, et l'on aura $\Sigma n^\circ(m) = n^\circ(0, 1, 2, \ldots m-1)$.

Au moyen de ces remarques, on trouverait aussi facilement que plus haut, les équations relatives aux cas de $p = 2h+1$, $p = 3h+1$, $p = 4h+1$.

L'équation $y^m - A_1 y^{m-1} + A_2 y^{m-2} \ldots \pm A_m = 0$ étant multipliée par $mh = p-1$, prendra la forme

$$(p-1)y^m - [p\sigma_1 - (mC1)h]y^{m-1} + [p\sigma_2 - (mC2)h^2]y^{m-2} - \ldots = 0,$$

ou bien encore

$$p(y^m - \sigma_1 y^{m-1} + \sigma_2 y^{m-2} - \ldots) - [y^m - (mC1)hy^m + (mC2)hy^{2m-2} - \ldots] = 0.$$

ou enfin

$$p(y^m - \sigma_1 y^{m-1} + \sigma_2 y^{m-2} \ldots \pm \sigma_m) - (y-h)^m = 0;$$

d'où l'on tire en négligeant le multiple de p,

$$(y-h)^m \equiv 0 \pmod{p}.$$

On a donc les résultats (57) et (58) énoncés dans la règle qui commence cet article II.

On n'ajoutera rien de plus ici, sur les équations donnant les sommes des racines composant les périodes dans lesquelles on a divisé et subdivisé la suite des racines imaginaires R, R', R^2, ... R^{p-1}, de l'équation $x^p = 1$, et l'on finira ce paragraphe par la formation de l'équation qui donne les différents termes d'une période.

III.

Sur l'équation donnant les termes qui composent une des racines de l'équation en y.

Ce qui paraît le plus simple dans le calcul de cette équation, c'est de former les sommes des puissances des racines, et d'en déduire les coefficients de l'équation. On peut cependant obtenir ces coefficients par le moyen des nombres de solutions de congruences telles que

$$x_1^m + x_2^m + \ldots + x_l^m \equiv 0 \text{ ou } \rho^s \pmod{p},$$

en supposant d'abord que ces solutions se comptent en remplaçant x_1^m, x_2^m, x_l^m par les résidus de $m^{ième}$ puissance r_1, r_2, ... r_h, ensuite que l'on a évité de répéter un même résidu et rejeté les solutions qui ne diffèrent que par l'ordre des termes d'autres solutions déjà obtenues.

Cela posé, l'on représentera les nombres de solutions ainsi définis par

N_k^0 si le second membre de la congruence est 0,
N_k' si c'est un non-résidu de première classe,
N_k'' si c'est un non-résidu de deuxième classe,

et ainsi de suite jusqu'à

$N_k^{(m-1)}$ si le deuxième membre est un non-résidu de $m-1$ classe, et N_k si c'est un résidu.

On reconnaît de suite entre les quantités N des relations analogues à celles trouvées entre les N dans le § 1. Ainsi pour $m = 2$ on a

$$(60) \qquad N_k^0 + h(N_k + N_k') = \frac{h \cdot h-1 \ldots h-k+1}{1.2.. k} = (hCk),$$

qui se démontre comme la formule (9).

On a encore, pour $m = 2$, les relations

$$(61)\qquad N_k^\circ = N_{h-k}^\circ \quad \text{quel que soit} \quad p = 2h+1,$$

$$(62)\qquad \left\{\begin{array}{l} N_k = N_{h-k} \\ N_k' = N_{h-k}' \\ N_k - N_k' = N_{h-k} - N_{h-k}' \end{array}\right\} \text{pour } p = 4g+1,$$

$$(63)\qquad \left\{\begin{array}{l} N_k = N_{h-k}' \\ N_k' = N_{h-k} \\ N_k - N_k' = -(N_{h-k} - N_{h-k}') \end{array}\right\} \text{pour } p = 4g-1,$$

$$(64)\qquad N_k + N_k' = N_{h-k} + N_{h-k}' \text{ quel que soit } p,$$

qui résultent de ce que la somme des carrés $1+2^2+3^2+\ldots+\left(\frac{p-1}{2}\right)^2$ et par suite des résidus quadratiques, est multiple de p, sauf le cas de $p=3$. Ainsi pour $p=2h+1$, si la somme d'une partie des résidus quadratiques $r_1, r_2, r_3, \ldots r_h$, est divisible par p, la somme des autres résidus le sera aussi; et de même, si la somme d'une partie des résidus est congrue à a, la somme des autres résidus sera congrue à $-a$. Dans la démonstration il faudra considérer séparément le cas de -1 résidu quadratique, qui a lieu pour $p=4g+1$, et celui de -1 non-résidu quadratique, qui a lieu pour $p=4g-1$.

Ces préliminaires posés, on démontrera facilement les théorèmes suivants.

« *Théorème.* Si l'on représente par

$$x^h - A_1 x^{h-1} + A_2 x^{h-2} \ldots \pm A_h = 0$$

» l'équation dont les racines sont les différents termes de

$$y_u = R_p^u + R_p^{u+m} + R_p^{u+2m} + \ldots + R_p^{u+(h-1)m},$$

» on aura

$$(65)\qquad A_i = N_i^\circ + N_i^{(m-u)} y_0 + N_i^{(m+1-u)} y_1 + \ldots + N_i^{(m+m-1-u)} y_{m-1},$$

» où l'accent de N_i doit être diminué de m, quand cela est possible.

Démonstration. L'équation en x étant

$$(x - R_p^u)(x - R_p^{u+m})(x - R_p^{u+2m}) \ldots = 0,$$

on aura

$$A_i = \Sigma R \rho^{u\left(\rho^{am} + \rho^{bm} + \rho^{cm} + \ldots\right)},$$

où il faudra mettre pour a, b, $c\ldots$ toutes les combinaisons i à i des nombres $1, 2, \ldots h$, puis chercher combien il y en a qui rendent l'exposant de R congru à zéro, combien il y en a qui le rendent congru à ρ^{1+m}, ρ^{1+2m}, etc., combien il y en a qui le rendent congru à ρ^{2+fm} et ainsi de suite, et l'on aura la valeur de A_s en remarquant que la congruence

$$x_1^m + x_2^m + \ldots + x_i^m \equiv 0 \text{ ou } \rho^a \pmod{p = hm + 1},$$

a le même nombre de solutions pour des valeurs de a congrues suivant le module m.

