

Sur une formule relative à la théorie des nombres.

(Par M. *Emile Mathieu* à Paris.)

Désignons par ω une racine de la congruence irréductible

$$\omega^2 + \omega + 1 \equiv 0 \pmod{2},$$

et représentons huit nombres par

$$x_0, \quad x_1, \quad x_\omega, \quad x_{1+\omega}, \quad x'_0, \quad x'_1, \quad x'_\omega, \quad x'_{1+\omega};$$

nous aurons l'égalité suivante:

$$(A.) \quad \left\{ \begin{aligned} & (x_0^2 + x_1^2 + x_\omega^2 + x_{1+\omega}^2)(x_0'^2 + x_1'^2 + x_\omega'^2 + x_{1+\omega}'^2) \\ & = (x_0 x'_0 + x_1 x'_1 + x_\omega x'_\omega + x_{1+\omega} x'_{1+\omega})^2 \\ & \quad + (x_0 x'_1 - x_1 x'_0 - x_\omega x'_{1+\omega} + x_{1+\omega} x'_\omega)^2 \\ & \quad + (x_0 x'_\omega - x_\omega x'_0 - x_{1+\omega} x'_1 + x_1 x'_{1+\omega})^2 \\ & \quad + (x_0 x'_{1+\omega} - x_{1+\omega} x'_0 - x_1 x'_\omega + x_\omega x'_1)^2. \end{aligned} \right.$$

Cette formule, sauf la manière de représenter les huit nombres, qui nous est propre, est une égalité très connue due à *Euler*. La formule (A.) est très facile à poser; car les deux dernières lignes du second membre se déduisent de la deuxième par la substitution circulaire $(z, \omega z)$ faite sur les indices, ou ce qui revient au même par la substitution

$$(x_1 x_\omega x_{1+\omega})(x'_1 x'_\omega x'_{1+\omega})$$

faite sur les nombres de la formule.

Nous voyons d'après cela que nous aurons dans le second membre les quatre mêmes carrés si nous faisons sur les indices la permutation circulaire $(1, \omega, \omega^2)$ ou

$$(1, \omega, 1 + \omega);$$

on vérifie ensuite que la composition du second membre n'est pas non plus altérée, si l'on fait sur les indices la permutation circulaire $(0, \omega, \omega^2)$ ou

$$(0, \omega, 1 + \omega).$$

On conclut de là facilement que par la permutation des quatre indices $0, 1, \omega, 1 + \omega$ le second membre ne peut donner que deux décompositions différentes en quatre carrés; autrement dit, des 24 permutations de ces 4 indices, 3×4 donnent *une* décomposition en carrés, 3×4 en donnent une autre.

Permutons les 4 nombres $x_0, x_1, x_\omega, x_{1+\omega}$ de toutes les manières possibles; permutons de même entr'eux les 4 nombres $x'_0, x'_1, x'_\omega, x'_{1+\omega}$ et nous aurons $(1.2.3.4)^2$ permutations qui ne changent pas le premier membre. Or étant donnée une quelconque de ces permutations, il y en a 3×4 qui donnent pour le second membre la même décomposition en carrés. Donc on obtiendra de la sorte pour le second membre $\frac{(1.2.3.4)^2}{3 \times 4} = 48$ décompositions différentes en quatre carrés.

Donnons maintenant à la lettre ω une autre signification, et supposons qu'elle représente une racine imaginaire de la congruence $z^8 \equiv z \pmod{2}$; prenons par exemple pour ω une racine de la congruence irréductible

$$(a.) \quad \omega^3 + \omega + 1 \equiv 0 \pmod{2},$$

et représentons 16 nombres par

$$\begin{aligned} x_0, x_1, x_\omega, x_{1+\omega}, x_{\omega^2}, x_{1+\omega^2}, x_{\omega+\omega^2}, x_{1+\omega+\omega^2}, \\ x'_0, x'_1, x'_\omega, x'_{1+\omega}, x'_{\omega^2}, x'_{1+\omega^2}, x'_{\omega+\omega^2}, x'_{1+\omega+\omega^2}, \end{aligned}$$

nous aurons la formule suivante:

