Analyse indéterminée de 2e degré : Résolution en nombres entiers de l'équation x²+y² =N

Bulletin de la Société Vaudoise des Sciences naturelles.
Vol. XIII. N° 74. 1875.

ANALYSE INDÉTERMINÉE DU 2e DEGRÉ.

Résolution en nombres entiers de l'équation

$$x^2 + y^2 = N$$

par

F.-L.-Fréd. CHAVANNES.

I. Commençons par quelques remarques fort simples dont nous aurons à tirer parti.

1° Quel que soit le signe de x et celui de y, la somme de leurs carrés est positive. Ainsi N doit être positif; ou ce qui est plus simple et plus correct, les nombres N, x, y, doivent être pris comme nombres absolus. Si dans les calculs destinés à déterminer x et y on trouve des soustractions à opérer, il faudra toujours retrancher un plus petit nombre d'un plus grand, sans se préoccuper du signe.

2° Tous les nombres entiers sont compris dans ces quatre formes, e désignant un nombre entier indéterminé, positif ou négatif:

$$4e, \quad 4e+1, \quad 4e+2, \quad 4e+3,$$
ou, ce qui revient au même, $4e-1$.

Or si l'on fait la somme des carrés de deux nombres pairs, on la trouvera de la forme $4e$; c'est un nombre quadruple.

Si l'on fait la somme des carrés de deux nombres impairs, on la trouvera de la forme $4e+2$, soit $2\,(2e+1)$, c'est-à-dire un nombre pair double d'un nombre impair.

Si l'on fait la somme du carré d'un nombre pair et du carré d'un nombre impair, on la trouvera de la forme $4e+1$.

Il n'existe donc aucune combinaison qui puisse fournir une somme de deux carrés de la forme $4e-1$.

Il s'ensuit que *si en divisant N par 4, on trouve le reste 3, ou, ce qui revient au même, le reste — 1, on est assuré qu'il n'y a aucune solution possible de l'équation proposée,* du moins dans les conditions que nous avons établies.

II. Abordons maintenant la résolution proprement dite de l'équation

$$x^2 + y^2 = \mathrm{N}. \qquad (1)$$

Comme on peut toujours décomposer N en facteurs, voyons, si par quelque artifice, nous ne parviendrons pas à en faire autant du premier membre $x^2 + y^2$?

Posons

$$x = r + s, \quad y = t + u;$$

il vient ainsi:

$$x^2 + y^2 = r^2 + 2\,rs + s^2 + t^2 + 2\,tu + u^2; \qquad (2)$$

supposons que $rs = tu$, en donnant à $2\,rs$ et à $2\,tu$ des signes contraires, ce qui revient à faire

$$x = r \pm s, \quad y = t \mp u, \qquad (3)$$

notre somme de deux carrés deviendra égale à celle des quatre carrés $r^2 + s^2 + t^2 + u^2$.

Or notre supposition $rs = tu$, nous donne la proportion suivante ou l'une de ses permutations :

$$r : t :: u : s.$$

En prenant pour α, β, γ, δ, des nombres entiers, la forme générale des proportions dont les termes sont entiers est :

$$\alpha\gamma : \beta\gamma :: \alpha\delta : \beta\delta.$$

Nous pouvons ainsi poser :

$$r = \alpha\gamma, \quad s = \beta\delta, \quad t = \beta\gamma, \quad u = \alpha\delta.$$

Enfin en substituant ces valeurs dans (2), en ayant soin de donner à s et à u des signes contraires, il vient :

$$x^2 + y^2 = \alpha^2\gamma^2 \pm 2\alpha\gamma\beta\delta + \beta^2\delta^2 + \beta^2\gamma^2 \mp 2\beta\gamma\alpha\delta + \alpha^2\delta^2,$$

d'où, en réduisant et en mettant les facteurs communs en évidence :

$$x^2 + y^2 = \alpha^2\gamma^2 + \beta^2\delta^2 + \beta^2\gamma^2 + \alpha^2\delta^2 = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = \mathrm{N}. \tag{4}$$

Nous avons aussi, par la même substitution (3) :

$$x = \alpha\gamma \pm \beta\delta, \quad y = \beta\gamma \mp \alpha\delta. \tag{5}$$

Soit $\mathrm{N} = \mathrm{FF'}$, nous déduirons de (4) :

$$(\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = \mathrm{FF'};$$

et nous pourrons poser :

$$\alpha^2 + \beta^2 = \mathrm{F}, \quad \gamma^2 + \delta^2 = \mathrm{F'}. \tag{6}$$

Ainsi la résolution de notre équation proposée (1) se ramène à la résolution de deux équations de même nature (6), mais dont les seconds membres sont facteurs du second membre de la proposée. Ces nouvelles équations sont ainsi plus simples que celle-ci.

Si N était un nombre premier, le facteur F serait égal à N, et le facteur F′ serait égal à 1. Nos équations (6) deviendraient ainsi :

$$\alpha^2 + \beta^2 = \mathrm{N}, \quad \gamma^2 + \delta^2 = 1.$$

L'une équivaut à la proposée, la seconde donne $\gamma = 1$ $\delta = 0$; ou $\gamma = 0$, $\delta = 1$. Dans ces deux cas la multiplication membre à membre de ces dernières égalités donne toujours $\alpha^2 + \beta^2 = \mathrm{N}$. Ainsi lorsque N est un nombre premier, la proposée ne peut se ramener à la résolution d'équations plus simples.

Relativement aux équations (6), on leur appliquera la même analyse dont nous avons fait usage pour la proposée, et l'on poursuivra de même jusqu'à ce que l'on soit arrivé à tous les facteurs premiers de N. Si l'on désigne ces facteurs par p, p', p'', etc., l'on aura ainsi une suite d'équations :

$$\iota^2 + \varkappa^2 = p, \quad \lambda^2 + \mu^2 = p', \quad \nu^2 + \xi^2 = p'', \text{ etc,} \tag{7}$$

au-delà desquelles on ne pourra pas remonter.

En multipliant toutes ces équations membre à membre, nous obtiendrons cette nouvelle forme pour la proposée (1) :

$$\begin{aligned} x^2 + y^2 &= (\iota^2 + \varkappa^2)\,(\lambda^2 + \mu^2)\,(\nu^2 + \xi^2) \text{ etc.} \\ &= pp'p'' \ldots. = \mathrm{N}. \end{aligned} \tag{8}$$

III. Avant d'aller plus loin, nous avons plusieurs remarques à faire qui sont indispensables pour la suite de notre calcul.

Posons pour simplifier $\alpha\gamma + \beta\delta = a$ et $\beta\gamma - \alpha\delta = b$, cette notation nous donnera d'après (5) $x = a$ et $y = b$, et par conséquent $\mathrm{N} = a^2 + b^2$.

Si nous faisons $\alpha\gamma - \beta\delta = c$ et $\beta\gamma + \alpha\delta = d$, nous aurons encore d'après (5) : $x = c$, $y = d$, et en conséquence $\mathrm{N} = c^2 + d^2$.

Or nous savons d'après (4) que $N = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)$. Il s'ensuite que *lorsqu'un nombre donné est le produit de deux facteurs dont chacun est la somme de deux carrés, ce nombre donné peut être décomposé de deux manières différentes en la somme de deux carrés.*

Ainsi 65 est égal à $5.13 = (2^2 + 1^2)(3^2 + 2^2)$, et l'on trouve $65 = 64 + 1 = 8^2 + 1^2$, pour une manière, et $65 = 16 + 49 = 4^2 + 7^2$ pour la seconde manière. Il suffit pour cela de faire $\alpha = 2$, $\beta = 1$, $\gamma = 3$, $\delta = 2$, dans les valeurs qui donnent a, b, c, d.

