SUR LA SOLUTION

DES

PROBLÈMES INDÉTERMINÉS

DU SECOND DEGRÉ (*).

(*Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin*, t. XXIII, 1769.)

Lorsque l'équation finale à laquelle conduit la solution d'une question renferme plus d'une inconnue, le Problème est indéterminé; et envisagé généralement, il est susceptible d'une infinité de solutions. Mais si la nature de la question exige que les quantités cherchées soient rationnelles, ou même qu'elles soient exprimées par des nombres entiers, alors le nombre des solutions peut être très-limité; et la difficulté se réduit à trouver, parmi toutes les solutions possibles, celles qui peuvent satisfaire à la condition prescrite. Quand l'équation finale n'est que du premier degré, toutes les solutions sont rationnelles par la nature même de cette équation; et si l'on veut de plus que les inconnues soient des nombres entiers, on peut les déterminer facilement par la méthode des fractions continues (*voyez* plus bas le n° 8). Il n'en est pas de même des équations qui passent le premier degré, et qui conduisent naturellement à des expressions irrationnelles. On n'a point de méthode directe et générale pour trouver les nombres commensurables qui peuvent satisfaire à ces équations lors même qu'elles ne sont qu'au second degré; et il

(*) Lu à l'Académie le 24 novembre 1768.

faut avouer que cette branche de l'Analyse, quoique peut-être une des plus importantes, est néanmoins une de celles que les Géomètres paraissent avoir le plus négligées, ou du moins dans lesquelles ils ont fait jusqu'à présent le moins de progrès.

Diophante et ses commentateurs ont à la vérité résolu un grand nombre de Problèmes indéterminés du second, du troisième et même du quatrième degré; mais la plupart de leurs solutions n'étant que particulières, il n'est pas étonnant qu'il se trouve encore des cas d'ailleurs fort simples, et en même temps fort étendus, pour lesquels les méthodes de Diophante soient absolument insuffisantes.

S'il s'agissait, par exemple, de résoudre l'équation $A + Bt^2 = u^2$, en supposant A et B des nombres entiers non carrés, c'est-à-dire de trouver une valeur rationnelle de t telle que $A + Bt^2$ devînt un carré, on verrait aisément que tous les artifices connus de l'Analyse de Diophante seraient en défaut pour ce cas; or, c'est précisément à ce cas que se réduit la solution générale des Problèmes indéterminés du second degré à deux inconnues, comme on le verra ci-après. Personne que je sache ne s'est occupé de ce Problème, si l'on en excepte M. Euler qui en a fait l'objet de deux excellents Mémoires qui se trouvent parmi ceux de l'Académie de Pétersbourg (t. VI des anciens *Commentaires* et t. IX des nouveaux); mais il s'en faut encore beaucoup que la matière soit épuisée. Car : 1° M. Euler n'a considéré, dans l'équation $A + Bt^2 = u^2$, que le cas où B est un nombre positif, et où t et u doivent être des nombres entiers; 2° dans ce cas même, M. Euler suppose qu'on connaisse déjà une solution de l'équation et il donne le moyen d'en déduire une infinité d'autres. Ce n'est pas que ce grand Géomètre n'ait tâché de donner aussi quelques règles pour connaître *a priori* si l'équation proposée est résoluble ou non; mais, outre que ces règles ne sont fondées que sur des principes précaires et tirés seulement de l'induction, elles ne sont d'ailleurs d'aucune utilité pour la recherche de la première solution, qui doit être supposée connue (*voyez* le premier Mémoire du t. IX des nouveaux *Commentaires de Pétersbourg*, et surtout la conclusion de ce Mémoire, p. 38); 3° les formules que M. Euler donne pour trouver une infinité de solu-

tions, dès qu'on en connaît une seule, ne renferment pas toujours et ne sauraient renfermer toutes les solutions possibles, à moins que A ne soit un nombre premier (*voyez* plus bas le n° 45).

