Section 182 des Recherches arithmétiques de Gauss[*]

182. Descendons maintenant à quelques cas particuliers remarquables autant à cause de leur élégance, que par l'assiduité avec laquelle *Euler* s'en est occupé.

1°. Aucun nombre, à moins que son résidu quadratique ne soit -1, ne peut être représenté par la forme $x^2 + y^2$, dans laquelle x et y sont premiers entre eux, ou sont décomposables en deux nombres quarrés premiers entre eux ; mais tous les nombres qui jouiront de cette propriété pourront se décomposer en deux quarrés. Soit M un de ces nombres et $\pm N$, $\pm N'$, $\pm N''$, etc. les valeurs de l'expression $\sqrt{-1}$ $(mod\ M)$; alors par le n° 176, la forme $\left(M, N, \frac{N^2+1}{M}\right)$ sera proprement équivalente à la forme $(1, 0, 1)$; soit $x = \alpha x' + \beta y', y = \gamma x' + \delta y'$ une transformation propre de la forme $(1, 0, 1)$ en la forme $\left(M, N, \frac{N^2+1}{2}\right)$; on aura les quatre représentations suivantes du nombre M par la forme $x^2 + y^2$, savoir, $x = \pm\alpha, y = \pm\gamma; x = \mp\gamma, y = \pm\alpha$.[†] (2°. -n°180).

Comme la forme $(1, 0, 1)$ est ambiguë, il est évident que la forme $\left(M, -N, \frac{N^2+1}{M}\right)$ lui est aussi proprement équivalente, et que la première se change en la seconde par la transformation propre $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$, d'où naissent quatre représentations de M appartenantes à $-N$, $x = \pm\alpha, y = \mp\gamma; x = \pm\gamma, y = \mp\alpha$. Il suit de là qu'il y a huit représentations du nombre M, dont quatre appartiennent à la valeur N, et quatre à la valeur $-N$. Mais toutes ces représentations donnent la même décomposition du nombre M en deux quarrés, $M = \alpha^2 + \gamma^2$, tant qu'on ne considère que les quarrés et non l'ordre et les signes des racines.

∗. (mise au format LaTex D.Vella-Chemla, 7.5.2019)

†. $\mp$ plutôt que $\pm$ pour le second y ?

Si donc il n'y a pas d'autres valeurs que N et $-N$ pour l'expression $\sqrt{-1}$ $(mod\ M)$, ce qui arrive, par exemple, toutes les fois que M est un nombre premier, M ne pourra être décomposé que d'une manière en deux quarrés. Or comme -1 est résidu de tous les nombres premiers de la forme $4n+1$ (n°108), et qu'un nombre premier ne peut évidemment se partager en deux quarrés non premiers entre eux, nous aurons le théorème suivant.

Tout nombre premier de la forme $4n+1$ *peut être décomposé en deux quarrés, et ne peut l'être que d'une seule manière.*

Ainsi :

$1 = 0 + 1$	$5 = 1 + 4$	$13 = 4 + 9$	$17 = 1 + 16$
$29 = 4 + 25$	$37 = 1 + 36$	$41 = 16 + 25$	$53 = 4 + 49$
$61 = 25 + 36$	$73 = 9 + 64$	$89 = 25 + 64$	$97 = 16 + 81$

etc.

Ce théorème élégant a été donné par *Fermat*, mais *Euler* est le premier qui l'ait démontré, *Comm. nov. Petr. T. V. ann. 1754 et 1755. p. 3.* Dans le *T. IV*, il existe une dissertation sur le même sujet, *p. 8* ; mais alors il n'était pas parvenu à son but.

Si donc un nombre de la forme $4n+1$ ne peut pas être décomposé en deux quarrés, ou peut l'être de plusieurs manières, on sera sûr que ce n'est pas un nombre premier.

Mais réciproquement, si l'expression $\sqrt{-1}$ $(mod\ M)$ a encore d'autres valeurs que N et $-N$, il y aura d'autres représentations de M. Ainsi, dans ce cas, M peut se décomposer en deux quarrés de plusieurs manières ; par exemple : $65 = 1 + 64 = 16 + 49, 221 = 25 + 196 = 100 + 121$.

Les autres représentations dans lesquelles x et y prennent des valeurs non premières entre elles, se trouvent facilement par notre méthode. Observons seulement que si le nombre M renferme des facteurs de la forme $4n + 3$, dont on ne puisse pas le délivrer en le divisant par un quarré, ce qui arrivera toutes les fois que le nombre M renfermera des puissances impaires de ces facteurs, il ne pourra en aucune manière être décomposé en deux quarrés (**).

(**) Soit le nombre $M = 2^{\mu}.S.a^{\alpha}b^{\beta}c^{\gamma}$, etc., ensorte que a, b, c, etc. soient des facteurs premiers inégaux de la forme $4m + 1$, et S le produit de tous les facteurs premiers de la forme $4n + 3$; cette forme donnée au nombre M convient dans tous les cas ; pour M impair, il suffit de faire $\mu = 0$; si M ne renferme aucun facteur de la forme $4n+3$, on fera $S = 1$: si S n'est pas un quarré, M ne pourra en aucune manière être décomposé en deux quarrés ; mais si S est un quarré, il y aura $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$, etc. décompositions de M, lorsque quelqu'un des nombres α, β, γ, etc. sont impairs, et il y en aura $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$, etc.$+\frac{1}{2}$, quand tous les nombres α, β, γ, etc. seront pairs, tant qu'on ne fait attention qu'aux carrés eux-mêmes. Ceux qui ont quelque habitude du calcul des combinaisons, déduiront sans peine de notre théorie générale la démonstration de ce théorème, auquel nous ne pouvons nous arrêter, non plus qu'à d'autres particuliers (Voyez n° 105).