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 2 (1837), p. 253-292.
<http://www.numdam.org/item?id=JMPA_1837_1_2__253_0>

RECHERCHES SUR LES NOMBRES;

PAR M. LEBESGUE,

Professeur-suppléant à la Faculté des Sciences de Grenoble

§ Ier *Nombre de solutions de la congruence* $ax^m+by^m+\ldots+ku^m\equiv l$ *(mod.* $p=hm+1$*). Le module étant supposé premier.*

Quoique M. Libri ait déjà donné une formule très remarquable qui détermine le nombre de solutions d'une congruence quelconque, j'ai cru devoir cependant reprendre la question en suivant une autre marche, afin de ne pas supposer la résolution de l'équation $x^p=1$, voulant au contraire la déduire des formules de ce paragraphe.

I.

Congruence conditionnelle à laquelle satisfait le nombre de solutions d'une congruence algébrique et entière $f(x_1, x_2\ldots x_k)\equiv 0 \pmod{p}$.

On suppose ici que la fonction $f(x_1, x_2,\ldots x_k)$ qui renferme k inconnues est une somme de termes de la forme $Ax_1^a x_2^b\ldots x_k^l$, où les exposants sont des entiers positifs et le coefficient A un entier positif ou négatif. De plus quand une inconnue manque dans un terme, on l'y fait entrer avec l'exposant zéro.

Il est question seulement ici des solutions en nombres entiers positifs et moindres que le module, zéro n'étant pas excepté des valeurs données aux inconnues. Voici comment on déterminerait les solutions et leur nombre, si la grandeur du module ne rendait pas le calcul impraticable. On arrangerait k à k, de toutes les manières possibles et

sans exclure la répétition d'un même nombre, les p nombres... $0, 1, 2, \ldots (p-1)$; ce qui donnerait p^k arrangements : les uns tels que $\alpha_1, \alpha_2, \ldots \alpha_k$ donnant $f(\alpha_1, \alpha_2, \ldots \alpha_k) \equiv 0 \pmod{p}$ seraient les solutions et les seules solutions, puisque les autres arrangements tels que $\beta_1, \beta_2, \ldots \beta_k$ ne donneraient pas $f(\beta_1, \beta_2, \ldots \beta_k) \equiv 0 \pmod{p}$. Le nombre de solutions ainsi déterminé peut être représenté par S_k, l'indice rappelant le nombre des inconnues que renferme la congruence.

Quelquefois il est avantageux d'exclure zéro des valeurs données aux inconnues : dans ce cas les solutions se trouvent parmi les $(p-1)^k$ arrangements k à k des $p-1$ nombres $1, 2, 3 \ldots (p-1)$. Ce nombre de solutions peut être représenté par s_k : il est en général moindre que S_k.

Ceci posé, voici la congruence conditionnelle à laquelle satisfait le nombre S_k de solutions d'une congruence

$$f(x_1, x_2, \ldots x_k) = X_k \equiv 0 \pmod{p}.$$

Théorème. *Soit* S_k *le nombre de solutions de la congruence* $f(x_1, x_2, \ldots x_k) \equiv 0 \pmod{p}$, *si l'on fait* $f(x_1, x_2, \ldots x_k) = X_k$ *et que l'on suppose* $X_k^{p-1} = \Sigma A x_1^a x_2^b \ldots x_k^s$, *on aura, en représentant par* $\Sigma A_{(p-1)}$ *la somme des coefficients des termes du développement de* X_k^{p-1}, *où les inconnues entrent toutes (c'est-à-dire en nombre* k*) avec des exposants multiples de* $p-1$ *et plus grands que zéro*,

$$(1) \qquad S_k \equiv (-1)^{k+1} \Sigma A_{(p-1)} \pmod{p}.$$

Démonstration. On substituera dans X_k^{p-1} pour $x_1, x_2, \ldots x_k$ les nombres qui résultent de chacun des p^k arrangements k à k des nombres $0, 1, 2, \ldots (p-1)$. Pour chaque solution $(\alpha_1, \alpha_2, \ldots \alpha_k)$ on trouvera $X_k^{p-1} \equiv 0 \pmod{p}$, puisque l'on aura $X_k \equiv 0 \pmod{p}$. Pour toute autre substitution, on aura $X_k^{p-1} \equiv 1 \pmod{p}$, puisque X_k ne sera pas divisible par p. La somme des résultats de ces substitutions successives sera donc

$$\equiv S_k \times 0 + (p^k - S_k) \times 1 \equiv -S_k \pmod{p}.$$

D'un autre côté, si l'on pose pour abréger

$$0^a + 1^a + 2^a + \ldots + (p-1)^a = fa,$$

la somme exacte des valeurs de X_k^{p-1} ou de $\Sigma A x_1^a x_2^b \ldots x_k^g$ sera $\Sigma A fa fb \ldots fg$. On le voit de suite en faisant d'abord les substitutions pour x_1 et sommant, ce qui donne $\Sigma A fa x_2^b \ldots x_k^g$; puis pour x_2 dans la somme précédente et sommant de nouveau, ce qui donne $\Sigma A fa fb \ldots x_3^h$; et ainsi de suite jusqu'à ce qu'on trouve $\Sigma A fa fb \ldots fg$ après avoir fait les substitutions pour les k inconnues, que l'on suppose toutes dans chaque terme, ce qui introduit des sommes $fo = p$, dans les termes où des inconnues manquent. Or on a par des théorèmes bien connus $fa \equiv o \pmod{p}$, si a n'est pas multiple de $p-1$, et $fa \equiv p-1 \equiv -1 \pmod{p}$, si a est multiple de $p-1$. D'après cela chaque terme de $\Sigma A fa fb \ldots fg$ sera $\equiv o \pmod{p}$, ou $\equiv A(-1)^k \pmod{p}$, ce cas arrivant et ne pouvant arriver que quand les exposants $a, b, \ldots g$ en nombre k sont tous multiples de $p-1$ et plus grands que zéro. Si pour rappeler cette circonstance on représente le coefficient A de $A(-1)^k$ par $A_{\epsilon(p-1)}$, la somme des valeurs de $X_k^{p-1} = \Sigma A x_1^a x_2^b \ldots x_k^g$ sera donc

$$\equiv \Sigma A_{\epsilon(p-1)} (-1)^k \pmod{p},$$

mais elle est aussi

$$\equiv -S_k \pmod{p}. \text{ De là résulte } -S_k \equiv (-1)^k \Sigma A_{\epsilon(p-1)} \pmod{p},$$

ou encore

$$S_k \equiv (-1)^{k+1} \Sigma A_{\epsilon(p-1)} \pmod{p}.$$

Comme il est dit dans l'énoncé.

Si l'on exclut les solutions renfermant une ou plusieurs inconnues égales à zéro, on trouvera tout-à-fait de même la formule

$$(2) \qquad S_k \equiv (-1)^k [1 - \Sigma A'_{\epsilon(p-1)}] \pmod{p}$$

où $\Sigma A'_{\epsilon(p-1)}$ indique la somme des coefficients du développement de X_k^{p-1} répondant à des termes dans lesquels les exposants des inconnues sont tous multiples de $p-1$, sans ajouter cette restriction qu'ils doivent être plus grands que zéro. C'est pour rappeler cette circonstance que la lettre A a été accentuée.

La formule (2) est beaucoup moins commode pour les applications que la formule (1), dont nous nous servirons principalement.

Quand il n'y aura qu'une ou deux inconnues, les congruences conditionnelles (1) et (2) détermineront complétement S_1 et S_2, ou s_1 et s. Mais pour un plus grand nombre d'inconnues il faudra employer une autre méthode. Car si les nombres S_k et s_k deviennent plus grands que le module, la congruence conditionnelle donnera pour S_k et s_k une expression $hp+\sigma$ où σ sera un nombre déterminé moindre que p, mais où h restera indéterminé. M. Libri a déjà donné des congruences analogues à celles (1) et (2); mais, comme les précédentes, elles ne sont qu'un premier pas vers la solution du problème qui fait l'objet de ce paragraphe.

II.

Nombre de solutions de la congruence $x^m \equiv a \pmod{p = hm+1}$.

La congruence $ax^m \equiv b \pmod{p = hm+1}$ se ramène à..... $y^m \equiv A \pmod{p}$ en faisant $A \equiv ba^{m-1}$ et $y \equiv ax \pmod{p}$, puisque l'on a $a^m x^m \equiv ba^{m-1} \pmod{p}$; ou bien encore à $x^m \equiv A \pmod{p}$, puisque, en posant $ag \equiv 1$, $bg \equiv A$, l'on a $agx^m \equiv bg \pmod{p}$. Comme d'ailleurs le nombre de solutions ne change pas, nous considérerons directement la congruence $x^m \equiv a \pmod{p}$.

Ici $X_1 = x^m - a$, et le terme général du développement de X_1^{p-1} est $\frac{p-1.p-2...p-n}{1.2...n}(-a)^n x^{m(p-1-n)} = \frac{Mp+1.2.3...n.a^n}{1.2.3...n} x^{m(p-1-n)}...$ $\equiv a^n x^{m(p-1-n)} \pmod{p}$.

On rendra l'exposant de x multiple de $p-1$, en posant $mn=(p-1)g$; et si d est le plus grand commun diviseur de m et de $p-1$, n prendra les valeurs $0, 1.\frac{p-1}{d}, 2.\frac{p-1}{d}, 3.\frac{p-1}{d}, \ldots (d-1).\frac{p-1}{d}$; de là, au moyen de la formule (1), où l'on fera $k=1$, on trouvera

$$(3) \qquad S_1 \equiv 1 + a^{\frac{p-1}{d}} + a^{2.\frac{p-1}{d}} \ldots + a^{(d-1)\frac{p-1}{d}} \equiv \frac{a^{p-1}-1}{a^{\frac{p-1}{d}}} \pmod{p}.$$

Or, évidemment, on ne peut avoir ni $S_1 = p$, ni $S_1 > p$, donc

1°. Si l'on a $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, il en résultera $S_1 = d$.

2°. Si l'on n'a pas $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, il en résultera $s_1 = 0$.

Ce dernier cas résulte de ce que $a^{p-1} - 1 \equiv 0 \pmod{p}$.

La condition de possibilité de la congruence $x^m \equiv a \pmod{p}$ est donc $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$ et le nombre de ses solutions est d, ce nombre représentant le plus grand commun diviseur de m et de $p-1$

La congruence $x^m \equiv a \pmod{p}$ n'ayant que d racines réelles, on la ramènera à la forme $x^d \equiv a^i \pmod{p = gd+1}$ en posant..... $mi \equiv d \pmod{p-1}$. D'après cela on considère principalement le cas de la congruence $x^m \equiv a \pmod{p = hm+1}$, pour lequel $d = m$; alors la condition de possibilité devient $a^{\frac{p-1}{m}} \equiv 1 \pmod{p}$ et le nombre de solutions est égal à m. Si l'on avait $a \equiv 0 \pmod{p}$ il n'y aurait qu'une solution, savoir $x = 0$. Quand la congruence.... $x^m \equiv a \pmod{p}$ est possible, on dit que a est un résidu de m^e puissance pour le module p; et particulièrement un résidu quadratique, cubique, biquadratique, selon que m est égal à 2, 3 ou 4.

Voici les énoncés de quelques propositions qui serviront plus loin.

Les résidus de m^e puissance pour le module $p = mh+1$ sont les racines de la congruence $x^{\frac{p-1}{m}} \equiv 1 \pmod{p}$. Ils sont en nombre $\frac{p-1}{m}$, et si l'un d'eux est représenté par a, la formule ay^m les contient tous.

Les nombres qui ne sont pas résidus de $m^{ième}$ puissance pour le module p, sont nommés non-résidus; ils sont en nombre.... $p - 1 - \frac{p-1}{m} = (m-1)\frac{p-1}{m}$: ils se subdivisent en $m-1$ classes de $\frac{p-1}{m}$ nombres chacune. Voici le principe de cette classification importante: il est bon de le rappeler ici, à cause de l'usage continuel que nous en ferons.

La congruence $x^m \equiv 1 \pmod{p = hm+1}$, ayant pour racine un certain nombre entier r, les nombres r, r^2, r^3, $\ldots r^m \equiv 1 \pmod{p}$ satisferont tous à la congruence $x^m \equiv 1 \pmod{p}$. Or si l'on a.....

