14.

Mémoire sur la théorie des nombres.

(Suite du mémoire No. 3. dans le cahier précédent.)

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

Soit proposé, par exemple, de trouver le nombre N des solutions entières positives et moindres que c, de la congruence

$$ax + b \equiv 0 \pmod{c},$$

la formule (24.) se changera, dans ce cas, dans la suivante

$$26.\quad \frac{1}{c}\sum_{x=0}^{x=c}\left(1+\cos 2(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2u(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2(c-1)(ax+b)\frac{\pi}{c}\right),$$

qui exprimera le nombre N cherché.

Si l'on considère le terme général de cette série, on aura l'équation

$$\frac{1}{c}\sum_{x=0}^{x=c}\cos 2u(ax+b)\frac{\pi}{c} = \frac{\sin 2u\left(b+ac-\frac{a}{2}\right)\frac{\pi}{c} - \sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c\sin\frac{ua\pi}{c}},$$

dans le second membre de laquelle le numérateur est toujours zéro, mais dont le dénominateur ne peut se réduire à zéro, que lorsque a et c ont un diviseur commun plus grand que l'unité, puisque u est toujours plus petit que c. Il résulte de là que si a et c sont premiers entre eux, tous les termes de la série (26.) s'évanouissent, excepté le premier dont la valeur se réduit à

$$\frac{1}{c}\sum_{x=0}^{x=c}1 = \frac{c}{c} = 1.$$

Mais si a et c ont un facteur commun g, on supposera $a = mg$; $c = ng$; et en faisant $u = n$, on obtiendra

$$\frac{1}{c}\sum_{x=0}^{x=c}\cos 2n(ax+b)\frac{\pi}{c} = \frac{\sin 2n\left(b+ac-\frac{a}{2}\right)\frac{\pi}{c} - \sin 2n\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c\sin\frac{na\pi}{c}}$$

$$= \frac{\sin 2\left(b+ang-\frac{a}{2}\right)\frac{\pi}{g} - \sin 2\left(b-\frac{a}{2}\right)\frac{\pi}{g}}{2ng\sin\frac{a\pi}{g}}.$$

Cette expression se réduit à $\frac{0}{0}$, en vertu de l'hypothèse $a = mg$. On devra donc différentier le numérateur et le dénominateur par rapport à a, pour avoir une valeur déterminée, et l'on trouvera après les réductions:

$$\frac{\sin 2\left(b+ang-\frac{a}{2}\right)\frac{\pi}{g}-\sin 2\left(b-\frac{a}{2}\right)\frac{\pi}{g}}{2ng\sin\frac{a\pi}{g}}=\cos\frac{2b\pi}{g}.$$

Si au lieu de prendre $u=n$, on fait en général $u=en$, e étant un nombre entier quelconque, on trouve

$$\frac{1}{c}\sum_{x=0}^{x=c}\cos en(ax+b)\frac{\pi}{c}=\cos\frac{2eb\pi}{g};$$

et comme le nombre n est compris $g-1$ fois dans $c-1$, on pourra faire successivement $e=0, 1, 2, 3, \ldots\, g-1$; et la valeur de l'intégrale (26.) sera exprimée (dans le cas actuel où l'on suppose que a et c ont un commun diviseur g) par la série

$$1+\cos\frac{2b\pi}{g}+\cos\frac{4b\pi}{g}\ldots\ldots+\cos\frac{2(g-1)b\pi}{g},$$

dont la somme

$$\frac{\sin 2\left(b-\frac{b}{2g}\right)\pi+\sin\frac{b\pi}{g}}{2\sin\frac{b\pi}{g}}$$

a pour valeur g, lorsque $\frac{b}{g}$ est un nombre entier, et qui se réduit à zéro dans le cas contraire.

De là résulte

1°. Que la congruence $ax+b\equiv 0$ (mod. c), a toujours une solution entière et plus petite que c, lorsque a et c n'ont d'autres diviseurs communs que l'unité.

2°. Que si a et c ont un commun diviseur g différent de l'unité, qui ne divise point b, cette congruence n'admet aucune solution entière.

3°. Qu'enfin si $\frac{b}{g}$ est un nombre entier, on trouvera pour x un nombre g de valeurs entières plus petites que c, qui satisfont à la congruence proposée.

Maintenant si l'on fait $\varphi=ax+b$, et $m=c$, dans l'intégrale (25.) on trouvera que la formule

27. $$\sum_{x=0}^{x=c}x\left(1+\cos 2(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2u(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2(c-1)(ax+b)\frac{\pi}{c}\right),$$

exprimera la somme des valeurs de x, entières et moindres que c, qui satisfont à la congruence $ax+b\equiv 0$ (mod. c), lorsqu'elle est résoluble, et que l'orsqu'elle ne l'est pas, cette intégrale se réduit à zéro.

Nous avons démontré que si a et c ont un facteur commun différent de l'unité, et qui ne divise pas b, la congruence $ax+b\equiv 0$ (mod. c) n'admet aucune solution entière; et comme, si ce facteur commun divise aussi b, on peut toujours le supprimer, il sera permis, dans ce cas, de supposer que a et c sont premiers entre eux; et alors on sera assuré qu'il existe toujours une valeur entière de x, comprise entre zéro et c, qui satisfait à la congruence proposée; mais comme il n'existe qu'une seule de ces valeurs, comprise entre les limites que nous venons d'indiquer, la formule (27.), qui exprime la somme des racines de la congruence

$$ax+b\equiv 0 \quad (\text{mod. } c),$$

aura pour valeur la plus petite de ces racines entières et positives.

Actuellement pour trouver cette valeur de x, on considèrera le terme général de l'intégrale (27.), et on aura

$$\frac{1}{c}\sum_{x=0}^{x=c} x\cos 2u(ax+b)\frac{\pi}{c} = \left\{\begin{array}{l} \dfrac{(c-1)\sin 2u\left(b+ca-\frac{a}{2}\right)\frac{\pi}{c}+\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c\sin\frac{ua\pi}{c}} \\ +\dfrac{\cos 2u\left(ca+b-a\right)\frac{\pi}{c}-\cos 2u(b-a)\frac{\pi}{c}}{c\left(2\sin\frac{ua\pi}{c}\right)^2} \end{array}\right\},$$

où il faudra faire successivement $u=1, 2, 3, \ldots. c-1$; et ajouter au résultat le premier terme de la série (27.), qui est

$$\frac{1}{c}\sum_{x=0}^{x=c} x = \frac{c(c-1)}{2c} = \frac{c-1}{2},$$

Puisque a et c sont premiers entre eux, et que u est plus petit que c, il s'en suit que le dénominateur $2c\sin\frac{ua\pi}{c}$ ne pourra jamais s'évanouir; on obtiendra par conséquent, en faisant les réductions nécessaires:

