Mémoire sur la théorie des nombres.

Libri, G.

in: Journal für die reine und angewandte Mathematik - 9 | Periodical
27 page(s) (54 - 80)

3.

Mémoire sur la théorie des nombres.

(Par Mr. *G. Libri* de Florence.)

Introduction.

Les géomètres qui se sont occupés de l'analyse indéterminée, sont parvenus par leurs recherches plutôt à résoudre des questions spéciales, qu'à faire avancer l'ensemble de la science. Leur méthodes, toujours bornées au problème qu'ils voulaient traiter, cessaient d'être utiles quand on tâchait de les appliquer à des questions plus étendues: bien plus, pour traiter un problème quelconque il fallait que les quantités connues fussent données en nombres; car sans cela, le manque absolu de formules générales empêchait de resoudre une équation indéterminée à coefficiens algébriques, même lorsqu'elle était du premier degré. De sorte que la théorie des nombres presqu'immobile au milieu des progrès des autres parties de l'analyse, qu'elle avait vu naître et s'élever successivement, s'en trouvait séparée et ne partageait pas leur perfectionnement commun. Cet isolement, qui forme la difficulté principales de la théorie des nombres, dépend de la méthode que l'on a suivie jusqu'ici pour mettre en équation les problèmes d'analyse indéterminée; car en exprimant seulement les relations qui doivent exister entre les valeurs des inconnues, on a toujours négligé de représenter par des signes algébriques les conditions auxquelles ces inconnues doivent satisfaire, afin qu'elles soient des nombres entiers ou rationnels. De sorte que ces conditions étant seulement sous-entendues, on ne peut pas les soumettre aux règles ordinaires de l'algèbre, et il en résulte un nouveau genre d'analyse, dont tout le sùccès dépend de la sagacité particulière de chacun des géomètres qui le cultivent, sans que les travaux des uns soient profitables aux recherches des autres. Il y a quelque tems que nous avons tâché de faire disparaître cette imperfection, et déjà nous avons montré ailleurs qu'en écrivant en analyse toutes les conditions du problème, les questions que l'on appelle indéterminées, deviennent toutes plus que déterminées, puisque l'on obtient toujours un nombre d'équations qui surpasse de l'unité celui des inconnues. Nous réproduisons d'abord ici

les formules que nous avons données dans cette occasion, pour exprimer par des séries convergentes le nombre ou la somme des racines d'une équation indéterminée, et nous y ajoutons de nouvelles expressions. Puis nous reprenons ce problème *à priori* dans toute sa généralité, et nous montrons comment, en partant des principes les plus élémentaires de l'analyse, on trouve pour chaque inconnue une équation algébrique dont le degré est égal à la limite que l'on attribue à l'inconnue, et qui exprime la condition que celle-ci doit être un nombre entier: de sorte qu'ayant de cette manière un nombre d'équations égal à celui des inconnues, en les combinant avec l'équation qui exprime les relations qui doivent exister entre les valeurs des variables, on aura après l'élimination une équation de condition qui ne contiendra que les coefficiens de l'équation proposée, et les limites qu'on aura attribuées aux inconnues. D'où il résulte que toute équation indéterminée, est réellement plus que déterminée. Ce résultat remarquable avait échappé à Euler qui croyait que les équations indéterminées, devenaient plus que déterminées, seulement lorsque le nombre des formes que devaient prendre des fonctions données des variables, surpassait celui des inconnues. On explique par là, la contradiction qui se manifestait entre le nom d'équations indéterminées, et le fait qui montrait que souvent elles n'admettaient pas de solutions: ce qui aurait dû faire soupçonner qu'il existait une équation de condition laquelle n'étant pas satisfaite, le problème ne pouvait pas être résolu. Et d'ailleurs en partant de la forme des racines des équations déterminées, et en observant que le nombre des solutions dans une équation indéterminée n'était pas donné par le degré de l'équation, on aurait pu prévoir que cette équation de condition était une fonction des coefficiens de l'équation proposée, et de la limite que l'on attribuait aux variables.

Les principes que nous exposons dans ce mémoire sont suffisans pour trouver, directement et sans tâtonnement, toutes les solutions d'une équation indéterminée, lorsque la limite que l'on attribue aux variables n'est pas l'infini: mais comme le degré de l'équation de condition augmente avec les limites des inconnues; si l'on cherche toutes les solutions possibles d'une équation indéterminée, on trouvera une série infinie dont il s'agira d'avoir la somme pour résoudre la question proposée. Cette somme pourra s'exprimer par des intégrales définies, mais leur valeur numérique sera en général fort difficile à calculer; pour en faciliter la recherche il

faudrait recourir à des principes que nous n'avons pas cru devoir exposer dans ce mémoire, qui a pour but seulement de montrer en général l'esprit de notre méthode. Cependant pour qu'on ne puisse pas croire que notre théorie n'est pas susceptible d'être appliquée aux problèmes particuliers, et pour montrer de quelle manière nos formules peuvent se simplifier dans le plus grand nombre des cas, nous considérons spécialement dans ce mémoire les équations qui sont du premier degré par rapport à l'une des inconnues, et que M. Gaufs a appellées congruences.

En donnant d'abord la théorie générale des congruences nous trouvons, que les relations existantes entre les coefficiens des équations algébriques et leurs racines, s'étendent aux congruences dont toutes les racines sont entières: nous démontrons de cette manière les théorèmes de Fermat et de Wilson, et beaucoup d'autres propositions nouvelles. Puis en appliquant aux congruences les principes qui renferment la théorie générale des équations indéterminées, on trouve les congruences de condition qui doivent être satisfaites afin que le problème soit résoluble: et ces conditions se simplifient beaucoup, à l'aide du théorème de Fermat lorsque le module est un nombre premier.

En effectuant l'élimination entre les congruences, de la même manière que pour les équations, il devient facile d'obtenir le résultat final; et on trouve ainsi les relations qui doivent exister entre les coefficiens d'une congruence et le module, afin qu'elle soit résoluble. Ces relations, qui sont des congruences de condition, renferment toutes les conditions connues jusqu'à présent. Nous plaçons ici une courte digression sur les congruences à module variable, dans laquelle nous faisons voir qu'à l'aide de ces congruences on peut résoudre une classe assez étendue d'équations indéterminées, dont les plus simples avaient été traitées par Lagrange.

Pour chercher les conditions qui doivent être satisfaites afin qu'une congruence soit résoluble, au lieu de faire l'élimination à l'aide des coefficiens, on peut substituer les racines des congruences réduites à la forme d'équations déterminées: de cette manière on introduit les fonctions circulaires dans la théorie des congruences, et on trouve des formules qui la comprennent toute entière. Mais ces expressions ne sont pas assez simples pour qu'on puisse les appliquer avec facilité aux cas particuliers: par conséquent nous avons dû reprendre ce sujet d'une autre manière; et en partant d'une propriété très-simple de l'équation binome, nous avons

trouvé des formules qui expriment le nombre et la somme des diviseurs d'un nombre quelconque, et nous avons formé deux intégrales aux différences finies qui donnent le nombre et la somme des racines d'une congruence quelconque. Ces formules étant appliquées à la congruence du premier degré, fournissent l'expression générale de ses racines, qui sont une fonction trigonométrique des coefficiens et du module: et comme cette congruence équivaut à l'équation indéterminée du premier degré, on trouve ainsi les racines de cette équation en fonction de ses coefficiens, ce qui n'avait jamais été fait.

Nos formules générales étant appliquées au congruences du second degré, donnent tous les théorèmes connus sur les résidus quadratiques: on en déduit aussi la manière de reconnaitre *à priori* si un nombre quelconque est ou n'est pas résidu quadratique d'un nombre premier donné; et il en resulte une proposition générale qui renferme la théorème fondamental de M. Gauss.

La formule qui sert de base à notre théorie, et qui établit un rapport si singulier entre les solutions des congruences et les fonctions circulaires, fournit le moyen de résoudre directement les équations à deux termes. M. Gauss qui a découvert le premier cette résolution par une méthode particulière, et Lagrange qui l'a ramenée ensuite à sa théorie générale des équations, ont supposé la connaissance des racines primitives. La théorie que nous exposons dans ce mémoire est indépendante de cette recherche, et d'ailleurs elle est beaucoup plus simple que les méthodes trouvées par ces deux grands géomètres, qui exigent de très-longs calculs pour être appliquées. On trouvera dans la suite de ces mémoires une méthode générale et très-simple pour traiter les équations de cette classe, de mêmes que celles d'où dépend la division en parties égales de l'arc de la Lemniscate, et beaucoup d'autres; et l'on verra alors pourquoi la résolution de ces équations déterminées se réduit toujours à un problème d'analyse indéterminée.

