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

AUGUSTIN CAUCHY

Sur la sommation de certaines puissances d'une racine primitive d'une équation binôme, et en particulier, des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné

Journal de mathématiques pures et appliquées 1re série, tome 5 (1840), p. 169-183.
<http://www.numdam.org/item?id=JMPA_1840_1_5__169_0>

SUR LA

SOMMATION DE CERTAINES PUISSANCES

D'UNE

RACINE PRIMITIVE D'UNE ÉQUATION BINOME,

Et en particulier, des puissances qui offrent pour exposants les résidus cubiques inférieurs au module donné;

PAR M. AUGUSTIN CAUCHY.

Le module p étant un nombre premier, concevons qu'une racine primitive d'une équation binome du degré p soit successivement élevée à des puissances qui offrent pour exposants les résidus quadratiques inférieurs au module p. La somme de ces puissances pourra seulement acquérir deux valeurs distinctes en vertu de la substitution d'une racine primitive à une autre; et la différence entre ces valeurs sera une fonction alternée que M. Gauss a le premier appris à déterminer. Or, après avoir exposé, dans la Note qui précède, une méthode fort simple qui reproduit les résultats de M. Gauss, j'ai dit que la même méthode pouvait être étendue à d'autres déterminations analogues. C'est ce que l'on verra dans cet article où la méthode dont il s'agit se trouvera particulièrement appliquée à la solution du problème que je vais indiquer.

Supposons que, le module p étant du nombre de ceux qui, divisés par 3, donnent 1 pour reste, on élève une racine primitive aux diverses puissances qui offrent pour exposants les résidus cubiques. La somme de ces puissances, quand on y remplacera la racine primitive donnée par d'autres, pourra successivement acquérir trois valeurs distinctes, et ces trois valeurs seront les trois racines d'une équation connue, à laquelle on parvient à l'aide de la théorie de M. Gauss. D'ailleurs la fonction alternée la plus simple que l'on puisse former avec ces trois valeurs est le produit des trois différences que l'on obtient en les retran-

chant l'une de l'autre. Or la détermination complète de cette fonction alternée est évidemment un problème analogue à celui dont j'ai donné deux solutions nouvelles dans l'article précédent. Seulement ce nouveau problème est d'un ordre plus élevé, attendu que les résidus quadratiques se trouvent ici remplacés par des résidus cubiques. Mais, quoiqu'en raison de cette circonstance la difficulté semble s'accroître, toutefois je parviens à la surmonter en suivant une marche semblable à celle que j'ai adoptée dans la Note citée.

J'indique aussi quelques-unes des conséquences auxquelles on se trouve immédiatement conduit par la solution du problème que je viens d'énoncer.

ANALYSE.

§ I^er^. *Théorèmes divers, relatifs aux modules qui, divisés par* 3. *donnent l'unité pour reste.*

Soient p un nombre premier impair, θ une racine primitive de l'équation

$$x^p = 1, \tag{1}$$

et t une racine primitive de l'équivalence

$$x^{p-1} \equiv 1, \pmod{p}. \tag{2}$$

Les divers entiers inférieurs au module p seront équivalents, suivant ce module, aux divers termes de la progression géométrique

$$1, t, t^2, t^3, \ldots t^{p-2};$$

et en conséquence les diverses racines primitives de l'équation (1) pourront être représentées ou par les termes de la suite

$$\theta, \theta^2, \theta^3, \ldots \theta^{p-1},$$

ou par les termes de la suite

$$\theta, \theta^t, \theta^{t^2}, \ldots \theta^{t^{p-2}}.$$

Si d'ailleurs on nomme s la somme de ces racines primitives, c'est-à-dire si l'on pose

$$s = \theta + \theta^t + \theta^{t^2} + \ldots + \theta^{t^{p-2}}, \tag{3}$$

on aura évidemment $1 + s = 0$, ou, ce qui revient au même,

$$s = -1. \tag{4}$$

Concevons maintenant que le module p, divisé par 3, donne l'unité pour reste, et posons