$$\frac{(c-1)\sin 2u\left(ac+b-\frac{a}{2}\right)\frac{\pi}{c}+\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c\sin\frac{ua\pi}{c}}+\frac{\cos 2u\left(ac+b-a\right)\frac{\pi}{c}-\cos 2u(b-a)\frac{\pi}{c}}{c\left(2\sin\frac{ua\pi}{c}\right)^2}$$

$$=\frac{\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{ua\pi}{c}};$$

et partant:

$$28.\quad \frac{1}{c}\sum_{x=0}^{x=c} x\left(1+\cos 2(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2u(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2(c-1)(ax+b)\frac{\pi}{c}\right)$$

$$=\left\{\begin{array}{l}\dfrac{c-1}{2}+\dfrac{\sin 2\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{a\pi}{c}}+\dfrac{\sin 4\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{2a\pi}{c}}\ldots\ldots\ldots\ldots \\ \qquad+\dfrac{\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{ua\pi}{c}}\ldots\ldots+\dfrac{\sin 2(c-1)\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin(c-1)\frac{a\pi}{c}}\end{array}\right\}$$

$$=\frac{c-1}{2}+\frac{1}{2}\sum_{u=1}^{u=c}\frac{\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{\sin\frac{ua\pi}{c}}=\alpha.$$

Cette formule très-simple donne pour α la plus petite valeur de x qui satisfasse à la congruence $ax+b\equiv 0$ (mod. c), en nombres entiers et positifs: mais toutes les valeurs entières de x sont données par l'équation

$$29.\quad x=\frac{c-1}{2}+\frac{1}{2}\sum_{u=1}^{u=c}\frac{\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{\sin\frac{ua\pi}{c}}+cz,$$

dans laquelle z est un nombre entier quelconque.

Il faut observer ici que la congruence

$$ax+b\equiv 0\quad(\text{mod. } c),$$

équivaut à l'équation du premier degré à deux inconnues

$$ax+b=cy;$$

et que la formule (29.) donnera toutes les valeurs de x qui résolvent cette équation.

Soit proposé, par exemple, de résoudre en nombres entiers l'équation $3x+1=4y$; en la comparant à l'équation générale $ax+c=cy$, on aura $a=3$, $b=1$, $c=4$; et par conséquent

$$\alpha=\frac{4-1}{2}+\frac{1}{2}\sum_{u=1}^{u=4}\frac{\sin 2u\left(1-\frac{3}{2}\right)\frac{\pi}{4}}{\sin\frac{3u\pi}{4}}=\frac{3}{2}-\frac{1}{2}\sum_{u=1}^{u=4}\frac{\sin\frac{u\pi}{4}}{\sin\frac{3u\pi}{4}},$$

c'est à dire

$$\alpha=\frac{3}{2}-\frac{\sin\frac{\pi}{4}}{2\sin\frac{3\pi}{4}}-\frac{\sin\frac{2\pi}{4}}{2\sin\frac{6\pi}{4}}-\frac{\sin\frac{3\pi}{4}}{2\sin\frac{9\pi}{4}}=\frac{3}{2}-\frac{1}{2}+\frac{1}{2}-\frac{1}{2}=1;$$

et toutes les valeurs de x, qui résolvent l'équation $3x+1=4y$, seront données par l'équation $x=1+4z$, comme on le sait d'ailleurs.

La valeur de α peut en général se calculer à l'aide des tables trigonométriques. Il est vrai que par ce moyen on n'obtiendra, le plus souvent, que des valeurs fractionnaires approchées, mais comme par supposition x ne peut avoir que des valeurs entières, on en trouvera la valeur exacte en substituant à cette valeur approchée, le nombre entier le plus voisin.

On peut observer que puisqu'on a

$$\frac{\sin\left(2b-a\right)\frac{u\pi}{c}}{\sin\frac{au\pi}{c}}=\frac{\sin\frac{2bu\pi}{c}\cos\frac{au\pi}{c}-\cos\frac{2bu\pi}{c}\sin\frac{au\pi}{c}}{\sin\frac{au\pi}{c}}$$

$$=\sin\frac{2bu\pi}{c}\cot\frac{au\pi}{c}-\cos\frac{2bu\pi}{c};$$

et que d'ailleurs

$$\sum_{u=1}^{u=c}\cos\frac{2bu\pi}{c}=-1;$$

on pourra écrire

$$\alpha=\frac{c-1}{2}+\frac{1}{2}\sum_{u=1}^{u=c}\sin\frac{2bu\pi}{c}\cot\frac{au\pi}{c}+\frac{1}{2}=\frac{1}{2}\left(c+\sum_{u=1}^{u=c}\sin\frac{2bu\pi}{c}\cot\frac{au\pi}{c}\right);$$

et cette expression servira, aussi bien que la précédente, à résoudre la congruence proposée.

Il serait aisé d'appliquer ces principes aux conguences du premier degré à plusieurs inconnues: mais nous allons passer de préférence aux congruences du second degré: et à cet effet nous rappellerons quelques propriétés élémentaires des résidus quadratiques, que nons pourrions déduire de nos formules générales, mais dont nous omettons les démonstration à cause de leur simplicité.

1°. Si n est un nombre premier, en élevant successivement au carré tous les nombres $1, 2, 3 \ldots\ldots n-1$; et divisant chaque carré par n, on aura $\frac{n-1}{2}$ restes différens (que M. Gauss a nommés résidus quadratiques de n) répétés chacun deux fois: et il restera, dans la série des nombres inférieurs à n, un nombre $\frac{n-1}{2}$ de non-résidus quadratiques.