En appliquant notre principe général aux congruence du troisième et du quatrième degré, nous avons trouvé des rélations fort remarquables entre le nombre des solutions de certaines congruences, et les racines de quelques équations indéterminées du second degré. Nous avons tiré de là des considérations générales sur les résidus cubiques et bicarrés, sur lesquels on n'avait encore rien publié, en montrant comment l'on devait

modifier les formes des nombres premiers qui servent de module, afin d'avoir des théorèmes généraux. On sait que pour avoir tous les théorèmes connus sur les résidus quadratiques d'un nombre premier, il suffit que la forme linéaire de ce nombre soit donnée. Mais cela est insuffisant pour les résidus cubiques et bicarrés, et il faut que le nombre qui sert de module soit alors d'une forme quadratique donnée. Nous parvenons de cette manière à trouver la forme cubique des nombres premiers qu'on n'avait jamais considérée jusqu'à présent. On pourrait pousser plus loin l'examen des formes des degrés supérieurs, en observant que pour chaque degré le nombre des innconnues doit égaler ou surpasser l'exposant. Le même chose arrive pour les congruences, et il est digne de remarque que quand on a déterminé le nombre des solutions d'une congruence, laquelle a autant d'inconnues qu'il y a d'unités dans l'exposant qui marque son degré, on aura tout de suite le nombre des solutions d'une autre congruence du même degré qui aurait le même module, mais qui contiendrait un plus grand nombre d'inconnues. C'est de cette considération que nous déduisons un théorème général sur les congruences de tous les degrés, qui renferme comme cas particulier un théorème de Lagrange sur les congruences du second degré à deux inconnues.

L'analyse succinte que nous venons de donner de notre mémoire suffit pour montrer la possibilité de déduire d'un seul principe général toute la théorie des nombres. Nous n'avons traité ici qu'une classe d'équations indéterminées: mais nous montrerons dans la suite comment on en peut résoudre un grand nombre d'autres, en appliquant le calcul d'approximation aux équations indéterminées, auxquelles il paraissait absolument inappliquable, mais qui cependant dans ce seul cas fournit des solutions exactes. Et nous fairons voir dans un mémoire particulier, comment l'on peut classer et discuter les trancendantes numériques, telles que les nombres premiers, les diviseurs des nombres, etc. En liant la théorie des nombres aux autres parties de l'analyse, il était certain que comme celles-ci contribueraient à son perfectionnement, elles en recevraient des secours; et c'est ce que nous montrerons dans la suite de ces recherches à l'egard des intégrales définies et fonctions circulaires, dont plusieurs propriétés remarquables et inconnues jusqu'à présent, découlent de l'analyse indéterminée. Enfin nous fairons voir comment la considération des différens ordres d'irrationalité devient très-utile dans la résolution des équations numériques.

Analyse.

Nous avons montré pour la première fois, dans le 28e Volume des *Mémoires de l'Académie Royale des Sciences de Turin*, qu'étant proposé de résoudre en nombres entiers l'équation

$$\varphi(x, y, z, \ldots \text{ etc.}) = 0,$$

(que nous indiquerons pour abréger par $\varphi = 0$) pour exprimer que x, y, z, ... etc., doivent être des nombres entiers, on a les équations

$$\sin x\pi = 0; \quad \sin y\pi = 0; \quad \sin z\pi = 0; \quad \ldots. \text{ etc.};$$

dont le nombre est égal à celui des inconnues, et qui doivent exister en même tems que l'équation proposée. Nous avons trouvé encore que le nombre des solutions entières et positives, plus grandes que zéro, de l'équation $\varphi = 0$, est exprimé, à très-peu près par la formule

$$\sum_{x=1}^{x=\infty} \sum_{y=1}^{y=\infty} \sum_{z=1}^{z=\infty} \ldots\ldots e^{-10(x+y+z\ldots.+\text{etc.})\varphi^2}.$$

S'il s'agissait d'exprimer le nombre des solutions entières de l'équation $\varphi = 0$, en donnant à $x, y, z, \ldots.$ etc., toutes les valeurs $1, 2, 3, \ldots. n-1$, on aurait la formule

$$13. \quad \sum_{x=1}^{x=n} \sum_{y=1}^{y=n} \sum_{z=1}^{z=n} \ldots\ldots\ldots\ldots e^{-10(x+y+z\ldots.+\text{etc.})\varphi^2} =$$

$$\sum_{x=1}^{x=n} \sum_{y=1}^{y=n} \sum_{z=1}^{z=n} \ldots. \left\{ \begin{array}{l} 1 - 10(x+y+z\ldots.+\text{etc.})\varphi + \frac{100}{1.2}(x+y+z\ldots+\text{etc.})^2\varphi^2 \ldots. \\ \ldots\ldots\ldots\ldots\ldots \pm \frac{10^a}{1.2.3\ldots a}(x+y+z\ldots+\text{etc.})^a\varphi^a \pm \text{etc.} \end{array} \right\}.$$

On pourrait encore faire usage de la formule

$$\sum_{x=1}^{x=n} \sum_{y=1}^{y=n} \sum_{z=1}^{z=n} \ldots\ldots \frac{1}{1+(10x)^2(10y)^2(10z)^2\ldots\ldots\varphi^2};$$

et il serait facile de trouver plusieurs autres expressions semblables, propres à représenter le nombre ou la somme des solutions de l'équation proposée.

Le second membre de l'équation (13.) est une série qui finira toujours par devenir convergente, et dont chaque terme pourra être calculé à l'aide des formules de la page 9. Mais pour avoir une valeur approchée du premier membre de l'équation (13.) il faut calculer, dans le second membre, un nombre de termes qui augmente avec la limite n de l'intégration; de manière que l'on obtient toujours une expression de degré indéfini, qui est fonction des coefficiens de l'équation $\varphi = 0$, et de la

limite n. Il faut remarquer surtout que les coefficiens des variables x, y, z, ... etc., dans le développement en série de l'intégrale qui forme le premier membre de l'équation (13.), sont tels qu'en calculant un certain nombre de termes, il ne reste à peu près que ce qu'il faut pour donner le nombre des solutions de l'équation proposée. C'est de cette considération, et de l'examen attentif de la nature de ces coefficiens (qui s'expriment aussi par des intégrales définies) que l'on pourrait déduire des considérations qui jetteraient beaucoup de lumière sur la marche de la fonction représentée par la formule (13.): mais ces recherches ne sauraient trouver place ici, et nous les exposerons dans un travail particulier.

Cet aperçu suffirait déjà pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire: mais nous allons reprendre maintenant cette question dans toute sa généralité.

Étant proposée une équation à plusieurs inconnues à résoudres en nombres rationnels, fractionnaires ou entiers, on pourra toujours la préparer de manière que tous les nombres cherchés doivent être entiers et positifs: puisqu'en général, si l'équation proposée est de la forme

$$\varphi(x, y, z, \ldots \text{ etc.}) = 0,$$

et que l'on cherche pour x, y, z, ... etc., des valeurs fractionnaires, en faisant

$$x = \frac{x_1}{x_2}, \quad y = \frac{y_1}{y_2}, \quad z = \frac{z_1}{z_2}, \ldots \text{ etc.},$$

on aura l'équation

$$\varphi\left(\frac{x_1}{x_2}, \frac{y_1}{y_2}, \frac{z_1}{z_2}, \ldots \text{ etc.}\right) = 0,$$

dans laquelle il ne faudra chercher pour

$$x_1, x_2, y_1, y_2, z_1, z_2, \ldots \text{ etc.},$$

que des valeurs entières: et d'ailleurs s'il y avait des solutions négatives on les obtiendrait en changeant les signes des variables. Nous supposerons par conséquent que ces réductions soient toujours effectuées dans les équations dont nous chercherons la résolution.

Soit proposé de résoudre en nombres entiers et positifs l'équation

$$\varphi(x, y, z, \ldots \text{ etc.}) = 0$$

que nous représenterons comme auparavant par $\varphi = 0$. Avec les méthodes connues on s'arrête là, et on tâche de résoudre cette équation en s'aidant de la forme particulière de ses coefficiens. Mais l'équatiou $\varphi = 0$, exprime seulement les relations qui doivent exister entre les inconnues,

et n'indique pas que ces inconnues ne doivent recevoir que des valeurs entières et positives: pour exprimer cette dernière condition l'on supposera d'abord que l'on veuille trouver toutes les solutions qui s'obtienneut en donnant à x des valeurs moindres qu'une limite donnée a; à y des valeurs plus petites que b; à z des valeurs moindres que c; et ainsi de suite: $a, b, c, \ldots$ etc., étant des nombres entiers et positifs. Il est clair qu'à cet effet l'on devra donner à $x, y, z, \ldots$ etc., toutes les valeurs comprises dans les séries

$$\begin{aligned} x &= 0, 1, 2, 3, \ldots\ldots\ldots a-1; \\ y &= 0, 1, 2, 3, \ldots\ldots\ldots b-1; \\ z &= 0, 1, 2, 3, \ldots\ldots\ldots c-1; \\ &\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}; \end{aligned}$$

et faire toutes les combinaisons possibles dans l'équation $\varphi = 0$. On observera que toutes ces valeurs de x se trouveront parmi les racines de l'équation

$$X = x(x-1)(x-2)\ldots\ldots(x-(a-1)) = 0;$$

et que de mêmes les valeurs de y et de z seront comprises parmi les racines des équations

$$\begin{aligned} Y &= y(y-1)(y-2)\ldots\ldots(y-(b-1)) = 0; \\ Z &= z(z-1)(z-2)\ldots\ldots(z-(c-1)) = 0; \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.} \end{aligned}$$

Les équations précédentes expriment les conditions que x soit un nombre entier positif moindre que a; que y soit un nombre entier positif moindre que b; et ainsi de suite. Ces équations dont le nombre est égal à celui des inconnues, étant combinées avec l'équation $\varphi = 0$, fournissent toutes les conditions du problème; de manière qu'ayant un nombre total d'équations qui surpasse de l'unité le nombre des inconnues, le problème sera plus que déterminé; en éliminant successivement toutes les inconnues entre ces équations, on aura une autre équation de condition $F = 0$, qui comprendra les limites $a, b, c, \ldots$ etc., assignées aux variables, et les coefficiens de l'équation proposée; et qui exprimera la relation qui doit exister entre ces quantités afin que le problème soit résoluble. Lorsque l'équation de condition sera satisfaite, et que l'on sera assuré que l'équation proposé peut être résolue, on reprendra l'une des équations à une seule inconnue que l'on a obtenues par l'élimination avant de parvenir à l'équation $F = 0$. Soit $X_1 = 0$, cette équation en x seul;

en cherchant le plus grand diviseur commun entre $X=0$, et $X_1=0$, on aura une équation de la forme $X_2=0$, qui ne contiendra que l'inconnue x, et dont le degré sera égal au nombre des valeurs de x qui satisfont à l'équation proposée; et en résolvant l'équation $X_2=0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi=0$. On pourrait trouver de même les valeurs des autres inconnues, qui résolvent l'équation proposée; et l'on voit que ce principe s'applique encore à la recherche directe des racines rationnelles d'une équation à une seule inconnue; car ce problème aussi dépend de la théorie des nombres.