Application pour le cas $m = 2$.

Théorème : L'équation qui donne les racines, composant » $\gamma_1 = R\rho^1 + R\rho^4 + R\rho^6 + \ldots + R\rho^{2h}$, est

$$(66) \qquad Y + Z\sqrt{ip} = 0.$$

» Celle qui donne les racines composant

$$\gamma_2 = R\rho + R\rho^3 + R\rho^5 + \ldots + R\rho^{2h-1} \text{ est}$$

$$(67) \qquad Y - Z\sqrt{ip} = 0,$$

» en supposant $p = 4q + i$ ($i = +1$ ou -1).

» Le signe du radical dépendant du choix de ρ, mais n'étant » jamais le même pour γ_0 et γ_1.

» Les fonctions Y et Z étant

$$(68) \qquad Y = x^h - [N_1^0 - \tfrac{1}{2}(N_2 + N_1^1)]x^{h-1} + [N_2^0 - \tfrac{1}{2}(N_3 + N_2^1)]x^{h-2} - \ldots \pm [N_h^0 - \tfrac{1}{2}(N_h + N_h')],$$

$$(69) \qquad Z = \tfrac{1}{2}[(N_1 - N_1')z^{h-1} - (N_2 - N_2')z^{h-2} + \ldots \mp (N_{h-1} - N_{h-1}')z],$$

» et satisfaisant à l'équation

$$(70) \qquad Y^2 - piZ^2 = \left(\frac{x^p - 1}{x - 1}\right).$$

Démonstration. Les valeurs de γ_0 et γ_1 étant les racines de l'équation $\gamma^2+\gamma+\frac{1\mp p}{4}=0$ ou $\gamma^2+\gamma+\frac{1-ip}{4}=0$, c'est-à-dire $-\frac{1}{2}\pm\frac{1}{2}\sqrt{ip}$, si l'on pose $\gamma_0=-\frac{1}{2}+\frac{1}{2}\sqrt{ip}$, on aura $\gamma_1=-\frac{1}{2}-\frac{1}{2}\sqrt{ip}$, d'où, par la substitution dans les valeurs de A_1, A_2, $A_3\ldots A_l$, résulteront les formules (66) — (69). Quant à la formule (70), on l'obtiendra en remarquant que le produit $(Y+Z\sqrt{ip})(Y-Z\sqrt{ip})$, doit égaler $x^{p-1}+x^{p-2}+\ldots+x^2+x+1=\frac{x^p-1}{x-1}$.

Remarque I. Si l'on multiplie Y et Z par 2, et qu'on simplifie leurs valeurs au moyen des relations (61) — (64), on trouvera

$$(71)\quad Y=(2x^h+a_1x^{h-1}+a_2x^{h-2}\ldots)+i(\ldots a_2x^2+a_1x+2),$$
$$(72)\quad Z=x^{h-1}+b_2x^{h-2}+b_3x^{h-3}+\ldots+b_3x^3+b_2x^2+x,$$

où l'on a

$$(73)\qquad a_i=2N_i^\circ-(N_i+N_i'),\quad b_i=N_i-N_i'.$$

Il faut remarquer que pour h pair ($i=1$), Y a un terme moyen, qui appartient à sa première partie.

Remarque II. Au moyen de la relation (60), la valeur de γ multipliée par $2h=p-1$ donnera $2N_i^\circ-(N_i+N_i')=\frac{1}{h}[pN_i^\circ-(mCi)]$, et par suite

$$(74)\quad (p-1)Y=2p(x^h-N_1^\circ x^{h-1}+N_2^\circ x^{h-2}-\ldots\pm N_p^\circ)-2(x-1)^h,$$

d'où la congruence

$$(75)\qquad Y\equiv 2(x-1)^h\ (\text{mod. } p).$$

L'équation (74) montre bien que les coefficients de Y ne sauraient se déduire uniquement de la congruence (75), ainsi que Legendre l'avait cru d'abord, après avoir démontré la congruence (75), d'une manière différente de la précédente.

Dans son mémoire sur la détermination des fonctions Y, Z de l'é-

quation

$$4(x^p - 1) = (x - 1)(Y^2 - piZ^2),$$

Legendre a rectifié sa solution et a donné le moyen de calculer les suites $a_1, a_2, a_3 \ldots b_1, b_2, b_3 \ldots$ Sa méthode conduit immédiatement à des formules générales, qu'on peut s'étonner de ne pas trouver dans son mémoire. Voici en quelques mots sa solution.

Il pose

$$Y + Z\sqrt{ip} = 2x^k - A_1 x^{k-s} + A_2 x^{k-2s} - \ldots = 0,$$

en supposant $\mp A_i = a_i + b_i\sqrt{ip}$. Il suffira donc pour avoir a_i et b_i de calculer A_i; or si l'on représente par $f_1, f_2, f_3, \ldots$ les sommes des racines de l'équation $Y + Z\sqrt{ip} = 0$ et que l'on fasse.... $f_1 = -\frac{1}{2} - \frac{1}{2}\sqrt{ip}$, il en résultera $f_2 = -\frac{1}{2} - \frac{1}{2}\left(\frac{n}{p}\right)\sqrt{ip}$, en représentant par $\left(\frac{n}{p}\right)$ le reste $+1$ ou -1 de $n^{\frac{p-1}{2}}$ divisé par p. Or, ces valeurs de f_2 donnent les valeurs de $A_1, A_2 \ldots$ au moyen des équations (51), où il suffit de remplacer $A_1, A_2 \ldots$ par $\frac{1}{2}A_1, \frac{1}{2}A_2$, etc., et d'où résultent ces valeurs de $a_1, a_2 \ldots b_1, b_2 \ldots$

