



RECHERCHES D'ARITHMÉTIQUE.

[Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres
de Berlin, années 1773 et 1775 (*).]

PREMIÈRE PARTIE.

Ces Recherches ont pour objet les nombres qui peuvent être représentés par la formule

$$Bt^2 + Ctu + Du^2,$$

où B, C, D sont supposés des nombres entiers donnés, et t, u des nombres aussi entiers, mais indéterminés. Je donnerai d'abord la manière de trouver toutes les différentes formes dont les diviseurs de ces sortes de nombres sont susceptibles; je donnerai ensuite une méthode pour réduire ces formes au plus petit nombre possible; je montrerai comment on en peut dresser des Tables pour la pratique, et je ferai voir l'usage de ces Tables dans la recherche des diviseurs des nombres. Je donnerai enfin la démonstration de plusieurs Théorèmes sur les nombres premiers de la même forme $Bt^2 + Ctu + Du^2$, dont quelques-uns sont déjà connus, mais n'ont pas encore été démontrés, et dont les autres sont entièrement nouveaux.

1. AVERTISSEMENT. — On suppose toujours dans la suite que toutes les lettres désignent des nombres entiers positifs ou négatifs, et l'on représentera ordinairement par les premières lettres de l'alphabet les nombres donnés, et par les dernières les nombres indéterminés.

(*) La première Partie de ce Mémoire a été insérée dans le volume de 1773, la seconde Partie dans le volume de 1775.
(Note de l'Éditeur.)

2. OBSERVATION. — La formule du premier degré $Bt + Cu$, où B et C sont des nombres quelconques donnés et premiers entre eux, peut représenter un nombre quelconque; mais il n'en est pas de même de la formule du second degré $Bt^2 + Ctu + Du^2$; car nous avons prouvé ailleurs [voyez les *Mémoires de l'Académie* pour les années 1767 et 1768 (*)] que l'équation

$$A = Bt + Cu$$

est toujours résoluble en nombres entiers, quels que soient les nombres A, B, C , pourvu que les deux derniers soient premiers entre eux; mais que l'équation

$$A = Bt^2 + Ctu + Du^2$$

ne l'est que dans certains cas, et lorsque certaines conditions ont lieu entre les nombres donnés A, B, C, D . On doit dire la même chose, à plus forte raison, des formules du troisième degré et au delà.

3. SCOLIE. — Il y a donc une grande différence entre les formules du premier degré et celles des degrés supérieurs, celles-là pouvant représenter tous les nombres possibles, au lieu que celles-ci ne peuvent représenter que certains nombres qui doivent être distingués de tous les autres par des caractères particuliers. De très-grands Géomètres ont déjà considéré les propriétés des nombres qui peuvent être représentés par quelques-unes des formules du second degré ou des degrés ultérieurs, comme celles-ci

$$t^2 + u^2, \quad t^2 + 2u^2, \quad t^2 + 3u^2, \quad t^4 + u^4, \quad t^6 + u^6, \dots$$

(Voyez les *Ouvrages* de M. Fermat et les *Nouveaux Commentaires de Pétersbourg*, t. 1, IV, V, VI, VIII). Mais personne, que je sache, n'a encore traité cette matière d'une manière directe et générale, ni donné des règles pour trouver *à priori* les principales propriétés des nombres qui peuvent se rapporter à des formules quelconques données.

Comme ce sujet est un des plus curieux de l'Arithmétique, et qu'il mérite particulièrement l'attention des Géomètres par les grandes diffi-

(*) *Oeuvres de Lagrange*, t. II, p. 377 et 655.

cultés qu'il renferme, je vais tâcher de la traiter plus à fond qu'on ne l'a encore fait; mais je me bornerai pour le présent aux formules du second degré, et je commencerai par examiner quelle doit être la forme des diviseurs des nombres qui peuvent être exprimés par ces sortes de formules.

THÉORÈME I.

4. Si le nombre A est un diviseur d'un nombre représenté par la formule

$$Bt^2 + Ctu + Du^2,$$

en supposant t et u premiers entre eux, je dis que ce nombre A sera nécessairement de la forme

$$A = Ls^2 + Mx + Nx^2,$$

où l'on aura

$$4LN - M^2 = 4BD - C^2,$$

s et x étant aussi premiers entre eux.

Car soit a le quotient de la division de $Bt^2 + Ctu + Du^2$ par A , en sorte qu'on ait

$$Aa = Bt^2 + Ctu + Du^2,$$

et soit b la plus grande commune mesure entre a et u (si a et u sont premiers entre eux, on aura $b = 1$), de manière qu'en faisant

$$a = bc, \quad u = bs,$$

c et s soient premiers entre eux; on aura donc

$$A bc = Bt^2 + Cbts + Db^2s^2;$$

par conséquent Bt^2 sera divisible par b ; mais t et u étant premiers entre eux (hypothèse), t sera aussi premier à b , qui est un diviseur de u ; donc il faudra que B soit divisible par b ; de sorte qu'on aura $B = Eb$, et l'équation étant divisée par b , elle deviendra

$$Ac = Et^2 + Cts + Dbs^2.$$

Maintenant, puisque c et s sont premiers entre eux, on peut supposer (par l'Observation précédente)

$$t = gs + cx,$$

ce qui, étant substitué, donnera

$$Ac = (E\theta^2 + C\theta + Db)s^2 + (2E\theta c + Cc)sx + Ec^2x^2,$$

de sorte qu'il faudra que le nombre $(E\theta^2 + C\theta + Db)s^2$ soit divisible par c ; et comme c et s sont premiers entre eux, il faudra que $E\theta^2 + C\theta + Db$ soit divisible par c ; donc divisant toute l'équation par c , et faisant

$$L = \frac{E\theta^2 + C\theta + Db}{c}, \quad M = 2E\theta + C, \quad N = Ec,$$

on aura

$$A = Lx^2 + Mx + Nx^2.$$

Or $4LN - M^2$ sera égal à

$$4E(E\theta^2 + C\theta + Db) - (2E\theta + C)^2 = 4EDb - C^2 = 4BD - C^2,$$

à cause de $B = Eb$. Donc, etc.

Maintenant, comme t et u sont premiers entre eux (hypothèse), t et s le seront aussi, à cause de $u = bs$; mais si x et s n'étaient pas premiers entre eux, il est clair que t devrait être divisible par leur plus grande commune mesure, à cause de $t = \theta s + cx$; ce qui ne pouvant être, il s'ensuit que x et s seront nécessairement premiers entre eux si t et u le sont.

THÉORÈME II.

5. Toute formule du second degré telle que celle-ci

$$Lx^2 + Mx + Nx^2,$$

dans laquelle M est plus grand que L ou N (abstraction faite des signes de ces quantités), peut se transformer en une autre du même degré, comme

$$L's^2 + M'sx' + N'x'^2,$$

dans laquelle on aura

$$4L'N' - M'^2 = 4LN - M^2,$$

et où M' sera plus petit que M .

Car soit par exemple $M > L$, on fera

$$s = mx + s',$$

et la formule proposée deviendra

$$(Lm^2 + Mm + N)x^2 + (2Lm + M)xs' + Ls'^2,$$

ou bien, en changeant x en x' ,

$$L's'^2 + M'sx' + N'x'^2,$$

où l'on aura

$$L' = L,$$

$$M' = 2Lm + M,$$

$$N' = Lm^2 + Mm + N,$$

de sorte qu'on aura d'abord, quel que soit le nombre m ,

$$4L'N' - M'^2 = 4L(Lm^2 + Mm + N) - (2Lm + M)^2 = 4LN - M^2.$$

Or, puisque L est moindre que M (hypothèse), il est clair qu'on peut déterminer le nombre m en sorte que $2Lm + M$ devienne moindre que M ; donc, etc.

6. COROLLAIRE I. — Donc, si dans la transformée

$$L's'^2 + M'sx' + N'x'^2,$$

l'un des nombres L' ou N' est moindre que M' , on pourra parvenir à une autre transformée telle que

$$L''s''^2 + M''s''x'' + N''x''^2,$$

dans laquelle on aura pareillement

$$4L''N'' - M''^2 = 4L'N' - M'^2 = 4LN - M^2,$$

et où M'' sera plus petit que M' , et ainsi de suite; donc, comme la série des nombres

$$M, M', M'', \dots$$

ne saurait aller à l'infini, à cause que ces nombres doivent être tous entiers et décroissants de l'un à l'autre, il faudra nécessairement qu'on arrive à une transformée, que je représenterai ainsi

$$Py^2 + Qyz + Rz^2,$$

dans laquelle Q ne sera pas plus grand que P, ni que R, et où l'on aura

$$4PR - Q^2 = 4LN - M^2.$$

7. COROLLAIRE II. — Si les nombres s et x de la formule proposée sont premiers entre eux, il est clair que les nombres s' et x' de la transformée seront aussi premiers entre eux; car si ceux-ci ne l'étaient pas il faudrait, à cause de $x' = x$ et de $s = mx + s'$, que s fût divisible par la plus grande commune mesure entre s' et x .

Donc les nombres s'' et x'' de la seconde transformée seront aussi par la même raison premiers entre eux, et ainsi de suite; d'où l'on peut conclure que les nombres y et z de la dernière transformée seront nécessairement premiers entre eux, si les nombres s et x le sont.

THÉORÈME III.

8. Si A est un diviseur d'un nombre de la forme

$$Bt^2 + Ctu + Du^2,$$

t et u étant premiers entre eux, je dis que ce nombre A sera nécessairement de la forme

$$Py^2 + Qyz + Rz^2,$$

y et z étant aussi premiers entre eux, et P, Q, R étant tels, qu'on ait

$$4PR - Q^2 = 4BD - C^2,$$

et de plus Q n'étant ni plus grand que P ni plus grand que R, abstraction faite des signes de P, Q et R.

La démonstration de ce Théorème suit naturellement des deux Théorèmes précédents et de leurs Corollaires.

9. COROLLAIRE I. — Si $4BD - C^2$ est un nombre positif, il faudra que $4PR$ soit aussi positif; donc, à cause que $P = ou > Q$, et $R = ou > Q$, il est clair que $4PR$ sera aussi $= ou > 4Q^2$, et par conséquent

$$4PR - Q^2 = ou > 3Q^2;$$

donc on aura aussi

$$4BD - C^2 = ou > 3Q^2,$$

et de là

$$Q = ou < \sqrt{\frac{4BD - C^2}{3}}.$$

10. COROLLAIRE II. — Soit maintenant $4BD - C^2$ un nombre négatif, en sorte que $C^2 - 4BD$ soit positif; on aura donc dans ce cas $Q^2 - 4PR > 0$, ce qui, à cause que Q n'est jamais plus grand que P ni plus grand que R, ne peut avoir lieu à moins que $4PR$ ne soit un nombre négatif; ainsi $-4PR$ sera un nombre positif $= ou > 4Q^2$, à cause de $P = ou > Q$ et $R = ou > Q$; de sorte que $Q^2 - 4PR$ sera $= ou > 5Q^2$, et par conséquent $C^2 - 4BD$ sera aussi $= ou > 5Q^2$; donc il faudra que

$$Q = ou < \sqrt{\frac{C^2 - 4BD}{5}}.$$

11. COROLLAIRE III. — Donc, puisque Q doit être un nombre entier, on ne pourra prendre pour Q que les nombres entiers positifs ou négatifs qui ne surpasseront pas les limites trouvées, en comprenant aussi le zéro parmi les nombres entiers; d'où l'on voit que Q ne pourra jamais avoir qu'un certain nombre de valeurs différentes.

De plus, il est clair que pour que l'équation

$$4PR - Q^2 = 4BD - C^2$$

puisse subsister en nombres entiers, il faut que Q soit pair ou impair, suivant que C sera pair ou impair, ce qui limite encore davantage le nombre des valeurs de Q.

Connaissant Q, on trouvera facilement P et R par la même équation;

car, à cause de

$$PR = \frac{4BD - C^2 + Q^2}{4},$$

il est clair qu'il n'y aura qu'à prendre pour P et R les facteurs du nombre entier

$$\frac{Q^2 + 4BD - C^2}{4},$$

en ayant soin de rejeter ceux dont l'un ou tous les deux seraient plus grands que Q.

PROBLÈME I.

12. Trouver toutes les formes possibles des diviseurs des nombres qui sont représentés par la formule du second degré

$$Bt^2 + Ctu + Du^2,$$

t et u étant des nombres premiers entre eux.

Il est évident, par ce que nous venons de démontrer ci-dessus, que chaque diviseur de la formule proposée est réductible à cette forme

$$Py^2 + Qyz + Rz^2,$$

y et z étant aussi premiers entre eux. Ainsi la difficulté se réduit à trouver les valeurs des coefficients P, Q, R, lorsque celles de B, C et D sont données.

Pour cet effet je distingue deux cas, l'un lorsque le nombre $4BD - C^2$ est positif, et l'autre lorsque ce nombre est négatif.

1° Soit $4BD - C^2 = K$ (K désignant un nombre positif); on déterminera d'abord Q par ces conditions : que Q soit pair ou impair suivant que K le sera, et qu'il ne surpasse pas le nombre $\pm \sqrt{\frac{K}{3}}$; ensuite on déterminera P et R par ces conditions-ci : que P et R soient deux facteurs du nombre $\frac{K + Q^2}{4}$, et que chacun de ces facteurs ne soit pas moindre que Q (9 et 11).

2° Soit $4BD - C^2 = -K$; on déterminera Q par ces conditions : que Q soit pair ou impair suivant que K le sera, et qu'il ne surpasse pas le nombre $\pm \sqrt{\frac{K}{5}}$; après quoi l'on déterminera les valeurs correspondantes de P et R par ces conditions, que P et R soient deux facteurs du nombre $\frac{Q^2 - K}{4}$, et que chacun d'eux ne soit pas moindre que Q (10 et 11).

13. REMARQUE I. — Si l'on avait $4BD - C^2 = 0$, alors K étant égal à zéro, on ne pourrait prendre que $Q = 0$, et ensuite on aurait aussi $PR = 0$, de sorte que l'un des nombres P ou R serait nul et l'autre serait tout ce qu'on voudrait. Mais il faut remarquer que dans ce cas la formule

$$Bt^2 + Ctu + Du^2$$

se réduit à celle-ci

$$\frac{(2Bt + Cu)^2}{4B};$$

de sorte que, comme $2Bt + Cu$ peut représenter un nombre quelconque (2), les diviseurs de la formule proposée peuvent aussi être quelconques.

14. REMARQUE II. — La même chose doit avoir lieu, en général, lorsque la formule

$$Bt^2 + Ctu + Du^2$$

est le produit de deux formules rationnelles du premier degré telles que $at + bu$ et $ct + du$, dont chacune peut représenter des nombres quelconques (2); c'est ce qui arrive quand $4BD - C^2$ est égal à un nombre carré pris négativement; car supposant

$$4BD - C^2 = -H^2,$$

on a

$$Bt^2 + Ctu + Du^2 = \frac{[2Bt + (C + H)u][2Bt + (C - H)u]}{4B}.$$

Or, quoique dans ce cas tout nombre puisse être un diviseur de la formule dont il s'agit, cependant si l'on cherche les formules des diviseurs

par le Problème précédent, on les trouvera comme dans les autres cas, de sorte qu'il en faudra conclure que ces formules renfermeront tous les nombres possibles.

Au reste, comme on a

$$4PR - Q^2 = 4BD - C^2 = -H^2,$$

il est clair que la formule générale des diviseurs

$$Py^2 + Qyz + Rz^2$$

sera aussi résoluble en deux formules rationnelles du premier degré.

15. REMARQUE III. — Il est remarquable que les formules des diviseurs ne dépendent que de la valeur de K , c'est-à-dire du nombre $4BD - C^2$; mais il est facile d'en voir la raison en remarquant que la formule

$$Bt^2 + Ctu + Du^2$$

peut se réduire à

$$\frac{(2Bt + Cu)^2 + (4BD - C^2)u^2}{4B},$$

de sorte que les diviseurs de la formule $Bt^2 + Ctu + Du^2$ peuvent être regardés aussi comme diviseurs de cette formule plus simple

$$x^2 \pm Ku^2.$$

Il résulte de là qu'il suffit de considérer les formules de cette dernière espèce; et pour cela nous ajouterons encore le Problème suivant, qui peut être regardé comme un cas particulier du précédent, mais qui dans le fond a la même généralité.

PROBLÈME II.

16. *Trouver toutes les formes possibles des diviseurs des nombres de la forme*

$$v \pm au^2,$$

a étant un nombre quelconque positif donné, et t et u étant des nombres indéterminés premiers entre eux.

1° Considérons la formule

$$t^2 + au^2,$$

et la comparant à la formule générale du Problème I, on aura

$$B = 1, \quad C = 0, \quad D = a;$$

donc $K = 4a$; donc Q devra être pair, et il ne devra pas être plus grand que $\pm \sqrt{\frac{4a}{3}}$; ainsi, faisant $Q = \pm 2q$ et regardant q comme positif, il faudra que q ne soit pas plus grand que $\sqrt{\frac{a}{3}}$; ensuite on aura

$$PR = \frac{4a + 4q^2}{4} = a + q^2;$$

de sorte que si p et r dénotent deux facteurs de $a + q^2$, dont aucun ne soit moindre que $2q$, on aura

$$py^2 \pm 2qyz + rz^2$$

pour la formule générale des diviseurs de $t^2 + au^2$.

Il est bon de remarquer que comme $pr = a + q^2$, il faudra que p et r soient de même signe, et il est clair qu'il faudra les prendre positivement pour que la formule

$$py^2 \pm 2qyz + rz^2$$

puisse représenter des nombres positifs.

De plus, comme cette formule ne change point de forme en y mettant p à la place de r , il ne sera pas nécessaire de prendre successivement pour p chacun des facteurs de $a + q^2$, et pour r tous les facteurs correspondants; c'est pourquoi dans chaque couple de facteurs de $a + q^2$ il suffira de prendre toujours le plus petit pour p , et le plus grand pour r ; et c'est ainsi que nous en userons dans la suite.

2° Considérons maintenant la formule

$$t^2 - au^2,$$

et l'on aura

$$B=1, \quad C=0, \quad D=-a,$$

donc $K=4a$, comme ci-dessus; c'est pourquoi on fera de même $Q=\pm 2q$, et il faudra que q ne soit pas plus grand que $\sqrt{\frac{a}{5}}$; ensuite on aura

$$PR=q^2-a;$$

de sorte que si l'on désigne par p et r deux facteurs de $a-q^2$ dont aucun ne soit plus petit que $2q$, on aura

$$P=p, \quad R=-r, \quad \text{ou} \quad P=-p, \quad R=r;$$

ce qui donnera ces deux formules

$$py^2 \pm 2qyz - rz^2, \quad -py^2 \pm 2qyz + rz^2,$$

pour les diviseurs de $t^2 - au^2$; et l'on trouverait la même chose pour la formule $au^2 - t^2$.

Quant aux nombres p et r , nous les prendrons tous les deux positifs, et nous supposerons toujours que p soit le plus petit des deux facteurs de $a-q^2$, et r le plus grand, comme nous l'avons dit plus haut; car il est visible qu'en changeant les signes de p et r , ou mettant l'un de ces nombres à la place de l'autre, on n'aurait pas de nouvelles formules.

17. COROLLAIRE. — Si l'on multiplie la formule

$$py^2 \pm 2qyz + rz^2$$

par p , elle pourra se mettre sous cette forme

$$(py \pm qz)^2 + (pr - q^2)z^2,$$

c'est-à-dire (à cause de $pr = a + q^2$) sous celle-ci

$$(py \pm qz)^2 + az^2,$$

qui est la même que celle de la formule $t^2 + au^2$. D'où il s'ensuit que tout diviseur d'un nombre de la forme $t^2 + au^2$ sera aussi nécessairement de la même forme si p n'a d'autres valeurs que l'unité, ou le deviendra étant multiplié par une des valeurs de p s'il y en a plusieurs. On prouvera de même que les formules

$$py^2 \pm 2qyz - rz^2, \quad -py^2 \pm 2qyz + rz^2$$

étant multipliées par p deviendront, à cause de $pr = a - q^2$,

$$(py \pm qz)^2 - az^2, \quad -(py \pm qz)^2 + az^2.$$

De sorte que tout diviseur d'un nombre de la forme $t^2 - au^2$ ou $au^2 - t^2$ sera nécessairement de l'une ou de l'autre de ces deux formes si p n'est que l'unité, ou bien le deviendra toujours étant multiplié par une des valeurs de p s'il y en a plus d'une.

THÉORÈMES SUR LES DIVISEURS DES NOMBRES DE LA FORME $t^2 + au^2$,
 t ET u ÉTANT SUPPOSÉS PREMIERS ENTRE EUX.