Avec la méthode que nous venons d'indiquer, on a seulement les racines inégales; mais s'il y a des racines égales, elles peuvent se trouver avec facilité de la manière suivante. Nous supposerons d'abord, pour simplifier la question, qu'il s'agisse d'une équation à deux inconnues seulement; puisque la méthode est absolument la même lorsque le nombre des variables est plus grand.

Maintenant soit proposé de résoudre en nombres rationnels l'équation

$$\varphi(x,y) = 0;$$

et supposons que n valeurs rationnelles de $x=a$, correspondent à une seule valeur rationnelles de $y=b$; (n étant un nombre plus grand que l'unité) en différentiant l'équation proposée par rapport à x, et cherchant le plus grand commun diviseur $\triangle$, entre

$$\frac{d.\varphi(x,y)}{dx} \quad \text{et} \quad \varphi(x,y),$$

on aura $\triangle = F(x,y)$, et il y aura un reste $R=f(y)$ qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait par conséquent $f(y)=0$, on cherchera les racines rationnelles $y=b$, $y=b_1$, $y=b_2$, ... etc., de cette équation, lorsqu'il en existe, et en substituant successivement b, b_1, b_2, ... etc., pour y dans l'expression de $\triangle$ on aura les équations

$$F(x,b)=0; \quad F(x,b_1)=0; \quad F(x,b_2)=0; \ldots . \text{ etc.}$$

que l'on tâchera de réduire à la forme $(x-a)^{n-1}=0$; et on trouvera de cette manière les valeurs multiples de x que l'on cherche.

Si l'on avait identiquement $R=0$, on trouverait l'équation

$$\triangle = F(x,y) = (x-\psi(y))^{n-1} = 0,$$

qui devrait exister en même tems que l'équation $\varphi(x,y)=0$, et qui en serait un facteur: l'on ne pourrait donc pas déterminer de cette manière

la valeur de $y = b$; mais en divisant le polynome $\varphi(x,y) = 0$ par Δ, le quotient Q contiendrait un seule des n racines égales; et en cherchant le plus grand commun diviseur entre Δ et Q, on aurait l'équation $x - \psi(y) = 0$. Nous avons supposé qu'il y avait seulement n valeurs de $x = a$, correspondantes à une valeur de $y = b$: mais si outre celles-là il y avait m valeurs de x égales à c, et r valeurs égales à e, etc., il serait facile d'appliquer encore à ce cas la méthode que nous venons d'exposer.

Soit proposée par exemple l'équation

$$x^2 - 2xy + 2y^3 - 1 = 0,$$

dans laquelle on veuille savoir si parmi les valeurs rationnelles de y qui la résolvent il y en a une égale à b, et telle qu'il lui corresponde n valeurs de $x = a$; n étant un nombre plus grand que l'unité. A cet effet on différentiera l'équation proposée par rapport à x, et l'on aura $x - y = 0$; puis en cherchant le plus grand commun diviseur, entre ces deux équations, l'on trouvera $x - y$ pour ce diviseur et $2y^3 - y^2 - 1 = 0$ pour reste, et comme cette dernière équation est satisfaite en faisant $y = 1$, si l'on substitue cette valeur dans l'équation proposée, on aura

$$x^2 - 2x + 1 = (x-1)^2 = 1;$$

et par conséquent l'équation

$$x^2 - 2xy + 2y^3 - 1 = 0,$$

est telle que deux valeurs de $x = 1$, correspondent à la racine $y = 1$.

On voit, par ce qui précède, quelles opérations il faudrait faire dans tous les cas; car si l'équation proposée contenait n inconnues, on la réduirait toujours à une autre qui en aurait $n - 1$ seulement.

Maintenant il et clair que toute la théorie des nombres se ramène au problème de l'élimination; puisqu'il suffirait d'éliminer toutes les inconnues entre les équations

$$\varphi(x, y, z, \ldots \text{ etc.}) = 0, \quad X = 0, \quad Y = 0, \quad Z = 0, \ldots \text{ etc.},$$

que nous avons établies précédemment, pour trouver l'équation de condition $F = 0$, qui renferme la resolution de l'équation proposée. L'élimination générale entre ces équations ne saurait s'effectuer avec les méthodes connues; il est vrai que l'on pourrait substituer directement les valeurs des inconnues, mais il serait très-difficile de résoudre la question par cette voie. Pour la traiter avec quelque succès il faut recourir aux intégrales définies, et specialement aux integrales dont la valeur est indépendante des constantes qu'elles renferment. Mais nous nous réservons de

donner cette théorie générale dans une autre occasion, et nous nous bornerons pour le moment à considérer les équations dans lesquelles l'une des inconnues est élevée seulement aux premier degré, et que M. Gauss a nommées congruences; et nous déduirons d'une seule formule tout ce que l'on savait sur ce genre d'équations, et beaucoup d'autres résultats nouveaux. Cela nous fournira l'occasion de montrer un exemple des simplifications remarquables dont notre méthode est susceptible, lorsqu'on l'applique aux cas particuliers, et des artifices d'analyse dont il faut faire usage pour résoudre ce genre de questions.

Soit proposé de resoudre l'équation

$$14. \quad \varphi(x, y, z, \ldots \text{etc.}) - pu = 0;$$

dans laquelle φ exprime une fonction rationnelle et entière quelconque des nombres entiers x, y, z, ... etc., et u doit être un nombre entier. Il est clair que s'il existe des valeurs de $x, y, z, \ldots$ etc. plus grandes que p, qui résolvent l'équation proposée, il y en aura aussi d'autres qui seront comprises entre zéro et p; et ce seront ces dernières que nous considérerons toujours dans ce qui suit, à moins que nous n'indiquions spécialement le contraire. A présent l'on sait que l'équation (14.) équivaut, d'après la notation de M. Gauss, à la congruence

$$\varphi(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{p}.$$

En supposant, pour simplifier le problème, que cette congruence se réduise à la forme

$$X = x^m + A_1 x^{m-1} + A_2 x^{m-2} \ldots + A_{m-1} x + A_m \equiv 0 \pmod{p},$$

(les coefficiens A_1, A_2, ... A_m étant toujours des nombres entiers et p étant un nombre entier) si elle a une racine entière $x = a_1$, on pourra toujours la mettre sous la forme $(x - a_1) X_1 \equiv 0 \pmod{p}$, X_1 étant un polynome entier en x du degré $m-1$; il résulte de là que la congruence $X \equiv 0 \pmod{p}$ ne peut avoir, tout au plus, qu'un nombre m de racines entières moindres que p, m étant le nombre qui exprime le degré du polynome X; et que si elle a les m racines entières

$$a_1, a_2, a_3, \ldots a_m,$$

on pourra faire

$$X \equiv (x - a_1)(x - a_2)(x - a_3) \ldots (x - a_m) \equiv 0 \pmod{p},$$

et on aura les congruences

$$15.\quad \left\{\begin{array}{l} a_1 + a_2 + a_3 \ldots\ldots + a_m \equiv -A_1 \pmod{p}, \\ \left\{\begin{array}{l} a_1a_2 + a_1a_3 \ldots\ldots + a_1a_m \\ + a_2a_3 + a_2a_4 \ldots\ldots + a_2a_m \\ \ldots\ldots\ldots\ldots\ldots + \text{etc.} \end{array}\right\} \equiv +A_2 \pmod{p}, \\ \left\{\begin{array}{l} a_1a_2a_3 + a_1a_2a_4 \ldots\ldots + a_1a_2a_m \\ + a_2a_3a_4 + a_2a_3a_5 \ldots\ldots + a_2a_3a_m \\ \ldots\ldots\ldots\ldots\ldots + \text{etc.} \end{array}\right\} \equiv -A_3 \pmod{p}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_1a_2a_3 \ldots\ldots\ldots\ldots a_m \equiv \pm A_m \pmod{p}. \end{array}\right.$$

Dans cette dernière congruence il faudra prendra le signe + si m est un nombre pair, et le signe — si m est un nombre impair.