$m = a^\alpha b^\beta c^\gamma \ldots$ où a, b, $c\ldots$ sont des nombres premiers différents, on a prouvé qu'il y a $m.\frac{a-1}{a}.\frac{b-1}{b}.\frac{c-1}{c}\ldots$ valeurs de r, telles que les puissances successives r^1, r^2, $r^3,\ldots r^m$ seront toutes incongrues suivant le module p, et formeront par conséquent la suite complète des racines de la congruence $x^m \equiv 1 \pmod{p = hm+1}$. Les racines r qui jouissent de cette propriété sont dites *primitives* (*). D'après cela on classe les nombres 1, 2, 3...$(p-1)$, ainsi qu'il suit :

Soit r une racine primitive de $x^m \equiv 1 \pmod{p}$ *et* ρ *une racine primitive de p ou de* $x^{p-1} \equiv 1 \pmod{p}$.

(*) Voici les énoncés de deux propositions qui prouvent l'existence des racines primitives et qui en déterminent le nombre.

Si l'on représente par A_1, $A_2\ldots A_g$ *des nombres entiers ou des polynomes de forme* $a+bx+ex^2+\ldots fx^k$, etc. *Si de plus l'on représente par* P_1 *le produit des quantités* $A_1, A_2\ldots A_g$, *par* P_2 *le produit des plus grands communs diviseurs des mêmes quantités combinées 2 à 2, par* P_3 *le produit desplus grands communs diviseurs des mêmes quantités combinées 3 à 3, et ainsi de suite : le plus petit nombre, ou le polynome de moindre degré divisible par* $A_1, A_2, \ldots A_g$ *sera* $\frac{P_1.P_3.P_5\ldots}{P_2.P_4.P_6\ldots}$.

Si l'on suppose $m = a^\alpha b^\beta c^\gamma \ldots\ldots\ldots$ (a, b, $c\ldots$ *étant des nombres premiers différents*) *et que l'on fasse* $A_1 = x^{\frac{m}{a}} - 1$, $A_2 = x^{\frac{m}{b}} - 1$, $A_3 = x^{\frac{m}{c}} - 1$, etc., *la congruence qui donne les racines primitives de la congruence* $x^m \equiv 1 \pmod{p}$ *sera* $\frac{(x^m-1).P_2.P_4.P_6\ldots}{P_1P_3P_5\ldots} \equiv 0 \pmod{p}$ *son degré* $m.\frac{a-1}{a}.\frac{b-1}{b}.\frac{c-1}{c}\ldots\ldots$ *marquera le nombre des racines primitives.*

Nous omettrons les démonstrations qui ne présentent aucune difficulté. Nous pourrons revenir dans un autre mémoire sur la détermination des racines primitives et la construction des tables qui résolvent la congruence $x^m \equiv a \pmod{p}$, comme les tables de logarithmes résolvent $x^m = a$. (V. les *Recherches arithmétiques* de M. Gauss.) Nous ajouterons seulement que la congruence précédente s'étend aux racines primitives imaginaires de la congruence $x^m \equiv 1 \pmod{p = hm-1}$. (V. *De Residuis cubicis commentatio numerosa*, J. de M. Crelle, tome II.)

Pour la détermination de la congruence aux racines primitives, on peut consulter les exercices mathématiques de M. Cauchy, année 1829. J'avais donné antérieurement la même congruence dans le *Bulletin du Nord*, journal scientifique et littéraire publié à Moscou.

1°. *On aura* $r \equiv \rho^h \pmod{p = hm + 1}$.

2°. *Les résidus de* $m^{ième}$ *puissance ou les racines de* $x^{\frac{p-1}{m}} \equiv 1 \pmod{p}$ *seront* $\rho^0, \rho^m, \rho^{2m}, \ldots \rho^{(h-1)m}$: *leur formule est* y^m.

3°. *Les non résidus de première classe, ou les racines de*..... $x^m \equiv r \equiv \rho^h \pmod{p}$ *seront les nombres* $\rho, \rho^{m+1}, \rho^{2m+1}, \ldots \rho^{(h-1)m+1}$ *leur formule est* ρy^m.

4°. *Les non-résidus de deuxième classe, ou les racines de*.... $x^h \equiv r^2 \equiv \rho^{2h} \pmod{p}$ *seront les nombres* $\rho^2, \rho^{m+2}, \ldots \rho^{(m-2)m+2}$. *leur formule est* $\rho^2 y^m$.

5°. *En général, les non-résidus de* $g^{ième}$ *classe, ou les racines de la congruence* $x^m \equiv r^g \equiv \rho^{gh} \pmod{p}$, *seront les nombres*..... $\rho^g, \rho^{m+g}, \ldots \rho^{(h-1)m+g}$, *dont la formule est* $\rho^g y^m$

On emploie fréquemment les conséquences suivantes :

Pour le cas de $\frac{p-1}{m}$ *nombre pair,* -1 *sera résidu de* $m^{ième}$ *puissance, pour le module p. Pour le cas de* $\frac{p-1}{m}$ *nombre impair, ce qui ne peut arriver que pour m pair,* -1 *sera un non-résidu de* $\left(\frac{m}{2}\right)^{ième}$ *classe.*

Le produit abcd... sera résidu de $m^{ième}$ *classe pour le module p, si la somme des numéros de classe des facteurs non-résidus, est multiple de m, ou de forme* Km. *Ce produit sera au contraire un non-résidu de* $g^{ième}$ *classe, si la somme des numéros de classe des facteurs non-résidus est de la forme* Km + g.

Si a est un non-résidu de première classe, les nombres $a^1, a^2, a^3, \ldots a^{m-1}$, *seront des non-résidus de* 1^{re}, 2^e, 3^e, ... $(m-1)^{ième}$ *classe respectivement.*

Quoiqu'il y ait de l'arbitraire dans le numérotage des classes de non-résidus qui change avec la racine primitive ρ, cette classification n'en est pas moins importante, ainsi que l'a prouvé M. Gauss par sa résolution de l'équation $x^n = 1$, où il ne reste guère à faire que des simplifications de calcul, qui n'entraient point dans le plan de son ouvrage.

III.

Nombre de solutions de la congruence $a_1x_1^m + a_2x_2^m \equiv a_3 \pmod{p = hm+1}$.

Pour le cas de $a_3 \equiv 0 \pmod{p}$; on a de suite ce théorème :

La congruence $a_1x_1^m + a_2x_2^m \equiv 0 \pmod{p}$ *a une seule solution* ($x_1 = 0$, $x_2 = 0$), *si* $-a_2a_1^{m-1}$ *est non-résidu de* $m^{ième}$ *puissance, et* $1 + m(p-1)$ *si* $-a_2a_1^{m-1}$ *est résidu de* $m^{ième}$ *puissance.*

Pour le second cas les $m(p-1)$ solutions autres que $x_1 = 0_3$, $x_2 = 0$, résultent de la résolution de $z^m \equiv -a_2x_1^{m-1} \pmod{p}$, en posant $zx_2 \equiv a_1x_1 \pmod{p}$.

La formule générale $a_1x_1^m + a_2x_2^m \equiv a_3 \pmod{p}$ se ramène de suite à la formule particulière $x^m - ay^m \equiv b \pmod{p}$ en posant $x \equiv a_1x_1$, $y \equiv x_2$, $a \equiv -a_2a_1^{m-1}$, $b \equiv a_3a^{m-1} \pmod{p}$, ce qui ne change pas le nombre de solutions, c'est donc cette dernière que nous allons considérer pour simplifier les calculs.

La congruence $x^m \equiv ay^m + b \pmod{p = hm+1}$, *a un nombre de solutions multiple de m et moindre que mp.*

En effet, si l'on peut avoir $ay^m + b \equiv 0 \pmod{p}$, cela aura lieu pour m valeurs de y, à chacune desquelles correspondra $x = 0$, on aura d'abord m solutions.

Ensuite toute valeur de y qui donne $ay^m + b$ congru à un résidu de $m^{ième}$ puissance, donne m valeurs correspondantes pour x, d'où résultent m solutions. Il faut encore remarquer que si la valeur de y qui rend $ay^m + b$ résidu de $m^{ième}$ puissance n'est pas zéro, il y aura m valeurs de y, qui donneront pour $ay^m + b$, la même valeur résidue, d'où m^2 solutions par la combinaison des m valeurs de y avec les m valeurs de x.

Enfin, pour toute valeur de y qui ne rend pas $ay^m + b$ résidu de $m^{ième}$ puissance, il n'y aura aucune solution. D'après cela :

Le nombre de solutions de la congruence..... $x^m \equiv ay^m + b \pmod{p = hm+1}$ *est toujours multiple de m et prend l'une des trois formes :*

1°. km^s *si* b *et* $-ba^{m-1}$ *sont non-résidus de* $m^{ième}$ *puissance par rapport au module* p.

2°. km^s+m, *si des deux nombres* b, $-ba^{m-1}$ *l'un est résidu et l'autre non-résidu de* $m^{ième}$ *puissance par rapport au module* p.

3°. km^s+2m, *si* b *et* $-ba^{m-1}$ *sont tous deux résidus de* $m^{ième}$ *puissance pour le module* p.

Il suit de ce qui précède que y ne prenant que p valeurs 0, 1, 2...$(p-1)$, le nombre des solutions ne saurait surpasser mp. Pour qu'il fût égal à mp, il faudrait avoir $(ay^m+b)^{\frac{p-1}{m}} \equiv 1 \pmod{p}$ pour toute valeur de y: mettant donc pour y les nombres 0, 1, 2...$(p-1)$ et sommant, il en résulterait $a^{\frac{p-1}{m}}(p-1) \equiv 0 \pmod{p}$ en remarquant que si l'on pose $0^s+1^s+2^s+\ldots(p-1)^s = fg$, toutes les sommes comprises dans le résultat seront $\equiv 0 \pmod{p}$ à l'exception de $f(p-1)$ qui sera $\equiv p-1 \pmod{p}$. Mais on ne peut avoir..... $a^{\frac{p-1}{m}}(p-1) \equiv 0 \pmod{p}$ sans supposer $a \equiv 0 \pmod{p}$, ce qui n'est point. Le nombre de solutions est donc toujours moindre que mp.

La congruence (1) prendra donc la forme..... $mS'_2 \equiv (-1)\Sigma A2(p-1) \pmod{p}$, en posant $S_2 = mS'_2$; et comme S'_2 est moindre que p, elle suffira pour déterminer cette inconnue.

Voici maintenant la congruence qui donne S_2; on y suppose

$$A_1 = 1.2.3....h,$$
$$A_2 = (h+1)(h+2)....2h,$$
$$A_3 = (2h+1).....3h,$$
$$\vdots$$
$$A_{m-1} = [(m-2)h+1]...(m-1)h = (p-h-1)(p-h-2)... \equiv A_s(-1)^k,$$
$$A_m = [(m-1)h+1].....mh = (p-1)(p-2)...p-h \equiv A_s(-1)^k.$$

La relation $A_{s+1} \equiv (-1)^k A_s \pmod{p}$ servira pour simplifier les résultats.

THÉORÈME. *La congruence qui donne le nombre* S_2 *des solutions de la congruence* $x^m - ay^m \equiv b \pmod{p}$ *est*

$$(4)\quad -S_a \equiv a^h \qquad (\text{mod. } p = hm+1)$$
$$+a^{2h}+\frac{A_2}{A_1}a^hb^h$$
$$+a^{3h}+\frac{A_3}{A_1}a^{2h}b^h+\frac{A_3}{A_2}a^hb^{2h}$$
$$+a^{4h}+\frac{A_4}{A_1}a^{3h}b^h+\frac{A_4A_3}{A_1A_2}a^{2h}b^{2h}+\frac{A_4}{A_2}a^hb^{3h}$$

$$+a^{(m-1)h}+\frac{A_{m-1}}{A_1}a^{(m-2)h}b^h+\frac{A_{m-1}A_{m-2}}{A_1A_2}a^{(m-3)h}b^{2h}+\ldots+\frac{A_{m-1}}{A_2}a^hb^{(m-2)h}.$$

Cette formule se trouve immédiatement par le développement de $(x^m - c)^{p-1}$; où l'on fait $c = ay^m + b$.