18. I. Soit $a=1$, donc q non plus grand que $\sqrt{\frac{1}{3}}$; donc $q=0$, $pr=1$; donc

$$p=1, \quad r=1.$$

Donc les diviseurs des nombres de la forme

$$t^2 + u^2$$

sont nécessairement renfermés dans la formule

$$y^2 + z^2;$$

c'est-à-dire que: *Tout diviseur d'un nombre égal à la somme de deux carrés est aussi la somme de deux carrés.*

II. Soit $a=2$, donc q non plus grand que $\sqrt{\frac{2}{3}}$; donc $q=0$, $pr=2$; donc

$$p=1, \quad r=2.$$

Donc les diviseurs des nombres de la forme

$$v^2 + 2u^2$$

sont renfermés dans la formule

$$y^2 + 2z^2;$$

c'est-à-dire que : *Tout diviseur d'un nombre égal à la somme d'un carré et d'un double carré est aussi la somme d'un carré et d'un double carré.*

III. Soit $a = 3$, donc q non plus grand que $\sqrt{\frac{3}{3}} = 1$; donc $q = 0$ ou 1 .
Faisant $q = 0$, on aura $pr = 3$, donc

$$p = 1, \quad r = 3;$$

ensuite faisant $q = 1$, on aura

$$pr = 3 + 1 = 4;$$

donc, comme ni p ni r ne doivent être $< 2q$, on aura

$$p = 2, \quad r = 2.$$

Donc les diviseurs des nombres de la forme

$$v^2 + 3u^2$$

seront renfermés dans ces deux formules

$$y^2 + 3z^2, \quad 2y^2 \pm 2yz + 2z^2.$$

Or comme la seconde de ces formules ne peut appartenir qu'à des nombres pairs, étant toute divisible par 2, il s'ensuit que tout diviseur impair de

$$v^2 + 3u^2$$

sera nécessairement renfermé dans la formule

$$y^2 + 3z^2;$$

c'est-à-dire que : *Tout diviseur impair d'un nombre qui est la somme d'un*

carré et d'un triple carré premiers entre eux, est aussi la somme d'un carré et d'un triple carré.

Au reste, comme il suffit de considérer les diviseurs impairs, nous ferons toujours abstraction, dans la suite, des formules qui ne pourraient convenir qu'à des diviseurs pairs; c'est pourquoi nous rejetterons toutes les valeurs de p et r qui seraient paires à la fois.

IV. Soit $a = 4$, donc q non plus grand que $\sqrt{\frac{4}{3}}$; donc $q = 0$ ou 1 .
Faisant $q = 0$, on a $pr = 4$; donc

$$p = 1, \quad r = 4$$

(car nous rejetons les valeurs $p = 2, r = 2$, parce qu'elles sont toutes deux paires); faisant $q = 1$, on a $pr = 5$; donc

$$p = 1, \quad r = 5,$$

ce qui doit être rejeté à cause que p serait $< 2q$.

Donc les diviseurs impairs des nombres de la forme

$$v^2 + 4u^2$$

seront aussi de la forme

$$y^2 + 4z^2.$$

V. Soit $a = 5$, donc q non plus grand que $\sqrt{\frac{5}{3}}$; donc $q = 0$ ou 1 .
Faisant $q = 0$, on a $pr = 5$, donc

$$p = 1, \quad r = 5;$$

et faisant $q = 1$, on a $pr = 6$, donc

$$p = 2, \quad r = 3.$$

Donc les diviseurs des nombres de la forme

$$v^2 + 5u^2$$

sont nécessairement de l'une ou de l'autre de ces formes-ci

$$y^2 + 5z^2, \quad 2y^2 \pm 2yz + 3z^2;$$

de sorte que ces diviseurs eux-mêmes ou leurs doubles sont toujours (17) de la forme $t^2 + 5u^2$.

VI. Soit $a = 6$, donc q non plus grand que $\sqrt{\frac{6}{3}}$, donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 6$; donc

$$p = 1, \quad r = 6, \quad \text{ou} \quad p = 2, \quad r = 3;$$

faisant $q = 1$, on aura $pr = 7$, donc

$$p = 1, \quad r = 7,$$

ce qui doit être rejeté parce que p serait $< 2q$.

Donc les diviseurs des nombres de la forme

$$t^2 + 6u^2$$

seront de l'une ou de l'autre de ces formes

$$y^2 + 6z^2, \quad 2y^2 + 3z^2;$$

de sorte que ces diviseurs eux-mêmes ou leurs doubles seront de la même forme $t^2 + 6u^2$.

VII. Soit $a = 7$, donc q non plus grand que $\sqrt{\frac{7}{3}}$, donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 7$; donc

$$p = 1, \quad q = 7;$$

faisant $q = 1$, on aura $pr = 8$; donc

$$p = 2, \quad r = 4;$$

ce qui ne peut convenir qu'aux diviseurs pairs.

Donc les diviseurs impairs des nombres de la forme

$$t^2 + 7u^2$$

sont nécessairement aussi de la forme

$$y^2 + 7z^2.$$

VIII. Soit $a = 8$, donc q non plus grand que $\sqrt{\frac{8}{3}}$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 8$; donc

$$p = 1, \quad r = 8;$$

et l'on rejettera les valeurs $p = 2, r = 4$ comme ne pouvant appartenir qu'à des diviseurs pairs; faisant ensuite $q = 1$, on aura $pr = 9$; donc

$$p = 3, \quad r = 3.$$

Donc les diviseurs des nombres de la forme

$$t^2 + 8u^2$$

sont de l'une ou de l'autre de ces formes

$$y^2 + 8z^2, \quad 3y^2 \pm 2yz + 3z^2;$$

de sorte que ces diviseurs eux-mêmes, ou leurs triples, seront toujours de la même forme

$$t^2 + 8u^2.$$

IX. Soit $a = 9$, donc q non plus grand que $\sqrt{\frac{9}{3}}$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 9$; donc

$$p = 1, \quad r = 9, \quad \text{ou} \quad p = 3, \quad r = 3;$$

faisant $q = 1$, on aura $pr = 10$; donc

$$p = 2, \quad r = 5.$$

Donc les diviseurs des nombres de la forme

$$t^2 + 9u^2$$

sont nécessairement de l'une de ces trois formes

$$y^2 + 9z^2, \quad 3y^2 + 3z^2, \quad 2y^2 \pm 2yz + 5z^2;$$

de sorte que ces diviseurs eux-mêmes, ou leurs doubles ou leurs triples, pourront toujours se rapporter à la même forme $t^2 + 9u^2$.

X. Soit $a = 10$, donc q non plus grand que $\sqrt{\frac{10}{3}}$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 10$; donc

$$p = 1, \quad r = 10, \quad \text{ou} \quad p = 2, \quad r = 5;$$

faisant $q = 1$, on aura $pr = 11$; donc

$$p = 1, \quad r = 11,$$

ce qui n'est point admissible à cause que p serait $< 2q$.

Donc les diviseurs des nombres de la forme

$$t^2 + 10u^2$$

sont toujours de l'une de ces formes

$$y^2 + 10z^2, \quad 2y^2 + 5z^2;$$

de sorte que ces diviseurs eux-mêmes ou leurs doubles seront nécessairement de la même forme

$$t^2 + 10u^2.$$

XI. Soit $a = 11$, donc q non plus grand que $\sqrt{\frac{11}{3}}$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on a $pr = 11$; donc

$$p = 1, \quad r = 11;$$

faisant $q = 1$, on a $pr = 12$; donc

$$p = 3, \quad q = 4;$$

car les valeurs $p = 2$ et $r = 6$ sont à rejeter à cause qu'elles ne conviendraient qu'aux diviseurs pairs.

Donc les diviseurs impairs des nombres de la forme

$$t^2 + 11u^2$$

sont de l'une ou de l'autre de ces formes

$$y^2 + 11z^2, \quad 3y^2 \pm 2y^2 + 4z^2;$$

de sorte que ces diviseurs eux-mêmes ou leurs triples seront toujours de la même forme

$$t^2 + 11u^2.$$

XII. Soit $a = 12$, donc q non plus grand que $\sqrt{\frac{12}{3}} = 2$; donc $q = 0$ ou $= 1$ ou $= 2$. Faisant $q = 0$, on aura $pr = 12$; donc

$$p = 1, \quad r = 2, \quad \text{ou} \quad p = 3, \quad r = 4,$$

en rejetant les valeurs $p = 2, r = 2$, qui ne conviendraient qu'aux diviseurs pairs; faisant $q = 1$, on aura $pr = 13$; donc

$$p = 1, \quad r = 13,$$

ce qui doit être rejeté à cause que p serait $< 2q$; faisant $q = 2$, on aura $pr = 12 + 4 = 16$; donc

$$p = 4, \quad r = 4$$

(car, à cause de $q = 2$, p ne doit pas être < 4), ce qui doit être rejeté si l'on ne considère que les diviseurs impairs.

Donc les diviseurs impairs des nombres de la formule

$$t^2 + 12u^2$$

sont de l'une ou de l'autre de ces formes

$$y^2 + 12z^2, \quad 3y^2 + 4z^2;$$

de sorte que ces diviseurs eux-mêmes ou leurs triples seront de la même forme

$$t^2 + 12u^2.$$

Nous n'étendrons pas ces Recherches plus loin, d'autant que les Exemples que nous venons de donner sont plus que suffisants pour montrer l'application de nos méthodes et pour mettre sur la voie ceux qui voudront en faire usage pour découvrir de nouveaux Théorèmes sur la forme des diviseurs des nombres $t^2 + au^2$.

19. REMARQUE. — Les trois premiers Théorèmes sont connus depuis longtemps des Géomètres, et sont dus, je crois, à M. Fermat; mais M. Euler est le premier qui les ait démontrés. On peut voir les démonstrations de ce dernier dans les tomes IV, VI et VIII des *Nouveaux Commentaires de Pétersbourg*. Sa méthode est totalement différente de la nôtre, et elle n'est d'ailleurs applicable qu'aux cas où le nombre a ne surpasse pas 3; c'est ce qui a peut-être empêché ce grand Géomètre de pousser plus loin ses recherches sur ce sujet.

A l'égard des Théorèmes qu'il avait déjà donnés auparavant sans démonstration dans le tome XIV des anciens *Commentaires*, il est vraisemblable qu'il ne les a trouvés que par induction, d'autant qu'il n'en a fait aucune mention dans les tomes cités des *Nouveaux Commentaires*, où il a même remarqué que ses démonstrations ne pouvaient s'étendre à d'autres nombres qu'à ceux de la forme $t^2 + u^2$, $t^2 + 2u^2$ et $t^2 + 3u^2$ (tome VI, page 214).

THÉORÈMES SUR LES DIVISEURS DES NOMBRES DE LA FORME $t^2 - au^2$
OU $au^2 - t^2$, t ET u ÉTANT SUPPOSÉS PREMIERS ENTRE EUX.

20. I. Soit $a = 1$, donc q non plus grand que $\sqrt{\frac{1}{5}}$; donc $q = 0$, $pr = 1$; donc

$$p = 1, \quad r = 1.$$

Donc les diviseurs des nombres de la forme

$$t^2 - u^2$$

sont de la forme

$$y^2 - z^2;$$

par conséquent (14) tout nombre est réductible à cette forme

$$y^2 - z^2;$$

c'est ce qu'on sait d'ailleurs.

II. Soit $a = 2$, donc q non plus grand que $\sqrt{\frac{2}{5}}$; donc $q = 0$, $pr = 2$;

donc

$$p = 1, \quad r = 2;$$

de sorte que les formes des diviseurs de

$$t^2 - 2u^2 \quad \text{ou} \quad 2u^2 - t^2$$

seront

$$y^2 - 2z^2 \quad \text{ou} \quad 2z^2 - y^2;$$

mais je remarque que ces deux formes reviennent à la même; car faisant

$$y = y' + 2z', \quad z = y' + z'$$

(ce qui donne $y' = 2z - y$ et $z' = y - z$, et par conséquent des valeurs entières pour y' et z'), la formule $y^2 - 2z^2$ devient $2z'^2 - y'^2$.

Donc les diviseurs des nombres de la forme

$$t^2 - 2u^2 \quad \text{ou} \quad 2u^2 - t^2$$

sont nécessairement de l'une et de l'autre de ces formes

$$y^2 - 2z^2, \quad 2z^2 - y^2.$$

III. Soit $a = 3$, donc q non plus grand que $\sqrt{\frac{3}{5}}$; donc $q = 0$, $pr = 3$; donc

$$p = 1, \quad r = 3.$$

Donc les diviseurs des nombres de la forme

$$t^2 - 3u^2 \quad \text{ou} \quad 3u^2 - t^2$$

sont de l'une ou de l'autre de ces deux formes

$$y^2 - 3z^2, \quad 3z^2 - y^2.$$

IV. Soit $a = 4$, donc q non plus grand que $\sqrt{\frac{4}{5}}$; donc $q = 0$, $pr = 4$; donc

$$p = 1, \quad r = 4, \quad \text{ou} \quad p = 2, \quad r = 2.$$

Donc les diviseurs des nombres de la forme

$$t^2 - 4u^2 \quad \text{ou} \quad 4u^2 - t^2$$

seront nécessairement renfermés dans les formules

$$y^2 - 4z^2, \quad 4z^2 - y^2, \quad 2y^2 - 2z^2;$$

par conséquent (14) tout nombre quelconque sera de l'une de ces formes.

Au reste, nous pouvons faire abstraction des formes qui ne sauraient convenir qu'à des diviseurs pairs, telles que celle-ci $2y^2 - 2z^2$; ainsi nous rejeterons dans la suite, comme nous l'avons déjà fait plus haut, les valeurs de p et de r qui se trouveront paires en même temps.

V. Soit $a = 5$, donc q non plus grand que $\sqrt{\frac{5}{5}} = 1$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on a $pr = 5$; donc

$$p = 1, \quad r = 5;$$

faisant $q = 1$, on aurait $pr = 4$; de sorte qu'à cause que p et r doivent n'être pas $< 2q$, on ne pourrait faire que

$$p = 2, \quad r = 2;$$

mais nous rejeterons ces valeurs à cause qu'elles sont toutes deux paires; ainsi l'on n'aura que ces deux formes de diviseurs

$$y^2 - 5z^2 \quad \text{et} \quad 5z^2 - y^2,$$

lesquelles se réduisent d'ailleurs à la même, comme on peut s'en convaincre en faisant

$$y = 2y' + 5z' \quad \text{et} \quad z = y' + 2z'$$

(ce qui donnerait $z' = y - 2z$ et $y' = 5z - 2y$, et par conséquent des valeurs entières pour y' et z') dans la formule $y^2 - 5z^2$, laquelle deviendra par ces substitutions celle-ci, $5z'^2 - y'^2$.

Donc les diviseurs impairs des nombres de la forme

$$p^2 - 5u^2 \quad \text{ou} \quad 5u^2 - p^2$$

sont en même temps de chacune de ces deux formes

$$y^2 - 5z^2, \quad 5z^2 - y^2.$$

VI. Soit $a = 6$, donc q non plus grand que $\sqrt{\frac{6}{5}}$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 6$; donc

$$p = 1, \quad r = 6, \quad \text{ou} \quad p = 2, \quad r = 3;$$

faisant ensuite $q = 1$, on aura $pr = 5$, ce qui ne donnerait que

$$p = 1, \quad r = 5,$$

valeurs qui ne sont point admissibles à cause que p serait $< 2q$; de sorte que les formules des diviseurs des nombres de la forme

$$p^2 - 6u^2 \quad \text{ou} \quad 6u^2 - p^2$$

seront

$$y^2 - 6z^2, \quad 6z^2 - y^2, \quad 2y^2 - 3z^2, \quad 3z^2 - 2y^2.$$

Mais j'observe que ces dernières se réduisent aux deux premières en faisant

$$2y + 3z = y', \quad y + z = z',$$

ce qui donne

$$y = 3z' - y', \quad z = y' - 2z',$$

et par conséquent

$$2y^2 - 3z^2 = 6z'^2 - y'^2, \quad 3z^2 - 2y^2 = y'^2 - 6z'^2.$$

Donc les diviseurs des nombres de la forme

$$p^2 - 6u^2 \quad \text{ou} \quad 6u^2 - p^2$$

seront toujours aussi de l'une ou de l'autre de ces formes.

VII. Soit $a = 7$, donc q non plus grand que $\sqrt{\frac{7}{5}}$; donc $q = 0$ ou $= 1$.
Faisant $q = 0$, on aura $pr = 7$; donc

$$p = 1, \quad r = 7,$$

et faisant $q = 1$, on aura $pr = 6$; donc

$$p = 2, \quad r = 3;$$

de sorte que les formules des diviseurs de

$$t^2 - 7u^2$$

seront

$$y^2 - 7z^2, \quad 2y^2 \pm 2yz - 7z^2$$

et leurs inverses

$$7z^2 - y^2, \quad 7z^2 \pm 2yz - 2y^2.$$

Mais je remarque ici que les deux premières de ces formules reviennent à la même, aussi bien que les deux dernières; car faisant

$$y = y' - 2z \quad \text{et} \quad z = y' - 3z'$$

(ce qui donne $y' = 3y \mp 2z$ et $z' = y \mp z$, c'est-à-dire des nombres entiers pour y' et z'), la formule

$$2y^2 \pm 2yz - 3z^2$$

deviendra

$$y'^2 - 7z'^2,$$

et la formule

$$3z^2 \mp 2yz - 2y^2$$

deviendra de même

$$7z'^2 - y'^2.$$

D'où il s'ensuit que les diviseurs des nombres de la forme

$$t^2 - 7u^2 \quad \text{ou} \quad 7u^2 - t^2$$

seront nécessairement aussi de la forme

$$y^2 - 7z^2 \quad \text{ou} \quad 7z^2 - y^2.$$

VIII. Soit $a = 8$, donc q non plus grand que $\sqrt{\frac{8}{5}}$; donc $q = 0$ ou $= 1$. Faisant $q = 0$, on aura $pr = 8$; donc

$$p = 1, \quad r = 8, \quad \text{ou} \quad p = 2, \quad r = 4;$$

mais ces dernières valeurs peuvent être rejetées à cause qu'elles sont

toutes deux paires; faisant ensuite $q = 1$, on aura $pr = 7$, ce qui ne donnerait que

$$p = 1 \quad \text{et} \quad r = 7,$$

valeurs qui ne sont point admissibles à cause que p serait $< 2q$.

Donc les diviseurs impairs des nombres de la forme

$$t^2 - 8u^2 \quad \text{ou} \quad 8u^2 - t^2,$$

seront de l'une ou de l'autre de ces deux formes

$$y^2 - 8z^2 \quad \text{ou} \quad 8z^2 - y^2.$$

IX. Soit $a = 9$, donc q non plus grand que $\sqrt{\frac{9}{5}}$; donc $q = 0$ ou $= 1$. Faisant $q = 0$, on aura $pr = 9$; donc

$$p = 1, \quad r = 9, \quad \text{ou} \quad p = 3, \quad r = 3;$$

et faisant $q = 1$, on aura $pr = 8$, ce qui, à cause de p non plus petit que $2q$, donnerait

$$p = 2, \quad r = 4,$$

valeurs qu'on peut rejeter à cause qu'elles sont l'une et l'autre paires.

Donc les diviseurs impairs des nombres de la forme

$$t^2 - 9u^2 \quad \text{ou} \quad 9u^2 - t^2$$

seront toujours de quelqu'une de ces formes

$$y^2 - 9z^2, \quad 9z^2 - y^2, \quad 3y^2 - 3z^2;$$

par conséquent (14) tout nombre quelconque impair sera réductible à l'une de ces formes.