Les recherches que j'ai faites depuis quelque temps sur cette matière m'ont conduit à des méthodes directes, générales et nouvelles, pour résoudre les équations de la forme $A + Bt^2 = u^2$, et en général toutes les équations du second degré à deux inconnues, soit que les inconnues puissent être des nombres quelconques entiers ou fractionnaires, soit qu'elles doivent être des nombres entiers. Ce sont ces méthodes qui font l'objet de ce Mémoire; je les crois d'autant plus dignes de l'attention des Mathématiciens qu'elles laissent encore un vaste champ à leurs recherches.

§ I. — *De la manière de ramener toute équation du second degré à deux inconnues à cette forme* $A = u^2 - Bt^2$, *et des cas dans lesquels les équations de cette forme peuvent se résoudre par les méthodes connues.*

1. Soit

$$\alpha x^2 + \beta xy + \gamma y^2 + \delta x + \varepsilon y + \zeta = 0$$

l'équation générale proposée dans laquelle α, β, γ, δ, ε et ζ soient des nombres donnés entiers, positifs ou négatifs (il est évident que si les coefficients α, β,... n'étaient pas des nombres entiers, on pourrait toujours les rendre tels en faisant évanouir tous les dénominateurs par la multiplication), et où x et y soient les deux inconnues qu'il s'agit de déterminer, en sorte qu'elles soient exprimées par des nombres rationnels. Qu'on tire de cette équation la valeur de l'une des deux inconnues, comme x, et l'on aura

$$2\alpha x + \beta y + \delta = \sqrt{(\beta y + \delta)^2 - 4\alpha(\gamma y^2 + \varepsilon y + \zeta)},$$

d'où l'on voit que la question se réduit à déterminer y en sorte que la

laquelle rentre dans l'équation générale $Ar^2 = p^2 - Bq^2$, en faisant $B = \mp 1$, $r = s$; or, si le signe inférieur a lieu, on aura déjà le cas du n° 19; et si c'est le signe supérieur qui ait lieu, alors on aura aussi le cas du n° 19 si $A = 1$; de sorte que nous supposerons ici $A > 1$, et par conséquent $A > B$.

De cette manière, la résolution de l'équation proposée se réduira toujours à celle d'une équation de la forme

$$Ar^2 = p^2 - Bq^2,$$

où p, q, r devront être des nombres entiers, et où A et B seront des nombres entiers donnés non carrés, ni contenant des facteurs carrés, et dont l'un A sera plus grand que l'autre B.

5. Je dis maintenant que les nombres p et q doivent être premiers entre eux; car, s'ils avaient un commun diviseur ρ, il faudrait que Ar^2 fût aussi divisible par ρ^2; mais, comme les fractions $\frac{p}{r}$ et $\frac{q}{r}$ sont supposées réduites à leurs moindres termes, il est clair que p, q et r n'auront aucun diviseur commun, et qu'ainsi r ne sera point divisible par ρ; d'ailleurs, il est clair que si p, q et r avaient un diviseur commun, on en pourrait toujours faire abstraction, parce que ce diviseur s'en irait de lui-même par la division; donc, il faudra que A soit divisible par ρ^2, ce qui ne se peut à cause que A est supposé ne contenir aucun facteur carré.

6. Cela posé, je remarque d'abord que, pour que l'équation

$$Ar^2 = p^2 - Bq^2$$

puisse subsister, il faut que A soit un diviseur d'un nombre de cette forme $\alpha^2 - B$, α étant un nombre entier, c'est-à-dire que B soit le résidu de la division d'un carré quelconque par A. Car, si l'on multiplie l'équation dont il s'agit par

$$p_1^2 - Bq_1^2,$$

on aura

$$Ar^2(p_1^2 - Bq_1^2) = (p^2 - Bq^2)(p_1^2 - Bq_1^2);$$

or,

$$(p^2 - Bq^2)(p_1^2 - Bq_1^2)$$

se réduit à cette forme

$$(pp_1 \pm Bqq_1)^2 - B(pq_1 \pm qp_1)^2,$$

comme il est facile de s'en assurer par le développement de ces deux expressions; donc, si l'on prend pour p_1 et q_1 des nombres entiers tels, que $pq_1 - qp_1$ soit 1 ou -1, ce qui est toujours possible à cause que p et q sont premiers entre eux (numéro précédent), et qu'on fasse

$$pp_1 - Bqq_1 = \alpha,$$

on aura

$$A r^2 (p_1 - Bq_1^2) = \alpha^2 - B;$$

par conséquent, A sera un diviseur de $\alpha^2 - B$.