2°. Si l'on fait $n=2p+1$, et que l'on représente par

$$a_1, a_2, a_3, \ldots\ldots a_u, \ldots\ldots a_p,$$

les p résidus quadratiques de n, et par

$$b_1, \; b_2, \; b_3, \; \ldots\ldots \; b_u, \; \ldots\ldots \; b_p,$$

les p non-résidus quadratiques, on aura les équations

$$\sum_{x=1}^{x=n} \cos\frac{2x^2\pi}{n} = 2\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n}; \quad \sum_{x=1}^{x=n} \sin\frac{2x^2\pi}{n} = 2\sum_{u=1}^{u=p+1} \sin\frac{2a_u\pi}{n};$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n} + \cos 2\frac{b_u\pi}{n}\right) = \sum_{y=1}^{y=n} \cos\frac{2y\pi}{n}; \quad \sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u\pi}{n} + \sin\frac{2b_u\pi}{n}\right) = \sum_{y=1}^{y=n} \sin\frac{2y\pi}{n}.$$

3°. En multipliant successivement un résidu quadratique quelconque a_r, par tous les autres, on aura la série

$$a_r a_1, \; a_r a_2, \; a_r a_3, \; \ldots\ldots \; a_r a_p,$$

qui fournira de nouveau, en divisant tous ses termes par n, p restes différens, qui seront tous les résidus quadratiques de n disposés dans un ordre quelconque; d'où l'on déduira

$$30. \quad \begin{cases} \sum_{x=1}^{x=n} \cos\frac{2a_r x^2\pi}{n} = 2\sum_{u=1}^{u=p+1} \cos\frac{2a_r a_u\pi}{n} = 2\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n}; \\ \sum_{x=1}^{x=n} \sin\frac{2a_r x^2\pi}{n} = 2\sum_{u=1}^{u=p+1} \sin\frac{2a_r a_u\pi}{n} = 2\sum_{u=1}^{u=p+1} \sin\frac{2a_u\pi}{n}. \end{cases}$$

4°. En multipliant le résidu quadratique a_r, successivement par tous les non-résidus quadratiques

$$b_1, \; b_2, \; b_3, \; \ldots\ldots \; b_u, \; \ldots\ldots \; b_p,$$

on aura de nouveau, après avoir divisé tous les produits par n, p restes différens, qui seront tous les non-résidus quadratiques de n, et on trouvera

$$31. \quad \begin{cases} \sum_{u=1}^{u=p+1} \cos\frac{2a_r b_u\pi}{n} = \sum_{u=1}^{u=p+1} \cos\frac{2b_u\pi}{n}; \\ \sum_{u=1}^{u=p+1} \sin\frac{2a_r b_u\pi}{n} = \sum_{u=1}^{u=p+1} \sin\frac{2b_u\pi}{n}. \end{cases}$$

5°. En multipliant le non-résidu quadratique b_r, successivement par tous les résidus quadratiques

$$a_1, \; a_2, \; a_3, \; \ldots\ldots \; a_u, \; \ldots\ldots \; a_p,$$

et divisant tous les produits par n, on aura pour restes tous les non-résidus quadratiques; et par conséquent on obtiendra

$$32. \quad \begin{cases} \sum_{u=1}^{u=p+1} \cos\frac{2b_r a_u\pi}{n} = \sum_{u=1}^{u=p+1} \cos\frac{2b_u\pi}{n}; \\ \sum_{u=1}^{u=p+1} \sin\frac{2b_r a_u\pi}{n} = \sum_{u=1}^{u=p+1} \sin\frac{2b_u\pi}{n}. \end{cases}$$

6°. Enfin en multipliant successivement un non-résidu quadratique quelconque b_r, par tous les non-résidus quadratiques

$$b_1, \; b_2, \; b_3, \; \ldots\ldots \; b_u, \; \ldots\ldots \; b_p,$$

on aura pour restes, après avoir divisé chaque produit par n, tous les résidus quadratiques, et partant on trouvera

$$\sum_{u=1}^{u=p+1}\cos\frac{2b_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2a_n\pi}{n};$$

$$\sum_{u=1}^{u=p+1}\sin\frac{2b_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}.$$

Maintenant si l'on représente par N le nombre des solutions entières et moindres que n, de la congruence

$$x^2+c\equiv 0 \pmod{n},$$

dans laquelle n est un nombre premier, on sait par ce que nous avons démontré précédemment, que N ne peut qu'être égale à zéro ou à 2, et en partant de la formule (24.), on trouvera

$$nN=\sum_{x=0}^{x=n}\left(1+\cos 2(x^2+c)\frac{\pi}{n}+\cos 4(x^2+c)\frac{\pi}{n}\ldots\ldots+\cos 2(n-1)(x^2+c)\frac{\pi}{n}\right)$$

$$=\sum_{x=0}^{x=n}\sum_{y=0}^{y=n}\cos 2y(x^2+c)\frac{\pi}{n}=n+\sum_{y=1}^{y=n}\cos\frac{2yc\pi}{n}+\sum_{x=1}^{x=n}\sum_{y=1}^{y=n}\cos 2y(x^2+c)\frac{\pi}{n}$$

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

Si l'on substitue dans cette formule les valeurs de

$$\sum_{y=1}^{y=n}\cos\frac{2yx^2\pi}{n}\cos\frac{2yc\pi}{n}=\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u x^2\pi}{n}\cos\frac{2ca_u\pi}{n}+\cos\frac{2b_u x^2\pi}{n}\cos\frac{2cb_u\pi}{n}\right),$$

$$\sum_{y=1}^{y=n}\sin\frac{2yx^2\pi}{n}\sin\frac{2yc\pi}{n}=\sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u x^2\pi}{n}\sin\frac{2ca_u\pi}{n}+\sin\frac{2b_u x^2\pi}{n}\sin\frac{2cb_u\pi}{n}\right),$$

on obtiendra

$$nN=n+\sum_{y=1}^{y=n}\cos\frac{2yc\pi}{n}+\sum_{x=1}^{x=n}\sum_{u=1}^{u=p+1}\left\{\begin{array}{l}\cos\frac{2a_u x^2\pi}{n}\cos\frac{2ca_u\pi}{n}+\cos\frac{2b_u x^2\pi}{n}\cos\frac{2cb_u\pi}{n}\\ -\sin\frac{2a_u x^2\pi}{n}\sin\frac{2ca_u\pi}{n}-\sin\frac{2b_u x^2\pi}{n}\sin\frac{2cb_u\pi}{n}\end{array}\right\};$$

ou bien, en séparant les intégrales,

$$nN=\left\{\begin{array}{l}n+\sum_{y=1}^{y=n}\cos\frac{2yc\pi}{n}+\sum_{u=1}^{u=p+1}\left(\cos\frac{2ca_u\pi}{n}\sum_{u=1}^{x=n}\cos\frac{2a_u x^2\pi}{n}\right)+\sum_{u=1}^{u=p+1}\left(\cos\frac{2b_u\pi}{n}\sum_{x=1}^{x=n}\cos\frac{2b_u x^2\pi}{n}\right)\\ -\sum_{u=1}^{u=p+1}\left(\sin\frac{2ca_u\pi}{n}\sum_{x=1}^{x=n}\sin\frac{2a_u x^2\pi}{n}\right)-\sum_{u=1}^{u=p+1}\left(\sin\frac{2cb_n\pi}{n}\sum_{x=1}^{x=n}\sin\frac{2b_u x^2\pi}{n}\right)\end{array}\right\}$$

et cette équation, à l'aide des équations (30.), (31.), (32.), se transformera dans la suivante

$$33.\quad nN=\left\{\begin{array}{l}n+\sum_{y=1}^{y=n}\cos\frac{2cy\pi}{n}+2\sum_{u=1}^{u=p+1}\left(\cos\frac{2ca_u\pi}{n}\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)+2\sum_{u=1}^{u=p+1}\left(\cos\frac{2cb_u\pi}{n}\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\\ -2\sum_{u=1}^{u=p+1}\left(\sin\frac{2ca_u\pi}{n}\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)-2\sum_{u=1}^{u=p+1}\left(\sin\frac{2cb_u\pi}{n}\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)\end{array}\right\}.$$