X. Soit $a = 10$, donc q non plus grand que $\sqrt{\frac{10}{5}} = \sqrt{2}$; donc $q = 0$ ou $= 1$. Faisant $q = 0$, on aura $pr = 10$; donc

$$p = 1, \quad r = 10, \quad \text{ou} \quad p = 2, \quad r = 5;$$

faisant $q = 1$, on aura $pr = 9$; donc

$$p = 3, \quad r = 3;$$

de sorte que les formules des diviseurs de

$$P = 10u^2$$

seront

$$y^2 - 10z^2, \quad 10z^2 - y^2, \quad 2y^2 - 5z^2, \quad 5z^2 - 2y^2, \quad 3y^2 \pm 2yz - 3z^2.$$

Or je remarque d'abord que cette dernière formule peut se réduire à ces deux-ci

$$2y'^2 - 5z'^2, \quad 5z'^2 - 2y'^2,$$

en faisant

$$\pm y = y' + z', \quad z = y' + 2z'$$

ou

$$\pm y = y' + 2z', \quad z = y' + z',$$

ce qui donne toujours pour y' et z' des nombres entiers; je remarque ensuite que les deux formules

$$y^2 - 10z^2, \quad 10z^2 - y^2$$

peuvent aussi se réduire à la même en faisant dans la première

$$y = 10z' + 3y', \quad z = 3z' + y',$$

ce qui la transformera en $10z'^2 - y'^2$; et quant aux nombres y' et z' il est clair qu'ils seront toujours entiers, puisque l'on aura

$$z' = y - 3z, \quad y' = 10z - 3y.$$

De là je conclus que les diviseurs des nombres de la forme

$$P = 10u^2 \quad \text{ou} \quad 10u^2 - P$$

seront toujours de l'une ou de l'autre de ces deux formes

$$y^2 - 10z^2, \quad 2y^2 - 5z^2,$$

aussi bien que de celles-ci

$$10z^2 - y^2, \quad 5z^2 - 2y^2.$$

XI. Soit $a = 11$, donc q non plus grand que $\sqrt{\frac{11}{5}}$; donc $q = 0$ ou $q = 1$.
Faisant $q = 0$, on aura $pr = 11$; donc

$$p = 1, \quad r = 11;$$

faisant $q = 1$, on a $pr = 10$; donc

$$p = 2, \quad r = 5.$$

De sorte que les formules des diviseurs seront, dans ce cas,

$$y^2 - 11z^2, \quad 11z^2 - y^2, \quad 2y^2 \pm 2yz - 5z^2, \quad 5z^2 \pm 2yz - 2y^2.$$

Mais je remarque que ces deux dernières formules peuvent se réduire aux deux premières; car en faisant

$$\pm y = y' + 4z', \quad z = y' + 3z'$$

(ce qui donne $z' = \pm y - z$ et $y' = 4z \mp 3y$, et par conséquent toujours des nombres entiers pour y' et z'), la formule

$$2y^2 \pm 2yz - 5z^2$$

devient

$$11z'^2 - y'^2,$$

et la formule

$$5z^2 \mp 2yz - 2y^2$$

devient de même

$$y'^2 - 11z'^2.$$

D'où il s'ensuit que les diviseurs des nombres de la forme

$$P = 11u^2, \quad 11u^2 - P$$

sont toujours de l'une ou de l'autre de ces formes

$$y^2 - 11z^2, \quad 11z^2 - y^2.$$

XII. Soit $a = 12$, donc q non plus grand que $\sqrt{\frac{12}{5}}$; donc $q = 0$ ou $q = 1$.
Faisant $q = 0$, on aura $pr = 12$; donc

$$p = 1, \quad r = 12, \quad \text{ou} \quad p = 3, \quad r = 4,$$

III.

en rejetant les valeurs paires $p = 2$ et $r = 6$; faisant ensuite $q = 1$, on aurait $pr = 11$; donc

$$p = 1, \quad r = 11,$$

valeurs qui ne sont point admissibles à cause que p serait $< 2q$; ainsi l'on n'aura que ces formules

$$y^2 - 12z^2, \quad 12z^2 - y^2, \quad 3y^2 - 4z^2, \quad 4z^2 - 3y^2,$$

sur lesquelles je remarque que les deux dernières sont réductibles aux deux premières, en faisant

$$y = 4y' + z' \quad \text{et} \quad z = 3y' + z',$$

ce qui donne $y' = y - z$ et $z' = 4z - 3y$, et par conséquent des valeurs entières pour y' et z' .

D'où l'on peut conclure que les diviseurs impairs des nombres de la forme

$$t^2 - 12u^2 \quad \text{ou} \quad 12u^2 - t^2,$$

seront toujours de l'une ou de l'autre de ces deux formes

$$y^2 - 12z^2, \quad 12z^2 - y^2,$$

aussi bien que de ces deux-ci

$$3y^2 - 4z^2, \quad 4z^2 - 3y^2.$$

21. REMARQUE. — Telle est la méthode qu'il faudra suivre pour trouver les formules des diviseurs des nombres de la forme

$$t^2 - au^2 \quad \text{ou} \quad au^2 - t^2,$$

en donnant à a des valeurs quelconques au delà de 12; cette méthode est, comme on voit, d'un usage très-facile et très-simple; mais elle paraît sujette à une espèce d'inconvénient, c'est qu'elle donne quelquefois plus de formules qu'il n'en faut pour représenter tous les diviseurs des nombres d'une forme donnée; de sorte qu'il arrive que quelques-unes de ces formules reviennent à la même, comme nous l'avons vu dans les Exemples précédents. Pour y remédier il faudrait donc avoir une règle

générale par laquelle on pût reconnaître facilement les formules qui sont identiques entre elles: c'est ce que nous allons examiner, avec toute la généralité dont la matière est susceptible; et comme il n'est pas démontré jusqu'ici que cette identité de formules ne puisse avoir lieu dans les diviseurs des nombres de la forme $t^2 + au^2$, quoique les différents cas du n° 18 n'en fournissent aucun exemple, pour ne rien laisser à désirer sur ce sujet, nous considérerons également les formules de l'une et de l'autre espèce.

PROBLÈME III.

22. Etant donnée la formule

$$py^2 + 2qyz + rz^2,$$

dans laquelle y et z sont des nombres indéterminés et p, q, r sont des nombres positifs ou négatifs, déterminés par ces conditions, que

$$pr - q^2 = a$$

(a étant un nombre positif donné) et que $2q$ ne soit ni $> p$ ni $> r$, abstraction faite des signes de p, q et r ; trouver si cette formule peut se transformer en une autre de la même espèce et qui soit assujettie aux mêmes conditions.

Comme la transformée doit être analogue à la proposée, il est visible qu'on ne saurait employer d'autres substitutions que celles-ci

$$y = Ms + Nx, \quad z = ms + nx,$$

s et x étant deux nouvelles indéterminées, et M, N, m, n des nombres arbitraires. En effet ces substitutions donneront une transformée de cette forme

$$Ps^2 + 2Qsx + Rx^2,$$

dans laquelle on aura

$$P = pM^2 + 2qMm + r m^2,$$

$$Q = pMN + q(Mn + Nm) + r mn,$$

$$R = pN^2 + 2qNn + r n^2,$$

et il ne s'agira que de voir si l'on peut déterminer les nombres M , N , m , n , en sorte que l'on ait

$$PR - Q^2 = a,$$

et que $2Q$ ne soit ni $> P$ ni $> R$.

Pour satisfaire à la première condition je substitue dans la quantité $PR - Q^2$ les valeurs de P , Q , R , et je trouve, en effaçant ce qui se détruit,

$$PR - Q^2 = (pr - q^2)(Mn - Nm)^2;$$

mais (hypothèse)

$$pr - q^2 = a,$$

donc, pour que $PR - Q^2$ soit aussi égal à a , il faudra que l'on ait

$$(Mn - Nm)^2 = 1,$$

et par conséquent

$$Mn - Nm = \pm 1.$$

A l'égard de la seconde condition, il est clair qu'elle ne saurait avoir lieu à moins que Q ne soit en même temps $< P$ et $< R$; ainsi nous supposerons que Q soit en effet $< P$ et $< R$, et nous allons voir ce qui doit s'ensuivre.

Soit $M > N$ (le raisonnement serait le même si N était $> M$, en prenant seulement N à la place de M), il est clair qu'on peut faire

$$M = \mu N + M',$$

et qu'on peut prendre μ tel que M' devienne moindre que N ; car il n'y a qu'à prendre pour μ le quotient de la division de M par N , et M' sera le reste; de plus il est facile de voir qu'on peut toujours supposer que μ ne soit pas moindre que 2; car si l'on trouvait $\mu = 1$, en sorte que $M = N + M'$, on pourrait faire

$$M = 2N - (N - M'),$$

c'est-à-dire prendre $\mu = 2$ et $N - M'$ à la place de M' . Or si l'on suppose aussi, ce qui est permis,

$$m = \mu n + m',$$

m' étant un nombre quelconque; et qu'on substitue ces valeurs de M et

de m dans l'expression de Q , elle deviendra

$$Q = \mu(pN^2 + 2qNn + rn^2) + pM'N + q(M'n + Nm') + rm'n,$$

de sorte qu'en faisant, pour abréger,

$$Q' = pM'N + q(M'n + Nm') + rm'n,$$

on aura

$$Q = \mu R + Q'.$$

Or il faut que Q soit $< R$; donc, puisque μ est ou > 2 , il est clair que cette condition ne saurait avoir lieu à moins que les deux quantités μR et Q' ne soient de signes différents et que Q' ne soit en même temps $> R$, abstraction faite des signes.

Maintenant on aura

$$y = (\mu N + M')s + Nx, \quad z = (\mu n + m')s + nx;$$

de sorte que si l'on fait

$$x' = \mu s + x,$$

on aura

$$y = M's + Nx', \quad z = m's + nx',$$

et la substitution de ces valeurs dans la formule

$$py^2 + 2qyz + rz^2$$

donnera la nouvelle transformée

$$P's^2 + 2Q'sx' + Rx'^2,$$

en supposant

$$P' = pM'^2 + 2qM'm' + rm'^2,$$

$$Q' = pM'N + q(M'n + Nm') + rm'n,$$

et

$$R = pN^2 + 2qNn + rn^2,$$

comme plus haut.

Or à cause de

$$Mn - Nm = \pm 1,$$

on aura

$$(\mu N + M')n - N(\mu n + m') = \pm 1,$$

et par conséquent

$$M'n - N'm' = \pm 1.$$

On trouvera aussi

$$P'R - Q'^2 = (pr - q^2)(M'n - N'm')^2,$$

et par conséquent

$$P'R - Q'^2 = a.$$

De sorte que, comme a est positif et que Q' est $> R$, il faudra que P' soit $> Q'$; ainsi la transformée précédente sera telle, que Q' sera $> R$ et $\leq P'$.

De la même manière, à cause que N est $> M'$, on pourra supposer

$$N = \mu' M' + N',$$

et prendre μ' en sorte qu'il ne soit pas < 2 et que N' soit $< M'$; et faisant ensuite

$$n = \mu' m' + n', \quad s' = \mu' x' + s,$$

en sorte que l'on ait

$$y = M's' + N'x', \quad z = m's' + n'x',$$

on parviendra, par des opérations et des raisonnements semblables aux précédents, à cette nouvelle transformée

$$P's'^2 + 2Q's's' + R'x'^2,$$

dans laquelle on aura

$$P' = pM'^2 + 2qM'm' + rm'^2,$$

$$Q' = pM'N' + q(M'n' + N'm') + rm'n',$$

$$R' = pN'^2 + 2qN'n' + rn'^2,$$

et où l'on aura aussi

$$M'n' - N'm' = \pm 1,$$

$$Q' = \mu' P' + Q'',$$

$$P'R' - Q'^2 = a.$$

en sorte que Q'' sera $> P'$ et $< R'$, abstraction faite des signes de P' , R' et Q'' .

On pourra trouver de même une troisième transformée telle que

$$P''s'^2 + 2Q''s's' + R'x'^2,$$

laquelle sera soumise aux mêmes conditions que les transformées précédentes, et ainsi de suite.

Je considère maintenant que comme les nombres

$$M, N, M', N', \dots$$

forment (abstraction faite de leurs signes) une suite décroissante, on arrivera nécessairement à un terme qui sera égal à zéro. Supposons que N' soit ce terme, en sorte que l'on ait $N' = 0$; donc à cause de

$$M'n' - N'm' = \pm 1$$

on aura

$$M'n' = \pm 1;$$

done

$$M' = \pm 1 \quad \text{et} \quad n' = \pm 1,$$

done

$$P' = p \pm 2qm' + rm'^2, \quad Q' = \pm q \pm rm', \quad R' = r,$$

les signes ambigus étant arbitraires.

Or il faut :

1° Que l'on ait $Q' < R'$, abstraction faite des signes de ces nombres; mais $R' = r$ et $q < r$, à cause de $2q$ non plus grand que r (hypothèse), donc Q' ne pourra être $< R'$, $< r$ à moins que m' ne soit égal à zéro ou égal à ± 1 .

2° Que Q' soit en même temps $> P'$; or si $m' = 0$, on a

$$Q' = \pm q, \quad P' = p;$$

de sorte qu'à cause de $2q$ non plus grand que p (hypothèse), Q' sera toujours $< P'$ au lieu d'être plus grand; si $m' = \pm 1$, on aura

$$P' = p \pm 2q + r \quad \text{et} \quad Q' = q \pm r;$$

mais on suppose que Q^2 soit $< r$; donc, pour que Q^2 soit $> P$, il faudrait que r pût être $> p \pm 2q + r$, ce qui ne se peut à cause que $2q$ n'est jamais $> p$, et que d'ailleurs p et r doivent être de mêmes signes en vertu de l'équation

$$pr - q^2 = \text{un nombre positif.}$$

De là je conclus qu'il est impossible que la formule proposée soit transformée en une autre où les conditions énoncées aient lieu; de sorte que si l'on a plusieurs formules où les mêmes conditions soient observées, on peut être assuré que ces formules sont essentiellement différentes entre elles, et qu'elles ne peuvent pas se réduire à un plus petit nombre.

PROBLÈME IV.

23. Étant donnée la formule

$$py^2 + 2qyz - rz^2,$$

dans laquelle y et z sont des nombres indéterminés, et p, q, r des nombres positifs ou négatifs, déterminés par ces conditions, que

$$pr + q^2 = a$$

(a étant un nombre positif donné) et que $2q$ ne soit ni $> p$ ni $> r$, abstraction faite des signes de p, q et r ; trouver si cette formule peut se transformer en une autre semblable, et où les mêmes conditions soient observées.

Faisant, comme dans le Problème précédent et par la même raison,

$$y = Ms + Nx, \quad z = ms + nx,$$

on aura la transformée

$$Ps^2 + 2Qsx - Rx^2,$$

dans laquelle

$$\begin{aligned} P &= pM^2 + 2qMm - rm^2, \\ Q &= pMN + q(Mn + Nm) - rmn, \\ R &= rn^2 - 2qNn - pN^2; \end{aligned}$$

ainsi la difficulté consiste à déterminer, s'il est possible, les nombres M, N, m, n , en sorte qu'on ait

$$PR + Q^2 = a,$$

et qu'en même temps ni P ni R ne soient $< 2Q$, abstraction faite des signes de P, Q et R .

Je remarque d'abord que la quantité $PR + Q^2$ devient, en mettant à la place de P, Q et R leurs valeurs,

$$(pr + q^2)(Mn - Nm)^2 = a(Mn - Nm)^2;$$

done il faudra qu'on ait comme dans le Problème précédent

$$(Mn - Nm)^2 = 1,$$

et par conséquent

$$Mn - Nm = \pm 1.$$

Comme M, N, m, n sont supposés des nombres entiers, il est clair que cette équation ne saurait subsister à moins que les produits Mn et Nm ne soient de mêmes signes; de sorte que si M et N sont de mêmes signes, il faudra que m et n en soient aussi.

Or, puisqu'on peut donner aux nombres indéterminés s et x tels signes que l'on veut, il est évident qu'on peut, sans nuire à la généralité du Problème, prendre toujours les nombres M et N positifs; et alors il faudra prendre les nombres m et n de mêmes signes, c'est-à-dire tous les deux positifs ou tous les deux négatifs; ainsi il n'y aura qu'à mettre $\pm m$ et $\pm n$ à la place de m et n , ou, ce qui revient au même, il n'y aura qu'à donner le signe ambigu $\pm$ à la quantité q , c'est-à-dire prendre la valeur de cette quantité en *plus* et en *moins*; moyennant quoi on pourra regarder les quatre nombres M, N, m, n comme positifs.

Maintenant il est clair que si $2Q$ n'est ni $> P$ ni $> R$, comme on le suppose, Q^2 sera toujours moindre que PR , de sorte que $PR + Q^2$ ne pourra être égal à un nombre positif, à moins que PR ne soit un nombre positif; d'où il s'ensuit qu'il faut nécessairement que P et R soient de même signe; et cette condition suffit, comme nous l'allons voir, pour faire trouver les nombres M, N, m, n .

Pour cela j'observe qu'à cause de

$$pr + q^2 = a,$$

la quantité P peut se mettre sous cette forme

$$P = p \left(M + \frac{q + \sqrt{a}}{p} m \right) \left(M + \frac{q - \sqrt{a}}{p} m \right),$$

et la quantité R sous celle-ci

$$R = -p \left(N + \frac{q + \sqrt{a}}{p} n \right) \left(N + \frac{q - \sqrt{a}}{p} n \right).$$

Or, comme $\sqrt{a}$ est $> q$, il est clair que la quantité $q + \sqrt{a}$ sera toujours positive, et la quantité $q - \sqrt{a}$ toujours négative; de sorte que les deux quantités

$$\frac{q + \sqrt{a}}{p}, \quad \frac{q - \sqrt{a}}{p}$$

seront nécessairement de signes différents. Nommant donc α celle de ces deux quantités qui sera positive, et $-\beta$ celle qui sera négative (α et β denotant des nombres positifs), on aura

$$P = p(M + \alpha m)(M - \beta m), \\ R = -p(N + \alpha n)(N - \beta n).$$

D'où l'on voit que, pour que les nombres P et R soient de mêmes signes, il faut que les facteurs $M - \beta m$ et $N - \beta n$ soient de signes différents, parce que les facteurs $M + \alpha m$ et $N + \alpha n$ sont tous les deux positifs.

Cela posé, soit $M > N$, on pourra faire

$$M = \mu N + M',$$

et prendre pour μ un nombre entier positif tel, que M' soit aussi positif et moindre que N; car pour cela il n'y aura qu'à diviser M par N, et faire le quotient égal à μ et le reste égal à M' . Qu'on fasse de même

$$m = \mu n + m',$$

m' étant un nombre quelconque, et substituant ces valeurs dans l'équation

$$Mn - Nm = \pm 1,$$

on aura celle-ci

$$M'n - Nm' = \pm 1,$$

d'où l'on voit qu'à cause de M, N et n positifs, il faudra que m' soit aussi un nombre positif.

Or les valeurs de y et de z deviendront par ces mêmes substitutions

$$y = (\mu s + x)N + M's, \quad z = (\mu s + x)n + m's,$$

ou bien, en faisant comme plus haut $x' = \mu s + x$,

$$y = M's + Nx', \quad z = m's + nx';$$

et, ces valeurs étant substituées dans la formule

$$py^2 + 2qyz - rz^2,$$

on aura la transformée

$$P's^2 + 2Q'sx' - Rx'^2,$$

où

$$P' = pM'^2 + 2qM'm' - rm'^2, \\ Q' = pM'N + q(M'n + Nm') - rm'n, \\ R = rn^2 - qNn - pN^2.$$

Et je dis que les nombres P' et R seront nécessairement de mêmes signes; car on aura

$$P' = p(M' + \alpha m')(M' - \beta m'), \\ R = -p(N + \alpha n)(N - \beta n);$$

or

$$M - \beta m = \mu(N - \beta n) + M' - \beta m';$$

donc, comme μ est un nombre positif et que $M - \beta m$ et $N - \beta n$ sont de signes différents, il faudra, pour que cette équation puisse subsister, que les quantités $M - \beta m$ et $M' - \beta m'$ soient de mêmes signes, et par conséquent que $N - \beta n$ et $M' - \beta m'$ soient de signes différents; mais $N + \alpha n$ et $M' + \alpha m'$ sont des quantités positives, N, n, M', m' et α étant

des nombres positifs; donc les deux nombres P' et R seront nécessairement de même signe.

De même, puisque $N > M'$, on pourra supposer

$$N = \mu' M' + N'$$

et prendre μ' positif et tel, que N' soit aussi positif et moindre que M' ; et faisant

$$n = \mu' m' + n',$$

on aura (en substituant ces valeurs dans l'équation $M'n - Nm' = \pm 1$)

$$M'n' - N'm' = \pm 1,$$

de sorte que n' sera nécessairement aussi positif.

Ensuite, si l'on fait

$$s' = \mu' x' + s,$$

on aura

$$y = M's' + N'x', \quad z = m's' + n'x';$$

et, substituant ces valeurs dans la formule

$$py^2 + 2qyz - rz^2,$$

on aura cette autre transformée

$$P's'^2 + 2Q's'x' - R'x'^2,$$

où

$$P' = pM'^2 + 2qM'm' - rm'^2,$$

$$Q' = pM'N' + q(M'n' + N'm') - rm'n',$$

$$R' = rn'^2 - qN'n' - pN^2.$$

Et l'on prouvera, comme on a fait plus haut, que les nombres P' et R' seront de mêmes signes.