7. Pour trouver les nombres p_1 et q_1, qui peuvent satisfaire à la condition

$$pq_1 - qp_1 = \pm 1,$$

on réduira la fraction $\frac{p}{q}$ en une fraction continue, d'où l'on déduira, comme on sait, une suite de fractions convergentes vers $\frac{p}{q}$ et alternativement plus grandes ou plus petites que cette même fraction (*voyez* plus bas le n° 29), et l'on prendra pour p_1 le numérateur de la fraction qui précédera immédiatement la fraction $\frac{p}{q}$, et pour q_1 le dénominateur de la même fraction; si la fraction $\frac{p_1}{q_1}$ est plus petite que la fraction $\frac{p}{q}$, on aura

$$pq_1 - qp_1 = 1,$$

et si $\frac{p_1}{q_1} > \frac{p}{q}$, on aura

$$pq_1 - qp_1 = -1.$$

8. Cette méthode est utile pour résoudre en général toutes les équations du premier degré à deux inconnues, lorsque ces inconnues doivent

en faisant

$$\begin{aligned} P &= p^2 + Bq^2, & Q &= 2pq, \\ P_1 &= p^3 + 3Bpq^2, & Q_1 &= 3pq^2 + Bq^3, \\ &\ldots\ldots\ldots\ldots, & &\ldots\ldots\ldots\ldots; \end{aligned}$$

et en général, si l'on fait

$$(p^2 - Bq^2)^m = P^2 - BQ^2,$$

on aura

$$P = p^m + \frac{m(m-1)}{2} p^{m-2}q^2B + \frac{m(m-1)(m-2)(m-3)}{2.3.4} p^{m-4}q^4B^2 + \ldots,$$

$$Q = mp^{m-1}q + \frac{m(m-1)(m-2)}{2.3} p^{m-3}q^3B + \frac{m(m-1)\ldots(m-4)}{2.3.4.5} p^{m-5}q^5B^2 + \ldots,$$

ou bien

$$P = \frac{(p + q\sqrt{B})^m + (p - q\sqrt{B})^m}{2},$$

$$Q = \frac{(p + q\sqrt{B})^m - (p - q\sqrt{B})^m}{2\sqrt{B}}.$$

10. Nous avons démontré plus haut (6) que l'équation

$$Ar^2 = p^2 - Bq^2$$

ne peut avoir lieu à moins que A ne soit un diviseur d'un nombre de cette forme $\alpha^2 - B$; or, je dis que l'on peut toujours supposer que le nombre α soit moindre que la moitié du nombre A. En effet, soit a un nombre tel que $a^2 - B$ soit divisible par A, il est clair qu'en faisant $\alpha = \mu A \pm a$, μ étant un nombre quelconque entier, $\alpha^2 - B$ sera aussi divisible par A; d'autre part il est facile de voir qu'on peut toujours déterminer le nombre μ et le signe ambigu de a en sorte que α soit $< \frac{A}{2}$; donc, s'il existe un nombre quelconque a, tel que $a^2 - B$ soit divisible par A, il doit exister aussi un nombre $\alpha < \frac{A}{2}$, qui ait la même propriété.

On doit conclure de là que, pour que l'équation

$$Ar^2 = p^2 - Bq^2$$

soit résoluble, il faut nécessairement que A soit un diviseur d'un nombre tel que $\alpha^2 - B$, α étant un nombre moindre que $\frac{A}{2}$.

On essayera donc successivement pour α tous les nombres naturels depuis 1 jusqu'à $\frac{A}{2}$, et si l'on n'en trouve aucun qui satisfasse à la condition dont il s'agit, ce sera une marque sûre que l'équation proposée n'admet aucune solution rationnelle.

Nous donnerons plus bas (*voyez* le § IV) des moyens directs pour pouvoir reconnaître si un nombre donné peut être un diviseur d'un nombre de la forme $\alpha^2 - B$, B étant aussi donné; il nous suffit ici qu'on puisse toujours s'en assurer par un tâtonnement fort simple.