Négligeant d'abord les termes où x n'a pas un exposant multiple de $p-1$, et le terme où x n'entre pas avec y, on aura en réduisant tous les coefficients à l'unité, d'après l'article précédent,

$$c^hx^{m(p-1-h)}+c^{2h}x^{m(p-1-2h)}+\ldots+c^{(m-1)h}x^{mh}.$$

Maintenant, si l'on développe la puissance $c^{kh} = (ay^m+b)^{kh}$, en effaçant tous les termes sans y et ceux où l'exposant n'est pas multiple de $p-1$, on trouvera

$$a^{kh}y^{m.kh}+\frac{A_k}{A}a^{(k-1)h}b^hy^{m(kh-h)}+\frac{A_k.A_{k-1}}{A_1A_2}a^{(k-2)h}b^{2h}y^{m(kh-2h)}+\ldots.$$
$$\frac{A_kA_{k-1}}{A_1A_2}a^{2h}b^{(k-2)h}y^{2mh}+\frac{A_k}{A}a^hb^{(k-1)h}y^{mh}.$$

On tirera de là les valeurs de c^h, c^{2h}, $\ldots c^{(m-1)h}$, d'où la congruence de de l'énoncé.

Si l'on voulait avoir la congruence donnant le nombre des solutions qui ne contiennent aucune inconnue égale à zéro, il faudrait prendre

$$(5)\quad s_a \equiv a^h b^h \pmod{p = hm+1}$$
$$+ a^{2h} + \frac{A_2}{A_1} a^h b^h + a^{2h}$$
$$+ a^{3h} + \frac{A_3}{A_1} a^{2h} b^h + \frac{A_3}{A_1} a^h b^{2h} + b^{3h}$$
$$\vdots$$
$$+ a^{(m-1)h} + \frac{A_{m-1}}{A_1} a^{(m-2)h} b^h + \ldots + \frac{A_{m-1}}{A_1} a^h b^{(m-2)h} + b^{(m-1)h}$$
$$+ a^{mh} + \frac{A_m}{A_1} a^{(m-1)h} b^h + \ldots + \frac{A_m}{A_1} a^h b^{(m-1)h} + b^{mh}$$

qui se trouve précisément de même en négligeant quelques termes de moins dans le développement de $(x^m - c)^{p-1}$.

Il faut remarquer que les congruences (4) et (5) ne contenant que a^h, b^h et leurs puissances, restent les mêmes, si a et b venant à changer, restent résidus de $m^{ième}$ puissance, quand ils sont résidus; et si quand ils sont non-résidus, ils restent non-résidus de la même classe. En un mot, les congruences (4) et (5) restent les mêmes, quand a et b changent de valeurs numériques sans changer de classe. En général pour toute congruence $ax^m + by^m + \ldots + ku^m \equiv l \pmod{p = hm+1}$, le nombre de solutions restera le même, quand les coefficients $a, b, \ldots k, l$ resteront des mêmes classes. En effet, si le terme ax^m devient $ag^m y^m = a(gy)^m$, y se tirera de x au moyen de la congruence... $gy \equiv x \pmod{p}$.

Les formules (4) et (5) donnent les valeurs de S_a et s_a quel que soit p : il est vrai cependant que les coefficients polynomiaux $\frac{A_2}{A_1}$, $\frac{A_3}{A_1}$, etc., rendent le calcul d'autant plus long que p est plus grand; mais, nous verrons, dans des cas particuliers, des théorèmes qui donneront un moyen expéditif de calculer ces coefficients.

Nous allons montrer maintenant comment les deux cas précédents conduisent aux valeurs de S_k et s_k, quel que soit le nombre k des inconnues.

IV.

Nombre de solutions de la congruence .....
$$a_1x_1^m + a_2x_2^m + \ldots + a_kx_k^m \equiv a_{k+1} \pmod{p = hm+1}.$$

Soient P et Q deux fonctions de la forme

$$a_1x_1^m + a_2x_2^m + \ldots + a_fx_f^m, \quad b_1y_1^m + b_2y_2^m + \ldots + b_fy_f^m;$$

représentons par P^0, P, P', P'', ... $P^{(m-1)}$ les nombres de solutions de la congruence $P \equiv A \pmod{p}$, selon que A sera zéro, résidu de $m^{ième}$ puissance, ou non-résidu de 1^{re}, 2^e, 3^e, ... $(m-1)^{ième}$ classe. Autrement g étant un non-résidu de première classe, soient

P^0 le nombre de solutions de la congruence $P \equiv 0 \pmod{p}$,
P ou $P^{(m)}$ le nombre de solutions de la congruence $P \equiv g^m \pmod{p}$,
P' le nombre de solutions de la congruence $P \equiv g \pmod{p}$,
P'' le nombre de solutions de la congruence $P \equiv g^2 \pmod{p}$,
⋮
$P^{(m-1)}$ le nombre de solutions de la congruence $P \equiv g^{m-1} \pmod{p}$.

Donnons à Q^0, Q, Q', Q'' ... $Q^{(m-1)}$ et à Π^0 des significations analogues et nous aurons la proposition suivante :

THÉORÈME. *Le nombre de solutions de la congruence* .....
$P \equiv Q \pmod{p = hm+1}$ *est en posant* $P - Q = \Pi$.

$$(6) \qquad \Pi^0 = P^0Q^0 + h[PQ + P'Q' + P''Q'' + \ldots + P^{(m-1)}Q^{(m-1)}],$$

DÉMONSTRATION. En effet pour une solution, on doit avoir simultanément $P \equiv A$, $Q \equiv A \pmod{p}$, A étant un nombre quelconque, qui peut être congru à zéro pour le module p, ou encore résidu ou non résidu de $m^{ième}$ puissance, par rapport au même module. Comme l'on devra prendre chaque solution de $P \equiv A \pmod{p}$ avec chaque solution de $Q \equiv A \pmod{p}$, pour en tirer les solutions de $P \equiv Q \pmod{p}$, on voit qu'à $A \equiv 0 \pmod{p}$, il répondra P^0Q^0 solutions de $P \equiv Q \pmod{p}$. Si A au lieu d'être $\equiv 0 \pmod{p}$ était résidu de $m^{ième}$ puissance pour

le module p, on montrerait de même qu'il y aurait PQ solutions qui donneraient $P \equiv Q \equiv A \pmod{p}$ et par conséquent $P \equiv Q \pmod{p}$. Maintenant si la congruence $P \equiv A \pmod{p}$ est possible, $P \equiv A f^m$ l'est également et a le même nombre de solutions, ces solutions s'obtenant, comme il est très facile de le voir, en multipliant par f les valeurs de $x_1, x_2, \ldots$ qui satisfont à $P \equiv A \pmod{p}$. Ainsi à chacune des $\frac{p-1}{m} = h$ valeurs résidues de $m^{ième}$ puissance qu'on peut prendre pour A, il répond PQ solutions, ou en tout hPQ solutions. On trouve semblablement hP'Q' solutions de $P \equiv Q \pmod{p}$, pour lesquelles on a $P \equiv Q \equiv$ à un non-résidu de $m^{ième}$ puissance et de première classe; pareillement on trouve hP''Q'' solutions de la congruence $P \equiv Q \pmod{p}$, pour lesquelles on a $P \equiv Q \equiv$ à un non-résidu de $m^{ième}$ puissance et de deuxième classe et ainsi de suite. D'où le résultat de l'énoncé.

La formule (6) subsistera pour $P + Q = \Pi \equiv 0 \pmod{p}$. Si h est impair il suffira, comme il est très aisé de le voir, d'augmenter les indices de Q de $\frac{m}{2}$. Cela vient de ce qu'en représentant par ρ une racine primitive de p, on a $-1 \equiv \rho^{\frac{hm}{2}} \pmod{p}$, ou en posant $h = 2h' + 1$, $-1 \equiv \rho^{h'm + \frac{m}{2}} \pmod{p}$, ou en d'autres termes de ce que -1 est un non-résidu de $\frac{m^{ième}}{2}$ classe.

Pour le cas particulier de $Q = g^k x^m$, g étant un non-résidu de première classe, et par conséquent g^k un non-résidu de $k^{ième}$ classe, on aura évidemment

$$Q^0 = 1, \quad Q' = Q'' = Q''' \ldots = Q^{(k-1)} = Q^{(k+1)} \ldots = Q^{(m-1)} = 0, \quad Q^{(k)} = m.$$

En sorte que l'équation (6) deviendra dans la supposition de... $\Pi = P - Q = P - g^k x^m \equiv 0 \pmod{p}$.

$$\Pi^0 = P^0 + (p-1) P^{(k)}, \tag{7}$$

d'où l'on tire

$$P^{(k)} = \frac{\Pi^0 - P^0}{p-1}. \tag{8}$$

On parviendra au même résultat pour $\Pi = P + g^k x^m \equiv 0 \pmod{p}$, si h est pair, mais si h est impair, il faudra changer $P^{(k)}$ en $P^{\left(k+\frac{m}{2}\right)}$.

Les formules précédentes ramènent tous les cas à ceux de $k=1$ et $k=2$, c'est-à-dire à ceux de une et deux inconnues, précédemment traités; car si l'on prend d'abord la congruence

$$a_1 x_1^m + a_2 x_2^m + \ldots + a_k x_k^m \equiv \pmod{p},$$

il suffira de poser $k = f + g$, et les nombres de solutions pour des congruences contenant l'une f inconnues et l'autre g inconnues

$$a_1 x_1^m + \ldots + a_f x_f^m \equiv A, \quad -a_{f+1} x_{f+1}^m - \ldots - a_k x_k^m \equiv A \pmod{p}$$

donnera le nombre de solutions d'une congruence contenant $f+g$ inconnues, savoir de

$$a_1 x_1^m + a_2 x_2^m + \ldots + a_k x_k^m \equiv 0 \pmod{p}.$$

Ensuite, par la formule (8), on passera du cas de la congruence $a_1 x_1^m + \ldots + a_k x_k^m - a_{k+1} x_{k+1}^m \equiv 0 \pmod{p}$, au cas de la congruence $a_1 x_1^m + \ldots + a_k x_k^m \equiv a_{k+1} \pmod{p}$.

Nous allons donner des exemples de ces calculs.

V.

Formules générales pour le nombre de solutions de la congruence $a_1 x_1^2 + a_2 x_2^2 + \ldots + a_k x_k^2 \equiv a_{k+1} \pmod{p = 2h+1}$.

Examinons le cas de $a_{k+1} = 0$, auquel les autres se ramènent, comme nous venons de le voir.

La congruence $a_1 x_1^2 + \ldots + a_k x_k^2 \equiv 0 \pmod{p}$ se réduit ainsi qu'il suit à une forme plus simple.

1°. Tous les termes tels que $a_i x_i^2$ dont le coefficient a_i est un résidu quadratique de p, pourront être remplacés par d'autres termes, tels que y_i^2. En effet, soit $a_i \equiv g^2 \pmod{p}$ et $g x_i \equiv y_i \pmod{p}$, il en résultera $a_i x_i^2 \equiv y_i^2 \pmod{p}$.

2°. Tous les termes tels que $a_f x_f^2$ dont le coefficient a_f est un non-résidu quadratique, étant passés dans le second membre, quand -1 sera non-résidu quadratique, ce qui arrive pour p de forme $4q-1$, la congruence prendra la forme

$$y_1^2+y_2^2+\ldots+y_f^2\equiv z_1^2+z_2^2+\ldots+z_i^2 \pmod{p}.$$

3°. Mais si -1 est résidu quadratique, ce qui arrive pour... $p=4q+1$, $-a_f$ sera non-résidu quadratique aussi bien que a_f, dans ce cas n étant un non-résidu quadratique déterminé, on posera $-a_f\equiv nz^2 \pmod{p}$ ou $(nz)^2\equiv -a_f n \pmod{p}$, ce qui est possible ; et la congruence prendra la forme

$$y_1^2+y_2^2+\ldots+y_f^2\equiv n(z_1^2+z_1^2+\ldots z_i^2) \pmod{p}.$$

Si tous les coefficients sont de même espèce résidus ou non-résidus quadratiques, la congruence devient

$$y_1^2+y_2^2+\ldots+y_k^2\equiv 0 \pmod{p}$$

qui est un cas particulier des précédentes.