$$\varpi = \frac{p-1}{3}. \tag{5}$$

La progression géométrique

$$1,\ t,\ t^2,\ t^3,\ \ldots\ t^{p-2},$$

pourra être décomposée en trois autres, savoir

$$\begin{aligned} &1,\ t^3,\ t^6,\ \ldots\ t^{p-4},\\ &t,\ t^4,\ t^7,\ \ldots\ t^{p-3},\\ &t^2,\ t^5,\ t^8,\ \ldots\ t^{p-2}; \end{aligned}$$

et la somme s en trois parties correspondantes

$$s_0,\ s_1,\ s_2,$$

respectivement déterminées par les équations

$$\begin{cases} s_0 = \theta + \theta^{t^3} + \theta^{t^6} + \ldots + \theta^{t^{p-4}},\\ s_1 = \theta^t + \theta^{t^4} + \theta^{t^7} + \ldots + \theta^{t^{p-3}},\\ s_2 = \theta^{t^2} + \theta^{t^5} + \theta^{t^8} + \ldots + \theta^{t^{p-2}}. \end{cases} \tag{6}$$

Cela posé, comme les divers résidus cubiques, inférieurs au module p, seront équivalents, suivant ce module, aux divers termes de la progression géométrique

$$1,\ t^3,\ t^6,\ \ldots\ t^{p-4},$$

il est clair que s_0 représentera la somme des puissances de θ qui offriront

pour exposants ces résidus cubiques. Quant aux sommes s_1, s_2, on les déduira évidemment de la somme s_0, en remplaçant la racine primitive θ de l'équation (1) par la racine primitive θ^t ou θ^{t^2}. Il y a plus : si à la racine primitive θ on substitue successivement toutes les autres, la somme des puissances de θ, qui offrent pour exposants les résidus cubiques inférieurs au module p, pourra seulement acquérir trois valeurs distinctes qui seront précisément

$$s_0,\ s_1,\ s_2.$$

Enfin, si l'on nomme S_0 la somme des puissances de θ qui ont pour exposants les cubes des nombres

$$0,\ 1,\ 2,\ 3,\ldots\ p-1,$$

et S_1, S_2, ce que devient S_0 quand on y remplace successivement θ par θ^t et par θ^{t^2}, on aura

$$(7)\qquad S_0 = 1 + 3s_0,\quad S_1 = 1 + 3s_1,\quad S_2 = 1 + 3s_2.$$

En effet, les nombres

$$1,\ 2,\ 3,\ldots\ p-1,$$

peuvent être censés représenter les diverses racines de l'équivalence

$$x^{p-1} \equiv 1,\quad \text{ou}\quad x^{3\omega} \equiv 1,\quad (\text{mod. } p),$$

qui se décompose en plusieurs autres, savoir,

$$(8)\qquad x^3 \equiv 1,\quad x^3 \equiv t^3,\quad x^3 \equiv t^6,\ldots\ x^3 \equiv t^{p-4},\quad (\text{mod. } p);$$

et par conséquent trois d'entre eux vérifieront chacune des équivalences (8). Donc si l'on pose

$$(9)\qquad S_0 = 1 + \theta^1 + \theta^{2^3} + \theta^{3^3} + \ldots + \theta^{(p-1)^3},$$

on aura encore

$$S_0 = 1 + 3(\theta + \theta^{t^3} + \theta^{t^6} + \ldots + \theta^{t^{p-4}}),$$

ou, ce qui revient au même,

$$S_0 = 1 + 3s_0.$$

On retrouve ainsi la première des formules (7), de laquelle on déduira la seconde et la troisième en remplaçant θ par θ^t et par θ^{t^2}.