On pourra trouver pareillement une troisième transformée telle que

$$P''s''^2 + 2Q''s''x'' - R''x''^2,$$

dans laquelle

$$x'' = \mu'' s' + x',$$

et où P'' et R' seront de mêmes signes, et ainsi de suite.

Maintenant, comme les nombres

$$M, N, M', N', \dots$$

forment une suite décroissante de nombres entiers, il est clair qu'on doit parvenir nécessairement à un terme qui soit nul. Supposons donc, par exemple, que l'on ait $N' = 0$, et à cause de

$$M'n' - N'm' = \pm 1,$$

on aura

$$M'n' = 1$$

(car, à cause que les nombres M' et n' sont tous deux positifs, il est évident qu'il faut prendre dans ce cas le signe supérieur), donc

$$M' = 1 \quad \text{et} \quad n' = 1;$$

de sorte qu'on aura dans ce cas

$$y = s', \quad z = m's' + x'.$$

D'où je conclus que, pour transformer la formule proposée

$$py^2 + 2qyz - rz^2$$

en celle-ci

$$Ps^2 + 2Qsx - Rx^2,$$

dans laquelle on ait

$$PR + Q^2 = pr + q^2 = a,$$

et où P et R soient de mêmes signes, il faut faire les substitutions suivantes

$$z = m'y + x', \quad y = \mu'x' + s, \quad x' = \mu s + x,$$

et prendre les nombres m' , μ' et μ positifs et tels, que dans les transformées résultantes

$$P'y'^2 + 2Q'y'x' - R'x'^2,$$

$$P''s'^2 + 2Q''s'x' - R'x'^2,$$

$$P''s'^2 + 2Q''s'x' - R'x'^2,$$

les coefficients R', P', R et P soient tous de mêmes signes.

Voyons donc comment on pourra remplir ces conditions.

En faisant d'abord la substitution de $m'y + x'$ à la place de z , on aura

la première transformée, où

$$\begin{aligned} R' &= r, \\ Q' &= q - r m', \\ P' &= p + 2q m' - r m'^2 = \frac{a - Q'^2}{R'}. \end{aligned}$$

Or

$$P' = -r \left(m' + \frac{\sqrt{a} - q}{r} \right) \left(m' - \frac{\sqrt{a} + q}{r} \right);$$

done, pour que P' et R' soient de mêmes signes, il faudra que les facteurs

$$m' + \frac{\sqrt{a} - q}{r}, \quad m' - \frac{\sqrt{a} + q}{r}$$

soient de signes différents; mais, à cause de $\sqrt{a} > q$, il est clair que $\sqrt{a} \pm q$ sera toujours un nombre positif; donc, si r est positif, $m' + \frac{\sqrt{a} - q}{r}$ sera toujours positif, et il faudra que $m' - \frac{\sqrt{a} + q}{r}$ soit négatif, et par conséquent que

$$m' < \frac{\sqrt{a} + q}{r};$$

si au contraire r est négatif, $m' - \frac{\sqrt{a} + q}{r}$ sera positif, et il faudra que $m' + \frac{\sqrt{a} - q}{r}$ soit négatif; donc

$$m' < \frac{\sqrt{a} - q}{-r}.$$

Substituons ensuite $\mu' x' + s$ à la place de y , et l'on aura la seconde transformée, dans laquelle

$$\begin{aligned} Q' &= Q'' + P' \mu', \\ R &= R' - 2Q' \mu' - P' \mu'^2 = \frac{a - Q''^2}{P'}. \end{aligned}$$

J'observe que

$$R = -P' \left(\mu' + \frac{\sqrt{a} + Q''}{P'} \right) \left(\mu' - \frac{\sqrt{a} - Q''}{P'} \right),$$

de sorte que pour que R et P' soient de mêmes signes il faut que les deux facteurs

$$\mu' + \frac{\sqrt{a} + Q''}{P'}, \quad \mu' - \frac{\sqrt{a} - Q''}{P'}$$

soient de signes différents; or comme

$$P' R' = a - Q'^2$$

(P' et R' étant de mêmes signes), il s'ensuit que Q'^2 sera plus petit que a , et par conséquent $Q' < \sqrt{a}$, de sorte que $\sqrt{a} \pm Q''$ sera toujours un nombre positif; donc, si P' est positif, $\mu' + \frac{\sqrt{a} + Q''}{P'}$ sera positif, et il faudra que $\mu' - \frac{\sqrt{a} - Q''}{P'}$ soit négatif; donc

$$\mu' < \frac{\sqrt{a} - Q''}{P'};$$

mais, μ' devant être un nombre entier, il faudra que $\frac{\sqrt{a} - Q''}{P'}$ soit plus grand que l'unité; donc $P' < \sqrt{a} - Q''$; donc, à cause de

$$P' R' = a - Q'^2 = (\sqrt{a} + Q'') (\sqrt{a} - Q''),$$

il faudra que R' soit plus grand que $\sqrt{a} + Q''$, c'est-à-dire

$$r > \sqrt{a} + q - r m',$$

et par conséquent

$$(m' + 1) r > \sqrt{a} + q,$$

et de là

$$m' > \frac{\sqrt{a} + q}{r} - 1.$$

Or P' doit être positif lorsque r est positif, auquel cas on a déjà trouvé $m' < \frac{\sqrt{a} + q}{r}$; donc on aura dans ce cas

$$m' < \frac{\sqrt{a} + q}{r}, \quad m' > \frac{\sqrt{a} + q}{r} - 1,$$

$$\mu' < \frac{\sqrt{a} - Q''}{P'}.$$

On trouvera de même, pour le cas de r négatif,

$$m' < \frac{\sqrt{a}-q}{-r}, \quad m' > \frac{\sqrt{a}-q}{-r} - 1,$$

$$\mu' < \frac{\sqrt{a}+Q'}{p'}.$$

D'où l'on voit que le nombre m' , devant être entier, sera nécessairement déterminé, puisque les deux limites entre lesquelles il doit se trouver ne diffèrent que de l'unité.

Enfin on substituera $\mu s + x$ à la place de x' , et l'on aura la troisième transformée dans laquelle

$$Q = Q' - R\mu,$$

$$R = P' + 2Q'\mu - R\mu^2 = \frac{a-Q'}{R}.$$

Et, en faisant attention que

$$P = -R \left(\mu + \frac{\sqrt{a}-Q'}{R} \right) \left(\mu - \frac{\sqrt{a}+Q'}{R} \right)$$

(à cause de $RP' = a - Q'^2$), on prouvera comme ci-dessus que, dans le cas de r positif, on aura

$$\mu' < \frac{\sqrt{a}-Q'}{p'}, \quad \mu' > \frac{\sqrt{a}-Q'}{p'} - 1,$$

$$\mu < \frac{\sqrt{a}+Q'}{R},$$

et dans le cas de r négatif

$$\mu' < \frac{\sqrt{a}+Q'}{p'}, \quad \mu' > \frac{\sqrt{a}+Q'}{p'} - 1,$$

$$\mu < \frac{\sqrt{a}-Q'}{R}.$$

De sorte que le nombre μ' sera aussi déterminé, et qu'il n'y aura d'indéterminé que le nombre μ .

Or, si l'on veut de plus que $2Q$ ne soit ni plus grand que P ni plus grand que R , comme les conditions du Problème l'exigent, il faudra d'abord déterminer μ en sorte que $Q = Q' - \mu R$ ne soit pas plus grand que $\frac{R}{2}$, abstraction faite des signes de Q et R ; et il est clair que prenant pour μ un nombre entier positif, il n'y aura qu'une seule valeur de μ qui puisse satisfaire à cette condition; de sorte que le nombre μ sera par ce moyen entièrement déterminé. Ainsi il ne restera plus qu'à voir si Q est aussi $< \frac{P}{2}$; auquel cas la transformée

$$Ps^2 + 2Qsx - Rx^2$$

aura les conditions requises.

On voit par là comment on peut résoudre la question proposée sans aucun tâtonnement, et voici la méthode qu'il faut suivre pour cet objet.

MÉTHODE POUR TRANSFORMER LA FORMULE $py^2 + 2qyz - rz^2$, DANS LAQUELLE ON A $pr + q^2 = a$ (a ÉTANT UN NOMBRE ENTIER POSITIF DONNÉ) ET OU $2q$ N'EST NI $> p$ NI $> r$ (ABSTRACTION FAITE DES SIGNES DE p, q, r), EN D'AUTRES FORMULES SEMBLABLES ET ASSUJETTES AUX MÊMES CONDITIONS.

24. Nous changerons d'abord, pour mieux conserver l'analogie dans nos formules, les lettres z et p en y' et r' ; de sorte que notre formule deviendra

$$r'y'^2 + 2qyy' - ry'^2,$$

où

$$rr' + q^2 = a \quad \text{et} \quad q \text{ non} > \frac{r}{2} \text{ ni} > \frac{r'}{2}.$$

Maintenant, comme r et r' doivent être de mêmes signes en vertu de l'équation $r'r' + q^2 = a$, nous les supposerons d'abord tous les deux positifs; mais q pourra être positif ou négatif, et devra même être pris successivement en *plus* et en *moins*.

Cela posé :

1° On fera

$$y' = m'y'' + y''',$$

ce qui donnera cette première transformée

$$r'y'^2 + 2q'y''y''' - r''y''^2,$$

où l'on aura

$$q' = q + r'm', \\ r'' = r - 2q'm' - r'm'^2 = \frac{a - q'^2}{r'}.$$

On prendra, s'il est possible, pour m' un nombre entier positif, tel que $q + r'm'$ ne soit pas $> \frac{r'}{2}$; ensuite on verra si r'' est $> q'$ ou non, et dans ce dernier cas la transformée trouvée aura les conditions requises.

2° On déterminera m' en sorte que

$$m' < \frac{\sqrt{a} - q}{r'}, \quad m' > \frac{\sqrt{a} - q}{r'} - 1.$$

Ensuite on fera

$$y' = m''y'' + y''',$$

ce qui donnera cette seconde transformée

$$r''y''^2 + 2q''y''y''' - r'''y'''^2,$$

en faisant

$$q'' = q' - r''m'', \\ r''' = r'' - 2q''m'' - r''m''^2 = \frac{a - q''^2}{r''}.$$

On prendra m'' entier positif et tel que $q' - r''m''$ ne soit pas $> \frac{r''}{2}$; et si en même temps q'' ne surpasse pas $\frac{r''}{2}$ la transformée précédente aura les conditions requises.

3° On déterminera m'' en sorte que

$$m'' < \frac{\sqrt{a} + q'}{r''}, \quad m'' > \frac{\sqrt{a} + q'}{r''} - 1.$$

Ensuite on fera

$$y'' = m'''y''' + y''',$$

et l'on aura cette troisième transformée

$$r'''y'''^2 + 2q'''y''y''' - r''''y'''^2,$$

dans laquelle

$$q''' = q'' + r'''m''', \\ r'''' = r''' - 2q'''m''' - r'''m'''^2 = \frac{a - q'''^2}{r'''},$$

On prendra pour m''' un nombre entier positif et tel que $q'' + r'''m'''$ ne soit pas $> \frac{r'''}{2}$, et si la valeur de q''' n'est pas en même temps $> \frac{r'''}{2}$, on sera assuré que la transformée trouvée aura les conditions requises.

4° On déterminera m''' en sorte que

$$m''' < \frac{\sqrt{a} - q''}{r'''}, \quad m''' > \frac{\sqrt{a} - q''}{r'''} - 1.$$

Ensuite on fera

$$y'' = m''''y''' + y''',$$

ce qui donnera la quatrième transformée

$$r''''y'''^2 + 2q''''y''y''' - r'''''y'''^2,$$

où

$$q'''' = q''' - r''''m''', \\ r''''' = r'''' - 2q''''m''' - r''''m'''^2 = \frac{a - q''''^2}{r''''}.$$

On prendra m'''' tel que $q''' - r''''m''''$ ne soit pas $> \frac{r''''}{2}$, et si q'''' n'est pas en même temps $> \frac{r''''}{2}$ la transformée aura les conditions requises.

5° On déterminera m'''' , ...

De cette manière on trouvera successivement toutes les transformées de la formule proposée, dans lesquelles les conditions prescrites pour

ront avoir lieu; et il est clair que le nombre des transformées différentes sera nécessairement limité; car nous avons vu dans le Problème II qu'il ne peut y avoir qu'un nombre limité de formules différentes où les mêmes conditions soient observées.

Mais, pour avoir toutes les différentes transformées possibles d'une même formule, il faudra faire un double calcul en prenant la valeur de q successivement en *plus* et en *moins*.

Si les nombres r et r' , au lieu d'être tous deux positifs, comme nous l'avons supposé, étaient tous deux négatifs, il n'y aurait qu'à changer les signes de ces nombres aussi bien que celui du nombre q , c'est-à-dire qu'on prendrait la formule

$$r'y^2 + 2qy'y' - ry'^2$$

négativement; et ensuite on changerait de même tous les signes des transformées qu'on aurait trouvées. Ou bien, ce qui est encore plus simple, on écrira $-r$ à la place de r' , $-r'$ à la place de r , et y' à la place de y , ce qui donnera la formule

$$-ry'^2 + 2qy'y' + r'y^2$$

où r et r' seront des nombres positifs.

25. COROLLAIRE. — Il suit de l'analyse du Problème précédent que les nombres $r, r', r'', r''', \dots$ seront tous de mêmes signes et tels que

$$a = rr' + q^2 = r'r'' + q'^2 = r''r''' + q''^2 = \dots;$$

ainsi chacun de ces nombres sera moindre que le nombre donné a , par conséquent en continuant la série $r, r', r'', \dots$ il faudra nécessairement que le même nombre revienne plusieurs fois, et même que la même couple de deux nombres successifs revienne aussi; donc, en continuant le calcul, suivant la méthode précédente, on retrouvera nécessairement une transformée identique avec quelqu'une de celles qu'on aura déjà eues; c'est ce qu'on reconnaîtra aisément lorsqu'on trouvera, par exemple,

$$q^{(p+2)} = q^{(p)}, \quad r^{(p+2+1)} = r^{(p+1)},$$

et que y sera un nombre pair; alors il sera inutile de pousser le calcul plus loin, parce que les transformées suivantes seraient les mêmes qu'on aurait déjà trouvées.

Donc, dès qu'on aura trouvé par le Problème II toutes les différentes formules

$$py^2 \pm 2qyz - rz^2$$

qui peuvent représenter les diviseurs des nombres de la forme

$$t^2 - au^2,$$

on pourra les réduire au plus petit nombre possible en excluant celles qui ne sont que des transformées de quelques-unes de ces formules. Ainsi, comme la formule $y^2 - az^2$ est toujours une de celles des diviseurs de $t^2 - au^2$ (en faisant $q = 0$ et $p = 1, r = a$), on commencera par chercher toutes les transformées de cette même formule, où les propriétés prescrites pourront avoir lieu, et comme ces transformées se trouveront nécessairement parmi les autres formules des diviseurs de $t^2 - au^2$ on pourra d'abord les rejeter comme étant identiques entre elles. Ensuite on fera la même opération sur les formules qui resteront; et après les avoir parcourues toutes, rejeté celles qui se trouveront identiques entre elles, on sera sûr que les restantes seront toutes différentes entre elles, et qu'elles seront en même temps toutes nécessaires pour représenter tous les diviseurs possibles des nombres de la forme donnée.

Au reste il arrivera le plus souvent que les transformées de la formule $y^2 - az^2$ renfermeront toutes les autres formules des diviseurs de $t^2 - au^2$, surtout lorsque a est un nombre premier; mais on aurait tort d'en faire une règle générale; car nous apporterons des Exemples où elle se trouverait en défaut: ce qui servira en même temps à montrer l'utilité et l'importance des méthodes que nous venons de donner.

EXEMPLES.

26. Soit proposée la formule

$$y^2 - 2z^2;$$

donc

$$r' = 1, \quad q = 0, \quad r = 2 = a;$$

ainsi l'on aura

$$q' = m', \quad r' = \frac{2 - q'^2}{1};$$

or il est clair qu'on ne peut rendre $q' < r' < 1$; ainsi l'on passera à une seconde transformée.

Pour cela, on prendra donc

$$m' < \frac{\sqrt{2}}{1}, \quad m' > \frac{\sqrt{2}}{1} - 1,$$

c'est-à-dire $m' = 1$, ce qui donnera

$$q' = 1, \quad r' = \frac{2 - 1}{1} = 1;$$

ensuite on aura

$$q'' = q' - r''m'' = 1 - m'', \quad r'' = \frac{2 - q''^2}{1};$$

or, pour que q' ne soit pas $> \frac{r''}{2} > \frac{1}{2}$, il faut prendre $m'' = 1$, ce qui donne

$$q'' = 0, \quad r'' = 2;$$

de sorte que, comme q'' est en même temps non $> \frac{r''}{2}$, on aura la transformée

$$r''y''^2 + 2q''y''y''' - r''y''^3,$$

c'est-à-dire

$$2y''^2 - y''^3,$$

qui aura les conditions requises; or cette transformée est semblable à la formule

$$2z^2 - y^2,$$

de sorte que les deux formules

$$y^2 - 2z^2 \quad \text{et} \quad 2z^2 - y^2,$$

que notre méthode générale donne pour les diviseurs des nombres de la forme $t^2 - 2u^2$, reviennent à la même, comme nous l'avons déjà remarqué (20, II).

On trouvera, de même, que les deux formules

$$y^2 - 5z^2 \quad \text{et} \quad 5z^2 - y^2$$

reviennent à la même, comme on l'a observé dans le numéro cité, V.

Considérons, pour donner un autre Exemple, le cas du n° 20, VII, où nous avons trouvé que les formules des diviseurs de

$$t^2 - 7u^2$$

étaient

$$y^2 - 7z^2, \quad 2y^2 \pm 2yz - 3z^2, \quad 7z^2 - y^2, \quad 3z^2 \pm 2yz - 2y^2.$$

1° Soit donc

$$r' = 1, \quad q' = 0, \quad r' = 7 = a;$$

on aura

$$q' = m', \quad r' = \frac{7 - q'^2}{1},$$

où l'on voit que q' ne saurait devenir $< \frac{r'}{2} < \frac{1}{2}$.

2° On prendra donc

$$m' < \frac{\sqrt{7}}{1}, \quad m' > \frac{\sqrt{7}}{1} - 1,$$

donc

$$m' = 2, \quad q' = 2, \quad r' = 3;$$

de là on aura donc

$$q'' = 2 - 3m'', \quad r'' = \frac{7 - q''^2}{3},$$

et pour que q'' ne soit pas $> \frac{r''}{2} > \frac{3}{2}$ il faudra faire $m'' = 1$, ce qui donnera

$$q'' = -1, \quad r'' = 2;$$

de sorte que, comme q'' est en même temps non $> \frac{r''}{2}$, la transformée

$$r''y''^2 + 2q''y''y''' - r''y''^3,$$

c'est-à-dire

$$2y''^2 - 2y''y''' - 3y''^3,$$

aura les conditions requises.

3° On prendra

$$m'' < \frac{\sqrt{7}+2}{3}, \quad m'' > \frac{\sqrt{7}+2}{3} - 1;$$

donc $m'' = 1$; d'où

$$q'' = -1, \quad r'' = 2;$$

ensuite de quoi on aura

$$q''' = -1 + 2m'', \quad r''' = \frac{7-q''}{2};$$

donc, pour que q''' ne soit pas $> \frac{r'''}{2}$, il faudra prendre $m'' = 1$, ce qui donnera

$$q'' = 1, \quad r'' = 3;$$

de là on aura la nouvelle transformée

$$2y^{r''} + 2y^{r''}y^{q''} - 3y^{q''},$$

qui aura aussi les conditions requises.

4° On fera

$$m''' < \frac{\sqrt{7}+1}{2}, \quad m''' > \frac{\sqrt{7}+1}{2} - 1;$$

donc $m''' = 1$, et de là

$$q''' = 1, \quad r''' = 3;$$

ensuite on aura

$$q^{iv} = 1 - 3m''', \quad r^{iv} = \frac{7-q'''}{3};$$

où l'on voit qu'on ne saurait prendre m''' en sorte que q^{iv} ne devienne pas $> \frac{r^{iv}}{2}$.

5° On fera

$$m^{iv} < \frac{\sqrt{7}+1}{3}, \quad m^{iv} > \frac{\sqrt{7}+1}{3} - 1,$$

donc $m^{iv} = 1$; et de là

$$q^{iv} = -2, \quad r^{iv} = 1;$$

ensuite on aura

$$q^v = -2 + m^v, \quad r^v = \frac{7-q^{iv}}{1};$$

donc, pour que q^v ne soit pas $> \frac{r^v}{2}$, on fera $m^v = 2$, ce qui donnera

$$q^v = 0, \quad r^v = 7;$$

de sorte qu'on aura la transformée

$$y^{r^v} - 7y^{q^v},$$

qui aura les conditions prescrites.