Au reste, il faut remarquer, pour éviter toute équivoque, que quand nous disons que α doit être $< \frac{A}{2}$, nous entendons que α et A soient pris positivement, quoiqu'ils puissent être d'ailleurs positifs ou négatifs; de sorte qu'on ne doit avoir égard, dans cette comparaison des nombres α et A, qu'à leur valeur absolue.

11. Reprenons maintenant l'équation

$$(A) \qquad A r^2 = p^2 - B q^2,$$

et supposons qu'on ait trouvé un nombre entier $\alpha < \frac{A}{2}$ (abstraction faite des signes de α et A), tel que $\alpha^2 - B$ soit divisible par A; dénotons par A_1 le quotient de la division de $\alpha^2 - B$ par A, on aura l'équation

$$AA_1 = \alpha^2 - B.$$

Qu'on fasse $\alpha_1 = \mu_1 A_1 \pm \alpha$, μ_1 étant un nombre quelconque entier, et qu'on prenne le nombre μ_1 et le signe de α en sorte que l'on ait $\alpha_1 < \frac{A_1}{2}$ (abstraction faite des signes de α_1 et A_1), ce qui est évidemment toujours possible, comme nous l'avons déjà observé plus haut; il est clair que, puisque $\alpha^2 - B$ est déjà divisible par A_1, $\alpha_1^2 - B$ le sera aussi, de sorte qu'en dénotant le quotient de cette division par A_2, on aura cette

équation analogue à la précédente

$$A_1 A_2 = \alpha_1^2 - B.$$

Faisant de même $\alpha_2 = \mu_2 A_2 \pm \alpha_1$, et prenant μ_2 et le signe de α_1, en sorte que l'on ait $\alpha_2 < \frac{A_2}{2}$ (les nombres α_2 et A_2 étant considérés comme positifs), on aura $\alpha_2^2 - B$ divisible par A_2; de sorte qu'en dénotant le quotient de cette division par A_3, on aura cette troisième équation

$$A_2 A_3 = \alpha_2^2 - B,$$

et ainsi de suite.

12. De cette manière on pourra trouver une suite d'équations telles que

$$(a) \qquad \begin{cases} A\, A_1 = \alpha^2 - B, \\ A_1 A_2 = \alpha_1^2 - B, \\ A_2 A_3 = \alpha_2^2 - B, \\ \ldots\ldots\ldots\ldots, \end{cases}$$

dans lesquelles on ait (en considérant les nombres α, α_1, α_2,..., A, A_1, A_2,... comme positifs) $\alpha < \frac{A}{2}$, $\alpha_1 < \frac{A_1}{2}$, $\alpha_2 < \frac{A_2}{2}$, ...

Or, je dis que les nombres A, A_1, A_2, A_3,... formeront nécessairement une suite décroissante, jusqu'à ce que l'on arrive à un terme comme A_n, l'indice n dénotant le quantième du terme A_n, lequel soit $= B$ ou $< B$, abstraction faite des signes de A_n et de B. Pour prouver cette proposition, il est à propos de distinguer les deux cas de B positif et de B négatif.

13. Supposons d'abord que B soit un nombre positif; dans ce cas il est clair que A pourra être positif ou négatif.

1° Soit A positif et soit $\alpha^2 > B$, il est clair que A_1 sera aussi positif; or, puisque $\alpha < \frac{A}{2}$, on aura aussi $\alpha^2 < \frac{A^2}{4}$, et à plus forte raison

$$\alpha^2 - B < \frac{A^2}{4};$$

donc $AA_1 < \frac{A^2}{4}$, et par conséquent (A et A_1 étant positifs) $A_1 < \frac{A}{4}$.

De même, puisque A_1 est positif, si $\alpha_1^2 > B$, on aura aussi A_2 positif,

quelconques de V, en sorte que $V = MN$. Ainsi, si V a plusieurs facteurs parmi lesquels il faudra toujours compter l'unité, on aura autant de différentes expressions de x, y et z qu'il y aura de manières de partager le nombre V en deux facteurs.

EXEMPLES.