Réciproquement : *Si un nombre est décomposable de deux manières en la somme de deux carrés, il est le produit de deux facteurs dont chacun est la somme de deux carrés.*

Ainsi soit $N = a^2 + b^2 = c^2 + d^2$.

Nous tirons de là

$$a^2 - c^2 = d^2 - b^2,$$

et par conséquent

$$(a - c)(a + c) = (d - b)(d + b).$$

Donc

$$(a - c) : (d - b) :: (d + b) : (a + c).$$

Si nous faisons la somme des carrés de ces quatre termes nous trouverons :

$$a^2 - 2ac + c^2 + d^2 - 2bd + b^2 + d^2 + 2bd + b^2 + a^2 + 2ac + c^2 = 2a^2 + 2c^2 + 2d^2 + 2b^2 = 2N + 2N = 4N.$$

Pour retrouver simplement N, il faut prendre la moitié de chacun des termes de notre proportion, et écrire

$$\frac{a - c}{2} : \frac{d - b}{2} :: \frac{d + b}{2} : \frac{a + c}{2}. \qquad \text{(A)}$$

Si N est de la forme $4e$, alors a, b, c, d seront tous des nombres pairs, et par conséquent les quatre termes de notre proportion (A) seront entiers.

Si N est de la forme $4e + 2$, alors a, b, c, d seront tous des nombres impairs et les quatre termes de notre proportion (A) seront encore entiers.

Si N est de la forme $4e + 1$, l'un des nombres a et b sera pair et l'autre impair; il en sera de même de c et d. Prenons a et c pour les nombres pairs, b et d seront les nombres impairs et les quatre termes de notre proportion seront encore entiers.

Nous pouvons ainsi mettre notre proportion (A) sous la forme générale des proportions dont les termes sont entiers, savoir:

$$\alpha\gamma \;:\; \beta\gamma \;::\; \alpha\delta \;:\; \beta\delta.$$

La somme des quatre carrés que nous savons être égale à N, sera donc $\alpha^2\gamma^2 + \beta^2\gamma^2 + \alpha^2\delta^2 + \beta^2\delta^2 = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)$ ainsi,

$$N = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2). \qquad \text{C. Q. F. D.}$$

Nous tirons de là: *un nombre premier ne peut être décomposé en la somme de deux carrés que d'une seule manière.*

IV. Notre égalité

$$a^2 + b^2 = c^2 + d^2$$

qui nous a donné $a^2 - c^2 = d^2 - b^2$, nous donne aussi

$$a^2 - d^2 = c^2 - b^2$$

ou, ce qui revient au même,

$$(a - d)(a + d) = (c - b)(c + b),$$

d'où nous avons la proportion:

$$\frac{a-d}{2} : \frac{c-b}{2} :: \frac{c+b}{2} : \frac{a+d}{2} \qquad \text{(B)}$$

Lorsque N est pair, les quatre termes de cette proportion sont entiers. Lorsque N est impair, les quatre termes de la proportion (B) sont fractionnaires, ce qui la fait sortir des conditions générales de notre calcul. Dans tous les cas cependant on trouvera, comme ci-dessus, que la somme des carrés des quatre termes de la proportion (B) est égale à N. On peut ainsi tenir compte de la proportion (B) lors même que N est impair; mais il faut noter l'exception.

V. Nous allons nous permettre une digression, pour recueillir en passant de curieuses propriétés dont jouissent les proportions. Pour faciliter le discours nous donnerons aux proportions (A) et (B) le nom de *proportions conjuguées*. Nous demandons maintenant s'il est possible de passer de la proportion (A) à sa conjuguée (B), sans remonter à l'égalité primitive $a^2 + b^2 = c^2 + d^2$?

Retranchons chaque terme de (A) de son terme correspondant dans (B); nous aurons;

1° $$\frac{a-d}{2} - \frac{a-c}{2} = \frac{c-d}{2};$$

2° $$\frac{c-b}{2} - \frac{d-b}{2} = \frac{c-d}{2};$$

3° $$\frac{c+b}{2} - \frac{d+b}{2} = \frac{c-d}{2};$$

4° $$\frac{a+d}{2} - \frac{a+c}{2} = \frac{d-c}{2} = -\frac{c-d}{2}.$$

Les quatre différences ont des valeurs absolues égales, mais la quatrième est de signe différent des trois autres, qui ont toutes les trois le même signe. Si donc on ajoute aux trois premiers termes de (A) la différence constante $\frac{c-d}{2}$, et qu'on retranche cette même différence du quatrième terme, on obtiendra la proportion (B); et si l'on retranche des trois premiers termes de (B) cette même différence constante, et qu'on l'ajoute au quatrième terme, on retrouvera (A).

Toute proportion a-t-elle sa conjuguée? En d'autres termes, existe-t-il, pour toute proportion donnée, un nombre positif ou négatif, qui étant ajouté aux trois premiers termes et retranché du quatrième, donne une nouvelle proportion, telle que la somme des carrés des quatre termes de l'une soit égale à la somme des carrés des quatre termes de l'autre ?

Ecrivons une proportion quelconque sous cette forme:

$$m \ : \ mr \ :: \ n \ : \ nr$$

sans assujettir les nombres m, n, r, à aucune restriction. Soit x le nombre demandé, notre proportion hypothétique sera :

$$m+x \ : \ mr+x \ :: \ n+x \ : \ nr-x.$$

Donc,

$$(m+x)(nr-x) = (mr+x)(n+x),$$
$$mnr + nrx - mx - x^2 = mnr + nx + mrx + x^2,$$
$$2x^2 - nrx + mx + mrx + nx = 0,$$
$$x^2 - \frac{nr-m-mr-n}{2}\,x = 0.$$

Nous avons ainsi une équation du 2^{d} degré dont les deux racines sont

$$x=0, \qquad x=\frac{nr-m-mr-n}{2}.$$

La première racine nous fait retomber sur la proportion donnée elle-même; nous n'avons pas à nous en occuper. Substituons à x la valeur donnée par la seconde racine, nous aurons :

$$m + \frac{nr - m - mr - n}{2} : mr + \frac{nr - m - mr - n}{2}$$

$$:: n + \frac{nr - m - mr - n}{2} : nr - \frac{nr - m - mr - n}{2};$$

ou, en effectuant les opérations et en mettant en évidence les facteurs communs,

$$\frac{(n-m)\ (r-1)}{2} : \frac{(n+m)\ (r-1)}{2} :: \frac{(n-m)\ (r+1)}{2}$$

$$: \frac{(n+m)\ (r+1)}{2};$$

proportion évidente. En divisant chaque conséquent par son antécédent, nous trouvons que la raison est égale à $\frac{m+n}{m-n}$. Faisons la somme des carrés des quatre termes de cette dernière proportion, il vient:

$$\frac{(n^2 - 2nm + m^2)\ (r^2 - 2r + 1)}{4} +$$

$$\frac{(n^2 + 2nm + m^2)\ (r^2 - 2r + 1)}{4} +$$

$$\frac{(n^2 - 2nm + m^2)\ (r^2 + 2r + 1)}{4} +$$

$$\frac{(n^2 + 2nm + m^2)\ (r^2 + 2r + 1)}{4} =$$

$$\frac{2(n^2 + m^2)(r^2 - 2r + 1)}{4} + \frac{2(n^2 + m^2)(r^2 + 2r + 1)}{4} =$$

$$\frac{4\ (n^2 + m^2)\ (r^2 + 1)}{4} = m^2 + m^2r^2 + n^2 + n^2r^2.$$

Or ce dernier membre de nos égalités successives n'est autre chose que la somme des carrés des quatre termes de notre proportion donnée.