$$(76)\quad \begin{cases} a_1 = 1, \\ a_2 = \frac{1}{4}(3 + ip), \\ a_3 = \frac{1}{24}\left\{15 + \left[3 + 6\left(\frac{2}{p}\right)\right]ip\right\}, \\ a_4 = \frac{1}{192}\left\{105 + \left[30 + 24\left(\frac{2}{p}\right) + 32\left(\frac{3}{p}\right)\right]ip + p^2\right\}, \\ \text{etc.} \end{cases}$$

$$(77)\quad \begin{cases} b_1 = 1, \\ b_2 = \frac{1}{4}\left[2 + 2\left(\frac{2}{p}\right)\right], \\ b_3 = \frac{1}{24}\left[9 + 6\left(\frac{2}{p}\right) + 8\left(\frac{3}{p}\right) + ip\right], \\ b_4 = \frac{1}{192}\left\{108 + 36\left(\frac{2}{p}\right) + 32\left(\frac{3}{p}\right) + \left[4 + 12\left(\frac{2}{p}\right)\right]ip\right\}. \\ \text{etc.} \end{cases}$$

Ces formules, dont la loi dérive de celle des formules (51), sont bien propres à montrer l'utilité du signe $\left(\frac{n}{p}\right)$, qui assujétit à une loi

constante des quantités qui dépendent non de la grandeur du nombre premier p, mais de sa forme. Or il arrive ici que ce sont les seuls nombres $\left(\frac{n}{p}\right)$ qui varient avec la forme de p.

Exemple. Soit $p=19=4.5-1$. On a ici $i=-1$ et $\left(\frac{2}{p}\right)=\left(\frac{3}{p}\right)=-1$, d'où il résulte

$$a_1=1,\ a_2=-4,\ a_3=3,\ a_4=5;\ b_1=1,\ b_2=0,\ b_3=-1,\ b_4=1,$$

et par conséquent

$$\begin{aligned} Y &= 2x^9+x^8-4x^7+3x^6+5x^5-5x^4-3x^3+4x^2-x-2, \\ Z &= \quad x^8 \quad -x^6+x^5+x^4-x^3 \quad +x. \end{aligned}$$

Ayant ainsi déterminée les deux séries $a_1, a_2, a_3\ldots\ b_1, b_2, b_3\ldots$ Au moyen des équations (76) et (77), on pourra en déduire les nombres N_i°, N_i, N_i', au moyen des formules

$$78) \qquad \begin{cases} N_i^\circ = \frac{1}{p}[(hCi) \mp ha_i], \\ N_i = \frac{1}{2p}[2(hCi) \pm (a_i + pb_i)], \\ N_i' = \frac{1}{2p}[2(hCi) \pm (a_i - pb_i)]; \end{cases}$$

où le signe supérieur est pour i impair et l'inférieur pour i pair.

Ces formules se tirent immédiatement des équations (60) et (73), c'est-à-dire de

$$\begin{aligned} N_i^\circ + h(N_i + N_i') &= (hCi), \\ 2N_i^\circ - (N_i' + N_i') &= \mp a_i; \\ N_i - N_i' &= \pm b_i. \end{aligned}$$

La valeur de $N_i^{(a)}$ pourrait aussi se déduire par voie d'exclusion de celle de $N_i^{(a)}$; mais le calcul serait probablement moins simple.

Nous terminerons ici les applications des formules du § 1, à la résolution de l'équation $x^p=1$, et nous passerons à une autre non moins utile, savoir la démonstration des lois de réciprocité dans la théorie des résidus de puissances.

§ III. *Des résidus de puissances en général et des résidus quadratiques en particulier.*

I.

Caractère propre à exprimer la classe d'un nombre premier donné.

On a dit dans l'article II du § 1, (t. II, p. 259), que pour le module $p=hm+1$ premier, les hm nombres $1, 2, 3, \ldots p-1$ se distribuaient en une classe de résidus de $m^{ième}$ puissance, et $m-1$ classes de non-résidus, et l'on a donné une règle pour trouver la classe d'un nombre composé, quand celles de ses facteurs premiers étaient connues.

Dans l'article I du § 2, l'on a donné un théorème par lequel on peut déterminer l'un des nombres $N_q^{(a)}$, $n_q^{(a)}$ en fonction de l'autre, ces nombres indiquant combien la congruence

$$x_1^m + x_2^m + \ldots + x_k^m \equiv \rho^a \pmod{p},$$

a de solutions (sans excepter ou en exceptant celles où des inconnues sont nulles) le nombre ρ étant une racine primitive de p.

Voici maintenant sur la forme du nombre $n_q^{(a)}$, un théorème qui conduira au caractère servant à décider si le nombre premier q appartient ou non à la classe $a^{ième}$.

« Théorème. Le nombre de solutions n_q de la conséquence » $x_1^m + x_2^m + \ldots + x_q^m \equiv \rho^a \pmod{p}$, où q est premier a nécessai- » rement l'une des formes suivantes :

» 1°. $m^q(q.Q+1)$, si q est de la classe $a^{ième}$, et
» 2°. $m^q(q.Q\quad)$, si q n'est pas de la classe $a^{ième}$. »

Démonstration. Soit $x_1 = \alpha_1$, $x_2 = \alpha_2, \ldots x_q = \alpha_q$, une solution de la congruence précédente, elle en fera obtenir m^q, si l'on combine sans transposition les m valeurs de x, donnant $x_1^m \equiv \alpha_1^m \pmod{p}$, avec les m valeurs de x_2 donnant $x_2^m \equiv \alpha_2^m \pmod{p}$, et ainsi des autres. Le nombre de solutions n_q est donc de la forme $m^q.P$. Quant