Mais comme les quantités

$$\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n},\quad \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n},$$
$$\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n},\quad \sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n},$$

qui sont des intégrales définies, deviennent indépendantes de u et égales à des constantes, on pourra les transporter en dehors de la première intégration dans l'équation (33.), et on aura

$$34.\quad nN=\left\{\begin{array}{l} n+\sum_{y=1}^{y=n}\cos\frac{2cy\pi}{n}+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\cos\frac{2ca_u\pi}{n}+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\cos\frac{2cb_u\pi}{n}\\ -2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\sin\frac{2ca_u\pi}{n}-2\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n},\end{array}\right.$$

et cette équation devra exister en même tems que les suivantes

$$35.\quad \left\{\begin{array}{l} \sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\cos\frac{2b_u\pi}{n}\right)=\sum_{y=1}^{y=n}\cos\frac{2y\pi}{n}=\sum_{y=1}^{y=n}\cos\frac{2cy\pi}{n}=-1,\\ \sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u\pi}{n}+\sin\frac{2b_u\pi}{n}\right)=\sum_{y=1}^{y=n}\sin\frac{2y\pi}{n}=0.\end{array}\right.$$

A présent supposons $c=\pm 1$; $n=4m+1$; et chacune des congruences

$$x^2+1\equiv 0\ (\text{mod.}\ n);\quad x^2-1\equiv 0\ (\text{mod.}\ n)$$

aura deux solutions: par conséquent N sera égale à 2, et l'équation (34.) se transformera dans la suivante

$$2n=\left\{\begin{array}{l} n-1+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2\\ \qquad\mp 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2\mp 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2\end{array}\right.$$

d'où l'on tirera

$$\frac{n+1}{2}=\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2;$$
$$\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2+\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2=0;$$

et puisque, par les équations (35.), l'on a

$$\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2=\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+1\right)^2;$$
$$\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2=\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2;$$

on trouvera

$$n+1=4\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+4\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+2;$$

et partant

$$n = \left(2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+1\right)^2;$$

d'où l'on déduira les équations

$$36.\quad \begin{cases} \sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} = -\frac{1}{2}\pm\frac{1}{2}\sqrt{n}; & \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} = -\frac{1}{2}\mp\frac{1}{2}\sqrt{n}; \\ \sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n} = 0; & \sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n} = 0. \end{cases}$$

Lorsque n est un nombre premier de la forme $4m+3$, si l'on fait $c=\pm 1$, la congruence $x^2-1\equiv 0$ (mod. n) aura deux solutions, tandis que l'autre $x^2+1\equiv 0$ (mod. n) ne sera pas résoluble; alors on aura les deux équations

$$2n = \left\{\begin{aligned} & n+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2 \\ & +2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2 \end{aligned}\right\};$$

$$0 = \left\{\begin{aligned} & n+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2 \\ & -2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2-2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2 \end{aligned}\right\};$$

qui, étant combinées avec les équations (35.), donnent

$$37.\quad \begin{cases} \sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} = -\frac{1}{2}; & \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} = -\frac{1}{2}; \\ \sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n} = \pm\frac{1}{2}\sqrt{n}; & \sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n} = \mp\frac{1}{2}\sqrt{n}. \end{cases}$$

Ces intégrales définies ont été données pour la première fois par M. Gauss dans ses Recherches Arithmétiques; et il les a trouvées en partant de sa théorie de la division du cercle en parties égales. Cet illustre géomètre a repris le même sujet dans un mémoire particulier, où il les a démontrées de nouveau. Mais les deux démonstrations de M. Gauss, qui sont les seules connues jusqu'ici, quoique tres-ingénieuses, nous paraissent moins directes que celle que nous venons d'exposer, qui se déduit tout simplement de la formule fondamentale (24.), avec beaucoup d'autres résultats. Cependant comme les équations (36.) et (37.) sont la base de tout ce que l'on sait sur les congruences du second degré, nous allons reprendre la démonstration que nous avons donnée, pour la rendre plus simple et plus claire.

On sait que lorsque $n=2p+1$ est un nombre premier de la forme $4m+1$, les congruences

$$x^2+1\equiv 0 \pmod{n}, \quad x^2-1\equiv 0 \pmod{n},$$

seront résolubles toutes deux, et auront chacune deux solutions: alors par la formule (24.) on obtiendra l'équation

$$2n=\sum_{x=0}^{x=n}\left\{\begin{array}{l}\left(\cos\frac{0\pi}{n}+\sqrt{(-1)}\sin\frac{0\pi}{n}\right)^{x^2\pm 1}+\left(\cos\frac{2\pi}{n}+\sqrt{(-1)}\sin\frac{2\pi}{n}\right)^{x^2\pm 1}\ldots\ldots\ldots\ldots \\ +\left(\cos\frac{2t\pi}{n}+\sqrt{(-1)}\sin\frac{2t\pi}{n}\right)^{x^2\pm 1}\ldots+\left(\cos\frac{2(n-1)\pi}{n}+\sqrt{(-1)}\sin\frac{2(n-1)\pi}{n}\right)^{x^2\pm 1}\end{array}\right\};$$

et par conséquent l'autre

$$2n=\left\{\begin{array}{l}\left(\cos\frac{0\pi}{n}\pm\sqrt{(-1)}\sin\frac{0\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{0x^2\pi}{n}+\sqrt{(-1)}\sin\frac{0x^2\pi}{n}\right) \\ +\left(\cos\frac{2\pi}{n}\pm\sqrt{(-1)}\sin\frac{2\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2x^2\pi}{n}+\sqrt{(-1)}\sin\frac{2x^2\pi}{n}\right) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ +\left(\cos\frac{2t\pi}{n}\pm\sqrt{(-1)}\sin\frac{2t\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2tx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2tx^2\pi}{n}\right) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ +\left(\cos\frac{2(n-1)\pi}{n}\pm\sqrt{(-1)}\sin\frac{2(n-1)\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2(n-1)x^2\pi}{n}+\sqrt{(-1)}\sin\frac{2(n-1)x^2\pi}{n}\right).\end{array}\right.$$