Nous obtenons ainsi ce théorème : *Dans toute proportion, si l'on fait la somme des trois premiers termes, si l'on retranche algébriquement cette somme du quatrième terme, et si l'on prend la moitié de cette différence ; si ensuite on ajoute algébriquement ce résultat aux trois premiers termes, et qu'on le retranche algébriquement du quatrième :*

1° *Les quatre nombres ainsi obtenus sont en proportion,*

2° *La somme des carrés des termes de la première proportion est égale à la somme des carrés des termes de la seconde. Les deux proportions sont conjuguées.*

Il peut arriver que la somme des trois premiers termes soit égale au quatrième; dans ce cas la différence est nulle et les deux proportions conjuguées sont identiques.

Ceci revient à dire que, la différence $c - d$ étant nulle, $c = d$ et $N = 2c^2$. En effet si l'on met à la place de d son égal c, dans les deux proportions (A) et (B), on verra qu'elles deviennent identiques.

VI. Reprenons la suite de notre calcul principal.

Tout nombre premier autre que 2 est de la forme $4e - 1$ ou de la forme $4e + 1$.

Nous savons qu'aucun nombre de la forme $4e - 1$ ne peut être la somme de deux carrés.

Depuis Fermat on sait que tout nombre premier de la forme $4e + 1$ est égal à la somme de deux carrés. Euler le premier a donné une démonstration de ce théorème.

Supposons que les facteurs premiers de N soient tous inégaux et de la forme $4e + 1$, chacun de ces facteurs sera égal à la somme de deux carrés et nous pourrons écrire :

$$N = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)(\varepsilon^2 + \zeta^2)(\eta^2 + \theta^2)....$$

Convenons de la notation suivante :

$$N' = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2),$$
$$N'' = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)(\varepsilon^2 + \zeta^2) = N'(\varepsilon^2 + \zeta^2),$$
$$N''' = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)(\varepsilon^2 + \zeta^2)(\eta^2 + \theta^2) = N''(\eta^2 + \theta^2),$$

et ainsi de suite autant que N aura de facteurs premiers.

Nous pouvons ensuite établir les équations suivantes :

$$x'^2 + y'^2 = N', \quad x''^2 + y''^2 = N'', \quad x'''^2 + y'''^2 = N''', \text{ etc.},$$

dont la dernière sera $x^2 + y^2 = N$, c'est-à-dire la proposée.

Notre première équation subsidiaire $x'^2 + y'^2 = N'$, revient à

$$x'^2 + y'^2 = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)$$

et nous savons que, dans ce cas (5),

$$x' = \alpha\gamma \pm \beta\delta \qquad y' = \beta\gamma \mp \alpha\delta.$$

Pour mettre de l'ordre et de la netteté dans le calcul, on peut lui donner la forme suivante :

$$\left.\begin{matrix} \alpha, & \gamma \\ \beta, & \delta \end{matrix}\right\} \alpha\gamma \pm \beta\delta \text{ ou bien } \beta\delta \pm \alpha\gamma,\ \beta\gamma \mp \alpha\delta \text{ ou bien } \alpha\delta \mp \beta\gamma.$$

Après avoir placé sur une colonne verticale α et β, soit les deux racines des carrés qui forment le premier facteur, on met à côté sur une seconde colonne verticale, γ et δ qui appartiennent au second facteur. Puis on multiplie entre eux les nombres situés sur une même ligne horizontale et l'on place entre ces deux produits le double signe $\pm$. Après cela on multiplie entre eux le nombre supérieur de chacune des colonnes par le nombre inférieur de l'autre colonne, ce qui fournit encore deux produits entre lesquels on place le double signe $\mp$. D'après la 1re remarque du § I, il importe fort peu dans quel ordre on place les produits séparés par chacun des doubles signes; dans la pratique on s'attachera toujours à retrancher un plus petit nombre d'un plus grand.

En prenant les signes supérieurs nous avons une première solution :

$$x' = \alpha\gamma + \beta\delta, \qquad y' = \alpha\delta - \beta\gamma;$$

et au moyen des signes inférieurs nous en obtenons une seconde :

$$x' = \alpha\gamma - \beta\delta, \qquad y' = \alpha\delta + \beta\gamma.$$

Pour simplifier nous désignerons $\alpha\gamma + \beta\delta$ par a, $\alpha\delta - \beta\gamma$ par b, $\alpha\gamma - \beta\delta$ par c et $\alpha\delta + \beta\gamma$ par d. Nous aurons ainsi $x' = a$ ou c, $y' = b$ ou d, et nous en concluons les deux égalités :

$$\mathrm{N}' = a^2 + b^2, \qquad \mathrm{N}' = c^2 + d^2.$$

Passons à notre seconde équation subsidiaire $x''^2 + y''^2 = \mathrm{N}''$, que nous pouvons écrire: $x''^2 + y''^2 = \mathrm{N}'(\varepsilon^2 + \zeta^2)$. En substituant successivement à N' chacune de ses valeurs nous aurons deux équations distinctes qu'il faudra traiter séparément l'une après l'autre,

$$x''^2 + y''^2 = (a^2 + b^2)(\varepsilon^2 + \zeta^2),$$
$$\text{et } x''^2 + y''^2 = (c^2 + d^2)(\varepsilon^2 + \zeta^2).$$

Nous obtenons ainsi, pour la première :

$$\left.\begin{matrix} a, & \varepsilon \\ b, & \zeta \end{matrix}\right\} \; a\varepsilon \pm b\zeta, \quad a\zeta \mp b\varepsilon;$$

et pour la seconde :

$$\left.\begin{matrix} c, & \varepsilon \\ d, & \zeta \end{matrix}\right\} \; c\varepsilon \pm d\zeta, \quad c\zeta \mp d\varepsilon.$$

Nous avons ainsi quatre solutions distinctes.

$$\begin{array}{lll} \text{I} & x'' = a\varepsilon + b\zeta = e, & y'' = a\zeta - b\varepsilon = f; \\ \text{II} & x'' = a\varepsilon - b\zeta = g, & y'' = a\zeta + b\varepsilon = h; \\ \text{III} & x'' = c\varepsilon + d\zeta = i, & y'' = c\zeta - d\varepsilon = k; \\ \text{IV} & x'' = c\varepsilon - d\zeta = l, & y'' = c\zeta + d\varepsilon = m. \end{array}$$

Nous tirons de là les quatre égalités suivantes:

$$N'' = e^2 + f^2,\ N'' = g^2 + h^2,\ N'' = i^2 + k^2,\ N'' = l^2 + m^2.$$

Il s'ensuit que notre troisième équation subsidiaire $x'''^2 + y'''^2 = N'''$, qui peut s'écrire $x'''^2 + y'''^2 = N''\,(\eta^2 + \theta^2)$ prendra successivement les quatre formes suivantes qu'il faudra traiter l'une après l'autre:

$$\begin{aligned} x'''^2 + y'''^2 &= (e^2 + f^2)\,(\eta^2 + \theta^2), \\ x'''^2 + y'''^2 &= (g^2 + h^2)\,(\eta^2 + \theta^2), \\ x'''^2 + y'''^2 &= (i^2 + k^2)\,(\eta^2 + \theta^2), \\ x'''^2 + y'''^2 &= (l^2 + m^2)\,(\eta^2 + \theta^2). \end{aligned}$$

Cela fournira huit couples de valeurs, et ainsi cette troisième équation aura huit solutions différentes.

L'on continuera ainsi jusqu'à l'épuisement de tous les facteurs premiers de N; le dernier calcul donnera les solutions de l'équation proposée.

VII. Remontons aux équations (6) de notre § II, savoir:

$$\alpha^2 + \beta^2 = F, \qquad \gamma^2 + \delta^2 = F',$$

qui, étant multipliées membre à membre, redonnent la proposée (1) sous cette forme (4)

$$x^2 + y^2 = (\alpha^2 + \beta^2)\,(\gamma^2 + \delta^2) = FF' = N;$$

en suite de quoi nous avons (5):

$$x = \alpha\,\gamma \pm \beta\delta, \qquad y = \alpha\delta \mp \beta\gamma.$$

Supposons le cas particulier où l'on a $\beta = 0$. La proposée devient alors de la forme

$$x^2 + y^2 = \alpha^2 (\gamma^2 + \delta^2)$$

et les valeurs de x et de y se réduisent à

$$x = \alpha\gamma, \qquad y = \alpha\delta,$$

ce qui du reste dérive directement de la forme que la proposée a revêtue.