Pour trouver la somme des puissances r^{mes} des racines de la congruence $X \equiv 0 \pmod{p}$, on aura des formules semblables à celles que l'on obtient pour les équations algébriques; car en appellant P_r, P_{r-1}, P_{r-2}, etc., la somme des puissances r^{mes}, $(r-1)^{\text{mes}}$, $(r-2)^{\text{mes}}$, etc., de ces racines on aura

$$P_r + A_1 P_{r-1} + A_2 P_{r-2} \ldots + r A_r \equiv 0 \pmod{p}.$$

On peut de la même manière transformer les congruences et obtenir leurs fonctions symétriques. En général étant proposé de trouver une fonction symétrique donnée φ, des racines de la congruence $X \equiv 0 \pmod{p}$, qui à toutes ses racines entières, on cherchera la même fonction symétrique dans l'équation $X = 0$, et en exprimant dans l'équation la valeur de cette fonction par $\varphi = S$, on sera assuré que pour la congruence on aura

$$\varphi \equiv S \pmod{p}.$$

Soit maintenant proposé de résoudre la congruence

$$x^p - x \equiv 0 \pmod{p},$$

dans laquelle p est un nombre premier. Si l'on cherche une transformée en y dont les racines surpassent de l'unité celles de la proposée, on aura $y = x + 1$, et partant $x = y - 1$; d'où l'on déduira

$$(y-1)^p - (y-1) \equiv 0 \pmod{p}$$

et par suite, en négligeant les multiples de p,

$$y^p - y \equiv 0 \pmod{p}.$$

Mais comme cette dernière congruence est identique avec la proposée, il en résulte que celle-ci ayant la racine $x = a$, aura de même la racine $x = a + 1$, et par conséquent l'autre $x = a + 2$: et qu'en général elle

sera résolue par toutes les valeurs de x de la forme $a + z$; z étant un nombre entier positif quelconque: et puisque en faisant $x = 0$, on satisfait à la congruence proposée, elle aura pour racines tous les nombres naturels. Par conséquent la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

aura pour racines tous les nombres 1, 2, 3, ... $p-1$; ce qui forme le théorème de Fermat.

La congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

dans laquelle p est un nombre premier, étant comparé à l'autre

$$x^m + A_1 x^{m-1} + A_2 x^{m-2} \ldots + A_{m-1} x + A_m \equiv 0 \pmod{p},$$

que nous avons déjà considérée, donne

$$A_1 = 0,\ A_2 = 0,\ \ldots\ A_{m-1} = 0,\ A_m = -1;$$
$$m = p-1;\ a_1 = 1,\ a_2 = 2,\ \ldots\ a_m = p-1;$$

et par conséquent, en substituant les valeurs des racines $a_1, a_2, a_3, \ldots \ldots a_m$, dans les congruences (15.), on aura

$$1 + 2 + 3 \ldots\ldots + p-1 \equiv 0 \pmod{p},$$
$$\left\{\begin{array}{l} 1.2 + 1.3 \ldots\ldots + 1.(p-1) \\ + 2.3 + 2.4 \ldots\ldots + 2.(p-1) \\ \ldots\ldots\ldots\ldots\ldots + \text{etc.} \end{array}\right\} \equiv 0 \pmod{p},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}$$

et enfin

$$1.2.3 \ldots\ldots (p-1) + 1 \equiv 0 \pmod{p},$$

puisque $p-1$ est un nombre pair *). Cette dernière congruence équivaut au théorème de Wilson.

Si l'on voulait trouver un nombre z tel qu'en faisant le produit de tous les nombres inférieurs à p (p étant un nombre premier) moins le facteur g, on eût

$$1.2.3 \ldots\ldots (g-1)(g+1) \ldots\ldots (p-1) + z \equiv 0 \pmod{p},$$

on devrait chercher à déterminer les coefficiens de la congruence

$$x^{p-2} + \alpha x^{p-3} + \beta x^{p-4} \ldots\ldots + z \equiv 0 \pmod{p},$$

qui a pour racines tous les nombres entiers inférieurs à p, excepté le nombre g: à cet effet on divisera la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

par $x - g$, et le dernier terme du quotient sera le nombre z.

---

*) Si le nombre premier p était égal à 2, $p-1$ ne serait plus un nombre pair; mais alors on aurait identiquement

$$1 + 1 \equiv 0 \pmod{2}$$

En effectuant la divison l'on trouvera

$$\frac{x^{p-1}-1}{x-g} = x^{p-2}+g\,x^{p-3}+g^2x^{p-4}\ldots.+g^{p-3}x+g^{p-2}+\frac{g^{p-1}-1}{x-g} \equiv 0 \text{ (mod. } p),$$

et puisque $g^{p-1}-1 \equiv 0$ (mod. p), on obtiendra

$$\frac{x^{p-1}-1}{x-g} \equiv x^{p-2}+g\,x^{p-3}\ldots\ldots+g^{p-3}x+g^{p-2} \equiv 0 \text{ (mod. } p),$$

en partant

$$1.2.3\ldots.(g-1)\,(g+1)\ldots.(p-2)\,(p-1)+g^{p-2} \equiv 0 \text{ (mod. } p).$$

En faisant dans cette congruence $g=1$, on retrouve le théorème de Wilson qui est un cas particulier de celui-ci.

On pourrait déduire de là tous les théorèmes que M. Gauss a insérés dans la troisième section de ses Recherches arithmétiques, et beaucoup d'autres propositions nouvelles. Si l'on prend, par exemple, la somme des puissances n^{mes} des racines de la congruence

$$x^{p-1}-1 \equiv 0 \text{ (mod. } p),$$

on trouve que, p étant un nombre premier, on aura toujours

$$1+2^n+3^n\ldots.+(p-1)^n \equiv 0 \text{ (mod. } p),$$

lorsque n n'est pas divisible par $p-1$; tandis que si n est un multiple de $p-1$, on obtiendra

$$1+2^n+3^n\ldots.+(p-1)^n \equiv -1 \text{ (mod. } p).$$

M. Poinsot a démontré que les racines de la congruence

$$x^n-1 \equiv 0 \text{ (mod. } np+1),$$

dans laquelle $np+1$ est un nombre premier, se déduisent des racines de l'équation $x^n-1=0$, en ajoutant des multiples de $np+1$ sous les radicaux compris dans l'expression de ces racines: mais cette proposition n'est qu'un cas particulier d'un théorème plus général que nous allons démontrer. En effet la congruence

$$x^n+A_1x^{n-1}\ldots.+A_{n-1}x+A_n \equiv 0 \text{ (mod. } p),$$

dans laquelle p est un nombre quelconque, équivaut à l'équation à deux inconnues

$$x^n+A_1x^{n-1}\ldots.+A_{n-1}x+(A_n-py) = 0,$$

dont les racines sont exprimées par une formule de la forme

$$x = \varphi(A_1, A_2, \ldots.A_{n-1}, A_n-py),$$

qui se réduit à l'expression des racines de l'équation

$$x^n+A_1x^{n-1}\ldots.+A_{n-1}x+A_n = 0,$$

lorsqu'on y fait $y=0$. Si donc *vice-versâ* l'on ajoute des multiples de p sous les radicaux compris dans l'expression des racines de cette équa-

tion (en écrivaut partout $A_n - py$, au lieu d'A_n), on aura les racines de la congruence proposée.

En appliquant aux congruences ce que nous avons dit en général des équations à plusieurs inconnues en nombres entiers, on trouve que toutes les solutions inégales et moindres que p de la congruence

$$\varphi(x, y, z, \ldots \text{etc.}) = \Phi \equiv 0 \pmod{p},$$

sont comprises parmi les racines des congruences

$$X = x(x-1)(x-2)\ldots(x-(p-1)) \equiv 0 \pmod{p},$$
$$Y = y(y-1)(y-2)\ldots(y-(p-1)) \equiv 0 \pmod{p},$$
$$Z = z(z-1)(z-2)\ldots(z-(p-1)) \equiv 0 \pmod{p},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.};$$

et qu'en éliminant toutes les variables entre les congruences

$\Phi \equiv 0 \pmod{p}$, $X \equiv 0 \pmod{p}$, $Y \equiv 0 \pmod{p}$, $Z \equiv 0 \pmod{p}$, ... etc.,

on obtiendra une congruence de condition qui devra être satisfaite afin que la congruence proposée soit résoluble: de manière qu'au lieu d'avoir l'équation de condition $C = 0$, comme pour les équations, on aura la congruence de condition $C \equiv 0 \pmod{p}$, et l'expression qui aurait dû se réduire à zéro dans le premier cas, devra être divisible par p dans le second. Lorsque p est un nombre premier, la question se simplifie beaucoup, car par le théorème de Fermat on aura

$$x(x-1)(x-2)\ldots(x-(p-1)) \equiv x^p - x \equiv 0 \pmod{p},$$
$$y(y-1)(y-2)\ldots(y-(p-1)) \equiv y^p - y \equiv 0 \pmod{p},$$
$$z(z-1)(z-2)\ldots(z-(p-1)) \equiv z^p - z \equiv 0 \pmod{p},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.},$$

et l'on devra éliminer les inconnues entre les congruences

$$\Phi \equiv 0 \pmod{p}, \quad x^p - x \equiv 0 \pmod{p}, \quad y^p - y \equiv 0 \pmod{p},$$
$$z^p - z \equiv 0 \pmod{p}, \ldots\ldots \text{etc.},$$

pour avoir la congruence de condition.