Pour le cas de la congruence $y_1^2+y_2^2+\ldots+y_k^2\equiv a \pmod{p}$, nous représenterons le nombre de solutions par N_k°, N_k, N_k' selon que l'on aura $a\equiv 0 \pmod{p}$, ou que a sera résidu quadratique, ou enfin non-résidu quadratique. Si la congruence au lieu d'être du second degré était du $m^{ième}$, le nombre de solutions serait N_k° pour $a\equiv 0 \pmod{p}$; N_k pour a résidu de $m^{ième}$ puissance ; N_k' pour a congru à un non-résidu de première classe, N_k'' pour a congru à un non-résidu de deuxième classe, et ainsi de suite jusqu'à $N_k^{(m-1)}$ pour a non-résidu de $(m-1)^{ième}$ classe. Ici l'indice inférieur est indispensable pour marquer le nombre des inconnues.

Dans le cas de $m=2$, objet de ce numéro, quand les nombres N_i°, N_k, N_k' seront déterminés, le problème sera résolu, par la proposition suivante dont la vérité s'aperçoit immédiatement.

Le nombre de solutions de la congruence..... $y_1^2+y_2^2+\ldots y_f^2\equiv z_1^2+\ldots+z_i^2 \pmod{p=2h+1}$ *est égal à*

$$N_f^\circ N_i^\circ + h(N_f N_i + N_f' N_i').$$

Celui de la congruence $y_1^2+y_2^2+\ldots y_f^2 \equiv n(z_1^2+\ldots+z_i^2) \pmod{p=2h+1}$ où n est un non-résidu quadratique est égal à

$$N_f N_i^0 + h(N_f N_i' + N_f' N_i).$$

Ensuite pour le cas où l'on n'aurait pas $a_{k+1} = 0$, soient

P_0 le nombre de solutions de $a_1x_1^2+a_2x_2^2+\ldots+a_kx_k^2 \equiv 0 \pmod{p}$,
Π_0 le nombre de solutions de la congruence.....
$a_1x_1^2+\ldots+a_kx_k^2-a_{k+1}x^2 \equiv 0 \pmod{p}$,
Le nombre de solutions de $a_1x_2^2+\ldots+a_kx_k^2 \equiv a_{k+1} \pmod{p}$,

sera $\frac{\Pi^0-P^0}{p-1}$, comme il suit de la formule (8).

La recherche est donc ramenée à trouver le nombre de solutions de la congruence

$$x_1^2 + x_2^2 + x_3^2 + \ldots + x_k^2 \equiv a \pmod{p}.$$

Voici d'abord deux relations qui serviront à simplifier les calculs.

Théorème. *Quel que soit le module premier $p=2h+1$, on a toujours*

$$(9) \qquad N_k^0 + h(N_k + N_k') = p^k.$$

Démonstration. Cela se voit de suite en substituant dans.... $P = x_1^2+x_2^2+\ldots+x_k^2$, au lieu de $x_1, x_2, \ldots x_k$, chacun des arrangements k à k des p nombres $0, 1, 2, \ldots (p-1)$. De ces arrangements il y en aura N_k^0 qui donneront $P \equiv 0 \pmod{p}$ à un résidu quadratique déterminé, a par exemple, il en aura encore N_k qui donneront $P \equiv ay^2$, quel que soit y. Ainsi comme il y a h résidus quadratiques, il y aura hN_k arrangements qui donneront $P \equiv$ à un résidu quadratique. De même il y aura hN_k' arrangements qui donneront P congru à un non-résidu quadratique; or il faut avoir $P \equiv 0$, à un résidu ou à un non résidu quadratiques, d'ailleurs le nombre total des arrangements k à k est égal à p^k, on aura donc $N_k^0 + h(N_k + N_k') = p^k$. Ce qu'il fallait démontrer.

Théorème. *Si le module p est de forme $4q+1$, on aura*

$$(10) \quad N_i^0 = 1+(p-1)(N_{k-1}'+N_{k-2}+\ldots+N_2+N_1) = 1+(p-1)\Sigma N_{k-1},$$

et si p est de forme $4q-1$, *on aura*

$$(11)\quad N_k^\circ = 1+(p-1)(N'_{k-1}+\ldots+N'_2+N'_1)=1+(p-1)\Sigma N'_{k-1}.$$

Démonstration. En effet, dans le premier cas, on a par la formule (7) $N_k^\circ = N_{k-1}^\circ + (p-1)N_{k-1}$. Pareillement $N_{k-1}^\circ = N_{k-2}^\circ + (p-1)N_{k-2}$ et ainsi de suite jusqu'à $N_2^\circ = N_1^\circ + (p-1)N_1$: ajoutant ces équations membre à membre et remarquant que l'on a $N_1^\circ = 1$, on trouve de suite la formule (10).

La formule (11) se tire de même de l'équation

$$N_k^\circ = N_{k-1}^\circ + (p-1)N'_{k-1}.$$

Les formules (9), (10) et (11), pour le cas de la congruence

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

se changent en

$$(12)\quad N_k^\circ + h(N_k + N'_k + \ldots + N_k^{(m-1)}) = p^k,$$

$$(13)\quad N_k^\circ = 1 + (p-1)\Sigma N_{k-1} \quad \text{pour} \quad h \text{ pair},$$

$$(14)\quad N_k^\circ = 1 + (p-1)\Sigma N_{k-1}^{\left(\frac{m}{2}\right)} \quad \text{pour} \quad h \text{ impair}$$

La démonstration est absolument la même.

Si l'on voulait exclure les solutions renfermant des inconnues égales à zéro, il faudrait remplacer les équations (12), (13) et (14) par

$$(15)\quad N_k^\circ + h(N_k + N'_k + \ldots + N_k^{(m-1)}) = (p-1)^k,$$

$$(16)\quad N_k^\circ = (p-1)N_{k-1} \quad \text{pour} \quad h \text{ pair},$$

$$(17)\quad N_k^\circ = (p-1)N_{k-1}^{\left(\frac{m}{2}\right)} \quad \text{pour} \quad h \text{ impair}.$$

La démonstration est presque la même.

Venons-en aux formules générales pour le nombre de solutions de la congruence $x_1^2 + \ldots + x_k^2 \equiv a \pmod{p}$.

D'abord la congruence (3) donne immédiatement ce théorème déjà démontré par M. Libri.

Théorème. *Le nombre de solutions de la congruence*.....

$a_1x_1^2 + a_2x_2^2 \equiv a_3 \pmod{p}$ *est* $p-1$ si $-a_1a_2$ *est résidu quadratique, et* $p+1$, *si* $-a_1a_2$ *est non résidu.*

Démonstration. Mettons la congruence sous la forme..... $(a_1x_1)^2 - (-a_1a_2)x_2^2 \equiv a_1a_3 \pmod{p}$, ou $y_2^2 - ay_2^2 \equiv b \pmod{p}$: la congruence (3) devient $-S_2 \equiv a^h \pmod{p}$, ou bien $S_2 \equiv -(-a_1a_2)^h \pmod{p}$ ou $S_2 \equiv \mp 1 \pmod{p}$, selon que $-a_1a_2$ est résidu, ou non résidu quadratique. De plus, on a $S_2 < 2p$ et pair, il faut donc poser $S_2 \equiv p \mp 1$. Pour le cas de $a_1 = a_2 = 1$, $-a_1a_2 = -1$, il y a donc $p-1$ solutions, si $p = 4q+1$, et $p+1$, si $p = 4q-1$; car dans le premier cas, -1 est résidu, et dans le second, il est non résidu quadratique.

Dans le cas de $a_3 = 0$, *ou de la congruence* $a_1x_1^2 + a_2x_2^2 \equiv 0 \pmod{p}$, *il y a* $1 + 2(p-1)$ *solutions si* $-a_1a_2$ *est résidu quadratique, et seulement* 1, *si* $-a_1a^2$ *est non résidu.*

Cette proposition est un cas particulier d'une plus générale démontrée au commencement de l'article III.

Voici maintenant la proposition générale :

Théorème. *On a pour k nombre impair,*

$$(18)\qquad \begin{cases} N_k^0 = p^{k-1}, \\ N_k = p^{k-1} + (-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}} \cdot p^{\frac{k-1}{2}}, \\ N_k' = p^{k-1} - (-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}} \cdot p^{\frac{k-1}{2}}, \end{cases}$$

et pour k pair, on a

$$(19)\qquad \begin{cases} N_k^0 = p^{k-1} + (-1)^{\frac{p-1}{2}\cdot\frac{k}{2}} \cdot (p-1)\, p^{\frac{k}{2}-1}, \\ N_k = N_k' = p^{k-1} - (-1)^{\frac{p-1}{2}\cdot\frac{k}{2}} \cdot p^{\frac{k}{2}-1} \end{cases}$$

Démonstration. De la congruence $x_1^2 + x_2^2 + \ldots + x_k^2 \equiv a \pmod{p}$, nous tirerons les deux suivantes :

$$(20)\qquad \left\{ \begin{array}{l} x_1^2 + x_2^2 + \ldots + x_k^2 \equiv ax_{k+1}^2, \\ x_1^2 + \ldots\ldots + x_{k-1}^2 \equiv ax_{k+1}^2 - x_k^2, \end{array} \right\} \pmod{p},$$

qui n'en font qu'une. Nous égalerons leurs nombres de solutions; de

là nous tirerons N_k ou N'_k, d'où il sera facile de déduire N^0_k, et ensuite N'_k ou N_k.

Premier cas. $p = 4q + 1$ et a résidu quadratique. La première des congruences (20) a par la formule (7) un nombre de solutions égal à

$$N^2_k + (p - 1) N_k.$$

La deuxième des congruences (20) deviendra en posant

$$P = x_1^2 + x_2^2 + \ldots + x_{k-1}^2, \quad Q = a x_{k+1}^2 - x_k^2, \quad P \equiv Q \pmod{p}.$$

Si l'on représente par P^0, Q^0 les nombres de solutions des congruences $P \equiv 0$, $Q \equiv 0 \pmod{p}$; par P et Q les nombres de solutions des congruences $P \equiv$ à un résidu et $Q \equiv$ à un résidu, suivant le module p; et enfin par P' et Q' les nombres de solutions des congruences $P \equiv$ à un non-résidu, $Q \equiv$ à un non-résidu pour le module p, le nombre de solutions de la congruence $P \equiv Q \pmod{p}$, sera

$$P^0 Q^0 + h(PQ + P'Q');$$

mais d'après les notations convenues,

$$P_0 = N^0_{k-1}, \quad P = N_{k-1}, \quad P' = N'_{k-1},$$

et d'après les théorèmes qui donnent le nombre de solutions de $a x_1^2 - x_2^2 \equiv b \pmod{p}$.

$$Q^0 = 1 + 2(p - 1), \quad Q = p - 1, \quad Q' = p - 1,$$

car $-a \times -1 = a$ est résidu quadratique.

Le nombre de solutions de la congruence $P \equiv Q \pmod{p}$, devient donc

$$[1 + 2(p-1)] N^0_{k-1} + h[(p-1) N_{k-1} + (p-1) N'_{k-1}],$$

égalant ce nombre à $N^2_k + (p-1) N_k$ et simplifiant au moyen des équations (9) et (10), on aura, à cause de

$$\Sigma N_g = N_g + N_{g-1} + \ldots + N_2 + N_1,$$

l'équation $\Sigma N_k = p \Sigma N_{k-2} + p^{k-1} + 1$,

pareillement,

$$\Sigma N_{k-1} = p \Sigma N_{k-3} + p^{k-2} + 1,$$

d'où

$$N_k = pN_{k-2} + p^{k-1} - p^{k-2},$$

qui revient à

$$(21) \qquad N_k - p^{k-1} = p(N_{k-2} - p^{k-3}).$$

Cette équation montre que les quantités $N_1 - 1$, $N_2 - p$, $N_3 - p^2$, etc. forment une série récurrente dont l'échelle de relation est $0, p$.