à P il ne peut avoir qu'une des formes $q\mathrm{Q}+1$ ou $q\mathrm{Q}$. Supposons en effet une solution $\alpha_1, \alpha_2, \ldots \alpha_q$, ou tous les nombres $\alpha_1 \ldots \alpha_q$, ne soient pas égaux; par la transposition, elle en donnera un nombre $\frac{q.q-1\ldots2.1}{1.2.\mathrm{A}\times 1.2.\mathrm{B}\times\ldots}$ en supposant que parmi les nombres $\alpha_1 \ldots \alpha_q$, il y en ait A égaux entre eux, et à α_1, B égaux entre eux, et à α_2 et ainsi de suite. Or ce nombre $\frac{q.q-1\ldots2.1}{1.2\ldots\mathrm{A}\times 1.2\ldots\mathrm{B}\times}$ est de forme $q\mathrm{R}$ ou multiple de q. Supposons encore qu'on puisse avoir la solution $\alpha_1 = \alpha_2 = \ldots = \alpha_q$, elle n'en donnera aucune autre par la transposition, le nombre total des solutions sera donc $m^q(q\mathrm{Q}+1)$ si la solution $\alpha_1 = \alpha_2 \ldots = \alpha_q$ existe, et $m^q.q\mathrm{Q}$ si elle n'existe pas. Or, si l'on pose $x_1 = x_2 \ldots = x_q = \alpha_1$ on a $qx_1^m \equiv p^a$, $(qx_1)^m \equiv q^{m-1}p^a \pmod{p}$; posant $q \equiv p^b + fm$, il vient $(qx_1)^m \equiv p^{a+(m-1)(b+fm)}$, et pour la possibilité de cette congruence $a - b$ doit être multiple de m, ainsi $a \equiv b \pmod{m}$, c'est-à-dire que q doit être de la classe a. Réciproquement si q est de la classe a, en posant $q = p^{a+fm}$ la congruence $qx_1^m \equiv p^a$ deviendra $(p^f x_1)^m \equiv 1$ qui est possible, et l'on pourra faire $x_1 = x_2 \ldots = x_q$. Il résulte encore de là que si l'on ne peut faire $\alpha_1 = \alpha_2 \ldots = \alpha_q$, q n'est pas de la classe a et réciproquement; d'où l'énoncé.

Corollaire. Comme on a $n_q^{(a)} \equiv \mathrm{N}_q^{(a)} \pmod{q}$, il en résultera $\mathrm{N}_q^{(a)} \equiv m^q(q\mathrm{Q}+1) \pmod{q}$, ou bien encore $\mathrm{N}_q^{(a)} \equiv m \pmod{q}$, si q nombre premier impair est de classe $a^{ième}$, et $\mathrm{N}_q^{(a)} \equiv 0 \pmod{q}$, si q nombre premier impair n'est pas de classe $a^{ième}$. Nous allons dans l'article suivant appliquer ce caractère aux résidus quadratiques; nous l'appliquerons dans les §§ suivants, aux résidus cubiques et aux résidus bi-quadratiques.

II.

Des résidus quadratiques.

« Théorème I. Le nombre 2 est résidu quadratique des nombres » premiers de forme $8g \pm 1$, et non-résidu des nombres premiers » de forme $8g \pm 5$. »

Démonstration. Le nombre de solutions de la congruence... $x_1^2 + x_2^2 \equiv 1 \ (p^{\alpha\alpha})$ (mod. p) est $N_2 = p \mp 1$ (§ 1), pour $p = 4q \pm 1$; d'ailleurs $n_2 = N_2 - 2N_1 = N_2 - 4$: donc pour 2 résidu quadratique on aura $4(2Q+1) = p \mp 1 - 4$ ou $p = 8g \pm 1$. Pour 2 non-résidu quadratiques, on aura $4.2Q = p \mp 1 - 4$ ou $p = 8g \pm 5$.

« Théorème II. (Loi de réciprocité de Legendre. Théorème fonda- » mental.) Soient p et q deux nombres premiers impairs et $q^{\frac{p-1}{2}} \equiv i \pmod{p}$ (i étant $+1$ ou -1) on aura $p^{\frac{q-1}{2}} \equiv i(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ (mod. q).

N. B. Legendre représente par le symbole $\left(\frac{q}{p}\right)$ le reste $+1$ ou -1 de $q^{\frac{p-1}{2}}$ divisé par p. Le théorème revient donc à la relation $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ ou encore à $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ puisque $\left(\frac{q}{p}\right)^2 = 1$.

Démonstration. 1°. Si q est résidu quadratique de p, c'est-à-dire si $i=1$, il faut avoir $N_q \equiv 2$ (mod. q), ou bien d'après la formule (18) du § 1, $p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv 2 \pmod{q}$, d'où $p^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv i(-1)^{\frac{p-1}{2}\cdot\frac{-1}{2}} \pmod{q}$. 2°. Si q est non-résidu quadratique de p, c'est-à-dire si i est égal à -1, il faut avoir $N_q \equiv 0$ (mod. q) ou bien $p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv 0 \pmod{q}$ ou encore $p^{\frac{q-1}{2}} \equiv -(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv i(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod{q}$. C.Q.F.D.

Remarques. J'ai déjà donné cette démonstration dans une note sur les résidus présentée à l'Académie des Sciences. Avec cette seule différence, qu'au lieu de calculer directement les quantités N_q, je les ai déduites d'une formule de M. Libri [formule (40), § 1]. On peut encore tirer la démonstration, mais d'une manière beaucoup moins simple, de la valeur de n_q, qu'il serait peu utile de mettre ici.

Le théorème fondamental peut encore s'énoncer ainsi qu'il suit.

« Si p et q sont deux nombres premiers impairs, qui ne soient pas » tous deux de forme $4g-1$, la relation de p à q sera la même que

» celle de q à p. En d'autres termes, si l'on a p résidu de q (ou $p\mathrm{R}q$), » l'on aura aussi q résidu de p (ou $q\mathrm{R}p$). Mais si p et q sont tous deux » de forme $4g-1$, la relation de p à q ne sera pas la même que celle » de q à p. Autrement $p\mathrm{R}q$ donne $q\mathrm{N}p$ et $p\mathrm{N}q$ donne $q\mathrm{R}p$.