Si dans la congruence

$$\Phi \equiv 0 \pmod{p}$$

on cherchait seulement les racines différentes de zéro, on devrait éliminer les inconnues entre cette congruence et les suivantes

$x^{p-1} - 1 \equiv 0 \pmod{p}$, $y^{p-1} - 1 \equiv 0 \pmod{p}$, $z^{p-1} - 1 \equiv 0 \pmod{p}$, ... etc.,

et comme les racines congrues à zéro peuvent se trouver séparément avec facilité, nous supposerons, dans ce qui suit, que l'on cherche les racines différentes de zéro; ce qui simplifiera beaucoup nos recherches.

Il est clair, d'après ce que nous avons démontré sur les fonctions symétriques des congruences, qu'étant proposé d'éliminer les inconnues entre les congruences

$$\Phi = \varphi(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{p},$$
$$\Phi_1 = \varphi_1(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{p},$$
$$\Phi_2 = \varphi_2(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{p},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.},$$

on pourra effectuer l'élimination entre les équations

$$\Phi = 0, \quad \Phi_1 = 0, \quad \Phi_2 = 0, \ldots\ldots \text{etc.},$$

pourvu qu'au lieu de l'équation $F = 0$, qui résultera de cette élimination, on écrive

$$F \equiv 0 \pmod{p}.$$

Pour faire quelques applications de ce principe, soit proposé de résoudre la congruence

$$Ax + B \equiv 0 \pmod{p};$$

il est évident que si A et p ont un facteur commun, qui ne divise point B, cette congruence ne pourra pas se résoudre; et comme lorsque ce facteur commun existe et divise B, on peut toujours l'ôter, on pourra supposer que A et p sont premiers entre eux; et en faisant $x = Bz$, on aura

$$B(Az + 1) \equiv 0 \pmod{p};$$

et il faudra resoudre la congruence

$$Az + 1 \equiv 0 \pmod{p}.$$

Maintenant si l'on décompose p dans tous ses facteurs premiers, égaux ou inégaux, de manière que l'on ait

$$p = a.b.c\ldots\ldots n,$$

on devra résoudre la congruence

$$Az + 1 \equiv 0 \pmod{a.b.c\ldots\ldots n},$$

qui se change dans la suivante

$$Ay - 1 \equiv 0 \pmod{a.b.c\ldots\ldots n},$$

en faisant $z = -y$.

En considérant la congruence

$$Ay - 1 \equiv 0 \pmod{a},$$

il faudra éliminer entre celle-ci et la suivante $y^{a-1} - 1 \equiv 0 \pmod{a}$, qui équivaut à l'autre

$$A^{a-1} y^{a-2} - 1 \equiv 0 \pmod{a};$$

puisque par supposition a est un nombre premier qui ne divise point A: alors en divisant $A^{a-1} y^{a-2} - 1$, par $Ay - 1$, on obtiendra un quotient

exact; d'où l'on déduira que la congruence

$$Ay - 1 \equiv 0 \pmod{p},$$

est résolue en faisant

$$y = A^{a-2} s^{a-1} = Y_1;$$

en indiquant par s un nombre entier quelconque: on trouvera de même que toutes les congruences

$$Ay - 1 \equiv 0 \pmod{b}, \quad Ay - 1 \equiv 0 \pmod{c}, \quad \ldots\ldots \text{ etc.},$$

seront résolues en faisant successivement

$$y = A^{b-2} t^{b-1} = Y_2; \quad y = A^{c-1} u^{c-1} = Y_3; \quad \ldots\ldots \text{ etc.}$$

Il résulte de là que la congruence

$$(AY_1 - 1)(AY_2 - 1)(AY_3 - 1)\ldots\ldots \equiv 0 \pmod{a.b.c\ldots\ldots n},$$

et par suite l'autre

$$Y = (AY_1 - 1)^2 (AY_2 - 1)^2 (AY_3 - 1)^2 \ldots\ldots \equiv 0 \pmod{p},$$

seront toujours satisfaites: mais la valeur de Y étant composée d'un nombre pair de facteurs, pourra se réduire à la forme

$$Az + 1 \equiv 0 \pmod{p};$$

et puisque cette congruence est résoluble, l'autre

$$Ax + B \equiv 0 \pmod{p},$$

le sera de même, et on aura

$$x = \frac{B}{A}\left((A^{a-1} s^{a-1} - 1)^2 (A^{b-1} t^{b-1} - 1)^2 \ldots\ldots (A^{n-1} v^{n-1} - 1)^2 - 1\right),$$

pour une de ses racines; en observant que l'on peut prendre pour $s, t, \ldots \ldots v$, des nombres entiers quelconques. En général toutes les solutions possibles de la congruence proposée seront données par la formule

$$x = \frac{B}{A}\left((A^{a-1} - 1)(A^{b-1} - 1)\ldots\ldots(A^{n-1} - 1)\right)^2 - \frac{B}{A} + pu,$$

dans laquelle u est un nombre entier quelconque.

Soit proposé maintenant de résoudre la congruence du second degré

$$x^2 + qx + r \equiv 0 \pmod{2p+1},$$

$2p+1$ étant un nombre premier; il est clair que si elle a une racine $x = A$, il y en aura une autre $x = B \equiv -q - A$, et partant si elle est résoluble il faudra qu'en divisant $x^{2p} - 1$, par $x^2 + qx + r$, le reste soit divisible par $2p+1$. A présent on doit remarquer que si α et β sont les deux racines de l'équation

$$x^2 + qx + r = 0,$$

on aura

$$x^2 + qx + r = (x - \alpha)(x - \beta),$$

et par conséquent

$$\frac{x^{2p}-1}{x^2+qx+r} = \frac{x^{2p}-1}{(x-\alpha)(x-\beta)} = \frac{x^{2p}-1}{(\beta-\alpha)(x-\beta)} + \frac{x^{2p}-1}{(\alpha-\beta)(x-\alpha)};$$

En effectuant la division, on trouvera généralement

$$\frac{x^{2p}-1}{x^2+qx+r} = \frac{x^{2p}-1}{(\beta-\alpha)(x-\beta)} + \frac{x^{2p}-1}{(\alpha-\beta)(x-\alpha)}$$

$$= x^{2p-2} + A_1 x^{2p-3} + A_2 x^{2p-4} \ldots + A_{2p-2} + \frac{1}{\beta-\alpha}\left(\frac{\beta^{2p}-1}{x-\beta}\right) + \frac{1}{\alpha-\beta}\left(\frac{\alpha^{2p}-1}{x-\alpha}\right),$$

les coefficiens A_1, A_2, ... etc. étant toujours des nombres entiers. Il faudra, par conséquent, qu'en réduisant les deux derniers termes au même dénominateur, la quantité

$$\frac{1}{\beta-\alpha}\left((x-\alpha)(\beta^{2p}-1) - (x-\beta)(\alpha^{2p}-1)\right)$$

qui sera le reste de la division, soit divisible par $2p-1$, et partant

$$\left(\frac{\beta^{2p}-\alpha^{2p}}{\beta-\alpha}\right)x - \alpha\beta\left(\frac{\beta^{2p-1}-\alpha^{2p-1}}{\beta-\alpha}\right) + \frac{\alpha-\beta}{\beta-\alpha} \equiv 0 \pmod{2p+1};$$

d'où l'on déduira les deux congruences de condition

16. $$\frac{\beta^{2p}-\alpha^{2p}}{\beta-\alpha} \equiv 0 \pmod{2p+1}; \quad \alpha\beta\left(\frac{\beta^{2p-1}-\alpha^{2p-1}}{\beta-\alpha}\right)+1 \equiv 0 \pmod{2p+1}.$$

On voit ici qu'après avoir effectué la division par $\beta-\alpha$, les premiers membres de ces deux congruences pourront toujours s'exprimer à l'aide des quantités q et r, puisqu'ils ne renferment que des fonctions symétriques des racines α et β: et d'ailleurs il est clair que l'on pourra toujours substituer au lieu de α et β, les quantités

$$\frac{-q+\sqrt{(q^2-4r)}}{2}; \quad \frac{-q-\sqrt{(q^2-4r)}}{2}.$$

Si dans la congruence

$$x^2 + qx + r \equiv 0 \pmod{2p+1},$$

on fait $q=0$, $r=-s$; on devra dans les congruences (16.) faire $\alpha+\beta=0$, et partant $\alpha=-\beta$; mais l'on a aussi $\beta=\sqrt{s}$, $\alpha=-\sqrt{s}$, $\beta-\alpha=2\sqrt{s}$, $\beta\alpha=-s$; par conséquent les deux congruences (16.) se reduiront aux suivantes

$$\frac{\beta^{2p}-\beta^{2p}}{2\sqrt{s}} \equiv 0 \pmod{2p+1}; \quad -s\sqrt{s}\left(\frac{s^{p-1}-s^{p-1}}{2\sqrt{s}}\right)+1 \equiv 0 \pmod{2p+1};$$

dont la première est toujours satisfaite, et la seconde se réduit à l'autre

17. $$s^p - 1 \equiv 0 \pmod{2p+1};$$

qui est la condition déjà connue pour la résolution de la congruence

$$x^2 - s \equiv 0 \pmod{2p+1}.$$

Soit proposé, par exemple, de trouver la condition qui doit être satisfaite afin que la congruence $x^2+1\equiv 0 \pmod{2p+1}$, dans laquelle $2p+1$ est un nombre premier, soit résoluble; on devra faire $s=-1$, dans la congruence de condition (17.), et on aura

$$(-1)^p-1 \equiv 0 \pmod{2p+1};$$

ce qui montre que p doit être un nombre pair.