20. Appliquons maintenant notre méthode à quelques Exemples.

EXEMPLE I. — Soit proposé de résoudre l'équation

$$109 = u^2 - 7t^2.$$

En mettant $\frac{p}{r}$ au lieu de u, et $\frac{q}{r}$ au lieu de t, elle deviendra

$$109r^2 = p^2 - 7q^2, \tag{A}$$

de sorte qu'on aura $A = 109$ et $B = 7$; car, comme ces deux nombres ne renferment aucun facteur carré, il n'y aura aucune réduction à y faire.

Il faudra donc chercher un nombre entier α moindre que $\frac{109}{2}$ et tel, que $\alpha^2 - 7$ soit divisible par 109; mais pour cela, au lieu d'essayer successivement pour α tous les nombres naturels moindres que 54, il sera beaucoup plus commode de chercher un multiple de 109 qui soit de la forme $\alpha^2 - 7$, c'est-à-dire qui, étant augmenté de 7, devienne un carré.

En général, on remarquera que dans l'équation

$$AA_1 = \alpha^2 - B,$$

à laquelle il s'agit de satisfaire, A_1 doit être $< \frac{A}{4}$ lorsque B est positif, et $< \frac{A}{4} + 1$ lorsque B est négatif (13 et 14), de sorte qu'il n'y aura qu'à essayer successivement pour A_1 tous les nombres naturels moindres que $\frac{A}{4} + 1$, pris positivement ou négativement suivant que A sera positif ou négatif (numéros cités), et s'il ne s'en trouve aucun dont le produit par A étant augmenté de B devienne un carré, ce sera une marque certaine que le Problème n'admet point de solution rationnelle.

On en usera de même à l'égard des autres équations de condition

$$BB_1 = \beta^2 - C, \quad CC_1 = \gamma^2 - D, \ldots,$$

dans lesquelles il faudra aussi que $B_1 < \frac{C}{4} + 1$, $C_1 < \frac{D}{4} + 1, \ldots$.

Dans l'exemple proposé on trouve d'abord $2.109 + 7 = 225$; de sorte qu'on aura $A_1 = 2$, $\alpha = 15$; et comme A_1 est déjà $< B$, la première suite d'équations *secondaires* se réduira à cette seule équation (12)

$$(a) \qquad 109.2 = 15^2 - 7.$$

Ainsi l'on fera (15) $C = 2$, de sorte que la seconde équation *principale* sera

$$(B) \qquad 7r_1 = p_1^2 - 2q_1^2.$$

Il faudra donc satisfaire à l'équation

$$BB_1 = \beta^2 - C, \quad \text{savoir} \quad 7B_1 = \beta^2 - 2,$$

β étant $< \frac{7}{2}$, et l'on trouvera $\beta = 3$, $B_1 = 1$, de sorte que, comme β_1 est déjà $< C$, la seconde suite d'équations secondaires, que nous avons désignée par (b) au n° 17, se réduira à cette équation unique

$$(b) \qquad 7.1 = 3^2 - 2.$$

On fera donc $D = 1$, et la troisième équation principale sera

$$(C) \qquad 2r_2^2 = p_2^2 - q_2^2,$$

laquelle est déjà, comme on voit, dans le cas du n° 19.

Comparant donc cette dernière équation à l'équation

$$Vz^2 = x^2 - y^2,$$

on aura $V = 2$, $x = p_2$, $y = q_2$, $z = r_2$; donc $M = 1$, $N = 2$, et par conséquent

$$p_2 = m^2 + 2n^2, \quad q_2 = m^2 - 2n^2, \quad r_2 = 2mn;$$

ainsi, il n'y aura plus qu'à remonter de l'équation (C) à l'équation (B), et de celle-ci à l'équation proposée (A) par la méthode du n° 16.

Pour cela, on changera d'abord l'équation (C) en celle-ci

$$q_2^2 = p_2^2 - 2r_2^2,$$

et on la multipliera par l'équation (b) [s'il y avait plus d'une de ces équations *secondaires* (b), il faudrait multiplier l'équation dont il s'agit successivement par chacune de ces équations]; on aura, par les formules du n° 9, l'équation

$$7q_2^2 = (3p_2 \pm 2r_2)^2 - 2(3r_2 \pm p_2)^2,$$

laquelle, étant comparée à l'équation (B), donnera

$$p_1 = 3p_2 \pm 2r_2, \quad q_1 = 3r_2 \pm p_2, \quad r_1 = q_2,$$

les signes ambigus étant à volonté.