Nous verrons bientôt à quels cas cette observation est applicable.

VIII. Il résulte de ce que nous venons de voir, que lorsque l'on veut résoudre une équation donnée en nombres,

$$x^2 + y^2 = N,$$

il faut chercher les facteurs premiers de N. Désignons ces facteurs par p, p', p'', p'''...., nous avons ainsi $N = pp'p''p'''$.... Voyons ce qui a lieu suivant les diverses suppositions que l'on peut faire sur la nature de ces facteurs premiers.

a) Supposons d'abord qu'aucun de ces facteurs n'étant égal à 2, il y en ait un seul de la forme $4e - 1$, et que ce soit le facteur p. Ce facteur n'étant pas résoluble en la somme de deux carrés, il n'y a pas lieu d'appliquer le calcul du § VI. Ainsi N ne peut être égal à la somme de deux carrés. Ce résultat est confirmé par la remarque suivante. Tous les facteurs p', p'', p'''... sont d'après notre supposition, de la forme $4e + 1$; leur produit $p'p''p'''$... est en consépuence de la forme $4e + 1$. Il s'ensuit que le produit $p \times p'p''p'''$... ayant deux facteurs, l'un de la forme $4e - 1$ et l'autre de la forme $4e + 1$, sera lui-même de la forme $4e - 1$. C'est-à-dire que N, qui est égal à $p \times p'p''p'''$... ne sera pas résoluble en la somme de deux carrés.

b) Cette conclusion sera applicable au cas où avec un facteur p de la forme $4e - 1$, N en aurait un autre p' de la même forme et différent de p. Car si le calcul du § VI n'est pas applicable pour un de ces facteurs, il le sera encore moins, si au premier on en ajoute un second.

On pourrait objecter, toutefois, que si p et p' sont chacun de la forme $4e - 1$, et ne sont pas séparément résolubles, leur produit pp', qui est de la forme $4e + 1$, pourrait bien être résoluble et permettre ainsi l'emploi du calcul du § VI. Mais c'est ce qui n'a pas lieu (1).

Nous pouvons étendre notre remarque actuelle au cas où les facteurs de la forme $4e - 1$ seraient en nombre quelconque et tous inégaux entr'eux, ou du moins élevés à des puissances impaires. En somme, il suffit de la présence d'un seul facteur de la forme $4e - 1$ élevé à une puissance impaire pour mettre obstacle à la résolution de l'équation proposée.

c) Si les deux facteurs p et p' de la forme $4e - 1$ sont égaux, nous avons le cas du § VII. Le nombre N est de la forme $4e + 1$; nous pouvons poser $N = p^2 N'$, et le nombre N' n'aura que des facteurs de la forme $4e + 1$.

Notre équation proposée (1) pourra s'écrire :

$$x^2 + y^2 = p^2 N' ;$$

et après avoir résolu l'équation subsidiaire,

$$x'^2 + y'^2 = N',$$

les produits de p par chacune des valeurs de x' et de y' nous donneront les solutions de la proposée.

(1) Il est nécéssaire de démontrer ce lemme; mais cette démonstration étant assez longue, pour ne pas interrompre le fil de nos déductions actuelles nous la réservons pour une note que l'on trouvera à la fin de ce mémoire.

Cette remarque est applicable au cas ou p serait élevé à une puissance paire quelconque, ainsi qu'au cas où, au lieu d'un seul facteur de la forme $4e - 1$, il y en aurait plusieurs tous respectivement élevés à des puissances paires, en sorte que N serait égal à $p^{2r}p'^{2s}p''^{2t}...N'$. De cette manière les solutions de la proposée seraient égales aux produits de chacune des solutions de l'équation subsidiaire $x'^2 + y'^2 = N$, par le facteur $p^r p'^s p''^t$... Nous indiquerons désormais ce facteur carré, quelle qu'en soit la nature, par m^2.

d) Si deux facteurs premiers de la forme $4e + 1$ étaient égaux entre eux, on pourrait sans doute y retrouver le cas du § VII. Toutefois, en procédant ainsi on laisserait échapper telle ou telle solution de la proposée. C'est ce que nous allons faire voir.

Soit $N = (a^2 + b^2)\ (\eta^2 + \theta^2)\ (\eta^2 + \theta^2)$; a et b donnant une des solutions d'une des équations subsidiaires du § VI. Appliquons notre forme de calcul, comme si les deux facteurs premiers égaux à $(\eta^2 + \theta^2)$ se trouvaient être des facteurs quelconques.

Nous avons d'abord, au moyen du premier facteur $(\eta^2 + \theta^2)$:

$$\begin{array}{c|l} a,\ \eta & \\ b,\ \theta & a\eta \pm b\theta, \quad a\theta \mp b\eta. \end{array}$$

Puis, au moyen du second facteur $(\eta^2 + \theta^2)$:

$$\begin{array}{l|c} a\eta + b\theta, \eta & (a\eta^2 + b\eta\theta) \pm (a\theta^2 - b\eta\theta), \\ a\theta - b\eta, \theta & (a\eta\theta + b\theta^2) \mp (a\eta\theta - b\eta^2), \end{array}$$

$$\begin{array}{l|c} a\eta - b\theta, \eta & (a\eta^2 - b\eta\theta) \pm (a\theta^2 + b\eta\theta), \\ a\theta + b\eta, \theta & (a\eta\theta - b\theta^2) \mp (a\eta\theta + b\eta^2). \end{array}$$

Nos quatre solutions, toutes réductions opérées, sont ainsi :

1° $x = a(\eta^2 + \theta^2)$ $\quad y = b(\eta^2 + \theta^2)$

2° $x = a\eta^2 + 2b\eta\theta - a\theta^2$ $\quad y = 2a\eta\theta - b\eta^2 + b\theta^2$

3° $x = a(\eta^2 + \theta^2)$ $\quad y = b(\eta^2 + \theta^2)$

4° $x = a\eta^2 - 2b\eta\theta - a\theta^2$ $\quad y = 2a\eta\theta + b\eta^2 - b\theta^2$.

Sur ces quatre solutions nous en trouvons deux qui sont identiques, la première et la troisième ; c'est la solution que donne l'application du § VII. Mais il y a en outre la seconde et la quatrième que l'application du § VII ne nous aurait pas fournies. Si donc, parmi les facteurs premiers de N de la forme $4e+1$, on trouvait un certain nombre de facteurs égaux, on ne laisserait pas d'appliquer la méthode de calcul du § VI. Seulement on rencontrerait un certain nombre de solutions répétées, et l'on aurait soin de ne compter qu'une fois chacune de ces dernières.

e) Il nous reste à examiner le cas ou le nombre 2 se trouverait parmi les facteurs premiers de N.

Le nombre 2 est égal à la somme des deux carrés $1+1$; par conséquent on peut mettre en œuvre notre forme générale de calcul.

Soit donc $N = 2(a^2 + b^2)$, nous obtiendrons :

$$\begin{array}{cc|c} a, & 1 & \\ b, & 1 & \end{array}\; a \pm b,\ a \mp b; \quad \begin{array}{ll} x = a + b, & y = a - b, \\ x = a - b, & y = a + b; \end{array}$$

c'est-à-dire que nos deux solutions sont identiques et reviennent à une seule. En effet,

$$x^2 + y^2 = a^2 \pm 2ab + b^2 + a^2 \mp 2ab + b^2 = 2a^2 + 2b^2 = N.$$

Le facteur 2 n'augmente donc pas le nombre des solutions de la proposée.