Soit en général A, B l'échelle de relation d'une série récurrente : si l'on veut que $ax^n + by^n$ soit le terme de rang $n+1$, il faudra poser

$$ax^n + by^n = A(ax^{n-1} + by^{n-1}) + B(ax^{n-2} + by^{n-2}),$$

qui peut s'écrire

$$ax^{n-2}(x^2 - Ax + B) + by^{n-2}(y^2 - Ay - B) = 0,$$

à laquelle on satisfera en prenant pour x et y les racines de... $z^2 - Az - B = 0$. Puis il faudra déterminer a et b, de manière que $ax^0 + by^0$ et $ax + by$ soient respectivement égaux aux deux premiers termes. Dans le cas présent on a

$$A = 0, \quad B = p, \quad z^2 = p, \quad \text{d'où} \quad x = \sqrt{p}, \quad y = -\sqrt{p};$$

de plus,

$$N_1 - 1 = 2 - 1 = 1, \quad N_2 - p = p - 1 - p = -1.$$

Les équations qui déterminent a et b sont donc

$$a + b = 1, \quad (a - b)\sqrt{p} = -1,$$

d'où l'on tire

$$a = \frac{\sqrt{p}-1}{2\sqrt{p}}, \qquad b = \frac{\sqrt{p}+1}{2\sqrt{p}},$$

et par conséquent,

$$N_k - p^{k-1} = \frac{\sqrt{p}-1}{2\sqrt{p}}(\sqrt{p})^{k-1} + \frac{\sqrt{p}+1}{2\sqrt{p}}(-\sqrt{p})^{k-1},$$

ou bien encore,

$$(22)\quad N_k - p^{k-1} = \tfrac{1}{2}(\sqrt{p}-1)(\sqrt{p})^{k-2} - \tfrac{1}{2}(\sqrt{p}+1)(-\sqrt{p})^{k-2}.$$

Ce qui donne pour k nombre pair,

$$N_k = p^{k-1} - p^{\frac{k}{2}-1},$$

et pour k nombre impair,

$$N_k = p^{k-1} + p^{\frac{k-1}{2}}.$$

On aurait pu obtenir ces deux équations par de simples éliminations et sans recourir aux séries récurrentes, car la valeur de N_k dépend de celle de N_{k-2}, celle-ci s'obtient au moyen de N_{k-4} et ainsi de suite, jusqu'à ce qu'on parvienne à N_2 et N_1 dont les valeurs sont connues ; dans ce calcul, il faut traiter séparément le cas de k pair et celui de k impair.

Au moyen des valeurs trouvées pour N_k, l'équation

$$N_k^0 = 1 + (p-1)(N_{k-1} + N_{k-2} + \ldots + N_2 + N_1),$$

donnera pour k impair,

$$N_k^0 = p^{k-1},$$

et pour k pair,

$$N_k^0 = p^{k-1} + (p-1).p^{\frac{k}{2}-1}.$$

Deuxième cas. $P = 4q+1$ et a non-résidu.

Pour k impair l'équation $N_k^0 - h(N_k + N_k') = p^k$, donne

$$N_k + N_k' = \frac{2(p^k - p^{k-1})}{p-1} = 2p^{k-1}, \quad \text{d'où l'on tire} \quad N_k' = 2p^{k-1} - N_k,$$

ou bien

$$N_k' = p^{k-1} - p^{\frac{k-1}{2}}.$$

Pour k pair, on a

$$N_k + N_k' = 2\left[p^k - p^{k-1} - (p-1)p^{\frac{k}{2}-1}\right] : (p-1) = 2\left(p^{k-1} - p^{\frac{k}{2}-1}\right) = 2N_k',$$

d'où

$$N'_k = N_k.$$

Troisième cas. $P = 4q - 1$ et a non-résidu quadratique.

Les nombres de solutions de deux congruences (20), sont ici en vertu de $Q^0 = 1$, $Q = Q' = p + 1$, égaux respectivement à

$$N^0_k + (p-1)N'_k, \quad N^0_{k-1} + \frac{p-1}{2}[(p+1)N_{k-1} + (p+1)N'_{k-1}].$$

égalant ces deux nombres, il vient

$$\Sigma N'_k = -p\Sigma N'_{k-2} + \frac{p+1}{p-1}(p^{k-1} - 1);$$

pareillement

$$\Sigma N'_{k-1} = -p\Sigma N'_{k-3} + \frac{p+1}{p-1}(p^{k-2} - 1),$$

d'où

$$N'_k = -pN'_{k-2} + p^{k-1} + p^{k-2},$$

ce qui revient à

$$N - p^{k-1} = -p(N'_{k-2} - p^{k-3}). \tag{23}$$

Cette équation traitée comme l'équation (21) donnera

$$N'_k - p^{k-1} = \tfrac{1}{2}(\sqrt{-p}+1)(\sqrt{-p})^{k-2} + \tfrac{1}{2}(-\sqrt{-p}+1)(-\sqrt{-p})^{k-2}; \tag{24}$$

car il faut remarquer qu'on a ici $N'_1 - 1 = -1$ et $N'_2 - p = 1$, puisque $N'_1 = 0$, $N'_2 = p + 1$; de là résulte

$$a = \frac{-\sqrt{-p}+1}{2\sqrt{-p}}, \quad b = -\frac{\sqrt{-p}+1}{2\sqrt{-p}}.$$

Pour k nombre impair l'équation (24) donne

$$N'_k = p^{k-1} - (-p)^{\frac{k-1}{2}},$$

et pour k nombre pair, elle donne au contraire,

$$N'_k = p^{k-1} + (-p)^{\frac{k}{2}-1}$$

On pouvait obtenir ces valeurs de N'_k par de simples éliminations.

L'équation $N^0_k = 1 + (p-1)\Sigma N'_{k-1}$ donnera, comme plus haut, pour k impair,

$$N^0_k = p^{k-1},$$

et pour k pair,

$$N^0_k = p^{k-1} - (p-1)p^{\frac{k}{2}-1}.$$

Quatrième cas. $p = 4q - 1$ et a résidu quadratique. L'équation $N_k + \frac{p-1}{2}(N_k + N'_k) = p^k$ donne encore pour k impair $N_k + N'_k = 2p^{k-1}$, d'où $N_k = p^{k-1} + (-p)^{\frac{k-1}{2}}$, et pour k pair $N_k + N'_k = 2N_k$, d'où $N'_k = N_k$.

Si l'on remarque maintenant que l'on a $(-1)^{\frac{p-1}{2}} = +1$ pour... $p = 4q + 1$ et $(-1)^{\frac{p-1}{2}} = -1$ pour $p = 4q - 1$, on aura les résultats de l'énoncé.

Les formules (22) et (24) se déduisent avec la plus grande facilité d'une formule très générale et très remarquable donnée par M. Libri, dans son mémoire sur la *Théorie des Nombres*. nous reviendrons plus loin sur cette formule.

VI.

Nombre de solutions de la congruence.....

$$a_1x_1^3 + a_2x_2^3 \equiv a_3 \pmod{p = 3h+1}.$$

1°. Si $a_3 = 0$, il y aura, comme on l'a vu, 1 ou $1 + 3(p-1)$ solutions selon que $-a_2a_1^2$ sera résidu ou non résidu cubique (111).

2°. Dans le cas général, nous ramènerons la congruence précédente à la forme $y_1^3 - ay_2^3 \equiv b \pmod{p = 3h+1}$. Ici, en posant

$$\frac{2h\ (2h-1)\ (2h-2)\ldots(h+1)}{1\ .\ 2\qquad\qquad 3\ .\ .\ .\ .\ .\ h} = Q,$$

la congruence (3) donnera

$$(25) \qquad -S_s \equiv a^h + a^{2h} + Qa^h b^h \pmod{p = 3h+1}.$$

Comme h est pair, on voit que les signes de a et b venant a changer, S_s n'en conservera pas moins la même valeur. Comme a^h et b^h, selon les valeurs particulières de a et de b, peuvent prendre trois valeurs, qui sont les racines de la congruence $z^3 \equiv 1 \pmod{p}$, savoir 1, r, et r^2 en représentant par r une racine primitive de $z^3 \equiv 1 \pmod{p}$, ou ce qui est la même chose dans le cas présent, où il y a deux racines primitives, une des racines de $z^2 + z + 1 \equiv 0 \pmod{p}$, ou encore de $(2z+1)^2 \equiv -3 \pmod{p}$. On voit de suite que la congruence $y_1^3 - ay_2^3 \equiv b \pmod{p}$ peut présenter neuf cas correspondants aux neuf combinaisons des trois valeurs de a^h et des trois valeurs de b^h. Soit donc un a non-résidu cubique de première classe, nous aurons les neuf congruences suivantes à côté desquelles sont inscrits les nombres de solutions, représentés par les lettres A, B, C, différemment accentuées.

$y_1^3 - y_2^3 \equiv 1 \pmod{p}$	A sol.	$y_1^3 - ay_2^3 \equiv \pmod{p}$	A′ sol.	$y_1^3 = a^2 y_2^3 \equiv 1 \pmod{p}$	A″ sol.
$y_1^3 - y_2^3 \equiv a$	B	$y_1^3 - ay_2^3 \equiv a$	B′	$y_1^3 - a^2 y_2^3 \equiv a$	B″
$y_1^3 - y_2^3 \equiv a^2$	C	$y_1^3 - ay_2^3 \equiv a^2$	C′	$y_1^3 - a^2 y_2^3 \equiv a^2$	C″

Si l'on substitue dans la congruence (25) les valeurs de a^h et a^{2h}, qui sont r et r^2, on obtiendra, au moyen de la relation $1 + r + r^2 \equiv 0 \pmod{p}$, les congruences

$$\begin{aligned} &A \equiv -2 - Q, \quad A' \equiv 1 - Qr, \quad A'' \equiv 1 - Qr^2 \pmod{p}, \\ &B \equiv -2 - Qr, \quad B' \equiv 1 - Qr^2, \quad B'' \equiv 1 - Q, \\ &C \equiv -2 - Qr^2, \quad C' \equiv 1 - Q, \quad C'' \equiv 1 - Qr, \end{aligned}$$

d'où l'on déduira facilement les congruences

$$(26) \qquad \begin{aligned} &A + 3 = C' = B'' \equiv 1 - Q \pmod{p = 3h+1}, \\ &B + 3 = A' = C'' \equiv 1 - Qr, \\ &C + 3 = B' = A'' \equiv 1 - Qr^2. \end{aligned}$$

Par exemple, la congruence (25) donnant $A + 3 \equiv 1 - Q \pmod{p}$ et $C' \equiv 1 - Q \pmod{p}$, comme A et C′ sont moindres que $3p$ et que $A + 3$ et C′ sont divisibles par 3, il en résultera que la différence

$A+3-C'$ sera divisible par $3p$, d'où suit nécessairement $A+3=C'$, et ainsi des autres congruences.

Les congruences (26) donneront immédiatement A, B, C, A', B', C', A'', B'', C'', quand on aura déterminé Q et r. Pour déterminer r on a la congruence $(2r+1)^2 \equiv -3 \pmod{p}$

$$\text{ou } r \equiv \frac{-1 \pm \sqrt{-3}}{2} \pmod{p}.$$

Nous donnerons plus bas la manière de calculer presque à la fois r et Q, ou plutôt le reste de Q divisé par p.

Les congruences (26) donnent par addition

$$9+A+B+C=A'+B'+C'=A''+B''+C'' \equiv 3 \pmod{p},$$

ce qui résulte encore de l'équation

$$9+A+B+C=A'+B'+C'=A''+B''+C''=3(p+1),$$

qui est une conséquence immédiate des équations

$$\begin{aligned} 1+3(p-1)+h(A+B+C) &= p^2, \\ 1+h(A'+B'+C') &= p^2, \\ 1+h(A''+B''+C'') &= p^2, \end{aligned}$$

qui se prouvent précisément comme l'équation

$$N_2^2+h(N_0+N_2'+N_2'')=p^2.$$

On a donc entre A', B', C' la relation

$$A'+B'+C'=3(p+1). \tag{27}$$

Les deux autres équations qui donneraient $A+B+C$ et $A''+B''+C''$, résulteraient de (26) et de (27); de sorte qu'il est inutile de les écrire.

On peut trouver entre A', B', C' une autre relation qui conduira à la valeur du reste de Q divisé par p; mais pour les cas particuliers où p sera un petit nombre, il sera plus court de calculer le reste de Q au moyen de la formule $Q=\frac{2h.(2h-1)\ldots(h+1)}{1.2\ldots\ldots h.}$.