Il est bon d'observer que, si t^{3m} désigne un terme quelconque de la suite

$$1,\ t^3,\ t^6, \ldots\ t^{p-4},$$

un autre terme de la même suite sera équivalent à

$$-t^{3m} = (-t^m)^3;$$

et même, comme on aura

$$t^{\frac{p-1}{2}} = t^{3\frac{\varpi}{2}} \equiv -1, \quad (\text{mod. } p),$$

il est clair que le terme équivalent à $-t^{3m}$ sera

$$t^{\frac{p-1}{2}+3m} = t^{3\left(m+\frac{\varpi}{2}\right)}.$$

Cela posé, les différents termes de chacune des sommes

$$s_0,\ s_1,\ s_2,$$

seront deux à deux de la forme

$$\theta^l,\ \theta^{-l};$$

et comme θ étant une racine primitive de l'équation (1), θ^l, θ^{-l} représenteront deux expressions imaginaires conjuguées, la somme partielle

$$\theta^l + \theta^{-l}$$

se réduira simplement à une quantité réelle. Donc les trois sommes s_0, s_1, s_2 seront trois quantités réelles, et l'on pourra en dire autant des trois sommes S_0, S_1, S_2, qui seront d'ailleurs les trois racines d'une équation connue du troisième degré. Cette équation, et celle qui aura pour racines les trois autres sommes, pourront d'ailleurs s'obtenir à l'aide des considérations suivantes.

Si l'on élève au carré la valeur de s_0 fournie par la première des équations (6), on trouvera

$$(10)\quad \begin{cases} s_2^2 = \theta^{1+1} + \theta^{1+t^3} + \theta^{1+t^6} + \ldots\ldots\ldots + \theta^{1+t^{p-4}} \\ \quad + \theta^{t^3+t^3} + \theta^{t^3+t^6} + \theta^{t^3+t^9} + \ldots\ldots\ldots + \theta^{t^3+1} \\ \quad + \text{etc.} \\ \quad + \theta^{t^{p-4}+t^{p-4}} + \theta^{t^{p-4}+t} + \theta^{t^{p-4}+t^3} + \ldots + \theta^{t^{p-4}+t^{p-7}}. \end{cases}$$

Dans le second membre de cette dernière formule, les termes que renferme une même colonne verticale se déduisent les uns des autres quand on remplace successivement dans le premier

$$\theta \text{ par } \theta^{t^3}, \text{ ou par } \theta^{t^6}, \ldots \text{ ou par } \theta^{t^{p-4}}.$$

Donc la somme de ces termes se réduit toujours ou à l'une des sommes

$$s_0,\ s_1,\ s_2,$$

ou bien au nombre de ces termes, c'est-à-dire à $\frac{p-1}{3}$, dans le cas particulier où l'exposant de θ dans le premier terme s'évanouit, ce qui a lieu lorsque le premier terme est

$$\theta^{1+t\frac{p-1}{2}} = \theta^0 = 1.$$

Donc la formule (10) donnera

$$(11)\quad s_0^2 = \frac{p-1}{3} + as_0 + bs_1 + cs_2,$$

a, b, c désignant trois nombres entiers dont la somme, inférieure d'une unité au nombre des termes

$$\theta^{1+1},\quad \theta^{1+t^3},\quad \theta^{1+t^6}, \ldots \theta^{1+t^{p-4}},$$

sera

$$(12)\quad a + b + c = \frac{p-4}{3}.$$

Or, quoique au premier abord la détermination des entiers a, b, c

semble exiger le calcul numérique des divers termes de la suite

$$1+1,\quad 1+t^3,\quad 1+t^6,\ldots 1+t^{p-1},$$

néanmoins ce calcul n'est pas nécessaire, et la détermination dont il s'agit peut aisément s'effectuer, comme on va le voir, à l'aide d'une méthode analogue à celle que nous avons employée dans le précédent article.