Si l'on effectue les multiplications indiquées dans cette équation, en observant que les imaginaires doivent se détruire entre eux, on trouvera

$$2n=\left\{\begin{array}{l}\cos\frac{0\pi}{n}\sum_{x=0}^{x=n}\cos\frac{0x^2\pi}{n}+\cos\frac{2\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2x^2\pi}{n}\ldots+\cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n}\ldots+\cos\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2(n-1)x^2\pi}{n} \\ \pm\left(\sin\frac{0\pi}{n}\sum_{x=0}^{x=n}\sin\frac{0x^2\pi}{n}+\sin\frac{2\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2x^2\pi}{n}\ldots+\sin\frac{2t\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2tx^2\pi}{n}\ldots+\sin\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2(n-1)x^2\pi}{n}\right)\end{array}\right.$$

et partant

$$38.\quad\left\{\begin{array}{l}2n=n+\cos\frac{2\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2x^2\pi}{n}\ldots+\cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n}\ldots+\cos\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2(n-1)x^2\pi}{n}; \\ 0=0+\sin\frac{2\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2x^2\pi}{n}\ldots+\sin\frac{2t\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2tx^2\pi}{n}\ldots+\sin\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2(n-1)x^2\pi}{n}.\end{array}\right.$$

Il faut observer ici que t doit prendre successivement toutes les valeurs $1, 2, 3, \ldots. n-1$, dont la moitié sont des résidus quadratiques du nombre n et l'autre moitié des non-résidus quadratiques du même nombre: si l'on suppose donc t égal à un résidu quadratique quelconque a_r, on aura

$$\cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n}=\cos\frac{2a_r\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2a_rx^2\pi}{n}$$

$$=\cos\frac{2a_r\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2x^2\pi}{n}=\cos\frac{2a_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right);$$

et l'on trouvera de même, lorsque t est un non-résidu quadratique égal à b_r,

$$\cos\frac{2b_r\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2b_rx^2\pi}{n}=\cos\frac{2b_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right).$$

On voit pourtant que la valeur de

$$\cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n},$$

ne saurait être que l'une de celles-ci:

$$\cos\frac{2a_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right);\quad \cos\frac{2b_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right);$$

selon que t est un résidu quadratique ou un non-résidu quadratique de n; et comme parmi les nombres $1, 2, 3, \ldots. n-1$, représentés par t, il y en a p qui sont résidus quadratiques de n, et autant qui ne le sont pas, on pourra les réunir en deux groupes dans les équations (38.), et on aura les équations

$$39.\quad\begin{cases} n=\begin{cases}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\left(\cos\frac{2a_1\pi}{n}+\cos\frac{2a_2\pi}{n}\ldots.+\cos\frac{2a_p\pi}{n}\right)\\ +\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\left(\cos\frac{2b_1\pi}{n}+\cos\frac{2b_2\pi}{n}\ldots.+\cos\frac{2b_p\pi}{n}\right)\end{cases}\\ 0=\begin{cases}2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)\left(\sin\frac{2a_1\pi}{n}+\sin\frac{2a_2\pi}{n}\ldots.+\sin\frac{2a_p\pi}{n}\right)\\ +2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)\left(\sin\frac{2b_1\pi}{n}+\sin\frac{2b_2\pi}{n}\ldots.+\sin\frac{2b_p\pi}{n}\right).\end{cases}\end{cases}$$

Mais comme l'on a

$$\cos\frac{2a_1\pi}{n}+\cos\frac{2a_2\pi}{n}\ldots.+\cos\frac{2a_p\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n};$$

$$\cos\frac{2b_1\pi}{n}+\cos\frac{2b_2\pi}{n}\ldots.+\cos\frac{2b_p\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};$$

$$\sin\frac{2b_1\pi}{n}+\sin\frac{2a_2\pi}{n}\ldots.+\sin\frac{2a_p\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n};$$

$$\sin\frac{2b_1\pi}{n}+\sin\frac{2b_2\pi}{n}\ldots.+\sin\frac{2b_p\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n};$$

les deux équations (39.) deviendront

$$n=\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};$$

$$0=2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2;$$

et puisque l'on a aussi

$$\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}=-1;\quad \sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}+\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}=0;$$

on trouvera, en éliminant entre les quatre équations précédentes:

$$\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}=-\frac{1}{2}\pm\frac{1}{2}\sqrt{n};\quad \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}=-\frac{1}{2}\mp\frac{1}{2}\sqrt{n};$$

$$\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}=0.$$

Si n était de la forme $4m+3$, on aurait à la place des équations (38.), les deux autres

$$n=\begin{cases}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\\ +2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2\end{cases}$$

$$0=\begin{cases}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2b_u x}{n}\\ -2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2-2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2,\end{cases}$$

qui étant combinées avec les équations (35.) donneraient

$$\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}=-\frac{1}{2};$$

$$\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}=\pm\frac{1}{2}\sqrt{n};\quad \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}=\mp\frac{1}{2}\sqrt{n}.$$

Ces dernières équations coïncident avec celles que nous avions trouvées précédemment.

Il résulte de l'analyse précédente, qu'étant proposée la congruence

$$x^2+c\equiv 0 \pmod{n},$$

(dans laquelle n est un nombre premier égal à $2p+1$), si l'on représente par N le nombre de ses solutions, on aura

$$nN=\begin{cases}n+\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2ca_u\pi}{n}+\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2cb_u\pi}{n}\\ -2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}.\sum_{u=1}^{u=p+1}\sin\frac{2ca_u\pi}{n}-2\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}.\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n}.\end{cases}$$

Mais comme, lorsque n est de la forme $4m+1$, on a

$$\sum_{u=1}^{u=p+1} \sin\frac{2a_u\pi}{n} = \sum_{u=1}^{u=p+1} \sin\frac{2b_u\pi}{n} = 0,$$

on trouvera, dans ce cas,

$$N = 1 + \frac{1}{n}\Big(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\Big)\sum_{u=1}^{u=p+1}\cos\frac{2ca_u\pi}{n} + \frac{1}{n}\Big(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\Big)\sum_{u=1}^{u=p+1}\cos\frac{2cb_u\pi}{n};$$

et la valeur de N restera la même quand on changera $+c$ en $-c$. Donc si la congruence

$$x^2 + c \equiv 0 \pmod{n},$$

(dans laquelle n est un nombre premier de la forme $4m+1$) est résoluble, celle-ci

$$y^2 - c \equiv 0 \pmod{n}$$

le sera de même; et si l'une d'elles n'est pas résoluble, l'autre ne le sera pas non plus.