Il en résulte que, si ce facteur est élevé à une puissance paire, on peut appliquer le cas du § VII et faire entrer le facteur 2^{2n} dans le facteur m^2 du § VIII, c. Si le facteur 2 est élevé à une puissance impaire, nous pouvons décomposer la puissance 2^{2n+1} en deux facteurs, 2^{2n} et 2; nous ferons passer le premier dans le facteur m^2, et nous tiendrons compte du second dans le calcul des solutions subsidiaires.

IX. Quant à la résolution des nombres premiers de la forme $4e+1$ en la somme de deux carrés, c'est une affaire de tâtonnement.

Voir le tableau de ces nombres au-dessous de 1000 à la page suivante.

X. Si l'on veut passer des solutions de l'équation proposée aux proportions conjuguées qui en dépendent, les formules (A) et (B) des §§ III et IV font voir la marche à suivre. Il est cependant nécessaire de prendre quelques précautions pour donner au calcul de l'ordre et de la facilité.

Soient $x=a$, $y=b$; $x=c$, $y=d$, deux solutions de l'équation (1); il en résulte $a^2+b^2=c^2+d^2=\mathrm{N}$. Nous pouvons, sans nuire à la généralité de nos résultats, grâce à la symétrie en x et y de l'équation proposée, supposer $a>b$, et $a>c$, et $c>d$; il en résulte $b<d$. Nous voyons par l'inspection de la formule (A), que les extrêmes de cette proportion sont égaux à la demi-différence et à la demi-somme des valeurs de x, et que les moyens sont égaux à la demi-différence et à la demi-somme des valeurs de y. Pour passer à la conjuguée (B), le moyen le plus simple est d'ajouter aux trois premiers termes de

$2 = 1^2 + 1^2$	$277 = 14^2 + 9^2$	$617 = 19^2 + 16^2$
$5 = 2^2 + 1^2$	$281 = 16^2 + 5^2$	$641 = 25^2 + 4^2$
$13 = 3^2 + 2^2$	$293 = 17^2 + 2^2$	$653 = 22^2 + 13^2$
$17 = 4^2 + 1^2$	$313 = 13^2 + 12^2$	$661 = 25^2 + 6^2$
$29 = 5^2 + 2^2$	$317 = 14^2 + 11^2$	$673 = 23^2 + 12^2$
$37 = 6^2 + 1^2$	$337 = 16^2 + 9^2$	$677 = 26^2 + 1^2$
$41 = 5^2 + 4^2$	$349 = 18^2 + 5^2$	$701 = 26^2 + 5^2$
$53 = 7^2 + 2^2$	$353 = 17^2 + 8^2$	$709 = 22^2 + 15^2$
$61 = 6^2 + 5^2$	$373 = 18^2 + 7^2$	$733 = 27^2 + 2^2$
$73 = 8^2 + 3^2$	$389 = 17^2 + 10^2$	$757 = 26^2 + 9^2$
$89 = 8^2 + 5^2$	$397 = 19^2 + 6^2$	$761 = 20^2 + 19^2$
$97 = 9^2 + 4^2$	$401 = 20^2 + 1^2$	$769 = 25^2 + 12^2$
$101 = 10^2 + 1^2$	$409 = 20^2 + 3^2$	$773 = 22^2 + 17^2$
$109 = 10^2 + 3_2$	$421 = 15^2 + 14^2$	$797 = 26^2 + 11^2$
$113 = 8^2 + 7^2$	$433 = 17^2 + 12^2$	$809 = 28^2 + 5^2$
$137 = 11^2 + 4^2$	$449 = 20^2 + 7^2$	$821 = 25^2 + 14^2$
$149 = 10^2 + 7^2$	$457 = 21^2 + 4^2$	$829 = 27^2 + 10^2$
$157 = 11^2 + 6^2$	$461 = 19^2 + 10^2$	$853 = 23^2 + 18^2$
$173 = 13^2 + 2^2$	$509 = 22^2 + 5^2$	$857 = 29^2 + 4^2$
$181 = 10^2 + 9^2$	$521 = 20^2 + 11^2$	$877 = 29^2 + 6^2$
$193 = 12^2 + 7^2$	$541 = 21^2 + 10^2$	$881 = 25^2 + 16^2$
$197 = 14^2 + 1^2$	$557 = 19^2 + 14^2$	$929 = 23^2 + 20^2$
$229 = 15^2 + 2^2$	$569 = 20^2 + 13^2$	$937 = 24^2 + 19^2$
$233 = 13^2 + 8^2$	$577 = 24^2 + 1^2$	$941 = 29^2 + 10^2$
$241 = 15^2 + 4^2$	$593 = 23^2 + 8^2$	$953 = 28^2 + 13^2$
$257 = 16^2 + 1^2$	$601 = 24^2 + 5^2$	$977 = 31^2 + 4^2$
$269 = 13^2 + 10^2$	$613 = 18^2 + 17^2$	$997 = 31^2 + 6^2$

(A) la différence constante $\frac{c-d}{2}$, et de retrancher cette différence du quatrième terme (§ V).

En prenant ainsi deux à deux toutes les solutions de la proposée, on obtiendra tous les couples de proportions conjuguées que pourra fournir l'équation que l'on aura traitée. Soit n le nombre des solutions, le nombre des couples de proportions sera donc $\frac{n(n-1)}{2}$.

XI. Il nous reste à présenter des exemples de calcul.

Soit l'équation proposée:

$$x^2 + y^2 = 1034280.$$

Si nous recherchons les facteurs premiers du nombre donné nous trouverons

$$1034280 = 2^3 . 3^2 . 5 . 13^2 . 17.$$

Il en résulte que le facteur m^2 est égal à $2^2 . 3^2 . = 36$, et que $m = 6$. Divisons 1034280 par 36, nous avons pour équation subsidiaire, $\frac{1034280}{36}$ étant égal à 28730,

$$x'^2 + y'^2 = 28730 = 10 . 13 . 13 . 17.$$

Nous avons fait entrer 3^2 dans le facteur m^2, parce que 3 est de la forme $4e - 1$, tandis que nous avons réservé 13, pour le mettre deux fois en usage dans la résolution de l'équation subsidiaire, parce que 13 est de la forme $4e + 1$. Nous avons fait entrer 2^2 dans le facteur m^2; nous avons réuni le troisième facteur égal à 2 avec le facteur 5, pour former le facteur 10, ce qui abrége les calculs. Or

$$10 . 13 . 13 . 17 = (3^2 + 1^2)(3^2 + 2^2)(3^2 + 2^2)(4^2 + 1^2);$$

les deux premiers facteurs nous donnent:

$$\begin{array}{c|c|c} 3,\ 3 & & 11 \text{ ou } 7, \\ 1,\ 2 & 9 \pm 2,\ 6 \mp 3 & 3 \text{ ou } 9. \end{array}$$

Ainsi nous avons:

$$(3^2 + 1^2)(3^2 + 2^2) = 11^2 + 3^2,$$
$$(3^2 + 1^2)(3^2 + 2^2) = 9^2 + 7^2.$$

En conséquence le troisième facteur $(3^2 + 2^2)$ combiné avec les deux précédents nous donnera :

$$\begin{array}{r|c|r} 11,\ 3 & & 39 \text{ ou } 27\ ; \\ 3,\ 2 & \raise{1ex}{33 \pm 6,\ \ 22 \mp 9} & 13 \text{ ou } 31\ ; \end{array}$$

$$\begin{array}{r|c|r} 9,\ 3 & & 41 \text{ ou } 13; \\ 7,\ 2 & \raise{1ex}{27 \pm 14,\ 21 \mp 18} & 3 \text{ ou } 39. \end{array}$$