Soit la congruence $x_1^3-ax_2^3 \equiv y_1^3-a^2y_2^3 \pmod{p}$ où a est un

non-résidu cubique de première classe, la formule (6) donnera pour le nombre de ses solutions

$$1 + h(A'A'' + B'B'' + C'C''),$$

ou d'après les équations (26),

$$1 + h(A'B' + B'C' + A'C').$$

Mais si l'on écrit la congruence précédente sous la forme $x_1^3 - y_1^3 \equiv a(x_2^3 - ay_2^3) \pmod{p}$, la formule (6) donnera pour le nombre de ses solutions

$$1 + 3(p-1) + h(AC' + BA' + CB'),$$

nombre qui, par le moyen des équations (26), devient

$$1 + 3(p-1) + h(A'^2 + B'^2 + C'^2) - (p-1)(A' + B' + C');$$

égalant ces deux valeurs du même nombre, on a

$$A'B' + A'C' + B'C' = A'^2 + B'^2 + C'^2 - 3(A' + B' + C') + 9,$$

d'où, en simplifiant au moyen de l'équation (27), on tire

$$A'B' + A'C' + B'C' = 3(p^2 + p + 1).$$

Si l'on pose $A' - B' = 9u$, u sera nécessairement entier, et à cause de $A' + B' = 3(p+1) - C'$, on aura

$$A' = \tfrac{1}{2}[3(p+1) - C' + 9u], \quad B' = \tfrac{1}{2}[3(p+1) - C' - 9u].$$

Substituant dans $A'B' + A'C' + B'C'$, on trouvera, réduction faite,

$$(28) \qquad (C' - p - 1)^2 + 27u^2 = 4p.$$

Soit $4^2 + 27M^2 = 4p$, où L et M sont positifs, cette équation n'aura

qu'une solution (*); au moyen d'une table de carrés, il sera très facile de déterminer L et M par voie d'exclusion. Ce calcul fait, on posera

$$C' - p - 1 = \pm L \text{ et } u = \pm M, \text{ d'où } A' - B' = \pm 9M.$$

La première équation donne $C' = p + 1 \pm L$; et comme C' doit être divisible par 3, le signe de L sera déterminé, il faudra poser $\pm L = 3l + 1 = 3\lambda - 2$; en donnant à l et λ le signe convenable, il en résultera $C' = 3(h + \lambda)$, et parconséquent

$$(29) \quad \begin{aligned} A + 3 &= C' = B'' = 3(h + \lambda), \\ B + 3 &= A' = C'' = 3\left(h + 1 - \frac{\lambda \mp 3M}{2}\right), \\ C + 3 &= B' = A'' = 3\left(h + 1 - \frac{\lambda \pm 3M}{2}\right). \end{aligned}$$

Si l'on compare la première de ces équations avec la première des congruences (26), il en résultera $1 - Q \equiv 3(h + \lambda) \equiv 3h + 2 \pm L \pmod{p}$, ou bien $-Q \equiv \mp L \pmod{p}$: on a donc ce théorème qui est dû à M. Jacobi.

THÉOREME. *Le coefficient* $-\frac{2h.(2h-1)...(h+1)}{1.\ 2.....h}$ *étant divisé par p donne un reste* $\left(< \frac{p}{2}\right)$ *toujours égal à* L *sous la relation....* $L^2 + 27M = 4p$, *en prenant* L, *positif ou négatif, de la forme* $3l + 1$.

(J. de M. Crelle, tome 2. *De residuis cubicis commentatio numerosa*).

Quant au signe de M, il reste nécessairement ambigu dans les équa-

---

(*) Voici comment le prouve M. Gauss. Soit s'il est possible une nouvelle solution $L'^2 + 27M'^2 = 4p$, on obtiendrait

1°. $(LL' - 27\ MM')^2 + 27(LM' + L'M) = 16\ p^2$.
2°. $(LL' + 27\ MM') + 27(LM' - L'M) = 16p^2$.
3°. $(LM' + L'M)\ (LM' - L'M) = 4p^2\ (M'^2 - M^2)$.

La 3e équation montre que le nombre premier p, divise un des nombres $LM' + L'M$, $LM' - LM'$, tandis que la première et la deuxième font voir que chacun de ces nombres est moindre que p. Donc, etc

tions (29), parce qu'il dépend de la valeur de r, racine primitive de $z^3 \equiv 1 \pmod{p}$, et que cette congruence a deux racines primitives $\frac{-1 \pm \sqrt{-3}}{2} \pmod{p}$. L'équation $A' - B' = \pm 9M$ revient à

$-(2r+1)Q \equiv \pm 9M \pmod{p}$ qui se réduit à $L^2 + 27M^2 \equiv 0 \pmod{p}$.

Cette dernière congruence, qui se tire immédiatement de l'équation $L^2 + 27M^2 = 4p$, donnera très facilement la valeur de p, car on en tire $L \equiv 3M\sqrt{-3} \pmod{p}$, ou, si l'on veut, $9M \equiv L\sqrt{-3} \pmod{p}$. Cette dernière congruence revient à $-(2r+1)Q \equiv \pm 9M \pmod{p}$.

Les valeurs de A, B, C, A', B', C', A'', B'', C'', pourraient conduire à des formules générales pour le cas d'un nombre quelconque d'inconnues, et l'on obtiendrait encore, pour le cas principal, des séries récurrentes dont l'échelle de relation aurait trois termes; mais les calculs seraient assez longs. Nous donnerons plus loin la formule de M. Libri, qui ne présente point cet inconvénient, et qui deviendra très facilement applicable au moyen des propositions précédentes.

VII.

Nombre de solutions de la congruence.....

$$a_1 x^4 + a_2 x_2^4 \equiv a_3 \pmod{p = 4h+1}.$$

Nous traiterons ici le cas de la congruence $y_1^4 - a y_2^4 \equiv b \pmod{p}$, auquel les autres se ramènent. Les formules générales seront données à la fin du paragraphe.

Le nombre S_2 des solutions de la congruence précédente est déterminé complétement par la congruence (3), qui devient ici

$$-S_2 \equiv a^h + \left(a^{2h} + \frac{A}{A_1} b^h a^h\right) + a^{3h} + \frac{A_2}{A_1} a^{2h} b^h + \frac{A_2}{A} a^h b^{2h} \pmod{p}.$$

Or, $A_3 \equiv (-1)^h A_2 \pmod{p}$, on aura donc pour h pair, et en posant

$$\frac{2h(2h-1)\ldots(h+1)}{1.2\ldots\ldots h} = Q,$$

$$(30) \quad -S_2 \equiv a^h + a^{2h} + a^{3h} + Q a^h b^h (1 + a^h + b^h) \pmod{p},$$

et pour h impair

$$(31)\quad -S_2 \equiv a^h + a^{2h} + a^{3h} + Qa^h b^h (1 - a^h - b^h) \pmod{p}.$$

Les valeurs de a^h, b^h, et de leurs puissances, quelles que soient les valeurs de a et b, sont les racines de la congruence $z^4 \equiv 1 \pmod{p}$, savoir, 1, r, r^2, r^3, en représentant par r une racine primitive de la congruence $z^4 \equiv 1 \pmod{p}$, ou, ce qui est la même chose dans le cas présent, où il y a deux racines primitives, r satisfait à la congruence $z^2 + 1 \equiv 0 \pmod{p}$.

Ainsi la suite 1, r, r^2, r^3 pourra être remplacée par 1, r, -1, $-r$.

Quand on connaîtra r et le reste de Q divisé par p, on pourra employer les formules (30) et (31); mais comme le calcul direct du reste de Q est fort long, et même impraticable quand p est un grand nombre, nous démontrerons plus loin un théorème de M. Gauss, qui déterminera très expéditivement le reste de Q, au moyen de l'équation $L^2 + 4M^2 = p$, qui donnera aussi la racine primitive r.

Premier cas. $h = 2h'$, $p = 8h' + 1$.

Si l'on représente par a un non-résidu biquadratique de première classe, la congruence $y_1^4 - ay_2^4 \equiv b \pmod{p}$ sera susceptible de seize formes, dont nous écrirons le tableau avec les nombres correspondants de solutions, représentés par les lettres A, B, C, D, différemment accentuées.

$$\left.\begin{array}{l} y_1^4 - y_2^4 \equiv 1,\ \mathrm{A};\ y_1^4 - ay_2^4 \equiv 1,\ \mathrm{A}';\ y_1^4 - a^2 y_2^4 \equiv 1,\ \mathrm{A}'';\\ \qquad\qquad y_1^4 - a^3 y_2^4 \equiv 1,\ \mathrm{A}'''.\\ y_1^4 - y_2^4 \equiv a,\ \mathrm{B};\ y_1^4 - ay_2^4 \equiv a,\ \mathrm{B}';\ y_1^4 - a^2 y_2^4 \equiv a,\ \mathrm{B}'';\\ \qquad\qquad y_1^4 - a^3 y_2^4 \equiv a,\ \mathrm{B}'''.\\ y_1^4 - y_2^4 \equiv a^2,\ \mathrm{C};\ y_1^4 - ay_2^4 \equiv a^2,\ \mathrm{C}';\ y_1^4 - a^2 y_2^4 \equiv a^2,\ \mathrm{C}'';\\ \qquad\qquad y_1^4 - a^3 y_2^4 \equiv a^2,\ \mathrm{C}'''.\\ y_1^4 - y^4 \equiv a^3,\ \mathrm{D};\ y_1^4 - ay_2^4 \equiv a^3,\mathrm{D}';\ y_1^2 - a^2 y_1^4 \equiv a^3,\ \mathrm{D}'';\\ \qquad\qquad y_2^4 - a^3 y_2^4 \equiv a^3,\mathrm{D}'''. \end{array}\right\} (\mathrm{mod.}\ p = 4h + 1)$$

Substituant dans la formule (30) les valeurs de a^h, a^{2h}, a^{3h}, on aura, réductions faites,

$$\left.\begin{array}{llll} A\equiv -3-3Q, & A'\equiv 1-(2r-1)Q, & A''\equiv 1+Q, & \\ & A'''\equiv 1+(2r+1)Q, & & \\ B\equiv -3-(2r-1)Q, & B'\equiv 1+(2r+1)Q, & B''\equiv 1-Q, & \\ & B'''\equiv 1-Q, & & \\ C\equiv -3+Q, & C'\equiv 1-Q, & C''\equiv 1+Q, & \\ & C'''\equiv 1-Q, & & \\ D\equiv -3+(2r+1)Q, & D'\equiv 1-Q, & D''\equiv 1+Q, & \\ & D'''\equiv 1-(2r-1)Q, & & \end{array}\right\} (\text{mod. } p=4h+1)$$

d'où l'on tirera très facilement

$$(32)\quad \left.\begin{array}{l} A+4\equiv 1-3Q, \\ B+4=A'=D'''\equiv 1-(2r-1)Q, \\ C+4=A''=C'\equiv 1+Q, \\ D+4=B'=A'''\equiv 1+(2r+1)Q, \\ C'=D'=B''=D''=B'''=C'''\equiv 1-Q. \end{array}\right\} (\text{mod. } p=4h+1).$$

On trouve encore les équations

$$16+A+B+C+D=A'+B'+C'+D'=A''+B''+C''+D''$$
$$=A'''+B'''+C'''+D'''=4(p+1),$$

qui se prouvent tout-à-fait de même que l'équation

$$N_1^2+h(N_1+N_1'+N_1''+N_1''')=p^2.$$

On aura donc, au moyen des équations (32), les nouvelles équations

$$(33)\quad \begin{array}{l} A+B+C+D=4(p-3), \\ B+D+2B''=4(p-1), \\ C+B''=2(p-1). \end{array}$$

Les deux dernières conduisent à $B+D=2C$.