6° On fera

$$m^v < \frac{\sqrt{7}+2}{1}, \quad m^v > \frac{\sqrt{7}+2}{1} - 1;$$

donc $m^v = 4$, par conséquent

$$q^v = 2, \quad r^v = 3;$$

j'observe ici, sans aller plus loin, que ces valeurs de q^v et r^v sont les mêmes que celles de q' et r'' (2°, page 743); donc, puisque la différence des exposants de q est paire, il s'ensuit que les transformées qu'on pourrait trouver en continuant le calcul seraient les mêmes que celles qu'on a déjà trouvées ci-dessus (25).

Ainsi la formule $y^2 - 7y^{1/2}$ ne saurait fournir d'autres transformées qui aient les conditions prescrites que ces deux-ci

$$2y^{q''} - 2y^{q''}y^{q''} - 3y^{q''}, \quad 2y^{r''} + 2y^{r''}y^{q''} - 3y^{q''};$$

d'où l'on voit que les formules

$$y^2 - 7z^2, \quad 2y^2 \pm 2yz - 3z^2$$

reviennent à la même, comme aussi les formules

$$7z^2 - y^2, \quad 3z^2 \mp 2yz - 2y^2$$

qui ne sont que les négatives de celles-là; mais que les deux formules

$$y^2 - 7z^2, \quad 7z^2 - y^2$$

ne sauraient se réduire l'une à l'autre, comme cela a lieu dans les formules

$$y^2 - 5z^2, \quad 5z^2 - y^2$$

de l'Exemple précédent.

27. Pour développer davantage l'application de nos méthodes des Problèmes II et IV, nous allons chercher ici les formules des diviseurs des nombres de la forme

$$r^2 - 79u^2 \quad \text{ou} \quad 79u^2 - r^2.$$

On aura donc ici $a = 79$; donc il faudra que q ne soit pas $> \sqrt{\frac{79}{5}} > 3$, de sorte qu'on ne pourra faire que $q = 0, 1, 2, 3$. Faisant $q = 0$, on aura $pr = 79$, donc

$$p = 1, \quad r = 79;$$

faisant $q = 1$, on aura $pr = 78$, donc

$$p = 2, \quad r = 39, \quad \text{ou} \quad p = 3, \quad r = 26, \quad \text{ou} \quad p = 6, \quad r = 13;$$

faisant $q = 2$, on aura $pr = 75$, donc

$$p = 5, \quad r = 15;$$

enfin faisant $q = 3$, on aura $pr = 70$; donc

$$p = 7, \quad r = 10.$$

Ainsi l'on aura pour les diviseurs dont il s'agit les formules suivantes

$$\begin{aligned} y^2 - 79z^2, \quad 2y^2 \pm 2yz - 39z^2, \quad 3y^2 \pm 2yz - 26z^2, \\ 6y^2 \pm 2yz - 13z^2, \quad 5y^2 \pm 4yz - 15z^2, \quad 7y^2 \pm 6yz - 10z^2, \end{aligned}$$

et leurs inverses

$$\begin{aligned} 79z^2 - y^2, \quad 39z^2 \mp 2yz - 2y^2, \quad 26z^2 \mp 2yz - 3y^2, \\ 13z^2 \mp 2yz - 6y^2, \quad 15z^2 \mp 4yz - 5y^2, \quad 10z^2 \mp 6yz - 7y^2, \end{aligned}$$

ce qui fait en tout douze formules; mais il faut maintenant les trier, et en rejeter celles qui sont identiques entre elles.

Considérons d'abord la formule

$$y^2 - 79z^2 \quad \text{ou bien} \quad y^2 - 79y'^2.$$

1^o On aura

$$r' = 1, \quad q = 0, \quad r = 79 = a,$$

donc

$$q' = m', \quad r'' = \frac{79 - q'^2}{1};$$

or q' est toujours $> \frac{r'}{2}$, à moins qu'on ne fasse $m' = 0$, ce qui ne donnerait aucune nouvelle formule.

2^o Ainsi l'on fera

$$m' < \frac{\sqrt{79}}{1}, \quad m' > \frac{\sqrt{79}}{1} - 1,$$

donc $m' = 8$, par conséquent

$$q' = 8, \quad r'' = 15;$$

ensuite, on aura

$$q'' = 8 - 15m'', \quad r''' = \frac{79 - q''^2}{15},$$

où l'on fera $m'' = 1$ pour que q'' ne soit pas $> \frac{r''}{2}$; on aura donc

$$q'' = -7, \quad r''' = 2;$$

mais, comme q'' serait $> \frac{r''}{2}$, ces valeurs ne donnent point de transformation convenable.

3^o On fera donc

$$m'' < \frac{\sqrt{79} + 8}{15}, \quad m'' > \frac{\sqrt{79} + 8}{15} - 1;$$

donc $m'' = 1$, et de là

$$q''' = -7, \quad r'''' = 2;$$

ensuite on aura

$$q'' = -7 + 2m'', \quad r'' = \frac{79 - q''}{2};$$

qu'on prenne $m'' = 3$ ou $= 4$ pour avoir $q'' = \pm 1$, non $> \frac{r''}{2}$, et r'' deviendra égal à 39; de sorte qu'on aura cette transformée, qui aura toutes les conditions prescrites

$$2y^{112} \pm 2y^{11}y'' - 39y^{102}.$$

4° En poursuivant le calcul on fera

$$m'' < \frac{\sqrt{79} + 7}{2}, \quad m'' > \frac{\sqrt{79} + 7}{2} - 1,$$

c'est-à-dire $m'' = 7$; d'où

$$q'' = 7, \quad r'' = 15;$$

ensuite on fera

$$q^{11} = 7 - 15m^{11}, \quad r^{11} = \frac{79 - q^{11}}{15},$$

et l'on prendra $m^{11} = 1$ pour avoir q^{11} non $> \frac{r^{11}}{2}$; ainsi l'on aura

$$q^{11} = -8, \quad r^{11} = 1;$$

mais, comme q^{11} est plus grand que $\frac{r^{11}}{2}$, on rejettera ces valeurs comme inutiles.

5° On fera donc

$$m^{11} < \frac{\sqrt{79} + 7}{15}, \quad m^{11} > \frac{\sqrt{79} + 7}{15} - 1,$$

donc $m^{11} = 1$, par conséquent

$$q^{11} = -8, \quad r^{11} = 1;$$

après quoi on supposera

$$q'' = -8 + m'', \quad r'' = \frac{79 - q''}{1},$$

et l'on prendra $m'' = 8$ pour avoir

$$q'' = 0, \quad r'' = 79,$$

ce qui donnera la transformée

$$y^{112} - 79y^{11},$$

qui est entièrement semblable à la première formule

$$y^{12} - 79y^2.$$

6° Je fais

$$m' < \frac{\sqrt{79} + 8}{1}, \quad m' > \frac{\sqrt{79} + 8}{1} - 1,$$

savoir $m' = 16$, ce qui donne

$$q' = 8, \quad r' = 15;$$

or je remarque que ces valeurs de q' et r' sont les mêmes que celles de q' et r'' du 2°, page 747; de sorte que, comme la différence des exposants de q est paire, on retrouvera les mêmes transformées qu'on a déjà eues; d'où il s'ensuit que la formule

$$y^{112} - 79y^2$$

ne peut se changer en aucune autre qu'en celle-ci

$$2y^{112} \pm 2y^{11}y'' - 39y^{102},$$

et qu'ainsi parmi toutes les formules trouvées pour les diviseurs de $t^2 - 79u^2$ il n'y a que ces deux-ci

$$y^2 - 79z^2 \quad \text{et} \quad 2y^2 \pm 2yz - 39z^2$$

qui soient identiques entre elles, auxquelles on doit encore ajouter leurs inverses

$$79z^2 - y^2 \quad \text{et} \quad 39z^2 \mp 2yz - 2y^2,$$

qui seront aussi identiques entre elles.

Considérons maintenant la formule

$$3y^2 \pm 2yz - 26z^2,$$

savoir

$$3y^2 \pm 2yy' - 26y'^2.$$

1° On aura

$$r' = 3, \quad q = 1, \quad r = 26,$$

a étant toujours égal à 79; ainsi l'on supposera

$$q' = 1 + 3m', \quad r' = \frac{79 - q'^2}{3},$$

et comme on ne peut pas prendre m' tel que q' ne soit pas $> \frac{r'}{2}$, on passera à une autre transformée.

2° On fera donc

$$m' < \frac{\sqrt{79} - 1}{3}, \quad m' > \frac{\sqrt{79} - 1}{3} - 1;$$

donc $m' = 2$ et

$$q' = 7, \quad r' = 10;$$

ensuite on supposera

$$q'' = 7 - 10m'', \quad r'' = \frac{79 - q''^2}{10};$$

on prendra donc $m'' = 1$ pour avoir

$$q'' = -3 < \frac{10}{2},$$

et l'on aura

$$r'' = 7 > 2q'';$$

ainsi l'on aura la transformée

$$7y'^2 - 6y''y' - 10y''^2,$$

qui aura les conditions requises.

3° Soit

$$m'' < \frac{\sqrt{79} + 7}{10}, \quad m'' > \frac{\sqrt{79} + 7}{10} - 1;$$

donc $m'' = 1$ et

$$q'' = -3, \quad r'' = 7;$$

ensuite, soit supposé

$$q''' = -3 + 7m''', \quad r''' = \frac{79 - q'''^2}{7},$$

et comme on ne peut pas prendre m'' tel que q'' ne soit pas $> \frac{r''}{2}$, on passera à la transformée suivante.

4° On fera donc

$$m'' < \frac{\sqrt{79} + 3}{7}, \quad m'' > \frac{\sqrt{79} + 3}{7} - 1,$$

c'est-à-dire $m'' = 1$, et l'on aura

$$q'' = 4, \quad r'' = 9,$$

ensuite de quoi on supposera

$$q''' = 4 - 9m''', \quad r''' = \frac{79 - q'''^2}{9};$$

or on ne peut prendre m''' tel que q''' ne soit pas $> \frac{r'''}{2}$; donc, etc.

5° On fera

$$m''' < \frac{\sqrt{79} + 4}{9}, \quad m''' > \frac{\sqrt{79} + 4}{9} - 1,$$

c'est-à-dire $m''' = 1$; donc

$$q''' = -5, \quad r''' = 6;$$

après quoi on fera

$$q'''' = -5 + 6m''', \quad r'''' = \frac{79 - q'''^2}{6};$$

ici l'on peut prendre $m'''' = 1$, ce qui donne

$$q'''' = 1, \quad r'''' = 13;$$

valeurs qui ont les conditions requises; de sorte qu'on aura la transformée

$$6y''''^2 + 2y''''y''' - 13y'''^2,$$

6° Soit maintenant

$$m'''' < \frac{\sqrt{79} + 5}{6}, \quad m'''' > \frac{\sqrt{79} + 5}{6} - 1,$$

donc $m'''' = 2$ et

$$q'''' = 7, \quad r'''' = 5;$$

ensuite soit supposé

$$q^{vi} = 7 - 5m^{vi}, \quad r^{vi} = \frac{79 - q^{vi}}{5},$$

et il est clair qu'en prenant $m^{vi} = 1$ on aura $q^{vi} < \frac{r^{vi}}{2}$; on aura donc

$$q^{vi} = 2, \quad r^{vi} = 15;$$

de sorte que la transformée

$$15y^{vii} + 4y^{vi}y^{vi} - 5y^{vii}$$

aura les conditions requises.

7° Qu'on prenne

$$m^{vi} < \frac{\sqrt{79} + 7}{5}, \quad m^{vi} > \frac{\sqrt{79} + 7}{5} - 1,$$

donc $m^{vi} = 3$ et

$$q^{vi} = -8, \quad r^{vi} = 3;$$

ensuite on supposera

$$q^{vii} = -8 + 3m^{vii}, \quad r^{vii} = \frac{79 - q^{vii}}{3},$$

et prenant $m^{vii} = 3$, on aura

$$q^{vii} = 1 < \frac{r^{vii}}{2}, \quad r^{vii} = 26 > 2q^{vii};$$

ce qui donnera la transformée

$$3y^{viii} + 2y^{vii}y^{vii} - 26y^{viii},$$

qui est semblable à la proposée.

8° On fera donc encore

$$m^{vii} < \frac{\sqrt{79} + 8}{3}, \quad m^{vii} > \frac{\sqrt{79} + 8}{3} - 1;$$

c'est-à-dire $m^{vii} = 5$, et par conséquent

$$q^{vii} = 7, \quad r^{vii} = 10;$$

valeurs qui sont les mêmes que celles de q' et r' ; de sorte que les mêmes

transformées qu'on a déjà trouvées reviendraient si l'on continuait le calcul.

Reprenons maintenant les mêmes valeurs de r' et r du 1°, page 750, mais au lieu de supposer $q = 1$, qu'on fasse $q = -1$; donc

$$q' = -1 + 3m', \quad r' = \frac{79 - q'}{3};$$

or, comme on ne saurait déterminer m' en sorte que q' devienne $< \frac{r'}{2}$, il faudra passer immédiatement à une autre transformée.

2° On fera donc

$$m' < \frac{\sqrt{79} + 1}{3}, \quad m' > \frac{\sqrt{79} + 1}{3} - 1,$$

donc $m' = 3$ et

$$q' = 8, \quad r' = 5;$$

ensuite on supposera

$$q'' = 8 - 5m'', \quad r'' = \frac{79 - q''}{5},$$

et il est clair que prenant $m'' = 2$, q'' ne sera pas $> \frac{r''}{2}$; ainsi l'on aura

$$q'' = -2, \quad r'' = 15;$$

de sorte qu'il en résultera la transformée

$$15y^{vi} - 4y''y'' - 5y^{vi},$$

qui a, comme on voit, les conditions requises.

3° On fera

$$m'' < \frac{\sqrt{79} + 8}{5}, \quad m'' > \frac{\sqrt{79} + 8}{5} - 1,$$

c'est-à-dire $m'' = 3$, d'où

$$q'' = -7, \quad r'' = 6;$$

ensuite on supposera

$$q''' = -7 + 6m''', \quad r''' = \frac{79 - q'''}{6};$$

et l'on prendra $m'' = 1$ pour avoir

$$q'' = -1, \quad r'' = 13,$$

ce qui donnera la transformée

$$6y^{''''} - 2y^{'''}y'' - 13y^{''},$$

qui a les conditions requises.

4° Soit

$$m'' < \frac{\sqrt{79} + 7}{6}, \quad m'' > \frac{\sqrt{79} + 7}{6} - 1;$$

donc $m'' = 2$ et

$$q'' = 5, \quad r'' = 9;$$

ensuite on supposera

$$q''' = 5 - 9m''', \quad r''' = \frac{79 - q'''}{7};$$

et l'on pourra prendre $m''' = 1$, ce qui donnera

$$q''' = -4 < \frac{r'''}{2};$$

mais alors on aura

$$r''' = 7 < 2q''',$$

de sorte que ces valeurs ne sont pas convenables.

5° Soit donc

$$m''' < \frac{\sqrt{79} + 5}{9}, \quad m''' > \frac{\sqrt{79} + 5}{9} - 1,$$

donc $m''' = 1$ et

$$q''' = -4, \quad r''' = 7;$$

ensuite on fera

$$q^{(4)} = -4 + 7m^{(4)}, \quad r^{(4)} = \frac{79 - q^{(4)}}{7}$$

et l'on pourra prendre $m^{(4)} = 1$, ce qui donnera

$$q^{(4)} = 3 < \frac{r^{(4)}}{2}, \quad r^{(4)} = 10 > 2q^{(4)};$$

de sorte qu'on aura cette transformée

$$7y^{(4)} + 6y^{(3)}y'' - 10y^{(2)}.$$

6° Soit

$$m'' < \frac{\sqrt{79} + 4}{7}, \quad m'' > \frac{\sqrt{79} + 4}{7} - 1;$$

donc $m'' = 1$ et

$$q'' = 3, \quad r'' = 10;$$

qu'on fasse ensuite

$$q''' = 3 - 10m''', \quad r''' = \frac{79 - q'''}{10},$$

et, comme on ne peut pas prendre m''' en sorte que q''' devienne non $> \frac{r'''}{2}$, on passera d'abord à la transformée suivante.

7° Soit donc

$$m''' < \frac{\sqrt{79} + 3}{10}, \quad m''' > \frac{\sqrt{79} + 3}{10} - 1,$$

donc $m''' = 1$ et

$$q''' = -7, \quad r''' = 3;$$

qu'on fasse ensuite

$$q^{(4)} = -7 + 3m^{(4)}, \quad r^{(4)} = \frac{79 - q^{(4)}}{3},$$

et prenant $m^{(4)} = 2$ on aura

$$q^{(4)} = -1 < \frac{r^{(4)}}{2}, \quad r^{(4)} = 26 > 2q^{(4)};$$

donc on aura la transformée

$$3y^{(4)} - 2y^{(3)}y'' - 26y^{(2)},$$

qui est analogue à la proposée.

8° Soit encore

$$m^{(4)} < \frac{\sqrt{79} + 7}{3}, \quad m^{(4)} > \frac{\sqrt{79} + 7}{3} - 1,$$

donc $m^{(4)} = 5$ et

$$q^{(4)} = 8, \quad r^{(4)} = 5,$$

valeurs qui sont les mêmes que celles de q' et r'' du 2°, page 753; ainsi l'opération sera terminée.

On voit donc que la formule $3y^2 \pm 2yy' - 26y'^2$ n'a pu fournir que ces transformées

$$7y'^2 - 6y''y' - 10y''^2, \quad 6y'^2 + 2y''y' - 13y''^2, \quad 15y'^2 + 4y''y' - 5y''^2, \\ 15y'^2 - 4y''y' - 5y''^2, \quad 6y'^2 - 2y''y' - 13y''^2, \quad 7y'^2 + 6y''y' - 10y''^2;$$

d'où et de ce qui a déjà été trouvé ci-dessus, je conclus que les douze formules que nous avons données pour les diviseurs des nombres de la forme $t^2 - 79u^2$ peuvent se réduire à ces quatre-ci

$$y^2 - 79z^2, \quad 79z^2 - y^2, \quad 3y^2 \pm 2yz - 26z^2, \quad 26z^2 \mp 2yz - 3y^2,$$

lesquelles doivent être regardées comme essentiellement différentes l'une de l'autre, en sorte qu'elles n'admettent plus aucune réduction.

28. D'après ces principes on pourra construire deux Tables pour les formes des diviseurs impairs des nombres $t^2 + au^2$ et $t^2 - au^2$ en supposant successivement $a = 1, 2, 3, \dots$

Voici ces Tables poussées jusqu'à $a = 31$; il serait bon de les continuer au moins jusqu'à 100; mais nous nous contentons ici de mettre sur la voie ceux qui voudront dans la suite se charger de ce travail.

On remarquera, à l'égard de la seconde Table, que les signes ambigus $\pm$ qu'on y trouve dénotent que les valeurs de p et de r qui en sont affectées peuvent être prises également avec les signes supérieurs ou avec les inférieurs; ainsi, puisque à $a = 2$ répond $p = \pm 1, q = 0, r = \pm 2$, il s'ensuit que tout diviseur impair de $t^2 - 2u^2$ sera en même temps de la forme $y^2 - 2z^2$ et $2z^2 - y^2$, et ainsi des autres; de sorte que, dans ce cas, on sera libre de prendre les signes supérieurs ou les inférieurs.

On doit remarquer encore que l'on a omis, pour plus de simplicité, toutes les valeurs de a qui seraient égales à des carrés ou divisibles par des carrés; c'est pourquoi dans la colonne des valeurs de a on ne trouve ni le nombre 4, ni le nombre 8, ni, etc.; en effet il est visible que la formule $t^2 + 4u^2$ est comprise sous celle-ci $t^2 + u^2$ où $a = 1$. On voit de même que la formule $t^2 + 8u^2$ est réductible à celle-ci $t^2 + 2u^2$ où $a = 2$, et ainsi des autres.

TABLE I.

Formule des nombres proposés $t^2 + au^2$,

Formule de leurs diviseurs impairs... $py^2 \pm 2qyz + rz^2$, où $pr - q^2 = a$.