Les notations $p\mathrm{R}q$, $p\mathrm{N}q$ et la signification particulière du mot *relation* sont de M. Gauss.

Sans compter la démonstration de Legendre, on en a beaucoup d'autres du théorème précédent, l'un des plus importants de la théorie des nombres. M. Gauss en a donné six: deux sont dans les *Recherches Arithmétiques* et les autres dans les *Commentaires de Gottingue*. M. Jacobi en a donné une qui est rapportée dans la *Théorie des nombres*: M. Cauchy en a donné aussi une dans un mémoire sur les résidus, (*Bulletin de Férussac*, tome XII).

Indépendamment de ces démonstrations générales, les seules importantes dans l'état présent de la théorie des nombres, on en connaît plusieurs relatives aux petits nombres premiers 2, 3, 5... En voici deux: l'une relative à 2 et l'autre relative à 3.

» Théorème. Si l'on pose $(1+\sqrt{-1})^p = \mathrm{P}+\mathrm{Q}\sqrt{-1}$, on aura

» pour $p = 4\mathrm{K}$ $\quad \mathrm{P} = (-1)^{\frac{p}{4}} 2^{\frac{p}{2}}$, $\quad \mathrm{Q} = 0$,

» pour $p = 4\mathrm{K}+2$, $\mathrm{P} = 0$, $\quad \mathrm{Q} = (-1)^{\frac{p-2}{4}} 2^{\frac{p}{2}}$,

» et pour $p = 4\mathrm{K}\pm 1$, $\mathrm{P} = \pm \mathrm{Q} = (-1)^{\frac{p\pm 1}{4}} 2^{\frac{p-1}{2}}$. »

Démonstration. $(1+\sqrt{-1})^4 = (2\sqrt{-1})^2 = -2^2$ donne $(1+\sqrt{-1})^{4k} = (-1)^k \cdot 2^{2k}$: multipliant successivement par $1+\sqrt{-1}$, $(1+\sqrt{-1})^2 = 2\sqrt{-1}$ et $\frac{1}{1+\sqrt{-1}} = \frac{1-\sqrt{-1}}{2}$, on aura

$$(1+\sqrt{-1})^{4k+1} = (-1)^k 2^{2k} + (-1)^k \cdot 2^{2k}\sqrt{-1},$$
$$(1+\sqrt{-1})^{4k+2} = +(-1)^k \cdot 2^{2k+1}\sqrt{-1},$$
$$(1+\sqrt{-1})^{4k-1} = (-1)^k 2^{2k-1} - (-1)^k \cdot 2^{2k-1}\sqrt{-1};$$

d'où les résultats de l'énoncé.

Corollaire. Soit p premier impair $P = 1 - \frac{p.p-1}{1.2} + \ldots$ donne $P \equiv 1 \pmod{p}$ ce qui réduit $P = (-1)^{\frac{p\pm1}{2}} 2^{\frac{p-1}{2}}$ à $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p\pm1}{2}}$, savoir 2 résidu, si $\frac{p\mp1}{4}$ est pair, c'est-à-dire si $p = 8g \pm 1$, et 2 non-résidu, si $\frac{p\mp1}{4}$ est impair, ou si $p = 8g \pm 5$ (*).

« Théorème. Si l'on pose $(1+\sqrt{-3})^p = P + Q\sqrt{-1}$, on aura

» pour $p = 3k$, $P = (-1)^{\frac{p}{3}} 2^p$, $Q = 0$,

» $p = 3k \pm 1$, $P = \pm Q = (-1)^{\frac{p\mp1}{3}} 2^{p-1}$.

Démonstration. $(1+\sqrt{-3})^3 = -2^3$, d'où $(1+\sqrt{-3})^{3k} = (-1)^k 2^{3k}$,

et $(1+\sqrt{-3})^{3k+1} = (-1)^k 2^{3k} + (-1)^k 2^{3k}\sqrt{-3}$,

$(1+\sqrt{-3})^{3k-1} = (-1)^k 2^{3k-2} - (-1)^k 2^{3k-2}\sqrt{-3}$,

en vertu de $\frac{1}{1+\sqrt{-3}} = \frac{1}{4}(1-\sqrt{-3})$. De là les valeurs de P et Q.

Corollaire. Si p est premier, on a

$$Q = p + \frac{p.p-1.p-3}{1.2.3}(-3) + \ldots + (-3)^{\frac{p-1}{2}} \text{ ou } (-3)^{\frac{p-1}{2}} \equiv Q \pmod{p},$$

ou encore

$$(-3)^{\frac{p-1}{2}} \equiv \pm(-1)^{\frac{p\mp1}{3}} . 2^{p-1} \equiv \pm(-1)^{\frac{p\mp1}{3}} \equiv \pm 1 \pmod{p},$$

puisque $\frac{p\mp1}{3}$ est nécessairement pair.

(*) Une autre conséquence dn théorème précédent est qu'en posant

$$(1+1)^p = 1 + Q_1 + Q_2 + Q_3 + \ldots Q_p,$$

et faisant

$S_0 = 1 + Q_4 + Q_8 + \ldots S_1 = Q_1 + Q_5 + \ldots S_2 = Q_2 + Q_6 + \ldots S_3 = Q_3 + Q_4 + \ldots$

on trouvera pour ces sommes de coefficients binomiaux pris de 4 en 4,

$2S_0 = 2^{p-1} + P$, $2S_2 = 2^{p-1} - P$, $2S_1 = 2^{p-1} + Q$, $S_3 = Q_3 + Q_4 + \ldots$

ce qui résulte de $P = S_0 - S_2$, $Q = S_1 - S_3$ et $(1-1)^p = 0$ qui donne

$S_0 + S_2 = S_1 + S_3 = 2^{p-1}$, puisque $(1+1)^p = S_0 + S_1 + S_2 + S_3 = 2^p$.