Si l'on pose $C-B''=16u$, $B-D=16v$, il s'ensuivra que u et v seront entiers, et les équations (33) donneront

$$B''=p-1-8u,\quad B=p-1+8u+8v,\quad A=p-9-24u,$$
$$C=p-1+8u,\quad D=p-1+8u-8v.$$

Or, il existe entre u et v une équation indéterminée qui les fait con-

naître sans ambiguité (sauf celle du signe), par la raison qu'elle n'a qu'une solution; c'est l'équation

$$p = (1 + 4u)^2 + 4v^2, \tag{34}$$

que l'on obtient de la manière suivante :

Le nombre a étant un non-résidu biquadratique de première classe, la congruence $x_1^4 - a^2x_2^4 \equiv a(y_1^4 - ay_2^4) \pmod{p}$ a, d'après la formule (6) et les relations précédentes, un nombre de solutions représenté par

$$1 + h(A''D' + B''A' + C''B' + D''C').$$

La même congruence, mise sous la forme $x_1^4 - ay_1^4 = a^2(x_2^4 - y_2^4)$, a pour nombre de solutions

$$1 + 16h + h(A'C + B'D + C'A + D'B);$$

égalant ces deux valeurs du même nombre, on trouve

$$B''(B'' + C - A + 8) = D^2 + C(B - D),$$

qui se réduit, par la substitution des valeurs de A, B, C, D, B'', à l'équation (34).

On prouvera, comme dans l'article précédent, que l'équation $L^2 + 4M^2 = p$ n'a qu'une seule solution en nombres positifs, et en déterminant convenablement le signe de L, on pourra faire $1 + 4u = \pm L$. D'ailleurs on a $C - B'' = 16u \equiv 2Q - 4 \pmod{p}$, ou $8u \equiv Q - 2 \pmod{p}$. Par conséquent l'on aura $Q \equiv \pm 2L \pmod{p = 8h' + 1}$. Comme L est moindre que $\frac{1}{2}p$, on pourra poser

$$\tfrac{1}{2}Q \equiv \pm L \pmod{p}.$$

De là ce théorème de M Gauss :

« *La quantité* $\frac{1}{2}\frac{2h.(2h-1)\ldots(h+1)}{1.2\ldots\ldots h} \pmod{p}$ *est toujours égale à* » $\pm L \left(< \frac{p}{2}\right)$, *en prenant* $p = L^2 + 4M^2$ *et* $\pm L = 1 + 4u$. »

Quant au signe de v il dépend de r, qui se détermine par $2M \equiv L\sqrt{-1} \equiv Lr \pmod{p}$, congruence qui revient à $B - D = 16v$, ou du moins qui s'en déduit.

Les quantités A, B, C, D, etc., étant déterminées par ce qui précède, on calculera, par le moyen de la formule (6), le nombre de solutions pour toute autre congruence contenant plus de deux inconnues. Voici un seul exemple qui suffira pour que l'on puisse appliquer dans tous les cas la formule générale qui sera donnée plus loin.

Pour trouver le nombre de solutions de la congruence

$$x_1^4 + x_2^4 + x_3^4 + 1 \equiv 0 \pmod{p = 4h + 1}:$$

Si l'on représente par Π^o et P^o les nombres de solutions des congruences $\Pi = x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0$ et $P = x_1^4 + x_2^4 + x_3^4 \equiv 0 \pmod{p}$, la formule (8) donnera pour le nombre cherché $\frac{\Pi^o - P^o}{p-1}$.

Or $x_1^4 + x_2^4 + x_3^4 \equiv 0 \pmod{p = 8h' + 1}$, revenant à $x_1^4 + x_2^4 \equiv y_1^4 \pmod{p}$, on aura

$$P^o = 1.[1 + 4(p-1)] + h.4.A = 1 + 4(p-1) + (p-1)A.$$

Quant à la valeur de Π^o, en mettant $x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0 \pmod{p}$ sous la forme $x_1^4 + x_2^4 \equiv y_1^4 + y_2^4 \pmod{p}$, ce sera

$$[1 + 4(p-1)]^2 + \frac{p-1}{4}(A^2 + B^2 + C^2 + D^2).$$

Le nombre cherché est donc

$$4[1 + 4(p-1)] + \frac{A^2+B^2+C^2+D^2}{4} - A = p^3 + 17p + 10 + 56u + 64u^2,$$

par la substitution des valeurs de A, B, C, D.

Les congruences (32) montrent de suite que ce nombre est indépendant de la racine primitive r.

Deuxième cas. $h = 2h' + 1$, $p = 8h' + 5$.

Dans ce cas la formule (31) donne

$$\left.\begin{array}{llll} A \equiv -3+Q, & A' \equiv 1-Q, & A'' \equiv 1+Q, & A''' \equiv 1-Q, \\ B \equiv -3-Q, & B' \equiv 1-(2r-1)Q, & B'' \equiv 1+(2r+1)Q, & B''' \equiv 1-Q, \\ C \equiv -3+Q, & C' \equiv 1+(2r+1)Q, & C'' \equiv 1-3Q, & C''' \equiv 1-(2r-1)Q, \\ D \equiv -3-Q, & D' \equiv 1-Q, & D'' \equiv 1-(2r-1)Q, & D''' \equiv 1+(2r+1)Q. \end{array}\right\} \pmod{p}$$

d'où l'on tire

$$(35)\quad \left.\begin{array}{l} A+4=C+4=A''\equiv 1+Q,\\ B+4=D+4=A'=D'=A'''=D'''\equiv 1-Q,\\ B'=D''=C'''\equiv 1-(2r-1)Q,\\ C'=B''=D'''\equiv 1+(2r+1)Q,\\ C''\equiv 1-3Q. \end{array}\right\}\ (\text{mod. } p=8h'+5).$$

On a de plus les équations

$$(36)\quad \begin{array}{r} A''+B''+C''+D''=4(p+1),\\ B''+D''+2B'''=4(p+1),\\ A''+B'''=Q(p+1), \end{array}$$

qui donnent les deux suivantes:

$$A''+C''=2B''',\quad B''+D''=2A''.$$

Si l'on pose $A''-B'''=4u$, $D''-B''=16v$, on aura, comme il est facile de le voir, u et v entiers, et de plus

$$B'''=p+1-2u,\quad B''=p+1+2u-8v,\quad C''=p+1-6u,$$
$$A''=p+1+2u,\quad D''=p+1+2u+8v.$$

Si l'on cherche, par le moyen de la formule (6), les nombres de solutions des congruences

$$x_1^4-ax_1^4\equiv y_1^4-ay_2^4,\quad x_1^4-y_1^4\equiv a(x_2^4-y_2^4)\ (\text{mod. } p=8h'+5),$$

qui reviennent à la même, et où le nombre a est un non-résidu biquadratique de première classe, on trouvera, en égalant ces nombres,

$$1+h(A'^4+B'^4+C'^4+D'^4)=(1+16h)^2+h(AB+BC+CD+DA),$$

ou, réductions faites,

$$(37)\quad p=u^2+4v^2.$$

Donc si l'on pose $p=L^2+4M^2$, L et M étant positifs, il faudra faire

$u = \pm L$, en choisissant le signe de sorte que $A'' = p + 1 \pm 2L$. devienne multiple de 8. Il faut, pour cela, prendre $\pm L = 1 + 4u'$. On a encore ici $A'' - B''' = 4u \equiv 2Q \pmod{p}$, et par suite $\frac{1}{2} Q \equiv L \pmod{p}$, comme dans le premier cas.

Pour donner un exemple de l'application des formules (6) et (8), nous chercherons le nombre de solutions de la congruence $x_1^4 + x_2^4 \ldots + x_3^4 + 1 \equiv 0 \pmod{p = 8h' + 5}$, nombre qu'il est nécessaire d'obtenir pour pouvoir employer dans tous les cas la formule générale qui sera démontrée plus bas. Nous représenterons par Π la fonction $x_1^4 + x_2^4 + x_3^4 + x_4^4$, et par P la fonction $x_1^4 + x_2^4 + x_3^4$.

Le nombre cherché sera, d'après la formule (8), $\frac{\Pi^0 - P_0}{p-1}$.

Si l'on écrit la congruence $\Pi \equiv 0 \pmod{p}$ sous la forme $x_1^4 - (-1)x_2^4 \ldots \equiv (-1)[x_3^4 - (-1)x_4^4] \pmod{p}$, qui rentre dans la forme $x_1^4 - a^4 x_2^4 \ldots \equiv a^4(x_3^4 - a^4 x_4^4) \pmod{p}$, on aura, pour le nombre de solutions,

$$\Pi^0 = 1 + h(A''C'' + B''D'' + C''A'' + D''B'').$$

Quant à la congruence $P \equiv 0$, ou $x_1^4 + x_2^4 \equiv -x_3^4 \pmod{p}$, elle a pour nombre de solutions $P^0 = 1 + 4h\,C''$.

Le nombre de solutions cherché sera donc

$$\frac{A''C'' + B''D''}{2} - C'' = p^3 - 7p + 10 + 56u + 64u^2,$$

par la substitution des valeurs de A'', B'', C'', D''.

Nous ferons observer, en terminant ici ces applications, que nous pourrons reprendre dans un autre mémoire pour le cas de $m = 5$, que pour ce cas et celui de $m = 6$, c'est-à-dire pour $p = 5h + 1$ et $p = 6h + 1$, les formules qui donnent les nombres de solutions des congruences $ax^5 + by^5 \ldots + ku^5 \equiv l \pmod{p = 5h + 1}$, $\ldots\ldots$ $ax^6 + by^6 + \ldots + ku^6 \equiv l \pmod{p = 6h + 1}$, renfermeraient les deux coefficients binomiaux

$$\frac{2h.(2h-1)\ldots(h+1)}{1.2\ldots h}, \quad \frac{3h.(3h-1)\ldots 2h}{1.2\ldots h};$$

et comme leur détermination directe serait fort longue, et souvent

même impraticable, on ferait dépendre leur détermination de la résolution de certaines équations indéterminées. Pareillement, pour $p=7h+1, \ldots p=8h+1$, les formules contiendraient les trois coefficients binomiaux

$$\frac{2h(2h-1)\ldots(h+1)}{1.\ 2\ldots\ldots h}, \quad \frac{3h.(3h-1)\ldots(2h+1)}{1.\ 2\ldots\ldots h}, \quad \frac{4h.(4h-1)\ldots(3h+1)}{1.\ 2\ldots\ldots h},$$

et ainsi de suite.

Il se présente donc ici un problème important à résoudre, et dont voici l'énoncé :

« *Soient* $p=mh+1$ et $A_1=1.2\ldots h$, $A_2=(h+1)(h+2)\ldots 2h$, $A_3=(2h+1)(2h+2)\ldots\ldots 3h, \ldots\ldots A_{mh}=(m-1)(h+1)\ldots mh$; *on demande les valeurs de* $\frac{A_2}{A_1}$, $\frac{A_3}{A_1}$, $\ldots\ldots \frac{A_n}{A_1}$ (mod. p), n *étant* $\frac{m}{2}$ *ou l'entier immédiatement supérieur; ou, s'il est possible, les valeurs de* $A_1, A_2\ldots\ldots A_n$ (mod. p), *c'est-à-dire les restes de ces quantités divisées par p nombre premier.* »

Ce problème a été résolu dans quelques cas particuliers; la solution générale serait fort utile pour la détermination des équations auxiliaires qui servent à l'abaissement de l'équation $x^p=1$; c'est ce qu'on verra dans l'article suivant; et elle ne serait pas moins utile pour l'établissement des lois de réciprocité dans la théorie des résidus de puissances, ainsi qu'on le montrera dans un autre paragraphe.

VIII.

Nombre de solutions de la congruence $A_0+A_1x_1^m+A_2x_2^m+\ldots\ldots+A_k^m x_k^m\equiv 0$ (mod. $p=hm+1$).

Pour trouver le nombre de solutions d'une congruence $\varphi(x_1, x_2\ldots x_k)\equiv 0$ (mod. p) déterminé ainsi qu'il a été dit dans l'article premier, il suffit de chercher une fonction $\downarrow(x_1, x_2\ldots, x_k)$ qui se réduise à l'unité pour toute solution $x_1=\alpha_1$, $x_2=\alpha_2\ldots$, $x_k=\alpha_k$, et qui se réduise à zéro pour toute substitution $x_1=\theta_1$, $x_2=\theta_2\ldots x_k=\theta_k$, qui ne satisfait pas à la congruence $\varphi(x_1, x_2\ldots, x_k)\equiv 0$ (mod. p) la somme des valeurs de $\downarrow(x_1, x_2\ldots\ldots x_k)$ formées en mettant suc-

cessivement, au lieu de $x_1, x_2 \ldots, x_k$, les p^k arrangements k à k des nombres 0, 1, 2... $p-1$, sera le nombre des solutions que nous représenterons par S_k.