$$(B.) \quad \left\{ \begin{aligned} & (x_0^2 + x_1^2 + x_\omega^2 + x_{1+\omega}^2 + x_{\omega^2}^2 + x_{1+\omega^2}^2 + x_{\omega+\omega^2}^2 + x_{1+\omega+\omega^2}^2) \\ & \times (x_0'^2 + x_1'^2 + x_\omega'^2 + x_{1+\omega}'^2 + x_{\omega^2}'^2 + x_{1+\omega^2}'^2 + x_{\omega+\omega^2}'^2 + x_{1+\omega+\omega^2}'^2) \\ & = \left(\begin{aligned} & x_0 x'_0 + x_1 x'_1 + x_\omega x'_\omega + x_{1+\omega} x'_{1+\omega} \\ & + x_{\omega^2} x'_{\omega^2} + x_{1+\omega^2} x'_{1+\omega^2} + x_{\omega+\omega^2} x'_{\omega+\omega^2} + x_{1+\omega+\omega^2} x'_{1+\omega+\omega^2} \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_1 - x_1 x'_0 - x_\omega x'_{1+\omega} + x_{1+\omega} x'_\omega \\ & - x_{\omega^2} x'_{1+\omega^2} + x_{1+\omega^2} x'_{\omega^2} - x_{\omega+\omega^2} x'_{1+\omega+\omega^2} + x_{1+\omega+\omega^2} x'_{\omega+\omega^2} \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_\omega - x_\omega x'_0 - x_{\omega^2} x'_{\omega+\omega^2} + x_{\omega+\omega^2} x'_{\omega^2} \\ & - x_{1+\omega} x'_1 + x_1 x'_{1+\omega} - x_{1+\omega+\omega^2} x'_{1+\omega^2} + x_{1+\omega^2} x'_{1+\omega+\omega^2} \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_{\omega^2} - x_{\omega^2} x'_0 - x_{1+\omega} x'_{1+\omega+\omega^2} + x_{1+\omega+\omega^2} x'_{1+\omega} \\ & - x_{\omega+\omega^2} x'_{\omega} + x_\omega x'_{\omega+\omega^2} - x_{1+\omega^2} x'_1 + x_1 x'_{1+\omega^2} \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_{1+\omega} - x_{1+\omega} x'_0 - x_{\omega+\omega^2} x'_{1+\omega^2} + x_{1+\omega^2} x'_{\omega+\omega^2} \\ & - x_{1+\omega+\omega^2} x'_{\omega^2} + x_{\omega^2} x'_{1+\omega+\omega^2} - x_1 x'_\omega + x_\omega x'_1 \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_{\omega+\omega^2} - x_{\omega+\omega^2} x'_0 - x_{1+\omega+\omega^2} x'_1 + x_1 x'_{1+\omega+\omega^2} \\ & - x_{1+\omega^2} x'_{1+\omega} + x_{1+\omega} x'_{1+\omega^2} - x_\omega x'_{\omega^2} + x_{\omega^2} x'_\omega \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_{1+\omega+\omega^2} - x_{1+\omega+\omega^2} x'_0 - x_{1+\omega^2} x'_{\omega} + x_\omega x'_{1+\omega^2} \\ & - x_1 x'_{\omega+\omega^2} + x_{\omega+\omega^2} x'_1 - x_{\omega^2} x'_{1+\omega} + x_{1+\omega} x'_{\omega^2} \end{aligned} \right)^2 \\ & + \left(\begin{aligned} & x_0 x'_{1+\omega^2} - x_{1+\omega^2} x'_0 - x_1 x'_{\omega^2} + x_\omega x'_1 \\ & - x_\omega x'_{1+\omega+\omega^2} + x_{1+\omega+\omega^2} x'_\omega - x_{1+\omega} x'_{\omega+\omega^2} + x_{\omega+\omega^2} x'_{1+\omega} \end{aligned} \right)^2. \end{aligned} \right.$$

Cette égalité peut être formée au moyen de la règle suivante: On déduit tous les carrés du second membre qui suivent le deuxième au moyen de celui-ci, en effectuant sur les indices la permutation circulaire $(z, \omega z)$ ou

$$(1, \omega, \omega^2, 1+\omega, \omega+\omega^2, 1+\omega+\omega^2, 1+\omega^2).$$

Quant aux signes, ils sont entièrement déterminés par la condition que les termes qui figurent dans le second membre de la formule (A.) se retrouvent avec les mêmes signes dans la formule (B.).

Cette formule est aussi très aisée à vérifier; car il suffit de constater que tous les doubles produits provenant du développement du second carré sont détruits par les doubles produits des autres carrés; puisque tous ces carrés (sauf le premier) se déduisent du second par une même permutation circulaire.

La formule (B.) a été trouvée par M. *Prouhet* et *Cayley* *); on voit qu'elle est très facile à obtenir au moyen de notre notation, et de la règle que nous venons de donner. Si dans cette formule, on fait

$$\begin{aligned} x_{\omega^2} &= x_{1+\omega^2} = x_{\omega+\omega^2} = x_{1+\omega+\omega^2} = 0, \\ x'_{\omega^2} &= x'_{1+\omega^2} = x'_{\omega+\omega^2} = x'_{1+\omega+\omega^2} = 0, \end{aligned}$$

on retombe sur la formule (A.).