On changera de même l'équation (B) en

$$2q_1^2 = p_1^2 - 7r_1^2,$$

et on la multipliera ensuite par l'équation (a), ce qui donnera

$$109.4q_1^2 = (15p_1 \pm 7r_1)^2 - 7(15r_1 \pm p_1)^2;$$

et, comparant cette équation avec l'équation (A), on aura enfin

$$p = 15p_1 \pm 7r_1, \quad q = 15r_1 \pm p_1, \quad r = 2q_1,$$

de sorte qu'il n'y aura plus qu'à substituer successivement les valeurs de p_1, q_1, r_1, et ensuite celles de p_2, q_2, r_2.

Les valeurs de p, q et r étant ainsi trouvées, on aura $u = \frac{p}{r}$ et $t = \frac{q}{r}$, et l'équation proposée

$$109 = u^2 - 7t^2$$

sera résolue.

Exemple II. — Qu'on propose maintenant l'équation suivante

$$-207 = u^2 - 13t^2.$$

Puisque le nombre 207 est divisible par le carré 9, je supposerai (4)

$u = \frac{3p}{r}$ et $t = \frac{3q}{r}$, ce qui donnera l'équation

(A) $$-23r^2 = p^2 - 13q^2.$$

Or, en suivant le même procédé que dans l'Exemple précédent, et marquant les équations analogues par les mêmes lettres, on trouvera les équations suivantes

(a) $$-23(-1) = 6^2 - 13,$$

(B) $$13r_1^2 = p_1^2 + q_1^2,$$

(b) $$\begin{cases} 13.2 = 5^2 + 1, \\ 2.1 = 1 + 1, \end{cases}$$

(C) $$-r_2^2 = p_2^2 - q_2^2,$$

dont la dernière est, comme on le voit, dans le cas du n° 19. On aura donc $p_2 = x$, $q_2 = y$, $r_2 = z$ et $V = -1$; donc $M = 1$ et $N = -1$; par conséquent,

$$p_2 = m^2 - n^2, \quad q_2 = m^2 + n^2, \quad r_2 = 2mn.$$

Ensuite on mettra la même équation (C) sous la forme des équations (b), en transposant les termes r_2^2 et q_2^2, en sorte que l'on ait $q_2^2 = p_2^2 + r_2^2$, et l'on multipliera successivement cette équation par les deux équations (b). Pour cela, on fera d'abord le produit de ces deux-ci, qui sera exprimé par $13.4 = (5 \pm 1)^2 + (5 \mp 1)^2$, ou bien simplement $13.4 = 6^2 + 4^2$, c'est-à-dire, en divisant par 4, $13 = 3^2 + 2^2$; donc, multipliant l'équation précédente par celle-ci, et comparant le produit à l'équation (B), on aura

$$p_1 = 3p_2 \pm 2r_2, \quad q_1 = 3r_2 \mp 2p_2, \quad r_1 = q_2.$$

On transposera de même le premier et le dernier terme de l'équation (B) pour la réduire à la forme de l'équation (a), et on la multipliera ensuite par cette dernière équation, ce qui donnera une équation semblable à l'équation (A), de sorte qu'on aura enfin

$$p = 6p_1 \pm 13r_1, \quad q = 6r_1 \pm p_1, \quad r = q_1.$$

Ainsi l'équation proposée sera résolue.

EXEMPLE III. — Si l'équation proposée était

$$51 = u^2 - 7t^2,$$

dans laquelle 51 et 7 ne renferment aucun facteur carré, on ferait $u = \frac{p}{r}$, $t = \frac{q}{r}$, pour avoir

$$51r^2 = p^2 - 7q^2,$$

et il faudrait d'abord satisfaire à l'équation

$$51A_1 = \alpha^2 - 7;$$

mais, en essayant pour A_1 tous les nombres naturels jusqu'à $\frac{51}{4} + 1$, c'est-à-dire jusqu'à 13, on n'en trouve aucun qui, étant multiplié par 51 et augmenté de 7, devienne un carré; d'où il s'ensuit que l'équation proposée n'admet aucune solution rationnelle.