VALEURS DE a	VALEURS CORRESPONDANTES DE		
	p	q	r
1	1	0	1
2	1	0	2
3	1	0	3
5	1, 2	0, 1	5, 3
6	1, 2	0, 0	6, 3
7	1	0	7
10	1, 2	0, 0	10, 5
11	1, 3	0, 1	11, 4
13	1, 2	0, 1	13, 7
14	1, 2, 3	0, 0, 1	14, 7, 5
15	1, 3	0, 0	15, 5
17	1, 2, 3	0, 1, 1	17, 9, 6
19	1, 4	0, 1	19, 5
21	1, 3, 2, 5	0, 0, 1, 2	21, 7, 11, 5
22	1, 2	0, 0	22, 11
23	1, 3	0, 1	23, 8
26	1, 2, 3, 5	0, 0, 1, 2	26, 13, 9, 6
29	1, 2, 3, 5	0, 1, 1, 1	29, 15, 10, 6
30	1, 2, 3, 5	0, 0, 0, 0	30, 15, 10, 6
31	1, 5	0, 2	31, 7

TABLE II.

Formule des nombres proposés $t^2 - au^2$,Formule de leurs diviseurs impairs... $py^2 \pm 2qyz - rz^2$, où $pr + q^2 = a$.

VALEURS DE a	VALEURS CORRESPONDANTES DE		
	p	q	r
1	1	0	1
2	± 1	0	± 2
3	1, -1	0	3, -3
5	± 1	0	± 5
6	1, -1	0	6, -6
7	1, -1	0	7, -7
10	$\pm 1, \pm 2$	0	$\pm 10, \pm 5$
11	1, -1	0	11, -11
13	± 1	0	± 13
14	1, -1	0	14, -14
15	1, -1, 3, -3	0	15, -15, 5, -5
17	± 1	0	± 17
19	1, -1	0	19, -19
21	1, -1	0	21, -21
22	1, -1	0	22, -22
23	1, -1	0	23, -23
26	$\pm 1, \pm 2$	0	$\pm 26, \pm 13$
29	± 1	0	± 29
30	1, -1, 2, -2	0	30, -30, 15, -15
31	1, -1	0	31, -31

SECONDE PARTIE.

J'ai donné, dans les Recherches précédentes, des méthodes directes et générales pour trouver toutes les formes dont sont susceptibles les diviseurs premiers des nombres de la forme

$$t^2 \pm au^2,$$

a étant un nombre entier donné, et t, u des nombres quelconques entiers et premiers entre eux; et j'ai prouvé que ces diviseurs sont toujours réductibles à la forme

$$py^2 \pm 2qyz \pm rz^2,$$

dans laquelle y et z sont des nombres entiers indéterminés, et où p, q, r sont des nombres entiers dépendants du nombre a , en sorte qu'ils ne peuvent avoir qu'un nombre fini de valeurs différentes, lesquelles sont faciles à trouver par les règles que j'ai données pour cet objet, et que j'ai déjà appliquées à toutes les valeurs non carrées de a depuis 1 jusqu'à 31.

Je me propose maintenant de donner les moyens de ramener la même formule

$$py^2 \pm 2qyz \pm rz^2$$

à cette autre beaucoup plus simple

$$4an + b,$$

n étant un nombre entier quelconque, et b un nombre donné dépendant des nombres p, q, r ; je donnerai ensuite des Tables pour toutes les valeurs de b répondantes aux valeurs non carrées de a depuis 1 jusqu'à 30, et je montrerai l'usage de ces Tables pour trouver facilement tous les diviseurs d'un nombre quelconque proposé; je traiterai enfin des nombres premiers de la forme $4an + b$ qui sont en même temps de la forme $u^2 \pm at^2$; j'établirai les principes généraux de la théorie de ces nombres, et j'en déduirai un grand nombre de Théorèmes, dont quelques-uns sont déjà connus, mais dont la plupart sont entièrement nouveaux.

Au reste, comme ce Mémoire n'est, à proprement parler, qu'une suite de celui qui est imprimé dans le volume de 1773, j'y conserverai, pour la commodité des citations, l'ordre des numéros et des Propositions.

DE LA MANIÈRE DE RAMENER LES DIVISEURS DES NOMBRES DE LA FORME $u^2 \pm a^2$
A LA FORME $4an + b$.

Comme nous avons déjà démontré que les diviseurs des nombres de la forme

$$u^2 \pm a^2$$

sont nécessairement de la forme

$$py^2 \pm 2qyz \pm rz^2,$$

il est clair qu'il ne s'agit plus que de ramener cette formule à celle-ci

$$4an + b;$$

c'est à quoi sont destinés les deux Problèmes suivants.

PROBLÈME V.

29. Étant donnée l'expression

$$py^2 \pm rz^2,$$

où p et r sont des nombres entiers donnés, et y , z des nombres entiers indéterminés, on propose de la réduire à la forme

$$4an + b,$$

a étant égal à pr , b étant un nombre positif ou négatif, égal ou moindre que $2a$, et n un nombre entier indéterminé.

Il est clair que, quels que soient les nombres y et z , on peut toujours les représenter par les formules $2mr \pm \rho$ et $2m'p \pm \varpi$, m , m' , ρ et ϖ étant des nombres entiers indéterminés; il est visible de plus qu'on pourra toujours prendre les nombres m , m' avec les signes des nombres ρ et ϖ , en sorte que ces derniers soient l'un, savoir ρ , moindre ou au moins non plus grand que r , et l'autre, savoir ϖ , non plus grand que p .

Qu'on substitue donc ces valeurs dans l'expression $py^2 \pm rz^2$, elle

deviendra, à cause de $pr = a$,

$$4a[m^2r \pm m\rho \pm (m'^2p \pm m'\varpi)] + p\rho^2 \pm r\varpi^2;$$

d'où l'on voit que la réduction proposée aura lieu en faisant

$$b = p\rho^2 \pm r\varpi^2,$$

et prenant successivement pour ϖ tous les nombres entiers jusqu'à p , et pour ρ tous les nombres entiers jusqu'à r ; et il est clair que les valeurs de b qu'on trouvera de cette manière pourront être augmentées ou diminuées de tels multiples de $4a$ qu'on voudra; moyennant quoi on pourra toujours réduire ces valeurs à être au-dessous, ou au moins à n'être pas plus grandes que $2a$; pour cela il n'y aura qu'à diviser d'abord b par $4a$, et si le reste est égal ou moindre que $2a$, on le prendra pour la vraie valeur de b ; mais si ce reste est plus grand que $2a$, on en retranchera $4a$, et l'on aura un reste qui sera nécessairement moindre que $2a$, et qu'on prendra à la place de b .

30. COROLLAIRE. — Il est clair que si l'on change en même temps les signes des nombres p et r , la valeur b devra aussi changer de signe; par conséquent, si $4an + b$ est la forme des nombres $py^2 - rz^2$, on aura sur-le-champ $4an - b$ pour celle des nombres $rz^2 - py^2$, les valeurs de b étant les mêmes.

31. REMARQUE. — Si l'on ne veut considérer que les nombres impairs qui peuvent être représentés par la formule $py^2 \pm rz^2$, lorsque p et r ne sont pas pairs à la fois, il faudra dans ce cas rejeter toutes les valeurs paires de b , et ne prendre par conséquent à la fois pour ϖ et ρ que des nombres qui rendent l'une des quantités $p\rho^2$, $r\varpi^2$, paire et l'autre impaire.

Si l'on voulait de plus ne considérer que les nombres qui seraient premiers à $a = pr$, il faudrait encore rejeter toutes les valeurs de b qui ne seraient pas premières à p ou à r ; et il est visible qu'il ne faudrait prendre alors pour ϖ que des nombres moindres que p et premiers à p , et pour ρ que nombres moindres que r et premiers à r .

PROBLÈME VI.

32. Étant donnée l'expression

$$py^2 + 2qyz \pm rz^2,$$

où p, q, r sont des nombres entiers donnés dont le premier ou le dernier est supposé impair, et y, z des nombres entiers indéterminés; on propose de la ramener à la forme

$$4an + b,$$

en supposant $a = pr \mp q^2$, b un nombre entier positif ou négatif qui ne soit pas plus grand que $2a$, et n un nombre entier indéterminé.

Supposons d'abord que p soit un nombre impair, et faisant l'expression proposée égale à X , en sorte que l'on ait

$$py^2 + 2qyz \pm rz^2 = X,$$

qu'on multiplie cette équation par p , elle deviendra

$$pX = (py + qz)^2 \pm az^2,$$

à cause de $a = pr \mp q^2$ (hypothèse), ou bien en faisant $py + qz = y'$,

$$pX = y'^2 \pm az^2.$$

Maintenant supposons, en général, que la plus grande commune mesure de a et p soit $p'c^2$, p' étant un nombre non carré ni divisible par aucun carré; et faisant

$$p = Pp'c^2, \quad a = r'p'c^2,$$

il est clair que P et r' seront premiers entre eux, et que l'équation

$$a = pr \mp q^2,$$

devenant

$$r'p'c^2 = P r p'c^2 \mp q^2,$$

ne pourra subsister en nombres entiers à moins que q ne soit divisible par $p'c$; ainsi l'on aura

$$q = q'p'c,$$

et divisant toute l'équation par $p'c^2$, il viendra

$$r' = P r \mp q'^2 p',$$

où je remarque que P sera nécessairement premier à p' ; car si ces deux nombres avaient une commune mesure autre que l'unité, il faudrait que le nombre r' fût aussi divisible par cette commune mesure; ainsi P et r' ne seraient plus premiers entre eux contre l'hypothèse. Donc P sera en même temps premier à p' et à r' , et par conséquent aussi à $p'r'$.

Cela posé, puisque p et q sont divisibles à la fois par $p'c$, il est clair que y' le sera aussi, de sorte qu'on aura

$$y' = p'cx,$$

et l'équation

$$pX = y'^2 \pm az^2,$$

étant toute divisée par $p'c^2$, deviendra

$$PX = p'x^2 \pm r'z^2.$$

Or faisant $p'r' = a'$, on pourra réduire, par le Problème précédent, l'expression $p'x^2 \pm r'z^2$ à la forme $4a'n + b'$, où n sera un nombre entier indéterminé, et b' aura des valeurs connues. Qu'on mette Y à la place de n , et l'on aura l'équation

$$PX = 4a'Y + b',$$

laquelle devra avoir lieu en prenant pour X et Y des nombres entiers, et qu'on pourra, par conséquent, résoudre par les méthodes connues. Voyez les *Mémoires* de cette Académie pour l'année 1768 (*).

Or, comme on suppose que p est impair, il est clair que P , qui est un facteur de p , sera aussi impair; par conséquent P et $4a'$ seront premiers entre eux, puisqu'on a déjà prouvé que P est premier à $a' = p'r'$; ainsi l'équation proposée sera toujours résoluble, quelques valeurs qu'on donne à b' .

Qu'on divise $4a'$ par P , puis P par le premier reste, puis le premier

(*) *Oeuvres de Lagrange*, t. II, p. 659.

reste par le second reste et ainsi de suite, jusqu'à ce que la division se fasse exactement, et nommant $l, l', l'', \dots$ les quotients provenant de ces divisions, on en formera les fractions convergentes

$$\frac{1}{0}, \frac{l}{1}, \frac{l'}{1}, \frac{l''+1}{l'}, \frac{(l''+1)l'+l}{l'l'+1}, \dots, \frac{L}{A}, \frac{L'}{A'}, \frac{L'l^{(s)}+L}{A'l^{(s)}+A}, \dots,$$

dont la dernière sera la fraction même $\frac{4a'}{p}$, et l'avant-dernière, que nous désignerons par $\frac{\alpha}{\beta}$, sera telle que $\alpha p - 4\beta a' = \pm 1$, le signe supérieur étant pour le cas où le quantième de la fraction $\frac{\alpha}{\beta}$ est impair, et l'inférieur pour celui où ce quantième est pair.

Cela fait, on aura, en général,

$$X = 4a'n' \pm \alpha b',$$

n' étant un nombre quelconque entier.

Telle sera donc la forme de l'expression proposée X ; d'où l'on voit que le Problème serait résolu si a' était égal à a ; ce qui a lieu lorsque $c = 1$, c'est-à-dire lorsque la plus grande commune mesure entre p et a n'est divisible par aucun carré. Dans ce cas il n'y aura donc qu'à prendre $b = \pm \alpha b'$, en ajoutant ou retranchant de cette valeur, s'il est nécessaire, un multiple de $4a$ tel, que la valeur résultante de b ne surpasse pas $2a$, comme on l'a dit dans le Problème précédent.

Mais, si c n'est pas égal à 1, alors, pour réduire la valeur de X à la forme

$$4an + b \quad \text{ou} \quad 4a'c'n + b$$

(a étant égal à $a'c^2$), on remarquera que, quel que soit le nombre entier n' , on pourra toujours le représenter par $c^2n + \gamma$, en prenant $\gamma < c^2$; ainsi, substituant cette valeur dans l'expression de X , on aura

$$X = 4an \pm \alpha b' + 4a'\gamma.$$

C'est pourquoi il n'y aura qu'à prendre

$$b = \pm \alpha b' + 4a'\gamma,$$

en donnant successivement à γ les valeurs 0, 1, 2, ... jusqu'à $c^2 - 1$.

Si les nombres p et a sont premiers entre eux, la solution sera plus simple, car on aura non-seulement $c = 1$, mais aussi $p' = 1$, et de là $r' = a$.

Nous avons supposé jusqu'ici que p était impair; mais si p était pair et r impair, il n'y aurait alors qu'à prendre la valeur de r à la place de celle de p , et si dans la formule

$$py^2 + 2qyz \pm rz^2$$

le signe supérieur a lieu, il n'y aura aucun changement à faire aux valeurs de b trouvées d'après cette valeur; mais si c'est le signe inférieur qui a lieu, il n'y aura qu'à prendre les valeurs de b avec des signes contraires; ce qui est évident par la nature même de la formule dont il s'agit.

A l'égard du cas où p et r seraient pairs à la fois, nous pouvons en faire abstraction, puisque dans ce cas l'expression

$$py^2 + 2qyz \pm rz^2$$

ne donnerait que des nombres pairs.

33. Par l'application des méthodes précédentes on pourra donc construire deux nouvelles Tables correspondantes à celles du n° 28, et qui donnent pour chaque valeur de a et de p les valeurs convenables de b , en sorte qu'étant proposé un nombre de la forme $t^2 + au^2$ ou $t^2 - au^2$, on ait sur-le-champ toutes les formes particulières de l'espèce $4an + b$ dont les diviseurs de ce nombre sont susceptibles.

La Table III, qui suit, répond, comme on voit, à la Table I, et la Table IV à la Table II; on y a omis, pour plus de simplicité, les valeurs paires de b , ainsi que celles qui ne seraient pas premières à $4a$; de sorte que ces Tables ne donnent que les formules des diviseurs impairs et premiers à a . Lorsque deux valeurs différentes de p ont donné les mêmes valeurs de b , on a réuni ces valeurs de p dans une même case.

TABLE III.

Formule des nombres proposés..... $t^2 + au^2$.
 Formule de leurs diviseurs impairs, et premiers à a ... $py^2 \pm 2qyz + rz^2 = 4an + b$.

VALEURS DE a	p	VALEURS CORRESPONDANTES DE b
1	1	1
2	1	1, 3
3	1	1, -5
5	1	1, 9
6	2	3, 7
7	1	1, 7
10	2	5, 11
11	1	1, 9, 11, -3, -5, -13
13	1	1, 9, 11, 19
14	2	7, 13, -3, -17
15	1, 3	1, 3, 5, 9, 15, -7, -13, -17, -19, -21
17	1	1, 9, 17, 25, -3, -23
19	2	7, 11, 15, 19, -5, -21
21	1, 2	1, 9, 15, 23, 25, -17
22	3	3, 5, 13, 19, 27, -11
23	1	1, 19, -11, -29
25	3	17, 23, -7, -13
26	1, 2	1, 9, 13, 21, 25, 33, -15, -19
29	3	3, 7, 11, 23, 27, 31, -5, -29
30	1, 4	1, 5, 7, 9, 11, 17, 23, 25, 35, -3, -13, -15, -21, -27, -29, -31, -33, -37
31	1	1, 25, 37
32	2	11, 23, -13
33	3	19, 31, -29
34	5	5, 17, 41
35	1	1, 9, 15, 23, 25, 31, -7, -17, -39, -41
36	2	13, 19, 21, 29, 35, 43, -3, -5, -27, -37
37	1, 3	1, 3, 9, 13, 25, 27, 29, 31, 35, 39, 41, -5, -7, -11, -15, -17, -19, -21, -33, -37, -43, -45
38	1, 3	1, 3, 9, 17, 25, 27, 35, 43, 49, 51, -23, -29
39	2, 5	5, 7, 15, 21, 31, 37, 45, 47, -11, -19, -33, -41
40	1, 5	1, 5, 9, 13, 25, 33, 45, 49, 53, 57, -7, -23, -35, -51
41	2, 3	3, 11, 15, 19, 27, 31, 39, 43, 47, 55, -17, -21, -37, -41
42	1	1, 31, 49, -41
43	2	17, 23, 47, -7
44	3	13, 37, 43, -53
45	5	11, 29, 59, -19

TABLE IV.

Formule des nombres proposés..... $t^2 - au^2$.
 Formule de leurs diviseurs impairs, et premiers à a ... $py^2 \pm 2qyz - rz^2 = 4an + b$.

VALEURS DE a	p	VALEURS CORRESPONDANTES DE b
1	1	± 1
2	± 1	± 1
3	1	1
5	± 1	$\pm 1, \pm 9$
6	1	1, -5
7	± 1	-1, 5
10	1	1, 9, -3
11	± 1	-1, -9, 3
13	± 2	$\pm 1, \pm 9$
14	± 1	$\pm 3, \pm 13$
15	1	1, 5, 9, -7, -19
17	± 1	-1, -5, -9, 7, 19
19	± 1	$\pm 1, \pm 3, \pm 9, \pm 17, \pm 23, \pm 25$
21	1	1, 9, 11, 25, -5, -13
22	± 1	-1, -9, -11, -25, 5, 13
23	1	1, -11
25	± 1	-1, 11
26	3	7, -17
27	± 1	-7, 17
29	± 1	$\pm 1, \pm 9, \pm 13, \pm 15, \pm 19, \pm 21, \pm 25, \pm 33$
31	1	1, 5, 9, 17, 25, -3, -15, -27, -31
32	± 1	-1, -5, -9, -17, -25, 3, 15, 27, 31
33	1	1, 25, 37, -5, -17, -41
34	± 1	-1, -25, -37, 5, 17, 41
35	1	1, 3, 9, 25, 27, -7, -13, -21, -29, -39
36	± 1	-1, -3, -9, -25, -27, 7, 13, 21, 29, 39
37	1	1, 9, 13, 25, 29, 41, -7, -11, -15, -19, -43
38	± 1	-1, -9, -13, -25, -29, -41, 7, 11, 15, 19, 43
39	± 1	$\pm 1, \pm 9, \pm 17, \pm 23, \pm 25, \pm 49$
40	± 2	$\pm 5, \pm 11, \pm 19, \pm 21, \pm 37, \pm 45$
41	± 1	$\pm 1, \pm 5, \pm 7, \pm 9, \pm 13, \pm 23, \pm 25, \pm 33, \pm 35, \pm 45, \pm 49, \pm 51, \pm 53, \pm 57$
42	1	1, 19, 49, -29
43	± 1	-1, -19, -49, 29
44	2	17, -7, -13, -37
45	± 2	-17, 7, 13, 37

34. On voit, par les deux Tables précédentes, que les valeurs de b ne renferment pas tous les nombres moindres que $2a$ et premiers à $2a$, mais seulement une partie d'entre eux; de sorte qu'il y en a toujours une partie d'exclue.

Ces nombres exclus, c'est-à-dire qui ne se trouvent point parmi les valeurs de b , donneront donc les formes des nombres qui ne peuvent jamais être diviseurs de $t^2 \pm au^2$, et que nous appellerons simplement *non-diviseurs*.

Ainsi l'on pourra construire encore deux autres Tables qui donneront les formes des non-diviseurs de $t^2 \pm au^2$ pour chaque valeur de a , en prenant pour b tous les nombres positifs ou négatifs moindres que $2a$, et premiers à $2a$, lesquels ne se trouveront pas parmi les valeurs de b contenues dans les deux Tables précédentes: c'est d'après ce principe qu'on a formé les Tables V et VI qui suivent.

TABLE V.

Formule des nombres proposés $t^2 + au^2$.Formule des non-diviseurs $4an + b$.