Au lieu de prendre pour ω une racine de la congruence (a.), on aurait pu prendre encore une racine de la congruence irréductible

$$\omega^3 + \omega^2 + 1 \equiv 0 \pmod{2}$$

dont les racines appartiennent aussi à $z^8 \equiv z \pmod{2}$, et on serait arrivé à un résultat semblable.

Au lieu de prendre la somme des carrés du second membre de la formule (B.), considérons une fonction symétrique quelconque de ces huit carrés, que nous appellerons Φ .

Φ reste invariable si l'on fait sur les indices la permutation circulaire

$$(1, \omega, \omega^2, 1+\omega, \omega+\omega^2, 1+\omega+\omega^2, 1+\omega^2),$$

qui peut aussi s'écrire

$$(\omega^z, \omega^{z+1})$$

z étant un des nombres 0, 1, 2, 3, 4, 5, 6. Remarquons maintenant que le

*) La formule dont il s'agit et au moyen de laquelle le produit de deux sommes de huit carrés est représenté sous la même forme a été donnée dans le cahier de mars 1845 du *Philosophical Magazine* par M. *Cayley*; le géomètre irlandais M. *J. T. Graves* l'avait déjà trouvée antérieurement à la fin de 1843 et l'avait communiquée à M. *Hamilton* dans une lettre écrite au commencement de 1844. (Voy. *Proceedings of the Royal Irish academy* 1847, June 14.)

deuxième carré du second membre de l'égalité (B.) peut être ainsi écrit :

$$(x_0 x'_1 + x_{\omega^3} x'_{\omega} + x_{\omega^6} x'_{\omega^2} + x_{\omega^5} x'_{\omega^4} - x_1 x'_0 - \dots)^2,$$

il est donc invariable par cette substitution effectuée sur les indices

$$(\omega, \omega^2, \omega^4)(\omega^3, \omega^6, \omega^5)$$

ou

$$(\omega^z, \omega^{2z});$$

on conclut de là que la fonction Φ est invariable par toutes les permutations renfermées dans l'expression

$$(b.) \quad (\omega^z, \omega^{az+b}).$$

On vérifie ensuite que la fonction Φ est invariable par la permutation circulaire

$$(c.) \quad (0, \omega, \omega^{\frac{1}{2}}, \omega^{\frac{1}{3}}, \omega^{\frac{1}{4}}, \omega^{\frac{1}{5}}, \omega^{\frac{1}{6}})$$

ou

$$(0, \omega, \omega + \omega^2, 1 + \omega + \omega^2, \omega^2, 1 + \omega, 1 + \omega^2);$$

les exposants $\frac{1}{2}, \frac{1}{3}$, etc. représentent les nombres entiers associés respectivement à 2, 3, etc., suivant le module 7.

La permutation (c.) peut s'écrire

$$(\omega^z, \omega^{\frac{1}{z}}),$$

et la fonction Φ étant invariable par cette permutation et par les permutations (b.), est invariable par les $3 \times 7 \times 8$ permutations

$$(\omega^z, \omega^{\frac{az+b}{cz+d}})$$

pour lesquelles $ad - bc$ est résidu quadratique de 7. Ainsi nous voyons encore que ces $3 \times 7 \times 8$ permutations n'altèrent pas la composition des carrés du second membre de la formule (B.).

Dans l'égalité (B.) permutons les nombres $x_0, x_1, x_{\omega}, \dots, x_{\omega^6}$ de toutes les manières possibles, puis aussi $x'_0, x'_1, x'_{\omega}, \dots, x'_{\omega^6}$, et nous aurons $(1.2.3\dots 8)^2$ permutations qui ne changent pas le premier membre, mais qui changeront en général la composition des carrés du second membre; le nombre de ces permutations qui ne changent pas la composition des carrés du second membre étant 3.7.8, ce deuxième membre est susceptible de prendre $\frac{(1.2.3\dots 8)^2}{3.7.8}$ formes. On en conclut que la formule (B.) donne par la permutation des indices $\frac{(1.2.3\dots 8)^2}{3.7.8} = 9676800$ décompositions en huit carrés.

Ce qui précède nous conduit tout naturellement à quelques remarques sur les fonctions de huit quantités; les observations que nous allons faire non seulement sont démontrées d'une manière particulière, mais comme celles qui viennent d'être faites, ne sont pas susceptibles de généralisation.