La valeur de s_0^2 donnée par la formule (11) peut s'écrire comme il suit :

$$(13)\quad \left\{\begin{aligned} s_0^2 = \tfrac{p-1}{3}\theta^0 &+ a(\theta^1 + \theta^{t^3} + \ldots + \theta^{t^{p-4}}) \\ &+ b(\theta^t + \theta^{t^4} + \ldots + \theta^{t^{p-3}}) \\ &+ c(\theta^{t^2} + \theta^{t^5} + \ldots + \theta^{t^{p-2}}); \end{aligned}\right.$$

et, pour déduire celle-ci de la formule (10), il suffit d'y faire croître ou décroître d'un multiple de p, l'exposant l de chaque terme de la forme

$$\theta^l.$$

Or concevons que, dans l'une ou l'autre formule, on remplace généralement

$$\theta^l \text{ par } l^{\frac{p-1}{3}} = l^\varpi.$$

Comme l^ϖ croîtra ou décroîtra d'un multiple de p, en même temps que l, il est clair qu'après le remplacement dont il s'agit, les seconds membres des formules (10) et (13), se transformeront en deux quantités qui seront équivalentes entre elles suivant le module p. D'ailleurs m, l étant deux nombres entiers, on aura

$$\left.\begin{aligned} (t^{3m})^\varpi &= (t^m)^{p-1} \equiv 1, \\ (t^{3m+1})^\varpi &= (t^m)^{p-1} t^\varpi \equiv t^\varpi, \\ (t^{3m+2})^\varpi &= (t^m)^{p-1} t^{2\varpi} \equiv t^{2\varpi}, \end{aligned}\right\} \pmod p,$$

et

$$(t^{3m} l)^\varpi \equiv (t^m)^{p-1} l^\varpi \equiv l^\varpi, \pmod p.$$

Donc les quantités dans lesquelles se transformeront les seconds mem-

bres des formules (10) et (13) seront équivalentes aux deux produits qu'on obtient en multipliant

$$\frac{p-1}{3} = \varpi,$$

d'un côté, par la somme

$$(1+t)^{\varpi} + (1+t^3)^{\varpi} + \ldots + (1+t^{p-4})^{\varpi},$$

d'un autre côté, par le trinome

$$a + bt^{\varpi} + ct^{2\varpi}.$$

On aura donc

$$(14)\quad a+bt^{\varpi}+ct^{2\varpi} \equiv (1+t)^{\varpi}+(1+t^3)^{\varpi}+\ldots+(1+t^{p-4})^{\varpi}, \pmod{p}.$$

De même, si, dans les seconds membres des formules (10) et (13), on remplace généralement

$$\theta^l \text{ par } l^{2\varpi},$$

on trouvera

$$(15)\quad a+bt^{2\varpi}+ct^{4\varpi} \equiv (1+t)^{2\varpi}+(1+t^3)^{2\varpi}+\ldots+(1-t^{p-4})^{2\varpi}, \pmod{p}.$$

Concevons à présent que, dans les seconds membres des formules (14), (15), on développe chaque binome de la forme

$$(1+t^{3m})^{\varpi} \quad \text{ou} \quad (1+t^{3m})^{2\varpi}.$$

La somme des valeurs que prendra un terme du développement, quand on attribuera successivement à m les diverses valeurs

$$0,\ 1,\ 2,\ \ldots\ \frac{p-4}{3} = \varpi - 1,$$

sera de la forme

$$1 + t^{3l} + t^{6l} + \ldots + t^{3(\varpi-1)l} = \frac{1-t^{(p-1)l}}{1-t^{3l}}.$$

Donc cette somme sera nulle, à moins qu'il ne s'agisse d'un terme dans lequel l'exposant de t soit multiple de $3\varpi = p - 1$. Il est aisé d'en conclure que les formules (14), (15) donneront

$$(16)\quad a + bt^{\varpi} + ct^{2\varpi} \equiv 2\varpi, \quad a + bt^{2\varpi} + ct^{\varpi} \equiv (2 + \Pi)\varpi, \ (\text{mod. } p),$$

la valeur de Π étant

$$(17)\qquad \Pi = \frac{(\varpi + 1)(\varpi + 2)\dots 2\varpi}{1.2.3\dots\varpi}.$$