On a donc d'abord — 3 résidu de $p = 3k + 1$, et non-résidu de $p = 3k - 1$; ensuite comme $3^{\frac{p-1}{2}} = \pm(-1)^{\frac{p-1}{2}}$, il en résultera que 3 est résidu quadratique des nombres de forme $12g \pm 1$, et non-résidu de ceux de forme $12g \pm 5$.

Cette démonstration est la même, au fond, que celle donnée par M. Libri pour ce cas particulier.

La loi de réciprocité a deux usages principaux. Elle fait connaître pour quelles formes de nombres premiers, un nombre a est résidu ou non-résidu quadratique d'un nombre premier donné. Elle fournit aussi un moyen fort court, même pour un fort grand nombre premier, de juger si a est résidu ou non-résidu quadratique d'un module premier p, ce qui ne serait guère praticable par le calcul direct du reste de $a^{\frac{p-1}{2}}$. Pour cette application, rien n'est plus commode qu'un algorithme ou procédé de calcul, que M. Gauss a joint postérieurement à sa troisième démonstration. Cet algorithme ne se trouvant point dans la troisième édition de la théorie des nombres de Legendre, bien que la troisième démonstration de M. Gauss y soit rapportée, nous pensons être utile et agréable aux amateurs de la théorie des nombres, en donnant dans l'article suivant la troisième démonstration de M. Gauss, avec l'algorithme qu'il a exposé dans le Mémoire intitulé *Theorematis fundamentalis in doctrinâ de residuis quadraticis demonstrationes et ampliationes novæ*. C'est, selon nous, ce qu'on peut donner de plus direct pour la démonstration et de plus simple pour l'application. Nous avons d'ailleurs simplifié la partie de la démonstration rapportée par Legendre.

III.

Démonstration du théorème fondamental de la théorie des résidus quadratiques. — Algorithme qui s'en déduit pour juger de la possibilité de la congruence $x^2 \equiv q \pmod{p}$.

Il a été démontré dans le § I, que q est résidu quadratique du nombre premier p, si l'on a $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, et non-résidu, si

l'on a $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$: on a donc toujours $q^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. Ainsi il faut trouver un moyen praticable de reconnaître si le nombre entier que l'on doit mettre pour n, est pair ou impair. C'est l'objet des propositions suivantes.

« Théorème I. Soit q un nombre premier à $p = 2p' + 1$ nombre » premier. Si l'on divise par p les produits $1q, 2q, 3q, 4q, \ldots p'q$, » en prenant les quotients $Q_1, Q_2, Q_3, \ldots Q_{p'}$, les plus approchés qu'il » est possible, en plus ou en moins, de sorte que les restes positifs » ou négatifs $r_1, r_2, \ldots r_{p'}$, soient au signe près $< \frac{p}{2}$, on aura en » supposant qu'il y ait n restes négatifs,

$$(A) \qquad q^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Démonstration. Dans les équations $1.q = pQ_1 + r_1$, $2q = pQ_2 + r_2 \ldots$ $nq = pQ_a + r_a \ldots$ $bq = pQ_b + r_b \ldots$ $p'q = pQ_{p'} + r_{p'}$ (B), tous les restes sont nécessairement inégaux, car si l'on avait $r_a = \pm r_b$, il viendrait $(a \mp b)\, q = p\,(Q_a \mp Q_b)$, ce qui est impossible, puisque $(a \mp b)$ moindre que p devrait être divisible par p. Ainsi $r_1, r_2, r_3, \ldots r_{p'}$, formant à l'ordre et au signe près, la suite $1, 2, 3, \ldots p' = \frac{p-1}{2}$, en multipliant les équations (B) membre à membre, on aura $1.2.3 \ldots \frac{p-1}{2}\, q^{\frac{p-1}{2}} \equiv 1.2.3 \ldots \frac{p-1}{2}\,(-1)^n \pmod{p}$, ou bien $q^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$, en divisant par $1.2.3 \ldots \frac{p-1}{2}$.

» Théorème II. Si l'on représente par $e\left(\frac{aq}{p}\right)$, l'entier immédiate- » ment au-dessous de $\frac{aq}{p}$, par $p'\left(= \frac{p-1}{2}\right)$ l'entier $e\left(\frac{p}{2}\right)$, et par $\left[\frac{q}{p}\right]$ » la somme $e\left(\frac{q}{p}\right) + e\left(\frac{2q}{p}\right) + e\left(\frac{3q}{p}\right) + \ldots + e\left(\frac{p'q}{p}\right)$, on aura

» (C) $\qquad n \equiv \left[\frac{q}{p}\right] + \frac{1}{8}(p^2 - 1)(q - 1) \pmod{2}$.

Démonstration. Si dans l'équation $aq = pQ_a + r_a$, on a r_a positif,

il en résultera $Q_a = e\left(\frac{aq}{p}\right)$, mais si r_a est négatif, on aura $Q_a = e\left(\frac{aq}{p}\right) + 1$, par conséquent $Q_1 + Q_2 + Q_3 + \ldots Q_{p'} = \left[\frac{q}{p}\right] + n$, d'ailleurs $1 + \quad + 3 \ldots + \frac{p-1}{2} = \frac{1}{8}(p^2 - 1)$. Ajoutant donc les équations (B) membre à membre, après avoir remplacé le reste négatif r_a par $-r_a + 2r_a$ et ainsi des autres, nous aurons

$$\frac{1}{8}(p^2 - 1)q = p\left\{\left[\frac{q}{p}\right] + n\right\} + \frac{1}{8}(p^2 - 1) + 2r_a + \ldots$$

Omettant les multiples de 2, en réduisant p à l'unité et effaçant les termes $2r_a$ et autres semblables, nous trouverons..... $n \equiv -\left[\frac{q}{p}\right] + \frac{1}{8}(p^2 - 1)(q - 1) \pmod 2$, d'où la congruence en ajoutant au deuxième membre $2\left[\frac{q}{p}\right]$, ce qui revient à changer le signe du terme négatif $-\left[\frac{q}{p}\right]$.

Cette congruence (C) fera connaître si n est pair ou impair, quand on connaîtra $\left[\frac{q}{p}\right]$, c'est l'objet des corollaires suivants.