La solution 19 et 13 se présente deux fois, nous n'en tiendrons compte qu'une seule fois. Il vient donc :

$$(3^2 + 1^2)\ (3^2 + 2^2)\ (3^2 + 2^2) = 41^2 + \ \ 3^2,$$
$$(3^2 + 1^2)\ (3^2 + 2^2)\ (3^2 + 2^2) = 39^2 + 13^2,$$
$$(3^2 + 1^2)\ (3^2 + 2^2)\ (3^2 + 2^2) = 31^2 + 27^2.$$

Combinons le quatrième facteur $(4^2 + 1^2)$ avec les trois précédents, nous aurons :

$$\begin{array}{r|c|r} 41,\ 4 & & 167 \text{ ou } 161\ ; \\ 3,\ 1 & \raise{1ex}{164 \pm 3,\ 41 \mp 12} & 29 \text{ ou } \ \ 53\ ; \\ 39,\ 4 & & 169 \text{ ou } 143\ ; \\ 13,\ 1 & \raise{1ex}{156 \pm 13,\ 52 \mp 39} & 13 \text{ ou } \ \ 91\ ; \\ 31,\ 4 & & 151 \text{ ou } \ \ 97\ ; \\ 27,\ 1 & \raise{1ex}{124 \pm 27,\ 108 \mp 31} & 77 \text{ ou } 139. \end{array}$$

Nous avons ainsi six solutions pour notre équation subsidiaire, savoir :

$$x' = 169,\ 167,\ 161,\ 151,\ 143,\ 139.$$
$$y' = \ \ 13,\ \ 29,\ \ 53,\ \ 77,\ \ 91,\ \ 97.$$

En multipliant chacun de ces nombres par 6, nous trouvons enfin pour la proposée les six solutions :

$$x = 1014,\quad 1002,\quad 966,\quad 906,\quad 858,\quad 834.$$
$$y = \quad 78,\quad 174,\quad 318,\quad 462,\quad 546,\quad 582.$$

Vérification :

$$1014^2 + 78^2 = 1028196 + 6084 = 1034280,$$
$$1002^2 + 174^2 = 1004004 + 30276 = 1034280,$$
$$966^2 + 318^2 = 933156 + 101124 = 1034280,$$
$$906^2 + 462^2 = 820836 + 213444 = 1034280,$$
$$858^2 + 546^2 = 736164 + 298116 = 1034280,$$
$$834^2 + 582^2 = 695556 + 338724 = 1034280.$$

Nous allons passer aux proportions conjuguées qui dérivent de nos solutions. Nous en aurons autant de couples qu'on peut faire de combinaisons 2 à 2 avec 6 nombres, c'est-à-dire 15.

Remettons sous nos yeux les formules qu'il nous faut appliquer.

$$N = a^2 + b^2 = c^2 + d^2$$

$$(A) \quad \frac{a-c}{2} : \frac{d-b}{2} :: \frac{d+b}{2} : \frac{a+c}{2},$$

d'où l'on passe à la conjuguée (B) au moyen de la différence

$$\frac{c-d}{2}.$$

1° $a = 1014,\ b = 78,\ c = 834,\ d = 582,\ \dfrac{c-d}{2} = 126,$
1re et 6e solutions.

(A) 90 : 252 : : 330 : 924 (B) 216 : 378 : : 456 : 798.

2° $a = 1002,\ b = 174,\ c = 834,\ d = 582,\ \dfrac{c-d}{2} = 126,$
2e et 6e solutions.

(A) 84 : 204 : : 378 : 918 (B) 210 : 330 : : 504 : 792.

3° $a = 966,\ b = 318,\ c = 834,\ d = 582,\ \dfrac{c-d}{2} = 126,$
3e et 6e solutions.

(A) 66 : 132 : : 450 : 900 (B) 192 : 258 : : 576 : 774.

4° $a = 906,\ b = 462,\ c = 834,\ d = 582,\ \dfrac{c-d}{2} = 126,$
4^e et 6^e solutions.

(A) 36 : 60 : : 522 : 870 (B) 162 : 186 : : 648 : 744.

5° $a = 858,\ b = 546,\ c = 834,\ d = 582,\ \dfrac{c-d}{2} = 126,$
5^e et 6^e solutions.

(A) 12 : 18 : : 564 : 846 (B) 138 : 144 : : 690 : 720.

6° $a = 1014,\ b = 78,\ c = 858,\ d = 546,\ \dfrac{c-d}{2} = 156,$
1re et 5^e solutions.

(A) 78 : 234 : : 312 : 936 (B) 234 : 390 : : 468 : 780.

7° $a = 1002,\ b = 174,\ c = 858,\ d = 546,\ \dfrac{c-d}{2} = 156,$
2^e et 5^e solutions.

(A) 72 : 186 : : 360 : 930 (B) 228 : 342 : : 516 : 774.

8° $a = 966,\ b = 318,\ c = 858,\ d = 546,\ \dfrac{c-d}{2} = 156,$
3^e et 5^e solutions.

(A) 54 : 114 : : 432 : 912 (B) 210 : 270 : : 588 : 756.

9° $a = 906,\ b = 462,\ c = 858,\ d = 546,\ \dfrac{c-d}{2} = 156,$
4^e et 5^e solutions.

(A) 24 : 42 : : 504 : 882 (B) 180 : 198 : : 660 : 726.

10° $a = 1014,\ b = 78,\ c = 906,\ d = 462,\ \dfrac{c-d}{2} = 222,$
1re et 4^e solutions.

(A) 54 : 192 : : 270 : 960 (B) 276 : 414 : : 492 : 738.

11° $a = 1002,\ b = 174,\ c = 906,\ d = 462,\ \dfrac{c-d}{2} = 222,$
2^e et 4^e solutions.

(A) 48 : 144 : : 318 : 954 (B) 270 : 366 : : 540 : 732.

12° $a = 966,\ b = 318,\ c = 906,\ d = 462,\ \dfrac{c-d}{2} = 222,$

3e et 4e solutions.

(A) 30 : 72 : : 390 : 936 (B) 252 : 294 : : 612 : 714.

13° $a = 1014,\ b = 78,\ c = 966,\ d = 318,\ \dfrac{c-d}{2} = 324,$

1re et 3e solutions.

(A) 24 : 120 : : 198 : 990 (B) 348 : 444 : : 522 : 666.

14° $a = 1002,\ b = 174,\ c = 966,\ d = 318,\ \dfrac{c-d}{2} = 324,$

2e et 3e solutions.

(A) 18 : 72 : : 246 : 984 (B) 342 : 396 : : 570 : 660.

15° $a = 1014,\ b = 78,\ c = 1002,\ d = 174,\ \dfrac{c-d}{2} = 414,$

1re et 2e solutions.

(A) 6 : 48 : : 126 : 1008 (B) 420 : 462 : : 540 : 594.

Dans toutes ces proportions la somme des carrés des quatre termes est égale à 1034280, ce que l'on peut vérifier. Prenons la première venue, par exemple, la proportion (B) du n° 8 — elle donnera : $210^2 + 270^2 + 588^2 + 756^2 = 44100 + 72900 + 345744 + 571536 = 1034280$. Tout autre proportion donnerait un même résultat.

Cet exemple peut être considéré comme complet ; cependant nous en ajouterons encore un, qui présente le cas très-spécial où plusieurs couples de proportions conjuguées se trouvent réduits chacun à une seule proportion, la différence constante $\dfrac{c-d}{2}$ étant égale à 0, comme nous l'avons indiqué à la fin du § V.