Si l'on examine avec attention la formule (B.), on voit facilement que les substitutions effectuées sur les indices qui laissent Φ invariable ne changent pas non plus la fonction F symétrique des fonctions suivantes:

$$(C.) \quad \left\{ \begin{array}{l} x_0 x_{1+\omega} x_{1+\omega^2} x_{1+\omega+\omega^2} + x_1 x_{\omega} x_{\omega^2} x_{\omega+\omega^2}, \\ x_0 x_{\omega+\omega^2} x_1 x_{1+\omega^2} + x_{\omega} x_{\omega^2} x_{1+\omega} x_{1+\omega+\omega^2}, \\ x_0 x_{1+\omega+\omega^2} x_{\omega} x_1 + x_{\omega^2} x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega^2}, \\ x_0 x_{1+\omega^2} x_{\omega^2} x_{\omega} + x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_1, \\ x_0 x_1 x_{1+\omega} x_{\omega^2} + x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_{1+\omega^2} x_{\omega}, \\ x_0 x_{\omega} x_{\omega+\omega^2} x_{1+\omega} + x_{1+\omega+\omega^2} x_{1+\omega^2} x_1 x_{\omega^2}, \\ x_0 x_{\omega^2} x_{1+\omega+\omega^2} x_{\omega+\omega^2} + x_{1+\omega^2} x_1 x_{\omega} x_{1+\omega}; \end{array} \right.$$

ainsi la fonction F est invariable par les substitutions

$$\left(\omega^z, \omega^{\frac{az+b}{cz+d}} \right)$$

pour lesquelles $ad-bc$ est résidu quadratique; mais elle est invariable par d'autres substitutions; en effet la fonction F' symétrique des fonctions

$$(D.) \quad \left\{ \begin{array}{l} x_0 x_{\omega} x_{\omega^2} x_{\omega+\omega^2} + x_1 x_{1+\omega} x_{1+\omega^2} x_{1+\omega+\omega^2}, \\ x_0 x_{\omega^2} x_{1+\omega} x_{1+\omega+\omega^2} + x_{\omega} x_{\omega+\omega^2} x_1 x_{1+\omega^2}, \\ x_0 x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega^2} + x_{\omega^2} x_{1+\omega+\omega^2} x_{\omega} x_1, \\ x_0 x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_1 + x_{1+\omega} x_{1+\omega^2} x_{\omega^2} x_{\omega}, \\ x_0 x_{1+\omega+\omega^2} x_{1+\omega^2} x_{\omega} + x_{\omega+\omega^2} x_1 x_{1+\omega} x_{\omega^2}, \\ x_0 x_{1+\omega^2} x_1 x_{\omega^2} + x_{1+\omega+\omega^2} x_{\omega} x_{\omega+\omega^2} x_{1+\omega}, \\ x_0 x_1 x_{\omega} x_{1+\omega} + x_{1+\omega^2} x_{\omega^2} x_{1+\omega+\omega^2} x_{\omega+\omega^2}; \end{array} \right.$$

est une fonction trois fois transitive qui a 30 valeurs *); or on passe de la fonction F à la fonction F' , comme on peut le vérifier, par la substitution

$$(\omega^z, \omega^{3z})$$

ou

$$(\omega, 1+\omega, \omega^2, 1+\omega^2, \omega+\omega^2, 1+\omega+\omega^2),$$

*) Journal de M. Liouville, 2^{me} série, tome VI, page 307.

et on passe de même de F' à F . Donc la fonction F est une fonction trois fois transitive qui a 30 valeurs.

D'après cela $F - F'$ ou, si l'on veut, la fonction formée par la somme des termes (C.) pris positivement et la somme des termes (D.) pris négativement est une fonction invariable par les substitutions

$$\left(\omega^z, \omega^{\frac{az+b}{cz+d}} \right)$$

pour lesquelles $ad - bc$ est résidu quadratique, et qui a 240 valeurs. $F + F'$ est de plus invariable par (ω^z, ω^{3z}) ; donc elle est invariable par les substitutions précédentes, $ad - bc$ étant alors quelconque (excepté zéro); c'est une fonction trois fois transitive qui a 120 valeurs. On peut prendre pour cette fonction la somme des termes (C.) et (D.).

On aura encore une fonction invariable par toutes les substitutions

$$\left(\omega^z, \omega^{\frac{az+b}{cz+d}} \right)$$

pour lesquelles $ad - bc$ est résidu quadratique de 7, en remplaçant dans le second membre de la formule (B.) les x' par x^m , sans rien changer aux indices.

Paris, le 19. novembre 1861.