En appliquant aux congruences du second degré les mêmes principes dont nous avons fait usage pour résoudre celles du premier degré, on pourrait trouver la résolution générale de la congruence

$$x^2+qx+r \equiv 0 \pmod{p},$$

dans laquelle p est un nombre quelconque, pourvu que l'on connût tous les facteurs premiers de p.

En général étant proposée une congruence d'un degré quelconque

$$X = x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots\ldots + a_{n-1} x + a_n \equiv 0 \pmod{p},$$

dans laquelle p est un nombre premier, on divisera $x^{p-1}-1$ par X (en faisant usage de la même méthode dont nous nous sommes servis pour les congruences du second degré) et on obtiendra un reste de la forme

$$X_1 = b_1 x^{n-1} + b_1 x^{n-2} \ldots\ldots + b_{n-1} x + b_n .$$

Maintenant si la congruence proposée a n racines entières, on devra avoir les n congruence de condition

$$b_1 \equiv 0 \pmod{p}, \quad b_2 \equiv 0 \pmod{p}, \ldots\ldots \quad b_n \equiv 0 \pmod{p},$$

et on sera assuré que si elles sont satisfaites, la congruence $X \equiv 0 \pmod{p}$, aura toutes ses racines entières; mais si cette congruence n'avait qu'un nombre $n-m$ de racines entières, alors on devrait chercher de nouveau le plus grand commun diviseur etre X et X_1, et on trouverait enfin pour reste une congruence de la forme

$$X_2 = c_1 x^{n-m-1} + c_2 x^{n-m-2} \ldots\ldots + c_{n-m} \equiv 0 \pmod{p},$$

qui donnerait les congruences de condition

$$c_1 \equiv 0 \pmod{p}, \quad c_2 \equiv 0 \pmod{p}, \ldots\ldots \quad c_{n-m} \equiv 0 \pmod{p},$$

dont le nombre sera toujours égal au nombre des racines entières de la congruence proposée. On voit par là que la résolution d'une congruence du degré n, qui n'a que $n-m$ racines entières, se réduira à la résolution d'une congruence du degré $n-m$, en cherchant le plus grand commun diviseur entre X et $x^{p-1}-1$.

Soit proposé, par exemple, de résoudre la congruence

$$x^a - b \equiv 0 \pmod{ap+1},$$

dans laquelle $ap+1$ est un nombre premier, on divisera $x^{ap}-1$ par x^a-b, et on trouvera un quotient N et le reste b^p-1; d'où il résulte que si la congruence

$$18. \quad b^p-1 \equiv 0 \pmod{ap+1}$$

est résoluble, la congruence proposée aura toutes ses racines entières.

Les deux congruences de condition (17.) et (18.) avaient été trouvées par Fermat, mais avec sa méthode on ne pouvait pas trouver les conditions qui devaient être satisfaites, lorsque les congruences proposées n'étaient pas binomes: ce qu'on peut toujours effectuer par les principes que nous venons d'exposer.

La congruence de condition (18.) montre que la congruence

$$x^3-1 \equiv 0 \pmod{6p+1},$$

a toujours trois racines entières lorsque $6p+1$ est un nombre premier; mais comme il est évident qu'une de ces racines est $x=1$, on pourra diviser par $x-1$, et on obtiendra la congruence du second degré

$$x^2+x+1 \equiv 0 \pmod{6p+1},$$

qui aura ses deux racines entières; il faudra par conséquent que les deux congruences (16.) soient satisfaites quand on substitue pour α et β les deux racines de l'équation $x^2+x+1=0$, et que l'on change $2p+1$ en $6p+1$. Maintenant on a

$$\beta = -\tfrac{1}{2}(1+\sqrt{(-3)}); \quad \alpha = -\tfrac{1}{2}(1-\sqrt{(-3)});$$

et partant, la congruence $\frac{\beta^{6p}-\alpha^{6p}}{\beta-\alpha} \equiv 0 \pmod{6p+1}$ deviendra la suivante:

$$\frac{1}{2^{6p}\sqrt{(-3)}}\left((1+\sqrt{(-3)})^{6p}-(1-\sqrt{(-3)})^{6p}\right) \equiv 0 \pmod{6p+1},$$

qui donnera en développant

$$\frac{1}{2^{6p}\sqrt{(-3)}}\left\{\begin{array}{l} 1+6p\sqrt{(-3)}-\frac{6p(6p-1)}{2}.3-\frac{6p(6p-1)(6p-2)}{2.3}.3\sqrt{(-3)}+\frac{6p(6p-1)(6p-2)(6p-3)}{2.3.4}.3^2+\text{etc.} \\ -1+6p\sqrt{(-3)}+\frac{6p(6p-1)}{2}.3-\frac{6p(6p-1)(6p-2)}{2.3}.3\sqrt{(-3)}-\frac{6p(6p-1)(6p-2)(6p-3)}{2.3.4}.3^2+\text{etc.} \end{array}\right.$$

$$= \frac{1}{2^{6p-1}}\left(6p-\frac{6p(6p-1)(6p-2)}{2.3}.3+\frac{6p(6p-1)(6p-2)(6p-3)(6p-4)}{2.3.4.5}.3^2-\text{etc.}\right) \equiv 0 \pmod{6p+1};$$

et par conséquent

$$19. \quad 6p-\frac{6p(6p-1)(6p-2)}{2.3}.3+\frac{6p(6p-1)(6p-2)(6p-3)(6p-4)}{2.3.4.5}.3^2-\text{etc.} \equiv 0 \pmod{6p+1}.$$

Si l'on substitue les valeurs de α et β dans la congruence

$$\alpha\beta\left(\frac{\beta^{6p-1}-\alpha^{6p-1}}{\beta-\alpha}\right)+1 \equiv 0 \pmod{6p+1},$$

on aura, après avoir développé, la congruence

$$20.\quad (6p-1)-\frac{(6p-1)(6p-2)(6p-3)}{2\,.\,3}.3+\frac{(6p-1)(6p-2)(6p-3)(6p-4)(6p-5)}{2\,.\,3\,.\,4\,.\,5}.3^2-\text{etc.}\ldots.-2^{6p-2}\equiv 0\,(\text{mod. } 6p+1).$$

Les deux congruences (19.) et (20.), que nous venons de trouver, et qui doivent toujours être satisfaites en même tems, lorsque $6p+1$ est un nombre premier, renferment un théorème exclusif et assez curieux, sur les nombres premiers de la forme $6p+1$.

A présent si l'on effectue l'élimination de $6p$, entre la congruence

$$6p-\frac{6p(6p-1)(6p-2)}{2\,.\,3}.3+\frac{6p(6p-1)(6p-2)(6p-3)(6p-4)}{2\,.\,3\,.\,4\,.\,5}.3^2-\text{etc.}\equiv 0\ (\text{mod. } 6p+1),$$

et l'autre, qui est toujours résoluble:

$$6p+1\equiv 0\quad (\text{mod. } 6p+1)$$

on trouvera, après les réductions,

$$-1+\frac{1.2.3}{1.2.3}.3-\frac{1.2.3.4.5}{1.2.3.4.5}.3^2+\ldots.\mp 3^{3p-1}$$

$$\equiv -1+3-3^2\ldots.\mp 3^{3p-1}\equiv\frac{(-3)^{3p}-1}{4}\equiv(-3)^{3p}-1\equiv 0\ (\text{mod. } 6p+1).$$

Lorsque $p=2n$, cette dernière congruence deviendra

$$3^{6n}-1\equiv 0\quad (\text{mod. } 12n+1),$$

et celle-ci sera toujours résoluble d'après ce qui précède: d'où il résulte, par la congruence de condition (17.), que la congruence $x^2-3\equiv 0$ (mod. $12n+1$) est toujours résoluble lorsque $12n+1$ est un nombre premier. On pourrait appliquer les mêmes principes à des congruences de degrés plus élevés, et on obtiendrait un grand nombre de théorèmes nouveaux, du même genre que ceux que nous venons d'énoncer; mais ces recherches nous écarteraient trop de notre but, et nous allons exposer de préférence quelques applications de la théorie des congruences à la résolution d'une classe d'équations indéterminées dont Lagrange a considéré les plus simples.

Soit proposé de résoudre en nombres entiers l'équation

$$y=\frac{a+a_1x+a_2x^2\ldots.+a_nx^n}{e+e_1x+e_2x^2\ldots.+e_mx^m}=\frac{X}{X_1};$$

on voit facilement que ce problème se réduit à la résolution de la congruence $X\equiv 0$ (mod. X_1); mais comme on a aussi identiquement $X_1\equiv 0$ (mod. X_1), on pourra éliminer x entre ces deux congruences et on trouvera, après l'élimination, une congruence de condition $D\equiv 0$ (mod. X_1), dans laquelle D sera une fonction donnée des coefficiens

$$a,\ a_1,\ a_2,\ldots.\ a_n;\quad e,\ e_1,\ e_2,\ldots.\ e_m;$$

et il faudra que X_1 divise le nombre D. Maintenant supposons que tous les diviseurs, positifs ou négatifs, de D soient représentés par la série des nombres

$$1,\ d_1,\ d_2,\ d_3,\ \ldots\ldots\ d_s,\ D;$$

on devra faire successivement

$$X_1 = 1;\quad X_1 = d_1;\quad X_1 = d_2;\quad \ldots,\quad X_1 = d_s;\quad X_1 = D;$$

et en cherchant les racines entières de ces équations, on aura toutes les valeurs de x qui résolvent la congruence $X \equiv 0 \pmod{X_1}$, et par suite l'équation

$$y = \frac{a + a_1 x + a_2 x^2 \ldots\ldots + a_n x^n}{e + e_1 x + e_2 x^2 \ldots\ldots + e_m x^m} = \frac{X}{X_1}.$$

Etant donnée la même fraction $\frac{X}{X_1}$, on peut trouver aussi tous les nombres entiers qui, pour une même valeur de x, divisent à la fois le numérateur et le dénominateur. En effet si l'on représente en général par δ l'un de ces facteurs communs, on aura $X \equiv 0 \pmod{\delta}$; $X_1 \equiv 0 \pmod{\delta}$; et en éliminant x entre ces deux congruences (ou ce qui revient au même entre les deux équations $X = 0$, $X_1 = 0$), on aura la congruence de condition $D \equiv 0 \pmod{\delta}$, et le nombre δ devra se trouver parmi les diviseurs de D. Il est clair que si X et X_1 avaient une racine commune α, il faudrait commencer par diviser ces deux polynomes par $x - \alpha$, autrement on aurait toujours $D = 0$.