Soit $$x^2 + y^2 = 8450;$$
nous trouvons
$$8450 = 2.\,5.\,5.\,13.\,13 = (3^2 + 1^2)\,(2^2 + 1^2)\,(3^2 + 2^2)\,(3^2 + 2^2).$$

Ainsi nous instituons notre calcul comme suit :

3, 2	$6 \pm 1,\quad 3 \mp 2$	7 ou 5 ;
1, 1		1 ou 5 ;
7, 3	$21 \pm 2,\quad 14 \mp 3$	23 ou 19 ;
1, 2		11 ou 17 ;
5, 3	$15 \pm 10,\quad 15 \mp 10$	25 ou 5 ;
5, 2		5 ou 25 ;
23, 3	$69 \pm 22,\quad 46 \mp 33$	91 ou 47 ;
11, 2		13 ou 79 ;
19, 3	$57 \pm 34,\quad 51 \mp 38$	91 ou 23 ;
17, 2		13 ou 89 ;
25, 3	$75 \pm 10,\quad 50 \mp 15$	85 ou 65 ;
5, 2		35 ou 65.

Nos solutions, au nombre de 5 à cause des doubles emplois, sont ainsi :
$$x = 91,\ 89,\ 85,\ 79,\ 65,$$
$$y = 13,\ 23,\ 35,\ 47,\ 65.$$

1° $a=91$, $b=13$, $c=65$, $d=65$, $\dfrac{c-d}{2} = 0$, 1re et 5^e solutions.

(A) et (B) 13 : 26 : : 39 : 78.

2° $a=89$, $b=23$, $c=65$, $d=65$, $\dfrac{c-d}{2} = 0$, 2^e et 5^e solutions.

(A) et (B) 12 : 21 : : 44 : 77.

3° $a=85$, $b=35$, $c=65$, $d=65$, $\dfrac{c-d}{2} = 0$, 3^e et 5^e solutions.

(A) et (B) 10 : 15 : : 50 : 75.

4° $a=79$, $b=47$, $c=65$, $d=65$, $\dfrac{c-d}{2} = 0$, 4^e et 5^e solutions.

(A) et (B) 7 : 9 : : 56 : 72.

Dans toutes ces proportions la somme des trois premiers termes est égale au quatrième, ensorte que la seconde méthode du § V pour calculer la différence entre les termes de même rang des proportions conjuguées nous conduit, de son côté, au même résultat. Pour être complet nous allons donner les autres proportions quoique nous n'ayons rien de particulier à y remarquer.

5° $a=91$, $b=13$, $c=79$, $d=47$, $\frac{c-d}{2}=16$, 1re et 4e solutions.

(A) 6 : 17 : : 30 : 85 (B) 22 : 33 : : 46 : 69.

6° $a=89$, $b=23$, $c=79$, $d=47$, $\frac{c-d}{2}=16$, 2e et 4e solutions.

(A) 5 : 12 : : 35 : 84 (B) 21 : 28 : : 51 : 68.

7° $a=85$, $b=35$, $c=79$, $d=47$, $\frac{c-d}{2}=16$, 3e et 4e solutions.

(A) 3 : 6 : : 41 : 82 (B) 19 : 22 : : 57 : 66.

8° $a=91$, $b=13$, $c=85$, $d=35$, $\frac{c-d}{2}=25$, 1re et 3e solutions.

(A) 3 : 11 : : 24 : 88 (B) 28 : 36 : : 49 : 63.

9° $a=89$, $b=23$, $c=85$, $d=35$, $\frac{c-d}{2}=25$, 2e et 3e solutions.

(A) 2 : 6 : : 29 : 87 (B) 27 : 31 : : 54 : 62.

10° $a=91$, $b=13$, $c=89$, $d=23$, $\frac{c-d}{2}=33$, 1re et 2e solutions.

(A) 1 : 5 : : 18 : 90 (B) 34 : 38 : : 51 : 57.

NOTE.

Démonstration du lemme énoncé au § VIII.

Deux nombres premiers p et p', tous deux de la forme $4e - 1$, ne sont ni l'un ni l'autre résolubles en la somme de deux carrés; leur produit pp', quoique étant de la forme $4e + 1$, n'est pas résoluble non plus en la somme de deux carrés.

Tel est le lemme qu'il s'agit de démontrer.

En admettant pour α, β, γ, δ, des valeurs imaginaires, nous pouvons poser les égalités,

$$p = \alpha^2 + \beta^2 \quad , \quad p' = \gamma^2 + \delta^2.$$

Nous savons (§ II) que, dans ce cas, l'équation

$$x^2 + y^2 = pp'$$

a pour solution (5)

$$x = \alpha\gamma \pm \beta\delta \quad , \quad y = \alpha\delta \mp \beta\gamma,$$

et la question est de savoir si, dans le calcul nécessaire pour obtenir les valeurs numériques de x et de y, il arrive, ou non, que les symboles imaginaires soient éliminés et que l'on obtienne des valeurs réelles.

I

Commençons par rechercher la forme que doivent prendre les imaginaires pour que p soit égal à la somme de deux carrés.

Posons par hypothèse, en désignant par a, b, c, d, des quantités réelles et entières qu'il s'agira de déterminer en fonction de p :

$$(a \pm b\sqrt{-1})^2 + (c \mp d\sqrt{-1})^2 = p. \qquad (a)$$

Or p étant réel, les termes affectés d'immaginaires doivent disparaître dans le développement de cette égalité, c'est pour cela que nous avons pris avec des signes contraires les termes qui renferment $\sqrt{-1}$.

Développons notre égalité il vient :

$$a^2 - b^2 \pm 2ab\sqrt{-1} + c^2 - d^2 \mp 2cd\sqrt{-1} = p. \qquad (b)$$

Ponr que les termes imaginaires disparaissent, il faut et il suffit que l'on ait $ab = cd$, ou, ce qui revient au même, que l'on ait la proportion $a : c :: d : b$.

En faisant $a = \varkappa\mu$, $c = \lambda\mu$, $d = \varkappa\nu$, $b = \lambda\nu$, notre proportion s'écrit $\varkappa\mu : \lambda\mu :: \varkappa\nu : \lambda\nu$, ce qui est la forme générale des proportions dont les termes sont des nombres entiers. Substituons ces valeurs de a, b, c. d, dans l'égalité (b), il vient après réduction :

$$\varkappa^2\mu^2 - \lambda^2\nu^2 + \lambda^2\mu^2 - \varkappa^2\nu^2 = p\,,$$

ou, ce qui est la même chose,

$$(\varkappa^2 + \lambda^2)\,(\mu^2 - \nu^2) = p. \qquad (c)$$

Or p est un nombre premier dont les facteurs sont 1 et p; de plus, p étant de la forme $4e - 1$ ne peut être égal à $\varkappa^2 + \lambda^2$. Ainsi nous avons évidemment

$$(\varkappa^2 + \lambda^2) = 1; \qquad (d)$$

$$(\mu^2 - \nu^2) = p. \qquad (e)$$

L'égalité (d) ne peut subsister qu'en faisant $\varkappa = 1$, $\lambda = 0$, ou bien $\varkappa = 0$, $\lambda = 1$. Mais, vu la symétrie de nos égalités, la conclusion générale sera la même dans les deux cas, la marche du calcul présentera seule quelques différences.

Prenons $x = 1$, $\lambda = 0$.

D'un autre côté l'égalité (e) peut se mettre sous la forme

$$(\mu - \nu)(\mu + \nu) = 1 . p,$$

d'où nous tirons évidemment

$$\mu - \nu = 1 , \qquad \mu + \nu = p,$$

ce qui donne,

$$\mu = \frac{p+1}{2}, \qquad \nu = \frac{p-1}{2}.$$

Or p étant un nombre impair, il s'ensuit que μ et ν sont des nombres entiers. Substituant les valeurs de x, λ, μ, ν, dans l'expression de a, b, c, d, nous obtenons $a = \frac{p+1}{2}$, $b = 0$, $c = 0$, $d = \frac{p-1}{2}$; et notre égalité (a) devient :

$$\left(\frac{p+1}{2}\right)^2 + \left(\frac{p-1}{2}\sqrt{-1}\right)^2 = p. \qquad (f)$$

En développant le premier membre on le trouve identique au second; en effet

$$\left(\frac{p^2+2p+1}{4}\right) - \left(\frac{p^2-2p+1}{4}\right) = \frac{4p}{4} = p.$$

Les quantités mises entre parenthèses dans (f) étant élevées au carré, nous n'avons pas à nous inquiéter de leurs signes. Telle est la seule manière dont p, nombre premier de la forme $4e - 1$, peut être décomposé en la somme de deux carrés.