Corollaire I. Si $q = 2$, on aura $n \equiv \frac{1}{8}(p^2 - 1) \pmod 2$, car ici $\left[\frac{q}{p}\right] = 0$, tous les termes de cette somme étant nuls, de là le théorème sur 2.

Corollaire II. Si q est impair, on aura $n \equiv \left[\frac{q}{p}\right] \pmod 2$, car $(q-1)$ étant pair, il en est de même de $\frac{1}{8}(p^2 - 1)(q - 1)$.

Ainsi le nombre impair q est résidu ou non-résidu quadratique, selon que $\left[\frac{q}{p}\right]$ est pair ou impair.

Corollaire III. Si q est pair, en réduisant $q - 1$ à l'unité, on aura $n \equiv \left[\frac{q}{p}\right] + \frac{1}{8}(p^2 - 1)$. Ainsi pour $\frac{1}{8}(p^2 - 1)$ pair, c'est-à-dire pour $p = 8g \pm 1$, q sera résidu, selon que $\left[\frac{q}{p}\right]$ sera pair ou impair.

Ce sera le contraire pour $\frac{1}{8}(p^2-1)$ impair, c'est-à-dire pour $p = 8g \pm 5$.

COROLLAIRE IV. Quel que soit q pair ou non, il est résidu ou non, selon que $\left[\frac{2q}{p}\right]$ est pair ou impair.

Si l'on représente par n' la valeur correspondante à n quand on change q en $2q$, on aura $n' = \left[\frac{2q}{p}\right] + \frac{1}{8}(p^2-1)$. Si $\frac{1}{8}(p^2-1)$ est pair q et $2q$ sont en même temps résidus ou non-résidus, selon que $\left[\frac{2q}{p}\right]$ est pair ou impair. Si $\frac{1}{8}(p^2-1)$ est impair, q et $2q$ sont l'un résidu et l'autre non-résidu. Si $2q$ est non-résidu q est résidu, et cela arrive pour $\left[\frac{2q}{p}\right]$ pair. Si $2q$ est résidu, q est non-résidu, et cela arrive pour $\left[\frac{2q}{p}\right]$ impair.

« THÉORÈME III. Si p et q sont deux nombres premiers entre eux, » mais d'ailleurs premiers ou non, on aura en représentant par p' » et q' les entiers égaux à $\frac{p}{2}$, $\frac{q}{2}$ ou immédiatement inférieurs,

» (D) $$\left[\frac{p}{q}\right] + \left[\frac{q}{p}\right] = p'q'.$$

Démonstration. Nous avons par hypothèse,

$$\left[\frac{q}{p}\right] = e\left(\frac{q}{p}\right) + e\left(\frac{2q}{p}\right) + e\left(\frac{3q}{p}\right) + \ldots + e\left(\frac{p'q}{p}\right).$$

Cette valeur, où l'on suppose $q < p$, peut se transformer au moyen des remarques suivantes :

1°. Aucun des nombres $\frac{q}{p}$, $\frac{2q}{p}$ ... $\frac{p'q}{p}$ n'est entier;

2°. $e\left(\frac{p'q}{p}\right) = q'$ pour q impair;

3°. $e\left(\frac{p'q}{q}\right) = q' - 1$ pour q pair, alors $e\left(\frac{q'p}{q}\right) = p'$;

4°. Soient $k'q$, $k''q$... $k^{(q')}q$ les multiples de q, immédiatement au-dessous de p, $2p$... $q'p$, on aura

$$0 = e\left(\frac{q}{p}\right) = e\left(\frac{2q}{p}\right) \ldots\ldots\ldots = e\left(\frac{k'q}{p}\right), \quad k' = e\left(\frac{p}{q}\right);$$

$$1 = e\left(\frac{k'+1.q}{p}\right) = e\left(\frac{k'+2.q}{p}\right) \ldots = e\left(\frac{k''q}{p}\right), \quad k'' = e\left(\frac{2p}{q}\right);$$

$$2 = e\left(\frac{k''+1.q}{p}\right) = e\left(\frac{k''+2.q}{p}\right) \ldots = e\left(\frac{k'''q}{p}\right), \quad k''' = e\left(\frac{3p}{q}\right);$$

$$q'-1 = e\left(\frac{k^{(q'-1)}+1.q}{p}\right) = e\left(\frac{k^{(q')}+2.q}{p}\right) \ldots = e\left(\frac{k^{(q')}q}{p}\right), \quad k^{(q')} = e\left(\frac{q'p}{q}\right);$$

$$q' = e\left(\frac{k^{q'}+1.q}{p}\right) = e\left(\frac{k^{(q')}+2.q}{p}\right) \ldots = e\left(\frac{p'q}{p}\right).$$

Ces équations ont lieu pour q impair. Si q est pair les deux dernières doivent être remplacées par

$$q'-2 = e\left(\frac{k^{(q'-2)}+1.q}{p}\right) = e\left(\frac{k^{(q'-2)}+2.q}{p}\right) = \ldots = e\left(\frac{k^{(q'-1)}q}{p}\right), \quad k^{(q'-1)} = e\left(\frac{q'-1.p}{q}\right),$$

$$q'-1 = e\left(\frac{k^{q'-1}+1.q}{p}\right) = e\left(\frac{k^{(q'-1)}+2.q}{p}\right) = \ldots = e\left(\frac{p'q}{p}\right).$$

Ainsi dans le premier cas l'expression $\left[\frac{q}{p}\right]$ sera

$$\left[\frac{q}{p}\right] = 0.k' + 1(k'' - k') + 2(k''' - k'') + \ldots + q'(p' - k^{q'}),$$

$$= p'q' - k' - k'' - \ldots - k^{q'} = p'q' - \left[\frac{p}{q}\right],$$

Dans le second cas, l'on aura

$$\left[\frac{q}{p}\right] = 0.k' + 1(k'' - k') + 2(k''' - k'') \ldots + (q' - 1)(p' - k^{q'-1}),$$

$$= p'q' - k' - k^{2} - \ldots - k^{(q'-1)} - p',$$

$$= p'q' - k' - k^{2} \ldots\ldots - k^{(q'-1)} - k^{(q')} = p'q' - \left[\frac{p}{q}\right].$$