Soit d'ailleurs

$$(18)\qquad r = t^{\varpi};$$

r représentera une racine primitive de l'équation

$$(19)\qquad x^3 \equiv 1, \ (\text{mod. } p),$$

et, comme on aura

$$\varpi = \frac{p-1}{3} \equiv -\frac{1}{3}, \ (\text{mod. } p),$$

les formules (12), (13) donneront

$$(20)\quad a + b + c \equiv -\frac{1}{3}, \quad a + br + cr^2 \equiv -\frac{2}{3}, \quad a + br^2 + cr \equiv -\frac{2}{3} - \frac{\Pi}{3}, \ (\text{mod. } p).$$

Enfin l'on tirera de ces dernières

$$(21)\quad a \equiv -\frac{8}{9} - \frac{\Pi}{9}, \quad b \equiv -\frac{2}{9} - \frac{\Pi}{9} r, \quad c \equiv -\frac{2}{9} - \frac{\Pi}{9} r^2, \ (\text{mod. } p).$$

Les valeurs de a, b, c, étant ainsi déterminées, on pourra les substituer dans la formule (11), et dans celles qu'on en déduit lorsqu'on y remplace θ par θ^t ou par θ^{t^2}, c'est-à-dire, dans les trois équations

$$(22)\quad s_0^2 = \varpi + as_0 + bs_1 + cs_2, \quad s_1^2 = \varpi + as_1 + bs_2 + cs_0, \quad s_2^2 = \varpi + as_2 + bs_1 + cs_0.$$

D'autre part, on aura, en vertu de l'équation (4),

$$(23)\qquad s_0 + s_1 + s_2 = -1,$$

et de cette dernière, combinée avec les formules (22), on tirera successivement

$$(24)\quad s_0^2 + s_1^2 + s_2^2 = 2\varpi + 1, \quad s_0 s_1 + s_1 s_2 + s_2 s_0 = -\varpi;$$

$$(25)\quad s_0^2 s_1 + s_1^2 s_2 + s_2^2 s_0 = bp - \varpi^2, \quad s_0 s_1^2 + s_1 s_2^2 + s_2 s_1^2 = cp - \varpi^2;$$

$$(26)\quad (s_0 - s_1)(s_1 - s_2)(s_2 - s_0) = (c - b)p;$$

$$(27)\quad s_1 s_2 s_0 = \frac{\varpi(2\varpi + 1)}{3} - \frac{b + c}{3} p;$$

puis, en ayant égard à la formule (12),

$$(28)\quad s_0 s_1 s_2 = \frac{1}{3} ap - \frac{\varpi^2 - 3\varpi - 1}{3}.$$

Il suit des formules (23), (24), (28), que s_0, s_1, s_2 sont les trois valeurs de s propres à vérifier l'équation

$$(29)\quad s^3 + s - \varpi s + \frac{\varpi^2 - 3\varpi - 1 - ap}{3} = 0.$$

Si, dans cette dernière, on pose

$$S = 1 + 3s \quad \text{ou} \quad s = \frac{S - 1}{3},$$

on obtiendra la suivante

$$(30)\quad S^3 - 3pS - pA = 0,$$

la valeur de A étant

$$(31)\quad A = 8 - p + 9a.$$

L'équation (30) étant précisément celle qui a pour racines les trois sommes réelles