Exemple. Soit $p = 19$, $x = \frac{19+1}{2} = 10$, $y = \frac{19-1}{2}\sqrt{-1} = 9\sqrt{-1}$.

Or $10^2 + (9\sqrt{-1})^2 = 100 - 81 = 19$.

II

Puisque nous avons $\left(\frac{p+1}{2}\right)^2 + \left(\frac{p-1}{2}\sqrt{-1}\right)^2 = p$, nous avons aussi $\left(\frac{p'+1}{2}\right)^2 + \left(\frac{p'-1}{2}\sqrt{-1}\right)^2 = p'$. Or nous savons § II, que N étant égal à $(\alpha^2+\beta^2)(\gamma^2+\delta^2)$, l'équation $x^2+y^2=\mathrm{N}$ a pour solutions $x=\alpha\gamma\pm\beta\delta$, $y=\alpha\delta\mp\beta\gamma$. Dans le cas actuel $\mathrm{N}=pp'=$

$$\left[\left(\frac{p+1}{2}\right)^2 + \left(\frac{p-1}{2}\sqrt{-1}\right)^2\right] \times$$
$$\left[\left(\frac{p'+1}{2}\right)^2 + \left(\frac{p'-1}{2}\sqrt{-1}\right)^2\right];$$

il en résulte que nous avons, en faisant

$$\alpha=\frac{p+1}{2},\ \beta=\frac{p-1}{2}\sqrt{-1},\ \gamma=\frac{p'+1}{2},$$
$$\delta=\frac{p'-1}{2}\sqrt{-1},$$
$$x=\frac{(p+1)(p'+1)}{4}\mp\frac{(p-1)(p'-1)}{4},$$
$$y=\left(\frac{(p+1)(p'-1)}{4}\mp\frac{(p-1)(p'+1)}{4}\right)\sqrt{-1}.$$

Ainsi pour x les imaginaires sont éliminées et les deux valeurs sont réelles; mais pour y les imaginaires n'ont pas disparu.

Il en résulte que l'équation $x^2+y^2=pp'$ n'a aucune solution réelle. C. Q. F. D.

Si l'on développe et réduit les valeurs de x et de y, on obtiendra les deux solutions séparées :

$$1^0 \quad x = \frac{p + p'}{2}, \qquad y = \frac{p - p'}{2}\sqrt{-1};$$

$$2^0 \quad x = \frac{pp' + 1}{2}, \qquad y = \frac{pp' - 1}{2}\sqrt{-1}.$$

Vérification :

$$1^0 \; x^2 + y^2 = \left(\frac{p + p'}{2}\right)^2 + \left(\frac{p - p'}{2}\sqrt{-1}\right)^2 =$$

$$\frac{p^2 + 2pp' + p'^2}{4} - \frac{p^2 - 2pp' + p'^2}{4} = \frac{4pp'}{4} = pp'.$$

$$2^0 \; x^2 + y^2 = \left(\frac{pp' + 1}{2}\right)^2 + \left(\frac{pp' - 1}{2}\sqrt{-1}\right)^2 =$$

$$\frac{p^2p'^2 + 2pp' + 1}{4} - \frac{p^2p'^2 - 2pp' + 1}{4} = \frac{4pp'}{4} = pp'.$$

Exemple : $p = 19, \; p' = 11, \; pp' = 209.$

L'équation à résoudre est ainsi :

$$x^2 + y^2 = 209$$

$$1^0 \; x = \frac{p + p'}{2} = \frac{19 + 11}{2} = 15, \; y = \frac{p - p'}{2}\sqrt{-1} =$$

$$\frac{19 - 11}{2}\sqrt{-1} = 4\sqrt{-1};$$

$$15^2 - 4^2 = 225 - 16 = 209.$$

$$2^0 \; x = \frac{pp' + 1}{2} = \frac{209 + 1}{2} = 105, \; y = \frac{pp' - 1}{2}\sqrt{-1} =$$

$$\frac{209 - 1}{2}\sqrt{-1} = 104\sqrt{-1};$$

$$105^2 - 104^2 = 11025 - 10816 = 209.$$

III

Nous pouvons faire ici une remarque qui ne nous semble pas dénuée d'intérêt. Les solutions imaginaires que nous venons de trouver pour les équations

$$x^2 + y^2 = p, \quad x^2 + y^2 = pp',$$

ne sont autre chose, quand on supprime le facteur $\sqrt{-1}$, que les solutions réelles des équations

$$x^2 - y^2 = p, \quad x^2 - y^2 = pp'.$$

La résolution de l'équation générale

$$x^2 - y^2 = \mathrm{N} \qquad (g)$$

est extrêmement simple. Posons $\mathrm{N} = \mathrm{FF}'$, en prenant $\mathrm{F} > \mathrm{F}'$; nous pouvons mettre l'équation (g) sous la forme :

$$(x + y)(x - y) = \mathrm{FF}'.$$

Nous tirons de là :

$$x + y = \mathrm{F}, \qquad x - y = \mathrm{F}';$$

et nous avons, en conséquence,

$$x = \frac{\mathrm{F} + \mathrm{F}'}{2}, \quad y = \frac{\mathrm{F} - \mathrm{F}'}{2}.$$

Pour que x et y soient des nombres entiers, il faut que F et F′ soient tous deux des nombres pairs, ou tous deux des nombres impairs.

Exemples. Soit $x^2 - y^2 = 40$, les facteurs utiles de 40 sont : 2 et 20, ou 4 et 10.

Ainsi :

$$1^0 \ x = \frac{20 + 2}{2} = 11, \qquad y = \frac{20 - 2}{2} = 9.$$

En effet

$$11^2 - 9^2 = 121 - 81 = 40.$$

$$2^0 \quad x = \frac{10+4}{2} = 7, \qquad y = \frac{10-4}{2} = 3.$$

En effet

$$7^2 - 3^2 = 49 - 9 = 40.$$

Soit $x^2 - y^2 = 117$, les facteurs, tous utiles, de 117 sont : 1 et 117, 3 et 39, 9 et 13.

Ainsi :

$$1^0 \quad x = \frac{117+1}{2} = 59, \quad y = \frac{117-1}{2} = 58,$$

$$59^2 - 58^2 = 3481 - 3364 = 117.$$

$$2^0 \quad x = \frac{39+3}{2} = 21, \; y = \frac{39-3}{2} = 18;$$

$$21^2 - 18^2 = 441 - 324 = 117.$$

$$3^0 \quad x = \frac{13+9}{2} = 11, \quad y = \frac{13-9}{2} = 2,$$

$$11^2 - 2^2 = 121 - 4 = 117.$$

C'est ainsi que $x^2 - y^2 = p$, donne $x = \frac{p+1}{2}$, $y = \frac{p-1}{2}$, résultats correspondants à la solution du § I; et que $x^2 - y^2 = pp'$, donne, 1^0 $x = \frac{p+p'}{2}$, $y = \frac{p-p'}{2}$, et 2^0 $x = \frac{pp'+1}{2}$, $y = \frac{pp'-1}{2}$, résultats correspondants à la solution du § II.

ERRATUM. Bull., p. 492, sép. p. 16, ligne 8, $x'^2 + y'^2 = \mathrm{N}$, **lisez** $x'^2 + y'^2 = \mathrm{N}'$.