EXEMPLE IV. — Soit encore proposée l'équation

$$1459 = u^2 - 30t^2;$$

comme 1459 est un nombre premier, on fera d'abord $u = \frac{p}{r}$, $t = \frac{q}{r}$ pour avoir l'équation

$$(A) \qquad 1459r^2 = p^2 - 30q^2.$$

Ayant donc ici $1459 = A$, $30 = B$, il faudra d'abord trouver un nombre $\alpha < \frac{1459}{2}$ et tel que $\alpha^2 - 30$ soit divisible par 1459, ou bien un nombre $A_1 < \frac{1459}{4}$ et tel que $1459A_1 + 30$ soit égal à un carré, comme nous l'avons dit dans l'Exemple I.

Après quelques essais, je trouve $A_1 = 241$ et $\alpha = 593$, et à l'aide de ces valeurs je forme cette première suite d'équations *secondaires* (12)

$$(a) \qquad \begin{cases} 1459 \cdot 241 = 593^2 - 30, \\ 241 \cdot 51 = 111^2 - 30, \\ 51 \cdot 1 = 9^2 - 30. \end{cases}$$

Donc, puisque 1 est < 30, on fera $C = 1$ (15), et j'aurai cette seconde

équation *principale*

$$(B) \qquad 30r_1^2 = p_1^2 - q_1^2,$$

laquelle est déjà, comme on voit, dans le cas du n° 19.

J'aurai donc $p_1 = x$, $q_1 = y$, $r_1 = z$ et $30 = V$; donc, puisque $30 = 2.3.5$, on aura $M = 1$, $N = 30$, ou $M = 2$, $N = 15$, ou $M = 3$, $N = 10$, ou enfin $M = 5$, $N = 6$; de sorte qu'on aura

$$p_1 = m^2 + 30n^2, \quad q_1 = m^2 - 30n^2, \quad r_1 = 2mn,$$

ou

$$p_1 = 2m^2 + 15n^2, \quad q_1 = 2m^2 - 15n^2, \quad r_1 = 2mn,$$

ou

$$p_1 = 3m^2 + 10n^2, \quad q_1 = 3m^2 - 10n^2, \quad r_1 = 2mn,$$

ou

$$p_1 = 5m^2 + 6n^2, \quad q_1 = 5m^2 - 6n^2, \quad r_1 = 2mn.$$

Ayant ainsi p_1, q_1 et r_1, on mettra l'équation (B) sous cette forme

$$q_1^2 = p_1^2 - 30r_1^2,$$

et on la multipliera successivement par chacune des équations (a). Pour faire cette multiplication plus aisément, on multipliera d'abord la deuxième et la troisième de ces équations ensemble, et faisant, pour abréger, $\mu = 9.111 \pm 30$, $\nu = 111 \pm 9$, on aura

$$241.51^2 = \mu^2 - 3\nu^2;$$

ensuite on multipliera cette équation par la première des équations (a), et faisant encore $\mu_1 = 593\mu \pm 30\nu$, $\nu_1 = 593\nu \pm \mu$, on aura

$$1459(241.51)^2 = \mu_1^2 - 30\nu_1^2,$$

équation qui, étant multipliée maintenant par l'équation

$$q_1^2 = p_1^2 - 30r_1^2,$$

donnera celle-ci

$$1459(241.51q_1)^2 = (\mu_1 p_1 \pm 30\nu_1 r_1)^2 - (\mu_1 r_1 \pm \nu_1 p_1)^2,$$

laquelle, étant comparée à l'équation (A), donnera enfin

$$p = \mu_1 p_1 \pm 30\nu_1 r_1,$$
$$q = \mu_1 r_1 \pm \nu_1 p_1,$$
$$r = 241.51\, q.$$

EXEMPLE V. — Si l'on avait l'équation

$$23 = u^2 + 5t^2,$$

on ferait toujours $u = \frac{p}{q}$ et $t = \frac{p}{r}$, ce qui donnerait celle-ci