Etant données les deux fonctions à deux inconnues $\varphi(x, y)$; $F(x, y)$; si elles ont un facteur commun δ, on aura toujours

$$\varphi(x, y) \equiv 0 \pmod{\delta};\quad F(x, y) \equiv 0 \pmod{\delta};$$

et en éliminant x ou y entre ces deux congruences, on aura deux autres congruences de la forme

$$\Psi(x) \equiv 0 \pmod{\delta};\quad \Psi_1(y) \equiv 0 \pmod{\delta}.$$

Soit proposé maintenant de résoudre en nombres entiers les deux équations simultanées

$$\varphi(x, y) = F(x, y) \cdot \psi(x, y, z);\quad \Phi(x, y) = 0;$$

que nous exprimerons pour abréger par $\varphi = F.\psi$; $\Phi = 0$; on pourra les réduire aux congruences

$$\varphi \equiv 0 \pmod{F};\quad \Phi \equiv 0 \pmod{F};\quad F \equiv 0 \pmod{F};$$

et en éliminant x et y entre ces trois congruences, on aura la congruence de condition

$$D \equiv 0 \pmod{F},$$

d'où l'on déduira toutes les valeurs possibles de F: l'on aura ainsi trois équations et trois inconnues, et les deux équations proposées seront résolues complètement.

Etant proposées les deux équations simultanées

$$\Phi(x, z) = \varphi(x, z).F(x, y, z); \quad \Phi_1(x, z) = \varphi(x, z).F_1(x, y, z);$$

que nous indiquerons, pour abréger, par

$$\Phi = \phi.F; \quad \Phi_1 = \varphi.F_1;$$

elles se transformeront dans les congruences

$$\Phi \equiv 0 \pmod{\varphi}; \quad \Phi_1 \equiv 0 \pmod{\varphi}; \quad \varphi \equiv 0 \pmod{\varphi};$$

d'où l'on déduira, par l'élimination, la congruence de condition $D \equiv 0 \pmod{\varphi}$, qui fournira toutes les valeurs possibles de φ; et l'on aura résolu complètement les deux équations proposées. On pourrait appliquer ces principes à des équations contenant un plus grand nombre d'inconnues; mais nous traiterons séparément cette matière dans un mémoire particulier sur les congruences à module variable.

En reprenant les congruences de condition, que nous avons données précédemment, il est clair que l'on pourra éliminer les inconnues entre la congruence à plusieurs inconnues

$$\varphi(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{p},$$

(dans laquelle p est un nombre premier) que nous indiquerons pour abréger par $\varphi \equiv 0 \pmod{p}$, et les suivantes

$x^{p-1} - 1 \equiv 0 \pmod{p}$; $y^{p-1} - 1 \equiv 0 \pmod{p}$; $z^{p-1} - 1 \equiv 0 \pmod{p}$; ... etc.;

de la même manière que s'il s'agissait d'éliminer entre les équations

$$\varphi = 0; \quad x^{p-1} - 1 = 0; \quad y^{p-1} - 1 = 0; \quad z^{p-1} - 1 = 0; \ldots \text{etc.};$$

et que le résultat sera de la même forme: à présent pour éliminer les inconnues entre ces équations, on peut substituer dans la première toutes les valeurs de $x, y, z, \ldots$ etc., déduites des autres équations, et comme l'on a

$$x = 1; \quad x = \cos\frac{2\pi}{p-1} + \sqrt{(-1)}\sin\frac{2\pi}{p-1}; \quad x = \cos\frac{4\pi}{p-1} + \sqrt{(-1)}\sin\frac{4\pi}{p-1};$$
$$\ldots\ldots x = \cos\frac{2(p-2)\pi}{p-1} + \sqrt{(-1)}\sin\frac{2(p-2)\pi}{p-1};$$
$$y = 1; \quad y = \cos\frac{2\pi}{p-1} + \sqrt{(-1)}\sin\frac{2\pi}{p-1}; \quad y = \cos\frac{4\pi}{p-1} + \sqrt{(-1)}\sin\frac{4\pi}{p-1};$$
$$\ldots\ldots y = \cos\frac{2(p-2)\pi}{p-1} + \sqrt{(-1)}\sin\frac{2(p-2)\pi}{p-1};$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.};$$

en substituant l'une après l'autre toutes ces valeurs dans l'équation $\varphi = 0$, et faisant le produit de toutes les fonctions semblables que l'on obtiendra de cette manière, on trouvera la congruence de condition

$$e^{\sum_{x=0}^{x=p-1}\sum_{y=0}^{y=p-1}\sum_{z=0}^{z=p-1} \ldots \log\varphi\left(\cos\frac{2x\pi}{p-1}+\sqrt{(-1)}\sin\frac{2x\pi}{p-1},\ \cos\frac{2y\pi}{p-1}+\sqrt{(-1)}\sin\frac{2y\pi}{p-1},\ \cos\frac{2z\pi}{p-1}+\sqrt{(-1)}\sin\frac{2z\pi}{p-1},\ \ldots.\text{ etc.}\right)} \equiv 0 \pmod{p}.$$

Cette congruence paraît assez singulière à cause des fonctions circulaires qu'elle renferme; cependant en observant le rapport qui existe entre la congruence $a \equiv a + px \pmod{p}$, et l'équation $\cos\frac{a\pi}{p} = \cos\frac{(a+px)\pi}{p}$, lorsque a, p et x, sont des nombres entiers, on pourrait se rendre compte aisément de la forme de cette expression. On pourrait déduire de là plusieurs théorèmes connus sur les congruences; mais cette route serait longue et pénible, et nous préférons de partir d'une autre équation fondamentale qui servira à retrouver directement tout ce que l'on savait sur la théorie des congruences, et à découvrir beaucoup de propositions nouvelles. En observant que quoique par notre théorie on ne trouve que les racines inégales de la congruence $\varphi = 0$, on obtiendra cependant les racines égales par la méthode dont nous avons fait usage pour les équations indéterminées; et même on les trouvera directement en éliminant entre les congruences

$$\varphi \equiv 0 \pmod{p};\quad \frac{d\varphi}{dx} \equiv 0 \pmod{p};\quad \frac{d\varphi}{dy} \equiv 0 \pmod{p};\ \ldots\ldots \text{ etc.}$$

Etant donnée l'équation à une seule inconnue

$$x^m - 1 = 0,$$

si l'on représente par P_n, P_{n-m}, P_{n-2m}, ... etc., les sommes des puissances n^{mes}, $(n-m)^{\text{mes}}$, $(n-2m)^{\text{mes}}$, ... etc. de ses racines, on aura

$$P_n = P_{n-m} = P_{n-2m} \ldots\ldots = P_{n-\nu m} = \text{etc.};$$

de sorte que si n est un multiple de m, on obtient $P_n = m$; et dans le cas contraire on trouve $P_n = 0$. En exprimant les racines de l'équation $x^m - 1 = 0$, en fonctions circulaires, on aura

$$P_n = \begin{cases} \left(\cos\frac{0\pi}{m} + \sqrt{(-1)}\sin\frac{0\pi}{m}\right)^n + \left(\cos\frac{2\pi}{m} + \sqrt{(-1)}\sin\frac{2\pi}{m}\right)^n \ldots\ldots \\ + \left(\cos\frac{2u\pi}{m} + \sqrt{(-1)}\sin\frac{2u\pi}{m}\right)^n \ldots\ldots + \left(\cos\frac{2(m-1)\pi}{m} + \sqrt{(-1)}\sin\frac{2(m-1)\pi}{m}\right)^n. \end{cases}$$

Si l'on transforme le second membre au moyen de la relation connue

$$(\cos z + \sqrt{(-1)}\sin z)^n = \cos nz + \sqrt{(-1)}\sin nz,$$

et qu'on néglige les imaginaires qui, dans le cas actuel, doivent nécessai-

rement se détruire, on obtiendra

$$21.\quad P_n = \cos\frac{0n\pi}{m} + \cos\frac{2n\pi}{m} + \cos\frac{4n\pi}{m} \ldots + \cos\frac{2un\pi}{m} \ldots + \cos\frac{2(m-1)n\pi}{m}$$

$$= \sum_{u=0}^{u=m} \cos\frac{2un\pi}{m} = \frac{\sin 2\left(n-\frac{n}{2m}\right)\pi + \sin\frac{n\pi}{m}}{2\sin\frac{n\pi}{m}};$$

et la valeur de cette expression sera m ou zéro, suivant que le nombre $\frac{n}{m}$ sera entier ou fractionnaire.