VALEURS DE a	VALEURS CORRESPONDANTES DE b
1	-1
2	-1, -3
3	5, -1
5	-1, -3, -7, -9
6	-1, -5, -7, -11
7	3, 5, 13, -1, -9, -11
10	3, 17, -1, -7, -9, -11, -13, -19
11	7, 13, 17, 19, 21, -1, -3, -5, -9, -15
13	3, 5, 21, 23, -1, -7, -9, -11, -15, -17, -19, -25
14	11, 17, -1, -3, -5, -9, -13, -15, -19, -23, -25, -27
15	7, 11, 13, 29, -1, -17, -19, -23
17	5, 15, 19, 29, -1, -3, -7, -9, -11, -13, -21, -23, -25, -27, -31, -33
19	3, 13, 15, 21, 27, 29, 31, 33, 37, -1, -5, -7, -9, -11, -17, -23, -25, -35
21	13, 29, -1, -5, -11, -17, -19, -23, -25, -31, -37, -41
22	3, 5, 7, 17, 27, 37, 39, 41, -1, -9, -13, -15, -19, -21, -23, -25, -29, -31, -35, -43
23	5, 7, 11, 15, 17, 19, 21, 33, 37, 43, 45, -1, -3, -9, -13, -25, -27, -29, -31, -35, -39, -41
26	11, 19, 23, 29, 33, 41, -1, -3, -5, -7, -9, -15, -17, -21, -25, -27, -31, -35, -37, -43, -45, -47, -49
29	7, 17, 21, 23, 35, 37, 41, 51, -1, -3, -5, -9, -11, -13, -15, -19, -25, -27, -31, -33, -39, -43, -45, -47, -49, -53, -55, -57
30	7, 19, 41, 53, -1, -11, -13, -17, -23, -29, -31, -37, -43, -47, -49, -59

TABLE VI.

Formule des nombres proposés $t^2 - au^2$.Formule des non-diviseurs $4an + b$.

VALEURS DE a	VALEURS CORRESPONDANTES DE b
1	
2	± 3
3	± 5
5	$\pm 3, \pm 7$
6	$\pm 7, \pm 11$
7	$\pm 5, \pm 11, \pm 13$
10	$\pm 7, \pm 11, \pm 17, \pm 19$
11	$\pm 3, \pm 13, \pm 15, \pm 17, \pm 21$
13	$\pm 5, \pm 7, \pm 11, \pm 15, \pm 19, \pm 21$
14	$\pm 3, \pm 15, \pm 17, \pm 19, \pm 23, \pm 27$
15	$\pm 13, \pm 19, \pm 23, \pm 29$
17	$\pm 3, \pm 5, \pm 11, \pm 23, \pm 27, \pm 29, \pm 31$
19	$\pm 7, \pm 11, \pm 13, \pm 21, \pm 23, \pm 29, \pm 33, \pm 35, \pm 37$
21	$\pm 11, \pm 13, \pm 19, \pm 23, \pm 29, \pm 31$
22	$\pm 5, \pm 15, \pm 17, \pm 19, \pm 23, \pm 31, \pm 35, \pm 37, \pm 41, \pm 43$
23	$\pm 3, \pm 5, \pm 17, \pm 21, \pm 27, \pm 31, \pm 33, \pm 35, \pm 37, \pm 39, \pm 45$
26	$\pm 3, \pm 7, \pm 15, \pm 27, \pm 29, \pm 31, \pm 33, \pm 35, \pm 41, \pm 43, \pm 47, \pm 51$
29	$\pm 3, \pm 11, \pm 15, \pm 17, \pm 19, \pm 21, \pm 27, \pm 31, \pm 37, \pm 39, \pm 41, \pm 43, \pm 47, \pm 55$
30	$\pm 11, \pm 23, \pm 31, \pm 41, \pm 43, \pm 47, \pm 53, \pm 59$

USAGE DES TABLES PRÉCÉDENTES DANS LA RECHERCHE DES DIVISEURS DES NOMBRES.

35. Cet usage se présente naturellement; car il suffit de ramener le nombre proposé dont on cherche les diviseurs ou un quelconque de ses multiples à la forme $t^2 \pm au^2$, ce qui est toujours possible de plusieurs manières, et si le nombre a se trouve dans les Tables III et IV on aura sur-le-champ toutes les valeurs de b que l'on peut admettre dans la forme générale $4an + b$ des diviseurs cherchés; en sorte qu'on sera assuré d'avance qu'il n'y aura que les nombres qui, étant divisés par $4a$, donneront pour restes quelques-unes des valeurs de b , qui pourront être diviseurs du nombre proposé; et comme pour trouver les diviseurs d'un nombre quelconque il suffit d'essayer successivement tous les nombres premiers moindres que la racine carrée de ce nombre, il est clair qu'on pourra d'abord exclure plusieurs de ces nombres premiers comme ne pouvant servir de diviseurs, ce qui épargnera beaucoup de tentatives inutiles, comme on va le voir par quelques Exemples.

Soit proposé de trouver les diviseurs du nombre 10001.

Suivant la méthode ordinaire il faudrait tenter successivement la division par tous les nombres premiers moindres que 100, qui est la racine carrée la plus proche de 10001; de sorte que comme entre 2 et 100 il y a vingt-quatre nombres premiers, il faudrait faire vingt-quatre divisions particulières.

Or

1° Je remarque que

$$10001 = (100)^2 + 1;$$

de sorte qu'on a ici $a = 1$, et la Table III donne $b = 1$; c'est pourquoi aucun nombre ne pourra être diviseur de 10001, à moins qu'il ne soit de la forme $4n + 1$, c'est-à-dire qu'étant divisé par 4 il donne 1 de reste; ce qui exclut déjà un grand nombre de nombres premiers tels que 3, 7, 11, 19, ...;

2° Je remarque ensuite que si l'on fait le carré de 101 on a 10201,

dont la différence avec le nombre proposé est

$$200 = 2(10)^2,$$

de sorte que le même nombre 10 001 peut aussi se représenter par

$$(101)^2 - 2(10)^2;$$

ainsi l'on aura $a = 2$, et la Table IV donnera $b = 1, -1$; d'où il s'ensuit que les diviseurs de 10 001 ne pourront être que de l'une ou de l'autre de ces deux formes $8n + 1, 8n - 1$; donc, puisqu'ils doivent être déjà de la forme $4n + 1$, il s'ensuit qu'ils ne pourront être que de la forme $8n + 1$; ainsi parmi tous les nombres premiers moindres que 100 il ne faudra choisir que ceux qui, étant divisés par 8, donneront l'unité pour reste; et l'on ne trouvera que ces cinq-ci

$$17, 41, 73, 89, 97,$$

qui seront admissibles; de sorte que l'on n'aura plus que cinq diviseurs à essayer au lieu de vingt-quatre. On pourrait encore réduire le nombre de ces mêmes diviseurs en ramenant d'une autre manière le même nombre 10 001 à la forme $t^2 \pm au^2$; mais cela est presque inutile dans le cas présent où le nombre des diviseurs utiles est déjà si petit; en effet, on trouve que 17 et 41 ne divisent pas 10 001, mais que 73 le divise, et donne pour quotient le nombre 137 qui est premier: d'où l'on conclut d'abord que les facteurs de 10 001 sont 73 et 137.

Je vais chercher de même les diviseurs du nombre suivant 10 003. J'aurai d'abord la forme

$$(100)^2 + 3,$$

qui donne $a = 3$ avec le signe +; ensuite, à cause de $(101)^2 = 10 201$, j'aurai aussi

$$10 003 = (101)^2 - 198 = (101)^2 - 22(3)^2;$$

dont $a = 22$ avec le signe -.

La Table III donne pour $a = 3, b = 1, -5$; de sorte qu'on aura d'abord ces deux formes

$$12n + 1, \quad 12n - 5 \quad \text{ou} \quad 12n + 7;$$

ensuite la Table IV donnera pour $a = 22$,

$$b = \pm 1, \pm 3, \pm 9, \pm 25, \pm 27, \pm 7, \pm 13, \pm 21, \pm 29, \pm 39;$$

d'où l'on tire les formes $88n \pm 1, 88n \pm 3, \dots$

Or puisqu'il suffit d'examiner les nombres premiers moindres que 100, on fera d'abord dans ces dernières formes $n = 0$ ou 1 , et, rejetant les nombres qui ne seraient pas premiers, on ne trouvera que ceux-ci

$$89, 3, 79, 97, 61, 7, 13, 67, 29, 59$$

qui soient admissibles; mais, en considérant les formes $12n + 1, 12n + 7$, on voit qu'il faut encore rejeter tous ceux qui, étant divisés par 12, donneront des restes différents de 1 ou de 7; ainsi il n'y aura que ces six

$$7, 13, 61, 67, 79, 97$$

qui puissent servir. La division réussit d'abord par 7, et le quotient étant 1429 qui est premier, il s'ensuit que les diviseurs de 10 003 sont seulement 7 et 1429.

Prenons encore pour exemple un nombre beaucoup plus grand, comme 100 003.

Il est visible qu'on aura d'abord la forme

$$10(100)^2 + 3,$$

ou bien en multipliant par 10,

$$(1000)^2 + 30;$$

de sorte qu'on aura $a = 30$ avec le signe +; ensuite je considère les carrés qui approchent le plus de 100 003, je trouve 99 856 et 100 489, dont les différences avec 100 003 sont $147 = 3(7)^2$ et $486 = 6(9)^2$, de sorte que j'aurai encore ces deux autres formes

$$(316)^2 + 3(7)^2 \quad \text{et} \quad (317)^2 - 6(9)^2;$$

dont la première donne $a = 3$ avec le signe +, et la seconde $a = -6$ avec le signe -.

Considérons d'abord ces deux dernières formes, et elles donneront,

suivant les Tables III et IV, l'une les formules $12n+1$, $12n-5$, et l'autre les formules $24n\pm 1$, $24n\pm 5$, d'où l'on voit que l'on ne peut admettre que ces deux-ci $24n+1$, $24n-5$ pour les diviseurs impairs du nombre proposé.

Maintenant la première forme où $a=30$ donnera, suivant la Table III, les formes suivantes :

$$\begin{array}{cccccc} 120n+1, & 120n+31, & 120n+49, & 120n-41, & 120n+17, & 120n+23, \\ 120n+47, & 120n-7, & 120n+13, & 120n+37, & 120n+43, & 120n-53, \\ 120n+11, & 120n+29, & 120n+59, & 120n-19; \end{array}$$

qu'il faudra comparer avec les précédentes $24n+1$, $24n-5$, pour en rejeter celles qui ne s'accorderont pas. Pour cela il n'y aura qu'à diviser successivement les expressions $120n+1$, $120n+31$,... par 24, et l'on ne retiendra que celles qui donneront pour reste 1, ou -5, ou bien 19, et comme le nombre 120 est divisible exactement par 24, il suffira de faire subir l'épreuve aux nombres 1, 31, 49,.... De cette manière on ne trouvera que les nombres

$$1, 49, 43, -53;$$

de sorte que les formules utiles se réduiront à ces quatre-ci

$$-120n+1, \quad 120n+49, \quad 120n+43, \quad 120n-53 \quad \text{ou bien} \quad 120n+67.$$

Par conséquent, aucun nombre premier ne pourra être un diviseur du nombre 100003, à moins qu'il ne soit de l'une de ces formes, c'est-à-dire qu'étant divisé par 120 il ne donne pour reste 1, ou 43, ou 49, ou 67. De plus, comme il suffit d'essayer pour diviseurs les nombres premiers qui sont moindres que $\sqrt{100003}$, c'est-à-dire moindres que 317, on fera dans les quatre formes précédentes $n=0$, $n=1$ et $n=2$, et l'on ne retiendra des nombres résultants que ceux qui seront premiers, savoir

$$43, 67, 163, 241, 283, 307;$$

ainsi il n'y aura que ces six diviseurs à essayer, tandis que par la méthode ordinaire il faudrait en essayer soixante-quatre. Or on trouve que

la division ne réussit par aucun de ces six nombres premiers; d'où l'on doit conclure sur-le-champ que le nombre 100003 est premier.

En général, on voit par la comparaison des Tables V et VI avec les Tables III et IV, que le nombre des formes des non-diviseurs est égal à celui des formes des diviseurs; de sorte que les formes admissibles ne composent que la moitié de toutes les formes possibles; ce qui doit nécessairement réduire le nombre des essais à faire à la moitié; mais en combinant ensemble plusieurs formes différentes, ainsi que nous l'avons fait dans les Exemples précédents, on parviendra encore à diminuer ce nombre autant qu'il sera possible.

DES NOMBRES PREMIERS DE LA FORME $4an+b$, LESQUELS SONT EN MÊME TEMPS DE LA FORME $u^2\pm at^2$.

36. M. Fermat a trouvé le premier les Théorèmes suivants :

1° Tous les nombres premiers de la forme $4n+1$ sont aussi de la forme y^2+z^2 .

2° Tous les nombres premiers de la forme $6n+1$ sont de la forme y^2+3z^2 .

3° Tous les nombres premiers de la forme $8n+1$ sont de la forme y^2+2z^2 .

4° Tous les nombres premiers de la forme $8n+3$ sont aussi de la forme y^2+2z^2 .

5° Tous les nombres premiers de la forme $8n\pm 1$ sont de la forme y^2-2t^2 .

6° Le produit de deux nombres premiers de la forme $4n+3$, et terminés par les caractères 3 ou 7, est toujours de la forme y^2+5z^2 ; et le carré de chacun de ces nombres en particulier est aussi de la même forme.

Les quatre premiers et le dernier de ces Théorèmes se trouvent dans une Lettre de M. Fermat à M. Digby insérée dans le *Commercium episto-*

licum de M. Wallis (*Wallisii Opera*, t. II, p. 857); le cinquième ne se trouve, à la vérité, que dans les *Lettres* de M. Frenicle à M. Fermat, imprimées dans les *Œuvres mathématiques* de Fermat, pages 168, 170; mais il paraît, par ces Lettres mêmes, que ce dernier l'avait aussi déjà trouvé de son côté.

Quant à la démonstration de ces Théorèmes, M. Fermat ne l'a point donnée, du moins on n'en trouve aucune trace dans les Ouvrages de ce savant qui nous sont restés; mais M. Euler a entrepris d'y suppléer, et a réussi en effet à démontrer les deux premiers Théorèmes, et même le troisième, quoiqu'il n'ait encore publié que la démonstration des deux premiers (voyez les *Nouveaux Commentaires de Pétersbourg*, t. V, VI, VIII).

A l'égard des autres Théorèmes de M. Fermat, et surtout du quatrième, M. Euler avoue qu'il n'a pu parvenir à le démontrer; il en est de même de quelques autres Théorèmes semblables que M. Euler a trouvés par induction (voyez t. VI, p. 221, et t. VIII, p. 127 des *Commentaires* cités), et que voici :

7° Tous les nombres premiers des formes $20n + 1$ et $20n + 9$ sont de la forme $y^2 + 5z^2$.

8° Tous les nombres premiers des formes $24n + 1$ et $24n + 7$ sont de la forme $y^2 + 6z^2$.

9° Tous les nombres premiers des formes $24n + 5$ et $24n + 11$ sont de la forme $2y^2 + 3z^2$.

10° Tous les nombres premiers de ces formes $28n + 1$, $28n + 9$, $28n + 11$, $28n + 15$, $28n + 23$, $28n + 25$ sont de la forme $y^2 + 7z^2$.

On trouve encore un plus grand nombre de pareils Théorèmes dans le tome XIV des anciens *Commentaires de Pétersbourg*, mais dont aucun n'a été démontré jusqu'à présent.

Les principes établis jusqu'ici peuvent servir à démontrer la plupart de ces Théorèmes et même à en trouver de nouveaux; mais il faut pour cela poser les Lemmes suivants.

LEMME I.

37. Si p est un nombre premier quelconque, et x un nombre non divisible par p , le nombre $x^{p-1} - 1$ est toujours divisible par p .

C'est le Théorème connu de M. Fermat dont M. Euler a donné différentes démonstrations dans les *Commentaires de Pétersbourg*. Voyez aussi à ce sujet les *Mémoires* de 1771 (*).

Il y a donc un nombre $p - 1$ de nombres entiers positifs ou négatifs, chacun moindre que $\frac{p}{2}$, qu'on peut prendre pour x , en sorte que $x^{p-1} - 1$ devienne divisible par p ; car ces nombres sont $\pm 1, \pm 2, \dots, \pm \frac{p-1}{2}$.

LEMME II.

38. Si le binôme $x^{p-1} - 1$ est résoluble en deux facteurs rationnels et entiers X et ξ , dont les degrés soient m et μ , en sorte que $m + \mu = p - 1$; je dis qu'il y aura nécessairement m valeurs de x moindres que $\frac{p}{2}$ qui rendront X divisible par p , et μ valeurs de x moindres que $\frac{p}{2}$ qui rendront ξ aussi divisible par p .

Car puisque par le Lemme précédent il y a $p - 1$ valeurs de x moindres que $\frac{p}{2}$, qui rendent $x^{p-1} - 1$ divisible par p , il y aura donc $m + \mu$ valeurs de x moindres que $\frac{p}{2}$ qui rendront $X\xi$ divisible par p ; mais p étant un nombre premier, $X\xi$ ne peut être divisible par p , à moins que X ou ξ ne le soit; d'autre part le nombre des valeurs de x moindres que $\frac{p}{2}$, lesquelles peuvent rendre le polynôme X ou ξ divisible par p , ne peut surpasser m ou μ , ainsi que nous l'avons démontré dans les *Mémoires* de 1768 (**); donc il faudra nécessairement que le nombre des valeurs

(*) *Œuvres de Lagrange*, t. III, p. 425.

(**) *Œuvres de Lagrange*, t. II, p. 667.

de x moindres que $\frac{p}{2}$, lesquelles rendront X divisible par p , soit m , et que celui des valeurs de x moindres que $\frac{p}{2}$, lesquelles rendront ξ divisible par p , soit μ .

En général, si Π est un polynôme quelconque entier et rationnel en x , dont le degré soit moindre que $p-1$, et que le polynôme $x^{p-1} \pm p\Pi - 1$ soit résoluble dans les deux polynômes X et ξ rationnels et entiers, il suit de la démonstration précédente qu'il y aura toujours m valeurs de x moindres que $\frac{p}{2}$ qui rendront X divisible par p , et μ valeurs de x moindres que $\frac{p}{2}$ qui rendront ξ divisible par p .

LEMME III.

39. Si un nombre premier p est un diviseur d'un nombre de la forme $t^2 - au^2$, a étant un nombre donné positif ou négatif, et t, u des nombres premiers entre eux, et non divisibles par p ; je dis que $a^{\frac{p-1}{2}} - 1$ sera nécessairement divisible par p .

Et réciproquement si $a^{\frac{p-1}{2}} - 1$ est divisible par p , ce nombre p pourra toujours être un diviseur d'un nombre de la forme $t^2 - au^2$.

Car :

1° Supposant $t^2 - au^2 = pM$, on aura

$$t^2 = au^2 + pM;$$

or, par le Lemme I, $t^{p-1} - 1$ et $u^{p-1} - 1$ sont divisibles par p ; donc

$$(au^2 + pM)^{\frac{p-1}{2}} - 1$$

sera aussi divisible par p ; mais en développant la puissance

$$(au^2 + pM)^{\frac{p-1}{2}},$$

on voit que tous les termes en sont d'eux-mêmes multiples de p , excepté

le premier

$$u^{p-1} a^{\frac{p-1}{2}};$$

donc

$$u^{p-1} a^{\frac{p-1}{2}} - 1$$

sera divisible par p ; mais $u^{p-1} - 1$ étant aussi divisible par p ,

$$u^{p-1} a^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}$$

sera encore divisible par p ; par conséquent la différence de ces nombres, c'est-à-dire

$$a^{\frac{p-1}{2}} - 1,$$

sera nécessairement divisible par p .

2° Si $a^{\frac{p-1}{2}} - 1$ est supposé divisible par p , alors, par le Lemme II, il y aura toujours quelques valeurs de x qui rendront chacun des facteurs de

$$x^{p-1} - a^{\frac{p-1}{2}}$$

(en prenant $a^{\frac{p-1}{2}} - 1 = p\Pi$) divisible par p ; mais ce binôme a pour facteur $x^2 - a$; donc p pourra être diviseur de $x^2 - a$, c'est-à-dire d'un nombre de la forme $t^2 - au^2$.

LEMME IV.

40. Si l'on a un nombre premier p de la forme $4n+1$, lequel soit un diviseur d'un nombre de la forme $t^2 - au^2$, il le sera aussi nécessairement d'un nombre de la forme $t^2 + au^2$.

Et vice versâ si p n'est jamais un diviseur d'un nombre de la forme $t^2 - au^2$, il ne pourra jamais l'être d'un nombre de la forme $t^2 + au^2$.