Si $n = 2p+1$, est un nombre premier de la forme $4m+3$, on aura

$$1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} = 1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} = 0;$$

et le nombre N des solutions de la congruence

$$x^2 + c \equiv 0 \pmod{n}$$

sera donné par l'équation

40. $$nN = n - 2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\sum_{u=1}^{u=p+1}\sin\frac{2ca_u\pi}{n} - 2\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n};$$

qui se réduira, lorsque c est un résidu quadratique de n, à l'autre

$$nN = n - 2\Big(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\Big)^2 - 2\Big(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\Big)^2 = n - \frac{n}{2} - \frac{n}{2} = 0.$$

Si l'on change $+c$ en $-c$ dans l'équation (40.), on trouvera que le nombre N des solutions de la congruence

$$y^2 - c \equiv 0 \pmod{p},$$

sera exprimé, lorsque c est un résidu quadratique de n, par l'équation

$$nN = n + 2\Big(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\Big)^2 + 2\Big(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\Big)^2 = n + \frac{n}{2} + \frac{n}{2} = 2n.$$

On déduit de là, que lorsque n est un nombre premier de la forme $4m+3$, l'une des deux congruences

$$x^2 + c \equiv 0 \pmod{n};\quad y^2 - c \equiv 0 \pmod{n}$$

sera toujours résoluble, mais qu'on ne pourra jamais les résoudre toutes deux à la fois.

En partant des équations (36.) et (37.), on trouve, qu'en indiquant toujours par a_r un résidu quadratique quelconque du nombre premier $n=2p+1$, et par b_r un non-résidu quadratique quelconque du même nombre, on aura, lorsque n est de la forme $4m+1$,

$$\sum_{x=0}^{x=n}\left(\cos\frac{2a_rx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2a_rx^2\pi}{n}\right)=1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+2\sqrt{(-1)}\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}$$
$$=1+2\left(-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{n}\right)=\pm\sqrt{n};$$
$$\sum_{x=0}^{x=n}\left(\cos\frac{2b_rx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2b_rx^2\pi}{n}\right)=1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}+2\sqrt{(-1)}\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}$$
$$=1+2\left(-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{n}\right)=\mp\sqrt{n};$$

tandis que lorsque n est de la forme $4m+3$, on trouvera

$$\sum_{x=0}^{x=n}\left(\cos\frac{2a_rx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2a_rx^2\pi}{n}\right)=1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+2\sqrt{(-1)}\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}$$
$$=1+2\left(-\tfrac{1}{2}\right)+2\sqrt{(-1)}\left(\pm\tfrac{1}{2}\sqrt{n}\right)=\pm\sqrt{(-n)};$$
$$\sum_{x=0}^{x=n}\left(\cos\frac{2b_rx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2b_rx^2\pi}{n}\right)=1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}+2\sqrt{(-1)}\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}$$
$$=1+2\left(-\tfrac{1}{2}\right)+2\sqrt{(-1)}\left(\mp\tfrac{1}{2}\sqrt{n}\right)=\mp\sqrt{(-n)};$$

de sorte que l'on obtiendra en général les équations

$$\sum_{x=0}^{x=n}\left(\cos\frac{2a_rx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2a_rx^2\pi}{n}\right)=\pm\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)};$$
$$\sum_{x=0}^{x=n}\left(\cos\frac{2b_rx^2\pi}{n}+\sqrt{(-1)}\sin\frac{2b_rx^2\pi}{n}\right)=\mp\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}.$$

Maintenant soit proposé de trouver le nombre N des solutions entières et moindres que n, de la congruence

$$x^2+ay^2+b\equiv 0 \pmod{n},$$

dans laquelle n est un nombre premier, et a, b, sont des nombres entiers non divisibles par n; il est clair que par la formule (24.) on obtiendra l'équation

$$nN=\sum_{x=0}^{x=n}\sum_{y=0}^{y=n}\left(1+\left(\cos\frac{2\pi}{n}+\sqrt{(-1)}\sin\frac{2\pi}{n}\right)^{x^2+ay^2+b}\ldots+\left(\cos 2(n-1)\frac{\pi}{n}+\sqrt{(-1)}\sin 2(n-1)\frac{\pi}{n}\right)^{x^2+ay^2+b}\right)=$$
$$\left[\begin{array}{l}\left(\cos\frac{2b\pi}{n}+\sqrt{(-1)}\sin\frac{2b\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2x^2\pi}{n}+\sqrt{(-1)}\sin\frac{2x^2\pi}{n}\right)\sum_{y=0}^{y=n}\left(\cos\frac{2ay^2\pi}{n}+\sqrt{(-1)}\sin\frac{2ay^2\pi}{n}\right)\\ \left(\cos\frac{4b\pi}{n}+\sqrt{(-1)}\sin\frac{4b\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{4x^2\pi}{n}+\sqrt{(-1)}\sin\frac{4x^2\pi}{n}\right)\sum_{y=0}^{y=n}\left(\cos\frac{4ay^2\pi}{n}+\sqrt{(-1)}\sin\frac{4ay^2\pi}{n}\right)\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ \left(\cos 2(n-1)\frac{b\pi}{n}+\sqrt{(-1)}\sin 2(n-1)\frac{b\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos 2(n-1)\frac{x^2\pi}{n}+\sqrt{(-1)}\sin 2(n-1)\frac{x^2\pi}{n}\right)\sum_{y=0}^{y=n}\left(\cos 2(n-1)\frac{ay^2\pi}{n}+\sqrt{(-1)}\sin 2(n-1)\frac{ay^2\pi}{n}\right)\end{array}\right.$$

et la valeur de N dépendra des nombres a et b.

Supposons d'abord que a et b soient tous les deux des résidus quadratiques de n, et nous aurons, en substituant dans l'équation précédente les valeurs déjà trouvées,

$$nN = \left\{ \begin{array}{l} n^2 + \left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}\right)\left(\pm\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}\right)\left(\pm\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}\right) \\ \quad + \left(-\frac{1}{2} \mp \frac{1}{2}\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}\right)\left(\mp\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}\right)\left(\mp\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)}\right) \end{array} \right\}$$

$$= n^2 - n(-1)^{\frac{n-1}{2}}.$$

Lorsque a et b sont tous les deux non-résidus quadratiques de n, on obtiendra

$$nN = n^2 + n(-1)^{\frac{n-1}{2}}.$$

Lorsque a est un résidu quadratique de n, et b un non-résidu quadratique du même nombre, on aura

$$nN = n^2 - n(-1)^{\frac{n-1}{2}}.$$

Et enfin lorsque a est un non-résidu quadratique de n, et b un résidu quadratique du même nombre, on trouvera

$$nN = n^2 + n(-1)^{\frac{n-1}{2}}.$$

Il résulte de là, que la congruence

$$x^2 + ay^2 + b \equiv 0 \quad (\text{mod. } n),$$

dans laquelle n est un nombre premier, aura toujours un nombre $n \pm 1$ de solutions.