$$S_0, \ S_1, \ S_2,$$

le produit des différences entre ces trois racines, savoir,

$$(S_0 - S_1)(S_1 - S_2)(S_2 - S_0) = 3^3 (s_0 - s_1)(s_1 - s_2)(s_2 - s_0),$$

aura pour carré, d'après une règle connue, le binome

$$4(3p)^3 - 27(Ap)^2 = 27p^2(4p - A^2).$$

On aura donc

$$(32) \qquad 27(s_0 - s_1)^2(s_1 - s_2)^2(s_2 - s_0)^2 = p^2(4p - A^2).$$

D'autre part, si l'on pose

$$(33) \qquad B = b - c,$$

l'équation (26) donnera

$$(34) \qquad (s_0 - s_1)(s_1 - s_2)(s_2 - s_0) = -Bp;$$

et l'on tirera des formules (32), (34),

$$(35) \qquad 4p = A^2 + 27B^2.$$

Enfin les équations (31), (33), jointes aux formules (21), donneront

$$(36) \qquad A \equiv -\Pi, \quad B \equiv \frac{r^2 - r}{9}\Pi, \quad (\text{mod. } p).$$

Donc, 1° l'équation (35) pourra être vérifiée, comme l'a dit M. Jacobi, par des nombres entiers $\pm A$, $\pm B$, et la quantité A dont la valeur numérique sera inférieure à

$$\sqrt{4p - 27} = \tfrac{1}{2}\sqrt{p^2 - (p-8)^2 - 44},$$

par conséquent à $\frac{1}{2}p$, pourra être complétement déterminée, ainsi que la quantité B, inférieure elle-même, abstraction faite du signe, à $\frac{1}{2}\sqrt{p}$, à plus forte raison à $\frac{1}{2}p$, par le moyen des formules (36); 2° si, dans la formule (30), on substitue la valeur de A choisie de manière à vérifier non-seulement la formule (35), mais encore la condition (31), présentée sous la forme

$$A \equiv -(p+1), \quad (\text{mod. } 9),$$

l'équation (30) aura pour racines réelles les trois sommes

$$S_0, \quad S_1, \quad S_2.$$

Cette dernière conclusion s'accorde avec des remarques déjà faites par M. Libri et par M. Lebesgue (voir ce Journal, février 1840). Nous ajouterons que, l'équation (28) pouvant être réduite à

$$27\, s_0 s_1 s_2 = (A+3)p - 1, \tag{37}$$

et le produit $s_0 s_1 s_2$ étant nécessairement une quantité entière, on aura par suite

$$(A+3)p \equiv 1, \pmod{27}. \tag{38}$$

Ainsi, en particulier, on trouve pour $p = 7$,

$$A = 1, \quad (1+3)7 = 28 \equiv 1, \pmod{27};$$

pour $p = 13$,

$$A = -5, \quad (-5+3)13 = -26 \equiv 1, \pmod{27},$$

etc... De plus la fonction alternée la plus simple que l'on puisse former avec les trois quantités s_0, s_1, s_2, ou le produit

$$(s_0 - s_1)(s_1 - s_2)(s_2 - s_0),$$

dont le carré peut se déduire de la formule (29) ou (30), offrira une valeur qui sera complétement déterminée par la formule (34).

§ II. *Conséquences diverses des principes établis dans le premier paragraphe.*

On peut, des formules établies dans le premier paragraphe, déduire diverses conséquences que nous nous bornerons à indiquer.

D'abord il résulte de la formule (34) que les trois sommes

$$s_0, \; s_1, \; s_2,$$

rangées d'après leur ordre de grandeur, seront trois termes consécutifs de la suite périodique

$$s_0, \; s_1, \; s_2, \; s_0, \; s_1, \; s_2, \ldots$$

si B est négatif, et trois termes consécutifs de la suite périodique

$$s_0,\ s_2,\ s_1,\ s_0,\ s_2,\ s_1,\ldots$$

si B est positif. Ajoutons que l'ordre de grandeur des sommes

$$S_0,\ S_1,\ S_2,$$

sera, en vertu des formules (7), précisément le même que l'ordre de grandeur des sommes

$$s_0,\ s_1,\ s_2.$$

Observons encore qu'en vertu du théorème de Lagrange, les racines de l'équation (30), rangées dans leur ordre de grandeur, seront respectivement