Pour le cas de p nombre premier, en représentant par R une racine imaginaire quelconque de l'équation $x^p = 1$, on sait que $\frac{1}{p}(1+R^i+R^{2i}+R^{3i}+\ldots+R^{(p-1)i})$ devient 1 ou 0, selon que le nombre entier i est divisible ou non divisible par p.

On peut donc poser

$$\psi_\cdot = \frac{1}{p}(1+R^{\varphi\cdot}+R^{2\varphi\cdot}+\ldots+R^{(p-1)\varphi\cdot}).$$

Pour abréger, on a écrit $\psi_\cdot$ et $\varphi_\cdot$ au lieu de $\psi(x_1, x_2\ldots, x_k)$.. $\varphi(x_1, x_2\ldots, x_k)$. De là résulte

$$S_k = \frac{1}{p}\Sigma(1+R^{\varphi\cdot}+R^{2\varphi\cdot}+\ldots R^{(p-1)\varphi\cdot}), \tag{38}$$

la somme étant prise, par rapport à x_1, depuis $x_1=0$ inclusivement jusqu'à $x_1=p$ (exclusivement); par rapport à x_2, depuis $x_2=0$ jusqu'à $x_2=p$, et ainsi des autres.

Pour calculer plus facilement cette somme, représentons par ρ une racine primitive de p ou de $x^{p-1}-1\equiv 0 \pmod{p=hm+1}$, et posons

$$\begin{aligned}
\gamma_0 &= R^{\rho^0}+R^{\rho^m}+R^{\rho^{2m}}+\ldots\ldots+R^{\rho^{(h-1)m}},\\
\gamma_1 &= R^{\rho^1}+R^{\rho^{m+1}}+R^{\rho^{2m+1}}+\ldots\ldots+R^{\rho^{(h-1)m+1}},\\
\gamma_2 &= R^{\rho^2}+R^{\rho^{m+2}}+R^{\rho^{2m+2}}+\ldots+R^{\rho^{(h-1)m+2}},\\
&\vdots\\
\gamma_\alpha &= R^{\rho^\alpha}+R^{\rho^{m+\alpha}}+R^{\rho^{2m+\alpha}}+\ldots+R^{\rho^{(h-1)m+\alpha}},\\
&\vdots\\
\gamma_{m-1} &= R^{\rho^{m-1}}+R^{\rho^{2m-1}}+R^{\rho^{3m-1}}+\ldots+R^{\rho^{hm-1}}
\end{aligned}$$

Ces m quantités seront nécessairement les racines d'une équation du

degré m, puisque si l'on remplace la racine R par une autre racine imaginaire, telle que R^{f^s}, la suite $\gamma_0, \gamma_1 \ldots \gamma_{m-1}$ deviendra $\gamma_s, \gamma_{s+1}, \gamma_{s+2} \ldots, \gamma_{s-1}$, qui n'en diffère que par l'ordre des termes.

Appliquons la formule (38) à la congruence

$$A_0 + A_1 x_1^m + A_2 x_2^m + \ldots + A_k x_k^m \equiv 0 \text{ (mod. } p = hm + 1),$$

ou plutôt à la congruence

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

puisque tout nombre entier est congru à une certaine puissance de la racine primitive ρ.

On voit de suite que la formule (38) donne

$$\rho S_k = p^k + \Sigma R^{\varphi} + \Sigma R^{2\varphi} + \ldots + \Sigma R^{(p-1)\varphi}.$$

Cherchons donc la valeur de $\Sigma R^{i\varphi}$, ou plutôt, en prenant pour le nombre entier positif i la puissance ρ^s qui lui est congrue suivant le module p, cherchons la valeur de $\Sigma R^{\rho^s \varphi}$. Mettant pour φ. sa valeur, on trouve immédiatement

$$\Sigma R^{\rho^s \varphi} = R^{\rho^{s+a}} \Sigma R^{\rho^{b+s} x_1^m} \Sigma R^{\rho^{c+s} x_2^m} \ldots \ldots \Sigma R^{\rho^{g+s} x_k^m},$$

chaque somme étant prise, comme on l'a dit, depuis zéro jusqu'à p.

Or, si l'on met pour x, les nombres 1, 2, 3, 4 ... $p-1$, ou $\rho, \rho^2 \ldots \rho^{p-1}$, x_1^m donne, à l'ordre près, les termes ρ^m, $\rho^{2m} \ldots \rho^{hm}$, pris chacun m fois.

Soit en effet $x_1 \equiv \rho^{ih+f} \text{ (mod. } p = hm + 1)$, i et f étant tous deux moindres que m, il en résultera $x_1^m \equiv \rho^{ihm+fm} \equiv \rho^{fm} \text{ (mod. } p)$; or i peut prendre m valeurs 0, 1, 2 ..., $m-1$; le terme ρ^{fm} se trouve donc répété m fois, et il en c t de même de ρ^m, ρ^{2m}, etc.

Ayant donc égard à la valeur $x_1 = 0$, on trouvera $\Sigma R^{\rho^s x_1^m} = \ldots\ldots$ $1 + m\gamma_s$, et par suite

$$\Sigma R^{\rho^s \varphi} = R^{\rho^{s+a}} (1 + m\gamma_{b+s})(1 + m\gamma_{c+s}) \ldots (1 + m\gamma_{g+s});$$

faisant successivement $n=0, 1, 2 \ldots p-2$, et ajoutant toutes les valeurs de $\Sigma R^{(n)\theta}$, on trouve

$$(39)\quad \begin{aligned} pS_k = p^k &+ \gamma_a(1+m\gamma_a)(1+m\gamma_b)(1+m\gamma_c)\ldots(1+m\gamma_g) \\ &\gamma_{a+1}(1+m\gamma_{a+1})(1+m\gamma_{b+1})(1+m\gamma_{c+1})\ldots(1+m\gamma_{g+1}), \\ &\vdots \\ &\gamma_{a+m-1}(1+m\gamma_{a+m-1})(1+m\gamma_{b+m-1})(1+m\gamma_{c+m-1})\ldots \\ &\quad (1+m\gamma_{g+m-1}), \end{aligned}$$

où il faut ôter m des indices qui surpassent ce nombre.

Examinons quelques cas particuliers.

Soit d'abord $1+x_1^m+x_2^m+\ldots+x_k^m \equiv 0 \pmod{p=hm+1}$, il faudra faire $a=b=c\ldots=g=0$. Si nous représentons le nombre de solutions par N_k, il viendra

$$(40)\quad pN_k = p^k + \gamma_0(1+m\gamma_0)^k + \gamma_1(1+m\gamma_1)^k + \ldots + \gamma_{m-1}(1+m\gamma_{m-1})^k,$$

formule due à M. Libri, qui la démontre de même.

Considérons encore la congruence

$$x_1^m + x_2^m + x_3^m + \ldots + x_k^m \equiv p^f \equiv -p^{f+\frac{hm}{2}} \pmod{p=hm+1}.$$

Comme on doit ôter m des indices qui surpassent ce nombre, pour h pair on posera $a=f$, $b=c\ldots=r=0$, et la formule (39) deviendra

$$(41)\quad \begin{aligned} pS_k = p^k &+ \gamma_f(1+m\gamma_0)^k + \gamma_{f+1}(1+m\gamma_1)^k + \ldots\ldots\ldots\ldots \\ &+ \gamma_{f-1}(1+\gamma_{m-1})^k. \end{aligned}$$

Mais, pour h impair, on fera $a=f+\frac{n}{2}$, $b=c\ldots=g=0$, et la formule (39) deviendra

$$(42)\quad \begin{aligned} pS_k = p^k &+ \gamma_{f+\frac{m}{2}}(1+m\gamma_0)^k + \gamma_{f+1+\frac{m}{2}}(1+m\gamma_1)^k + \ldots\ldots\ldots \\ &+ \gamma_{f-1+\frac{m}{2}}(1+m\gamma_{m-1})^k. \end{aligned}$$

Ces formules nous serviront plus loin

La formule (40) donnant les équations

$$pN_1 = p + \gamma_0(1 + m\gamma_0) + \gamma_1(1 + m\gamma_1) + \gamma_2(1 + m\gamma_1) + \ldots\ldots + \gamma_{m-1}(1 + m\gamma_{m-1}).$$

$$pN_2 = p^2 + \gamma_0(1 + m\gamma_0)^2 + \gamma_1(1 + m\gamma_1)^2 + \gamma_2(1 + m\gamma_2)^2 + \ldots\ldots + \gamma_{m-1}(1 + m\gamma_{m-1})^2.$$

$$pN_3 = p^3 + \gamma_0(1 + m\gamma_0)^3 + \gamma_1(1 + m\gamma_1)^3 + \gamma_2(1 + m\gamma_2)^3 + \ldots\ldots + \gamma_{m-1}(1 + m\gamma_{m-1})^3.$$

$$\vdots$$

$$pN_{m-1} = p^{m-1} + \gamma_0(1 + m\gamma_0)^{m-1} + \gamma_1(1 + m\gamma_1)^{m-1} + \gamma_2(1 + m\gamma_2)^{m-1} \ldots + \gamma_{m-1}(1 + m\gamma_{m-1})^{m-1},$$

auxquelles il faudra joindre

$$0 = 1 + \gamma_0 + \gamma_1 + \gamma_2 + \ldots + \gamma_{m-1}.$$

On tirera de ces m équations les valeurs des m sommes

$$\gamma_0 + \gamma_1 + \ldots + \gamma_{m-1},\ \gamma_0^2 + \gamma_1^2 + \ldots + \gamma_{m-1}^2, \ldots \gamma_0^m + \gamma_1^m + \gamma_2^m \ldots + \gamma_{m-1}^m,$$

et par les formules connues on en déduira les valeurs des coefficients de l'équation en γ. C'est là le procédé employé par M. Libri pour le calcul de l'équation en γ; il se trouve complété ici par le calcul des nombres $N_1, N_2, N_3 \ldots, N_{m-1}$, qui se fait au moyen des formules de l'article IV.

Nous ferons remarquer ici que les coefficients N_1, N_2, N_{m-1} seront uniquement fonctions de certains coefficients binomiaux, aussi bien que les coefficients de l'équation en γ, car r doit disparaître du résultat qui ne peut rien contenir d'indéterminé. Les exemples du paragraphe suivant confirment cette remarque.

La formule (40) qui ne contient que les fonctions

$$\gamma_0 + \gamma_1 + \ldots + \gamma_{m-1},\ \gamma_0^2 + \gamma_1^2 + \ldots + \gamma_{m-1}^2, \ldots \gamma_0^m + \gamma_1^m + \ldots \gamma_{m-1}^m,$$

qui se déterminent très facilement au moyen des coefficients de l'équation en γ, sans qu'il soit nécessaire de la résoudre, pourra toujours être employée dès qu'on aura trouvé l'équation en γ. Mais

il n'en est pas de même des formules (39), (41) et (42); les fonctions

$$y_f y_0 + y_{f+1} y_1 + \ldots + y_{f-1} y_{m-1}, \quad y_f y_0^2 + y_{f+1} y_1^2 + \ldots + y_{f-1} y_{-1}^2, \text{ etc.}$$

qui entrent dans la formule (41), par exemple, ne sont point des fonctions symétriques qui puissent se déterminer rationnellement par le moyen de l'équation en y. Cependant elles ont une propriété commune avec la somme $y_0^n + y_1^n + y_2^n + \ldots y_{m-1}^n$, c'est de conserver la même valeur quand la racine imaginaire de $x^p = 1$, qui a servi pour former les fonctions $y_0, y_1, \ldots, y_{m-1}$ vient à changer. Ce qui tient à ce que ce changement augmentant tous les indices d'un même nombre, le $g^{ième}$ terme, par exemple, devient le premier, le $(g+1)^{ième}$ le deuxième, le $(g+2)^{ième}$ le troisième, et ainsi de suite. Quand on aura calculé ces fonctions, qu'on pourrait appeler circulantes, on pourra faire usage des formules démontrées dans cet article, sans qu'il soit besoin de résoudre l'équation en y, en la ramenant à une équation à deux termes, ce qui serait fort long (*).

---

(1) Les autres paragraphes de ce mémoire forment, pour ainsi dire, autant de memoires séparés que nous publierons dans ce Journal, des que l'auteur nous les aura fait parvenir. (J. LIOUVILLE.)