Lagrange a démontré pour la première fois que la congruence

$$x^2 + ay^2 + b \equiv 0 \quad (\text{mod. } n),$$

était toujours résoluble, lorsque le nombre premier n ne divisait ni a ni b. Cet illustre géomètre est parti de ce théorème pour démontrer qu'un nombre entier quelconque est toujours la somme de quatre carrés en nombres entiers: mais sa méthode ne saurait servir à déterminer le nombre des solutions de la congruence proposée, comme nous l'avons fait en partant de notre formule fondamentale (24.). Il est clair que l'on pourrait appliquer les mêmes principes aux congruences du second degré, qui renferment un plus grand nombre d'inconnues. Mais nous allons nous occuper de préférence de la résolution des équations à deux termes.

On a vu que lorsque $n = 2p + 1$ est un nombre premier de la forme $4m + 1$, on trouve

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2t^2\pi}{n}+\sqrt{(-1)}\sin\frac{2t^2\pi}{n}\right)^{a_u}=-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{n};$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2t^2\pi}{n}+\sqrt{(-1)}\sin\frac{2t^2\pi}{n}\right)^{b_u}=-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{n};$$

en indiquant toujours par a_u un résidu quadratique quelconque de n, par b_u un non-résidu quadratique de n, et par t un nombre entier non divisible par n. Si l'on fait maintenant

$$\cos\frac{2t^2\pi}{n}+\sqrt{(-1)}\sin\frac{2t^2\pi}{n}=r^{t^2},$$

r exprimant la racine

$$x=\cos\frac{2\pi}{n}+\sqrt{(-1)}\sin\frac{2\pi}{n}$$

de l'équation

$$X=\frac{x^n-1}{x-1}=0,$$

on aura, par ce qui précède:

41. $$X_1=x^{a_1}+x^{a_2}\ldots\ldots+x^{a_p}+\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{n}=0;$$

et cette équation, qui sera satisfaite par la valeur $x=r$, le sera aussi par toutes les autres valeurs

$$x=r^{2^2};\quad x=r^{3^2};\ldots\ldots x=r^{(n-1)^2};$$

dont le nombre se réduira à la moitié, puisque $r^{s^2}=r^{(n-s)^2}$. Mais comme ces racines résolvent l'équation $X=0$, elles seront communes aux deux équations $X=0$, $X_1=0$. Les autres racines qui résolvent l'équation $X=0$, sans résoudre l'équation $X_1=0$, seront de la forme

$$x=r^{b_1};\quad x=r^{b_2};\ \ldots\ldots\ x=r^{b_p},$$

et ne pourront pas résoudre l'équation $X_1=0$; car si l'une d'elles, r^{b_1} par exemple, pouvait résoudre cette équation, comme on a toujours

$$r^{b_1a_u}=r^{b_t},$$

en substituant cette racine supposée $x=r^{b_t}$, dans l'équation $X_1=0$, elle deviendrait de la forme

$$r^{b_1}+r^{b_2}\ldots\ldots+r^{b_p}+\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{n}=0;$$

mais cette équation est absurde, puisque l'on a

$$r^{b_1}+r^{b_2}\ldots\ldots+r^{b_p}+\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{n}\neq 0.$$

Donc les deux équations $X=0$, $X_1=0$, auront les p racines communes

$$r^{a_1},\ r^{a_2},\ \ldots\ldots\ r^{a_p};$$

et en cherchant le plus grand commun diviseur Δ entre X et X_1, on aura l'équation $\triangle = 0$, qui sera du degré $\frac{n-1}{2}$, et qui contiendra toutes les racines de la forme $x = r^{a_t}$.

Si $n = 2p + 1$ était de la forme $4m + 3$, au lieu de l'équation (41.) on aurait trouvé l'autre

$$X_2 = x^{a_1} + x^{a_2} \ldots . x^{a_p} + \tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{(-n)} = 0;$$

et en cherchant le plus grand diviseur commun entre

$$\mathrm{X} = \frac{x^n - 1}{x - 1} = 0, \quad \text{et } \mathrm{X}_2 = 0,$$

on obtiendrait l'équation qui a p racines de la forme

$$x = r^{a_1}, \quad x = r^{a_2}, \ldots . x = r^{a_p},$$

et l'équation $\mathrm{X} = 0$ serait encore décomposée en deux autres du degré $\frac{n-1}{2}$.

Il faut remarquer ici que lorsque n est un nombre premier de la forme $4m + 1$, les coefficiens des diverses puissances de x dans l'équation $\triangle = 0$, sont des fonctions de $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$ en général, tandis que les coefficiens des puissances correspondantes dans l'équation $\frac{X}{\triangle} = \triangle_1 = 0$, sont des fonctions semblables de $-\frac{1}{2} \mp \frac{1}{2}\sqrt{n}$. En effet, si l'on fait

$$\triangle = x^p + A_1 x^{p-1} \ldots . + A_p = 0;$$
$$\triangle_1 = x^p + B_1 x^{p-1} \ldots . + B_p = 0;$$

les coefficiens A_1, A_2, ...A_p, pourront s'exprimer exclusivement par la somme des puissances des racines de l'équation $\triangle = 0$, somme que nous indiquerons en général par P_r; et les coefficiens B_1, B_2, ...B_p, s'exprimeront de la même manière par la somme des puissances des racines de l'équation $\triangle_1 = 0$, somme que nous indiquerons en général par P_r; et comme, lorsque r n'est pas un multiple de n, on a toujours

$$P_r = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}; \quad P_r + \mathrm{P}_r = -1; \quad \mathrm{P}_r = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n},$$

il n'y aura d'autre différence entre P_r et P_r, que dans le signe de $\frac{1}{2}\sqrt{n}$; par conséquent si l'on désigne par Y la somme de tous les termes de l'équation $\triangle = 0$, qui ne contiennent pas $\sqrt{n}$, et par $Z\sqrt{n}$ la somme de tous ceux qui contiennent $\sqrt{n}$, on aura

$$\triangle = Y + Z\sqrt{n}; \quad \triangle_1 = Y - Z\sqrt{n};$$

et partant

$$X = \frac{x^n - 1}{x - 1} = \triangle\triangle_1 = Y^2 - nZ^2.$$

Si n était de la forme $4m+3$, on trouverait

$$X = Y^2 + nZ^2;$$

et en général on obtiendra

$$X = Y^2 - nZ^2(-1)^{\frac{n-1}{2}},$$

n étant un nombre premier quelconque, et Y, Z, étant des fonctions entières et rationnelles de x. On trouvera aisément, par la comparaison des coefficiens dans l'équation

$$\triangle\triangle_1 = \frac{x^n-1}{x-1},$$

que les coefficiens numériques des diverses puissances de x dans les équations $\triangle = 0$, $\triangle_1 = 0$, ne peuvent admettre d'autre diviseur que le nombre 2; et l'on déduira de là que l'équation

$$\frac{4(x^n-1)}{x-1} = Y^2 \pm nZ^2$$

(dans laquelle Y et Z sont deux polynomes en x entiers et rationnels, à coefficiens entiers) aura toujours lieu.