On a donc dans les deux cas

$$\left[\frac{q}{p}\right] + \left[\frac{p}{q}\right] = p'q'.$$

Corollaire. Si p et q sont premiers et impairs, en représentant, avec Legendre, par $\left(\frac{q}{p}\right)$ le reste ± 1 de $q^{\frac{p-1}{2}}$ divisé par p, on aura

$$\left(\frac{q}{p}\right) = (-1)^n = (-1)^{\left[\frac{q}{p}\right]}, \text{ de même } \left(\frac{p}{q}\right) = (-1)^{\left[\frac{p}{q}\right]},$$

donc

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left[\frac{q}{p}\right]+\left[\frac{p}{q}\right]} = (-1)^{p'q'} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Multipliant par $\left(\frac{q}{p}\right)$ et remarquant qu'on a $\left(\frac{q}{p}\right)^2 = 1$, il en résultera

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

ce qui est la loi de réciprocité de Legendre.

Théorème IV. *Algorithme.* « Soit q un nombre positif non divisible » par p nombre premier impair, si l'on fait sur p et q l'opération du » plus grand commun diviseur ainsi qu'il suit :

» Divid., div., restes	p,	q,	r,	s	.....	u,	v,	1	
» Quotients		a,	b,	c	.....	k,	l,		(I)
» Demi-dividendes.	p',	q',	r',	s'	.....	u',	v',		(II),

» et que dans la série (II) il y ait β, permanences de nombres im- » pairs, ou β nombres impairs immédiatement suivis d'un nombre » impair, que dans la série (I) il y ait α quotients impairs au-dessus » desquels se trouvent dans la série (II) des nombres de forme $4g+1$ » ou $4g+2$, la parité ou imparité de $\alpha+\beta$ montrera si q est résidu » ou non-résidu de p par la règle suivante :

» 1° Pour q impair, et pour q pair si $p = 8g \pm 1$; q sera résidu ou » non résidu quad. de p, selon que $\alpha+\beta$ sera pair ou impair.

» 2°. C'est le contraire si q étant pair on a $p = 8g \pm 5$.

» 3°. La première règle a lieu sans exception quand on fait le » même calcul sur $2q$ et p. »

Démonstration. L'opération du plus grand commun diviseur donnant la suite d'équations

$$p = qa + r, \quad q = rb + s \ldots . \quad u = vl + 1.$$

On en tire $\frac{p}{q} = a + \frac{r}{q}$, d'où $\frac{mp}{q} = am + \frac{mr}{q}$,

mettant pour m les valeurs $1, 2, 3, \ldots . q'$ et sommant on trouvera $\left[\frac{p}{q}\right] = \frac{1}{2}(q'^2 + q')a + \frac{r}{q}$, qui, en vertu de $\left[\frac{p}{q}\right] = p'q' - \left[\frac{q}{p}\right]$ deviendra

$$\left[\frac{q}{p}\right] = p'q' - \frac{1}{2}(q'^2 + q')a - \left[\frac{r}{q}\right],$$

on aura semblablement

$$\left[\frac{r}{q}\right] = q'r' - \frac{1}{2}(r'^2 + r')b - \left[\frac{s}{r}\right],$$
$$\left[\frac{s}{r}\right] = r's' - \frac{1}{2}(s'^2 + s')c - \left[\frac{t}{s}\right],$$
$$\vdots$$
$$\left[\frac{v}{u}\right] = u'v' - \frac{1}{2}(v'^2 + v')f - \left[\frac{t}{v}\right].$$

Or $\left[\frac{1}{v}\right] = 0$, on trouvera donc par l'élimination

$$\left[\frac{q}{p}\right] = (p'q' - q'r' + r's' \ldots \pm u'v) - \left\{\frac{1}{2}(q'^2 + q')a - \frac{1}{2}(r'^2 + r')b + \ldots \pm \frac{1}{2}(v'^2 + v')\right\}$$

Comme il suffit de savoir si $\left[\frac{q}{p}\right]$ est pair ou impair, on pourra d'abord changer tous les signes — en +, ce qui revient à ajouter le double des termes négatifs, puis supprimer tous les termes pairs, et réduire tous les termes impairs à l'unité; on trouve, en opérant ainsi, $\left[\frac{q}{p}\right] \equiv \beta + \alpha \pmod 2$, ce qui donne la règle de l'énoncé, au moyen des corollaires du th. III.

Exemples. Quoique les deux exemples suivants se rapportent à des

nombres assez grands, on a mis ici le calcul sans l'abréviation qui consisterait à n'écrire les restes qu'une fois. Ils font bien voir la simplicité du procédé.

1^er^ Exemple. Le nombre 638 est-il résidu ou non résidu quadratique du nombre premier $1091 = 8.136 + 3$?

1081, 638, 453, 185, 83, 19, 7, 5, 2.
1, 1 : 2, 2, 4, 2, 1 : 2.
453, 185, 83, 19, 7, 5, 2, 1.
545 : 319, 226, 92, 41 : 9 : 3, 2, 1.

Ici l'on a $\beta = 3$, $\alpha = 2$, $\alpha + \beta = 5$, or 638 est pair et 1091 de forme $8k + 3$, donc 638 est résidu quadratique d'après la seconde partie de la règle (2°).

2^e^ Exemple. Calcul fait sur $2.638 = 1276$ et 1091.

1276, 1091, 185, 166, 19, 14, 5, 4.
1 : 5, 1, 8, 1, 2, 1 :
185, 166, 19, 14, 5, 4, 1.
638, 545, 92, 83 : 9 : 7, 2, 2.

Ici $\beta = 2$, $\alpha = 2$, $\alpha + \beta = 4$: il faut donc que 638 soit résidu par la troisième partie de la règle (3°).