$$S = -(3p)^{\frac{1}{2}}\mathcal{C} + \tfrac{1}{6}\alpha A,\quad S = -\tfrac{1}{3}\alpha A,\quad S = (3p)^{\frac{1}{2}}\mathcal{C} + \tfrac{1}{6}\alpha A,$$

les valeurs de α, $\mathcal{C}$ étant données par les formules

$$\alpha = 1 + \frac{A^2}{3^3 p} - \frac{6}{1.2}\frac{A^4}{3^6 p^2} + \frac{9.8}{1.2.3}\frac{A^6}{3^3 p^3} - \text{etc.},\ldots$$

$$\mathcal{C} = 1 - \tfrac{1}{2}\left(\frac{3}{4}\frac{A^2}{3^3 p} + \frac{5.7.9}{4.6.8}\frac{A^4}{3^6 p^2} + \text{etc.}\right),$$

et que les séries, dont les sommes représentent les seconds membres de ces formules, seront toujours convergentes, eu égard à la condition

$$A^2 < 4p.$$

Pour obtenir l'ordre de grandeur tel que nous venons de l'indiquer, il suffit d'observer que cet ordre reste le même pour toutes les valeurs de A qui vérifient la condition $A^2 < 4p$, et que les trois racines de l'équation (30), rangées d'après cet ordre, seront évidemment

$$-\sqrt{3p},\ 0,\ \sqrt{3p},$$

si l'on remplace A par zéro.

Enfin, si l'on cherche le nombre des solutions que peut admettre

chacune des formules

$$x+y\equiv z,\quad x+y+z\equiv 0,\quad (\text{mod. } p),$$

quand on prend pour x, y, z des résidus cubiques positifs et inférieurs à p, on conclura de la formule (11) que ce nombre est

$$a\varpi=\frac{p-1}{3}\,\frac{p+A-8}{9}.$$

Si l'on assujétissait x, y, z à vérifier la condition

$$x<y<z,$$

le nombre des solutions deviendrait

$$\frac{a\varpi}{1.2.3}=\frac{p-1}{2}\,\frac{p+A-8}{3^4}$$

dans le cas où 2 ne serait pas résidu cubique de p, et

$$\frac{a\varpi}{1.2.3}-\frac{1}{2}\,\varpi=\frac{p-1}{2}\,\frac{p+A-35}{3^4}$$

dans le cas contraire. D'ailleurs ce nombre de solutions sera pair, attendu que trois valeurs données de

$$x,\ y,\ z,$$

pourront être remplacées par trois autres valeurs de la forme

$$p-z,\quad p-y,\quad p-x;$$

et, pour qu'il s'évanouisse, il faudra que l'on ait, dans le premier cas,

$$p+A-8=0,$$

dans le second cas,

$$p+A-35=0.$$

Or ces dernières formules, jointes à la condition

$$-A<\frac{p}{2},$$

donneront, dans le premier cas,

$$\tfrac{1}{2}p < 8, \quad p < 16,$$

et dans le second cas,

$$\tfrac{1}{2}p < 35, \quad p < 70.$$

D'ailleurs les seuls nombres premiers, inférieurs à 16, et de la forme $3\varpi + 1$, sont 7 et 13, pour lesquels la condition

$$p + \mathrm{A} - 8 = 0$$

est effectivement vérifiée; et l'on reconnaîtra pareillement que la condition

$$p + \mathrm{A} - 35 = 0$$

se vérifie pour les nombres premiers 31, 43, qui, seuls au-dessus de 70, sont de la forme $3\varpi + 1$, et offrent des résidus cubiques dont l'un est égal à 2.

Au reste, les formules obtenues dans le premier paragraphe peuvent encore être déduites, comme je le montrerai dans un autre article, de la considération des facteurs primitifs du nombre premier p; et l'on peut, à l'aide des mêmes méthodes, établir des formules analogues qui soient relatives, non plus aux résidus cubiques, mais aux résidus des puissances supérieures à la troisième.