Pour donner une application de ce théorème à la théorie des congruences, nous observerons que puisque la congruence

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

a toujours a solutions, lorsque n est un nombre premier de la forme $ar+1$; et puisque, si a est un nombre premier impair on a aussi

$$4(x^a-1) = (x-1)(Y^2 \pm aZ^2),$$

il s'ensuit que $\mp a$ est résidu quadratique de $ar+1$, où il faut prendre le signe $\pm$, si a est de la forme $4m+1$, et le signe $-$, si a est de la forme $4m+3$. On déduit aussi de ce qui précède que lorsque a est un nombre premier, on peut toujours résoudre l'équation

$$(4a)^n = x^2 \pm ay^2$$

en nombres entiers, quel que soit l'exposant n, pourvu qu'il reste toujours entier et positif, dans laquelle il faut prendre le signe $+$, si a est de la forme $4m+3$, et le signe $-$, lorsque a est de la forme $4m+1$. On trouve de même que l'équation

$$5^a = x^2 \pm ay^2 + 1$$

est toujours résoluble en nombres entiers, lorsque a est un nombre premier quelconque; et il serait facile de trouver un grand nombre de propositions de la même nature.

Dans l'équation

$$A = \sum_{x=0}^{x=n}\left(\cos\frac{2x^2\pi}{n} + \sqrt{(-1)}\sin\frac{2x^2\pi}{n}\right) = \pm\sqrt{\left(n(-1)^{\frac{n-1}{2}}\right)},$$

trouvée précédemment, on n'a pas déterminé le signe du radical; cependant en observant que l'on a

$$A = (2\sqrt{(-1)})^{\frac{n-1}{2}} \sin\frac{2\pi}{n}\sin\frac{6\pi}{n}\sin\frac{10\pi}{n}\ldots\sin 2(n-2)\frac{\pi}{n},$$

et en cherchant combien de sinus positifs et de sinus négatifs il y aura dans le second membre de cette équation, on trouvera que, quelle que soit la forme du nombre premier n, il faut toujours prendre le radical avec le signe $+$ dans la valeur de A. Maintenant en faisant $n = 2p+1$, et en exprimant toujours par a_u un résidu quadratique quelconque du nombre premier n, et par b_u un non-résidu quadratique du même nombre, on aura les deux équations

42. $$\begin{cases} \sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n} + \sqrt{(-1)}\sin\frac{2a_u\pi}{n}\right) = -\frac{1}{2} + \frac{1}{2}\sqrt{(\pm n)}; \\ \sum_{u=1}^{u=p+1}\left(\cos\frac{2b_u\pi}{n} + \sqrt{(-1)}\sin\frac{2b_u\pi}{n}\right) = -\frac{1}{2} - \frac{1}{2}\sqrt{(\pm n)}; \end{cases}$$

dans les seconds membres desquelles il faut prendre le signe $+$, lorsque $n = 4m+1$, et le signe $-$, lorsque $n = 4m+3$.

Dans l'équation

$$\frac{4(x^n-1)}{x-1} = Y^2 \pm nZ^2$$

il y a plusieurs manières de trouver les coefficiens de x dans les polynomes Y et Z; et ce manières sont tout à fait indépendantes, comme l'on sait, de la considération des résidus quadratiques. Maintenant, parmi les deux équations

$$Y + Z\sqrt{(\pm n)} = 0; \quad Y - Z\sqrt{(\pm n)} = 0,$$

que nous avons déjà trouvées, il y en a toujours une qui a toutes ses racines de la forme

$$x = \cos\frac{2a_r\pi}{n} + \sqrt{(-1)}\sin\frac{2a_r\pi}{n},$$

en prenant pour a_r successivement tous les résidus quadratiques de n; tandis que l'autre de ces deux équations aura ses racines de la forme

$$x = \cos\frac{2b_r\pi}{n} + \sqrt{(-1)}\sin\frac{2b_r\pi}{n},$$

en prenant successivement pour b_r tous les non-résidus quadratiques de n.

Il résulte de là une méthode directe pour savoir si un nombre quelconque est résidu quadratique, ou non-résidu quadratique d'un nombre premier donné.

En effet si l'on ordonne l'équation

$$\tfrac{1}{2}Y + \tfrac{1}{2}Z\sqrt{n} = 0,$$

par les puissances descendantes de x, on pourra, par les formules connues, trouver la somme des puissances de ses racines; alors en appellant P_a la somme des puissances a^{mes} des racines de cette équation, on aura en général $P_a = P_1$, si a est un résidu quadratique de n, et $P_a = 1 - P_1$ dans le cas contraire.

On doit remarquer ici que comme les coefficiens de x, dans les polynomes Y et Z, se déterminent d'après la forme de n, et non d'après sa valeur numérique, on pourra transporter à tous les nombres premiers d'une forme donnée, les théorèmes qu'on aura trouvés par induction pour des petits nombres. Cette proposition, qui est de la plus haute importance, mériterait de longs développemens que nous réservons pour un travail particulier. On en peut déduire des conséquences fort singulières sur la manière de vérifier les *résultats de l'observation dans l'analyse pure*, en suivant la route tracée par Euler dans cette branche de l'algèbre, route qui a été quittée trop tôt par les géomètres. On pourrait tirer aussi de là la démonstration de la loi de réciprocité énoncée d'abord par M. Legendre; mais comme M. Gaus a déjà donné cette démonstration, en partant des équations (42.), nous ne nous arrêterons pas plus long temps sur ce sujet, puisque ce qui précède renferme toute la théorie des congruences du second degré, déduite de la seule équation fondamentale (24.). Mais en partant de cette même équation nous allons reprendre la résolution générale des équations à deux termes: en commençant par énoncer quelques propositions sur les résidus de tous les degrés, dont nous omettons les démonstrations qui sont très faciles à retrouver.

(La suite dans le cahier prochain.)