(A) $$23r^2 = p^2 + 5q^2,$$

et en opérant comme ci-dessus, on trouverait d'abord les équations

(a) $$23.3 = 8^2 + 5,$$

(B) $$-5r_1^2 = p_1^2 - 3q_1^2;$$

mais, comme il faudrait ensuite satisfaire à l'équation

$$-5B_1 = \beta^2 - 3,$$

en prenant pour $-B_1$ un nombre $< \frac{5}{4} + 1$, c'est-à-dire en faisant $B_1 = -1$ ou -2, et que ni l'une ni l'autre de ces deux valeurs étant multipliée par 5 et augmentée de 3 ne donne un carré, on en conclura que l'équation proposée n'est susceptible d'aucune solution rationnelle; ainsi, quoique le nombre 23 puisse être un diviseur d'une infinité de nombres de la forme $p^2 + 5q^2$, cependant il est impossible que le quotient de cette division soit jamais un carré.

21. Ces Exemples peuvent suffire pour faire connaître l'esprit et l'usage de notre méthode. Nous allons voir maintenant comment il faudra s'y prendre lorsqu'il s'agira d'avoir des solutions en nombres entiers; car quoique les solutions que fournit la méthode précédente soient générales et renferment par conséquent tous les nombres soit entiers, soit

fractionnaires, qui peuvent satisfaire à l'équation $A = u^2 - Bt^2$, cependant, comme les valeurs générales de u et de t se présentent toujours sous une forme fractionnaire, il serait souvent difficile et presque impossible de les réduire à des nombres entiers. De sorte que, pour ne rien laisser à désirer sur cette matière, il est nécessaire de donner aussi une méthode particulière pour résoudre l'équation $A = u^2 - Bt^2$, lorsque u et t doivent être des nombres entiers.

§ III. — *Résolution de l'équation* $A = u^2 - Bt^2$ *lorsque* u *et* t *doivent être des nombres entiers.*

22. Je remarque d'abord que si le nombre A n'a aucun facteur carré, les nombres u et t doivent être nécessairement premiers entre eux; car, si ces nombres avaient un commun diviseur ρ, il est clair que puisque u^2 et t^2 seraient divisibles par ρ^2, il faudrait aussi que A le fût. On voit par là que les nombres t et u ne sauraient avoir d'autres diviseurs communs que ceux dont les carrés sont aussi des diviseurs de A.

Ainsi, si A ne contient qu'un seul facteur carré, comme si $A = al^2$, l étant un nombre premier et a un nombre qui ne contient aucun facteur carré, les nombres u et t pourront être premiers entre eux ou bien pourront avoir le nombre l pour commun diviseur; et dans ce dernier cas, faisant $u = lp$, $t = lq$, l'équation $A = u^2 - Bt^2$ deviendra

$$a = p^2 - Bq^2,$$

p et q étant premiers entre eux. Si $A = al^2m^2$, l et m étant des nombres premiers, alors u et t pourront être premiers entre eux ou bien pourront être divisibles tous les deux par l, ou par m, ou par lm, de sorte qu'en faisant successivement $u = lp$, $t = lq$, $u = mp$, $t = mq$ et $u = lmp$, $t = lmq$, on aura

$$am^2 = p^2 - Bq^2, \quad \text{ou} \quad al^2 = p^2 - Bq^2, \quad \text{ou} \quad a = p^2 - Bq^2,$$

p et q étant toujours premiers entre eux. En général, si le nombre donné A

Mais, comme nous ne nous proposons pas ici de traiter cette matière à fond, nous ne nous y arrêterons pas davantage quant à présent; nous observerons seulement que M. de Fermat prétend, dans ses *Remarques sur Diophante*, avoir démontré en général ce théorème, que l'équation

$$r^n + s^n = q^n$$

n'est jamais résoluble d'une manière rationnelle lorsque n surpasse 2; mais ce Savant ne nous a pas laissé sa démonstration, et il ne paraît pas que personne l'ait encore trouvée jusqu'à présent. M. Euler a, à la vérité, démontré ce théorème dans le cas de $n = 3$ et de $n = 4$, par une analyse particulière et très-ingénieuse, mais qui ne paraît pas applicable en général à tous les autres cas; ainsi, ce théorème est un de ceux qui restent encore à démontrer, et qui méritent le plus l'attention des Géomètres.