Il résulte de là que si l'on prend successivement la somme des puissances n^{mes} des équations

$$x-1=0,\quad x^2-1=0,\quad x^3-1=0,\quad \ldots\ldots\quad x^m-1=0,$$

on aura la somme des diviseurs de n, compris dans les nombres 1, 2, 3, ... m; et cette somme pourra être représentée par la formule

$$\sum_{x=1}^{x=m+1}\sum_{y=0}^{y=x} \cos\frac{2nyn}{x} = \sum_{x=1}^{x=m+1} \frac{\sin 2\left(n-\frac{n}{2x}\right)\pi + \sin\frac{n\pi}{x}}{2\sin\frac{n\pi}{x}}.$$

On trouverait de même que le nombre des diviseurs de n, compris dans la série 1, 2, 3, ... m, est donné par l'expression

$$\sum_{x=1}^{x=m+1}\sum_{y=0}^{y=x} \frac{1}{x}\cos\frac{2nyn}{x} = \sum_{x=1}^{x=m+1} \frac{\sin 2\left(n-\frac{n}{2x}\right)\pi + \sin\frac{n\pi}{x}}{2x\sin\frac{n\pi}{x}}.$$

Si l'on voulait exprimer la somme et le nombre de tous les diviseurs de n, en représentant par $\int(n)$ la première de ces fonctions, et par $\delta(n)$ la seconde, on aurait

$$\int(n) = \sum_{x=1}^{x=n+1}\sum_{y=0}^{y=x} \cos\frac{2nyn}{x},$$

$$\delta(n) = \sum_{x=1}^{x=n+1}\sum_{y=0}^{y=x} \frac{1}{x}\cos\frac{2nyn}{x}.$$

On sait que lorsque n est un nombre premier, on a

$$\int(n) = n+1;\quad \delta(n) = 2;$$

nous aurons donc, en changeant les limites des variables, les deux équations

$$\sum_{x=1}^{x=n}\sum_{y=0}^{y=x} \cos\frac{2nyn}{x} = 1;\quad \sum_{x=1}^{x=n}\sum_{y=0}^{y=x} \frac{1}{x}\cos\frac{2nyn}{x} = 1;$$

qui renferment deux propriétés spéciales des nombres premiers.

On a vu que, n et m étant deux nombres entiers, la formule

$$\frac{\sin 2\left(n-\frac{n}{2m}\right)\pi+\sin\frac{n\pi}{m}}{2\sin\frac{n\pi}{m}}$$

a pour valeur m, si n est divisible par m, et qu'elle se réduit à zéro lorsque cette condition n'est pas satisfaite. Nous avons démontré de plus, que p étant un nombre premier, l'expression

$$\frac{1.2.3.....(p-1)+1}{p}$$

ne peut devenir un nombre entier que lorsque p est un nombre premier; en faisant donc

$$m=p, \quad \text{et} \quad n=1.2.3.....(p-1)+1,$$

dans la formule (21.), elle se transformera en celle-ci:

$$\frac{\sin 2\left(1.2.3....(p-1)+1-\frac{1.2.3....(p-1)+1}{2p}\right)\pi+\sin\left(\frac{1.2.3....(p-1)+1}{2p}\right)\pi}{2\sin\left(\frac{1.2.3....(p-1)+1}{2p}\right)\pi},$$

qui devient p lorsque p est un nombre premier, et qui se réduit à zéro dans le cas contraire. Ainsi cette formule représente exclusivement tous les nombres premiers. Si l'on voulait exprimer analytiquement la somme des nombres premiers compris dans la série

$$a, \quad a+1, \quad a+2, \ldots\ldots \quad a+b-1,$$

on aurait la formule

$$\sum_{x=a}^{x=a+b}\frac{\sin 2\left(1.2.3....(x-1)+1-\frac{1.2.3....(x-1)+1}{2x}\right)\pi+\sin\left(\frac{1.2.3....(x-1)+1}{2x}\right)\pi}{2\sin\left(\frac{1.2.3....(x-1)+1}{2x}\right)\pi}.$$

On peut généraliser beaucoup ces expressions, et les appliquer aux séries périodiques, aux fonctions discontinues et à d'autres recherches: mais ce que nous en venons de dire suffit pour le moment.

Puisque la formule

$$\frac{1}{m}\left\{\begin{array}{l}\left(\cos\frac{0\pi}{m}+\sqrt{(-1)}\sin\frac{0\pi}{m}\right)^n+\left(\cos\frac{2\pi}{m}+\sqrt{(-1)}\sin\frac{2\pi}{m}\right)^n....\\ .....+\left(\cos\frac{2(m-1)\pi}{m}+\sqrt{(-1)}\sin\frac{2(m-1)\pi}{m}\right)^n\end{array}\right\},$$

a pour valeur l'unité ou zéro, suivant que $\frac{n}{m}$ est un nombre entier ou fractionnaire, il s'en suit que le nombre N des racines inégales de la congruence à plusieurs inconnues

$$\varphi(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{m},$$

(que nous exprimerons pour abréger par $\varphi \equiv 0 \pmod{m}$) dans laquelle on considère pour x, y, z, ... etc., les valeurs entières

$$x = a,\ a+1,\ a+2,\ \ldots\ldots\ b;$$
$$y = c,\ c+1,\ c+2,\ \ldots\ldots\ d;$$
$$z = e,\ e+1,\ e+2,\ \ldots\ldots\ f;$$

sera donné par l'équation

$$22.\quad nN = \sum_{x=a}^{x=b}\sum_{y=c}^{y=d}\sum_{z=e}^{z=f}\ldots\left\{\begin{array}{l}\left(\cos\frac{0\varphi\pi}{m}+\sqrt{(-1)}\sin\frac{0\varphi\pi}{m}\right)+\left(\cos\frac{2\varphi\pi}{m}+\sqrt{(-1)}\sin\frac{2\varphi\pi}{m}\right)\ldots\ldots\\ +\left(\cos\frac{2u\varphi\pi}{m}+\sqrt{(-1)}\sin\frac{2u\varphi\pi}{m}\right)\ldots+\left(\cos\frac{2(m-1)\varphi\pi}{m}+\sqrt{(-1)}\sin\frac{2(m-1)\varphi\pi}{m}\right)\end{array}\right\}$$

qui peut servir dans plusieurs cas à trouver la valeur de l'intégrale définie

$$\sum_{x=a}^{x=b}\sum_{y=c}^{y=d}\sum_{z=e}^{z=f}\ldots\ldots\cos\frac{a\varphi(x, y, z, \ldots. \text{etc.})\pi}{m},$$

comme nous le montrerons dans la suite.

De même la somme des racines de la congruence $\varphi \equiv 0 \pmod{m}$, comprises entre les mêmes limites que celles qui ont servi à déterminer la formule (22.), sera donnée par l'intégrale

$$23.\quad \frac{1}{m}\sum_{x=a}^{x=b}\sum_{y=c}^{y=d}\sum_{z=e}^{z=f}\ldots.(x+y+z\ldots.+\text{etc.})\left\{\begin{array}{l}1+\left(\cos\frac{2\varphi\pi}{m}+\sqrt{(-1)}\sin\frac{2\varphi\pi}{m}\right)\ldots\ldots\\ \ldots.+\left(\cos\frac{2(m-1)\varphi\pi}{m}+\sqrt{(-1)}\sin\frac{2(m-1)\varphi\pi}{m}\right)\end{array}\right\}.$$

On pourrait trouver une infinité de formules du même genre; mais celles-ci suffisent déjà pour notre objet; et même elles sont trop générales, de manière qu'il faut les particulariser pour les appliquer avec facilité aux diverses questions que nous devrons résoudre.

Nous observerons d'abord que, d'après ce que nous avons dit précédemment, il suffira d'intégrer entre les limites

$$0 = x = y = z = \ldots\ldots\ \text{etc.},$$
$$m = x = y = z = \ldots\ldots\ \text{etc.},$$

pour savoir si la congruence proposée est ou n'est pas résoluble; et qu'ensuite les imaginaires devant se détruire entre eux, on pourra considérer l'intégrale

$$24.\quad \frac{1}{m}\sum_{x=0}^{x=m}\sum_{y=0}^{y=m}\sum_{z=0}^{z=m}\ldots.\left(1+\cos\frac{2\varphi\pi}{m}+\cos\frac{4\varphi\pi}{m}\ldots.+\cos\frac{2u\varphi\pi}{m}\ldots.+\cos\frac{2(m-1)\varphi\pi}{m}\right),$$

au lieu de celle fournie par l'équation (22.), et l'intégrale

$$25.\quad \frac{1}{m}\sum_{x=0}^{x=m}\sum_{y=0}^{y=m}\sum_{z=0}^{z=m}\ldots.(x+y+z\ldots.+\text{etc.})\left(1+\cos\frac{2\varphi\pi}{m}+\cos\frac{4\varphi\pi}{m}\ldots.+\cos\frac{2u\varphi\pi}{m}\ldots.+\cos\frac{2(m-1)\varphi\pi}{m}\right),$$

à la place de la formule (23.).

(La suite dans le cahier prochain.)