Car si p est un diviseur d'un nombre de la forme $t^2 - au^2$, on aura par le Lemme précédent $a^{\frac{p-1}{2}} - 1$ divisible par p ; mais $\frac{p-1}{2} = 2n$; donc

$a^{2n} - 1$ sera divisible par p ; donc aussi, changeant a en $-a$, $(-a)^{2n} - 1$ sera divisible par p ; c'est-à-dire que

$$(-a)^{\frac{p-1}{2}} - 1$$

sera divisible par p ; par conséquent, par la seconde partie du Lemme précédent, p sera un diviseur d'un nombre de la forme $t^2 + au^2$.

De même, en changeant a en $-a$ on prouvera que si p est un diviseur d'un nombre de la forme $t^2 + au^2$, il le sera aussi d'un nombre de la forme $t^2 - au^2$; par conséquent, si p ne peut être un diviseur de $t^2 - au^2$, il ne pourra l'être non plus d'un nombre de la forme $t^2 + au^2$.

LEMME V.

41. Si p est de la forme $4n - 1$, et que ce nombre soit un diviseur d'un nombre de la forme $t^2 - au^2$, il ne pourra jamais l'être d'un nombre de la forme $t^2 + au^2$.

Et réciproquement si p ne peut être un diviseur d'un nombre de la forme $t^2 - au^2$, il le sera nécessairement d'un nombre de la forme $t^2 + au^2$.

Car p étant un diviseur de $t^2 - au^2$, il faudra que l'on ait $a^{\frac{p-1}{2}} - 1$, savoir $a^{2n-1} - 1$ divisible par p (Lemme III); de même, pour que $t^2 + au^2$ fût divisible par p , il faudrait que l'on eût, en changeant a en $-a$, $(-a)^{2n-1} - 1$ divisible par p , c'est-à-dire (à cause que l'exposant $2n - 1$ est impair) que $a^{2n-1} + 1$ fût aussi divisible par p ; ce qui ne se peut.

Si p ne peut être un diviseur de $t^2 - au^2$, alors $a^{\frac{p-1}{2}} - 1$ ne sera pas divisible par p (Lemme III). Or $a^{p-1} - 1$ est toujours nécessairement divisible par p (Lemme I); mais

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

donc puisque p est premier et que $a^{\frac{p-1}{2}} - 1$ n'est pas divisible par p , il

faut nécessairement que $a^{\frac{p-1}{2}} + 1$ soit divisible par p . Ainsi dans ce cas

$$a^{\frac{p-1}{2}} + 1 \quad \text{ou bien} \quad a^{2n-1} + 1$$

sera divisible par p ; donc aussi

$$(-a)^{2n-1} - 1 \quad \text{ou bien} \quad (-a)^{\frac{p-1}{2}} - 1$$

sera divisible par p . Donc, par le Lemme III, le nombre p sera diviseur d'un nombre de la forme $t^2 + au^2$.

42. COROLLAIRE. — Il suit des deux derniers Lemmes :

1° Que si $4an + b$ est une des formes des diviseurs de $t^2 \pm au^2$, ce sera aussi une des formes des diviseurs de $t^2 \mp au^2$ lorsque b sera de la forme $4m + 1$; et que si $4an + b$ est une des formes des non-diviseurs de $t^2 \pm au^2$, ce sera aussi une des formes des non-diviseurs de $t^2 \mp au^2$.

2° Que si $4an + b$ est une des formes des diviseurs de $t^2 \pm au^2$, ce sera aussi une des formes des non-diviseurs de $t^2 \mp au^2$ lorsque b sera de la forme $4m - 1$; et que si $4an + b$ est une des formes des non-diviseurs de $t^2 \pm au^2$, ce sera aussi nécessairement une des formes des diviseurs de $t^2 \mp au^2$. Les quatre dernières Tables fournissent des exemples de la vérité de ces propositions.

LEMME VI.

43. Si un nombre premier p est à la fois diviseur de différents nombres de ces formes $t^2 - au^2$, $t^2 - a'u^2$, $t^2 - a''u^2$, ..., je dis qu'il sera aussi diviseur d'un nombre de la forme $t^2 - a'a'a''...u^2$.

Si p divise en même temps les deux nombres $t^2 - au^2$ et $t'^2 - a'u'^2$, il divisera aussi le nombre

$$t'(t^2 - a'u'^2) + a'u'(t^2 - au^2),$$

c'est-à-dire

$$(tt')^2 - aa'(uu')^2;$$

et, si le même nombre p divise encore le nombre $t'^2 - a''u''^2$, on prouvera pareillement qu'il divisera aussi le nombre

$$(tt't'')^2 - aa'a''(uu'u'')^2;$$

et ainsi de suite. Au reste, on voit par cette démonstration que la proposition est vraie, en général, quel que soit le nombre p , premier ou non.

LEMME VII.

44. Si le nombre premier p ne peut jamais être diviseur d'un nombre de la forme $t^2 - au^2$, je dis qu'il sera nécessairement un diviseur d'un nombre de la forme

$$\frac{(t + u\sqrt{a})^{p+1} - (t - u\sqrt{a})^{p+1}}{2t\sqrt{a}},$$

et même d'un facteur quelconque de cette formule.

Car si p ne peut être un diviseur de $t^2 - au^2$, alors $a^{\frac{p-1}{2}} - 1$ ne sera pas divisible par p (Lemme III); mais, $a^{p-1} - 1$ étant toujours divisible par p (Lemme I), il faudra que $a^{\frac{p-1}{2}} + 1$ soit divisible par p , puisque

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

Maintenant si l'on considère la quantité $(t + u\sqrt{a})^p$ et qu'on la résolve en série par le Théorème de Newton, on verra qu'à cause que p est un nombre premier, tous les termes seront d'eux-mêmes divisibles par p , excepté le premier t^p et le dernier $u^p a^{\frac{p}{2}}$, et cela indépendamment des valeurs de t, u, a . Donc

$$(t + u\sqrt{a})^p - t^p - u^p a^{\frac{p}{2}}$$

sera toujours divisible par p . Mais t et u n'étant pas divisibles par p , on a, par le Lemme I, $t^{p-1} - 1$ et $u^{p-1} - 1$ divisibles par p ; donc aussi

$$t^p - t \quad \text{et} \quad (u^p - u)a^{\frac{p}{2}},$$

et par conséquent

$$(t + u\sqrt{a})^p - t^p - u^p a^{\frac{p}{2}}$$

seront divisibles par p ; or $a^{\frac{p-1}{2}} + 1$ est divisible par p ; donc $u^p a^{\frac{p}{2}} + u\sqrt{a}$

le sera aussi; donc

$$(t + u\sqrt{a})^p - t^p - u\sqrt{a}$$

sera divisible par p ; donc, prenant le radical $\sqrt{a}$ en $-$,

$$(t - u\sqrt{a})^p - t^p - u\sqrt{a}$$

sera également divisible par p ; donc enfin multipliant la première de ces quantités par $t + u\sqrt{a}$, et la seconde par $t - u\sqrt{a}$, et prenant la différence, cette différence sera encore divisible par p ; ainsi

$$(t + u\sqrt{a})^{p+1} - (t - u\sqrt{a})^{p+1}$$

sera toujours divisible par p ; mais si l'on développe cette quantité, on voit qu'à cause que $p+1$ est pair, tous les termes sont divisibles par $2t\sqrt{a}$; donc, puisque ni t ni $\sqrt{a}$ n'est divisible par p , il s'en suit que la quantité

$$\frac{(t + u\sqrt{a})^{p+1} - (t - u\sqrt{a})^{p+1}}{2t\sqrt{a}}$$

sera divisible par p .

Cette quantité étant développée et ordonnée par rapport aux puissances de t , devient un polynôme entier et rationnel du degré $p-1$; ainsi, supposant u donné, il y aura $p-1$ valeurs de t tant positives que négatives, mais moindres que $\frac{p}{2}$, lesquelles rendront ce polynôme divisible par p , ces valeurs étant

$$\pm 1, \pm 2, \pm 3, \dots, \pm \frac{p-1}{2}.$$

Donc on prouvera, comme dans le Lemme II, que si ce polynôme a un facteur rationnel et entier de l'ordre m , il y aura nécessairement m valeurs de t qui rendront aussi ce facteur divisible par p .

THÉORÈMES SUR LES NOMBRES PREMIERS DE LA FORME $4n-1$.

45. Comme les nombres premiers de cette forme qui ne sont pas diviseurs de $t^2 \pm au^2$ le sont nécessairement de $t^2 \mp au^2$ par le Lemme V (41), on pourra appliquer à ces nombres les propriétés qui conviennent aux

diviseurs de $t^2 \mp au^2$; donc en combinant la Table V avec la Table II et la Table IV, et la Table VI avec la Table I et la Table III, et ne considérant que les valeurs de b qui sont de la forme $4m-1$, on aura les Théorèmes suivants :

1° Tous les nombres premiers de la forme $8n+3$ sont de la forme y^2+2z^2 .

2° Tous les nombres premiers de la forme $8n-1$ sont en même temps de ces deux formes y^2-2z^2 et $2z^2-y^2$.

3° Tous les nombres premiers de la forme $12n-5$ sont de la forme y^2+3z^2 .

4° Tous les nombres premiers de la forme $12n-1$ sont de la forme $3z^2-y^2$.

5° Tous les nombres premiers de ces formes $20n+3$, $20n+7$ sont de la forme $2y^2 \pm 2yz + 3z^2$; ou bien ces nombres étant multipliés par 2 deviendront de la forme y^2+5z^2 .

6° Tous les nombres premiers de ces formes $20n-1$, $20n-9$ sont en même temps de l'une et de l'autre des deux formes y^2-5z^2 et $5z^2-y^2$.

7° Tous les nombres premiers de la forme $24n+7$ sont de la forme y^2+6z^2 ; et tous ceux de la forme $24n+11$ sont de la forme $2y^2+3z^2$.

8° Tous les nombres premiers de la forme $24n-1$ sont de la forme $6z^2-y^2$; et ceux de la forme $24n-5$ sont aussi de la forme y^2-6z^2 .

9° Tous les nombres premiers de ces formes $28n+11$, $28n-5$, $28n-13$ sont de la forme y^2+7z^2 .

10° Tous les nombres premiers des formes $28n+3$, $28n-1$, $28n-9$ sont de la forme $7z^2-y^2$.

11° Tous les nombres premiers de ces formes $40n+11$, $40n+19$ sont de la forme y^2+10z^2 ; et ceux des formes $40n+7$, $40n-17$ sont de la forme $2y^2+3z^2$.

12° Tous les nombres premiers de ces formes $40n-1$, $40n-9$ sont en

même temps de l'une et de l'autre de ces formes y^2-10z^2 et $10z^2-y^2$; et ceux des formes $40n+3$, $40n-13$ sont de l'une et de l'autre des formes $2y^2-5z^2$ et $5z^2-2y^2$.

13° Tous les nombres premiers de ces formes $44n+3$, $44n+15$, $44n-13$, $44n-17$, $44n-21$ sont ou de la forme y^2+11z^2 , ou bien de la forme $3y^2 \pm 2yz + 4z^2$.

14° Tous les nombres premiers de ces formes $44n+7$, $44n+19$, $44n-1$, $44n-5$, $44n-9$ sont de la forme $11z^2-y^2$.

15° Tous les nombres premiers de ces formes $52n+7$, $52n+11$, $52n+15$, $52n+19$, $52n-5$, $52n-21$ sont de la forme $2y^2 \pm 2yz + 7z^2$, ou bien ces nombres étant multipliés par 2 deviendront de la forme y^2+13z^2 .

16° Tous les nombres premiers de ces formes $52n+3$, $52n+23$, $52n-1$, $52n-9$, $52n-17$, $52n-25$ sont en même temps de l'une et de l'autre de ces formes y^2-13z^2 et $13z^2-y^2$.

17° Tous les nombres premiers des formes $56n+15$, $56n+23$, $56n-17$ sont ou de la forme y^2+14z^2 , ou de celle-ci $2y^2+7z^2$; et les nombres premiers des formes $56n+3$, $56n+19$, $56n+27$ sont de la forme $3y^2 \pm 2yz + 5z^2$; ou bien ces nombres étant multipliés par 3 deviendront de la forme y^2+14z^2 .

18° Tous les nombres premiers de ces formes $56n+11$, $56n-5$, $56n-13$ sont de la forme y^2-14z^2 ; et tous ceux des formes $56n-1$, $56n-9$, $56n-25$ sont de la forme $14z^2-y^2$.

19° Tous les nombres premiers de ces formes $60n+19$, $60n-29$ sont de la forme y^2+15z^2 ; et tous ceux des formes $60n+23$, $60n-13$ sont de la forme $3y^2+5z^2$.

20° Tous les nombres premiers de ces formes $60n+11$, $60n-1$ sont de la forme $15z^2-y^2$; et ceux des formes $60n+7$, $60n-17$ sont de la forme $3y^2-5z^2$.

21° Tous les nombres premiers de ces formes $68n+3$, $68n+11$, $68n+23$, $68n+27$, $68n+31$, $68n-5$, $68n-29$ sont de la forme

$3y^2 \pm 2yz + 6z^2$; ou bien ces nombres étant multipliés par 3 deviendront de la forme $y^2 + 17z^2$.

22° Tous les nombres premiers de ces formes $68n + 15$, $68n + 19$, $68n - 1$, $68n - 9$, $68n - 13$, $68n - 21$, $68n - 25$, $68n - 33$ sont en même temps de ces deux formes $y^2 - 17z^2$ et $17z^2 - y^2$.

23° Tous les nombres premiers de ces formes $76n + 7$, $76n + 11$, $76n + 23$, $76n + 35$, $76n - 13$, $76n - 21$, $76n - 29$, $76n - 33$, $76n - 37$ sont ou de la forme $y^2 + 19z^2$, ou bien de la forme $4y^2 \pm 2yz + 5z^2$.

24° Tous les nombres premiers de ces formes $76n + 3$, $76n + 15$, $76n + 27$, $76n + 31$, $76n - 1$, $76n - 5$, $76n - 9$, $76n - 17$, $76n - 25$ sont de la forme $19z^2 - y^2$.

25° Tous les nombres premiers de ces formes $84n + 19$, $84n + 31$, $84n - 29$ sont de la forme $3y^2 + 7z^2$; et ceux des formes $84n + 11$, $84n + 23$, $84n - 13$ sont de la forme $2y^2 \pm 2yz + 11z^2$, ou bien ces nombres étant multipliés par 2 deviendront de la forme $y^2 + 21z^2$.

26° Tous les nombres premiers de ces formes $84n - 5$, $84n - 17$, $84n - 41$ sont de la forme $y^2 - 21z^2$; et ceux des formes $84n - 1$, $84n - 25$, $84n - 37$ sont de la forme $21z^2 - y^2$.

27° Tous les nombres premiers de ces formes $88n + 15$, $88n + 23$, $88n + 31$, $88n - 17$, $88n - 41$ sont de la forme $y^2 + 22z^2$; et ceux des formes $88n + 19$, $88n + 35$, $88n + 43$, $88n - 5$, $88n - 37$ sont de la forme $2y^2 + 11z^2$.

28° Tous les nombres premiers de ces formes $88n + 3$, $88n + 27$, $88n - 13$, $88n - 21$, $88n - 29$ sont de la forme $y^2 - 22z^2$; et ceux des formes $88n + 7$, $88n + 39$, $88n - 1$, $88n - 9$, $88n - 25$ sont de la forme $22z^2 - y^2$.

29° Tous les nombres premiers de ces formes $92n + 3$, $92n + 27$, $92n + 31$, $92n + 35$, $92n + 39$, $92n - 5$, $92n - 17$, $92n - 21$, $92n - 33$, $92n - 37$, $92n - 45$ sont ou de la forme $y^2 + 23z^2$, ou bien de la forme $3y^2 \pm 2yz + 8z^2$.

30° Tous les nombres premiers de ces formes $92n + 7$, $92n + 11$, $92n + 15$, $92n + 19$, $92n + 43$, $92n - 1$, $92n - 9$, $92n - 13$, $92n - 25$, $92n - 29$, $92n - 41$ sont de la forme $23z^2 - y^2$.

31° Tous les nombres premiers de ces formes $104n + 3$, $104n + 27$, $104n + 35$, $104n + 43$, $104n + 51$, $104n - 29$ sont ou de la forme $y^2 + 26z^2$, ou bien de la forme $3y^2 \pm 2yz + 9z^2$; et tous ceux de ces formes $104n + 7$, $104n + 15$, $104n + 31$, $104n + 47$, $104n - 33$, $104n - 41$ sont ou de la forme $2y^2 + 13z^2$, ou bien de la forme $5y^2 \pm 4yz + 6z^2$.

32° Tous les nombres premiers de ces formes $104n + 23$, $104n - 1$, $104n - 9$, $104n - 17$, $104n - 25$, $104n - 49$ sont de l'une et de l'autre de ces formes $y^2 - 26z^2$ et $26z^2 - y^2$; et ceux des formes $104n + 11$, $104n + 19$, $104n - 5$, $104n - 21$, $104n - 37$, $104n - 45$ sont en même temps de l'une et de l'autre de ces formes-ci $2y^2 - 13z^2$ et $13z^2 - 2y^2$.

33° Tous les nombres premiers de ces formes $116n + 3$, $116n + 11$, $116n + 15$, $116n + 19$, $116n + 27$, $116n + 31$, $116n + 39$, $116n + 43$, $116n + 47$, $116n + 55$, $116n - 17$, $116n - 21$, $116n - 37$, $116n - 41$ sont ou de la forme $2y^2 \pm 2yz + 15z^2$, ou bien de celle-ci $3y^2 \pm 2yz + 10z^2$.

34° Tous les nombres premiers de ces formes $116n + 7$, $116n + 23$, $116n + 35$, $116n + 51$, $116n - 1$, $116n - 5$, $116n - 9$, $116n - 13$, $116n - 25$, $116n - 33$, $116n - 45$, $116n - 49$, $116n - 53$, $116n - 57$ sont à la fois de ces deux formes $y^2 - 29z^2$ et $29z^2 - y^2$.

35° Tous les nombres premiers de ces formes $120n + 31$, $120n - 41$ sont de la forme $y^2 + 30z^2$; ceux des formes $120n + 23$, $120n + 47$ sont de la forme $2y^2 + 15z^2$; ceux des formes $120n + 43$, $120n - 53$ sont de la forme $3y^2 + 10z^2$; enfin ceux des formes $120n + 11$, $120n + 59$ sont de la forme $5y^2 + 6z^2$.

36° Tous les nombres premiers des formes $120n + 19$, $120n - 29$ sont de la forme $y^2 - 30z^2$; tous ceux des formes $120n - 1$, $120n - 49$ sont de la forme $30z^2 - y^2$; tous ceux des formes $120n + 7$, $120n - 17$ sont

de la forme $15z^2 - 2y^2$; enfin tous ceux des formes $120n - 13$, $120n - 37$ sont de la forme $2y^2 - 15z^2$.

Nous nous arrêtons ici, n'ayant poussé nos Tables que jusqu'à $a = 30$; mais ceux qui sont curieux de ces sortes de Théorèmes pourront aisément les continuer aussi loin qu'ils voudront à l'aide des principes et des méthodes que nous avons données jusqu'ici.

46. Maintenant il est clair que le Théorème 1^o du numéro précédent renferme le Théorème 4^o de M. Fermat (36); que le Théorème 2^o ci-dessus renferme une partie du Théorème 5^o de M. Fermat, et qu'il est même plus général que celui de ce Géomètre, en ce que le nôtre nous apprend que tous les nombres premiers de la forme $8n - 1$ sont non-seulement de la forme $y^2 - 2z^2$, mais aussi de celle-ci $2z^2 - y^2$. Enfin il est visible que notre Théorème 3^o renferme aussi le Théorème 2^o de M. Fermat, mais pour le cas seulement où n est impair.

Quant au Théorème 6^o de cet Auteur, quoiqu'il ne soit point contenu immédiatement dans le Théorème 5^o du numéro précédent, il est cependant facile de l'en déduire. En effet, on peut d'abord démontrer que tous les nombres de la forme $4m + 3$, qui sont terminés par les caractères 3 ou 7, sont nécessairement de l'une de ces deux formes $20n + 3$, $20n + 7$; car en faisant successivement

$$m = 5n, 5n + 1, 5n + 2, 5n + 3, 5n + 4,$$

la forme $4m + 3$ donne celles-ci

$$20n + 3, 20n + 7, 20n + 11, 20n + 15, 20n + 19;$$

où l'on voit qu'il n'y a que les deux premières qui puissent donner des nombres terminés par 3 ou par 7. Ainsi le Théorème de M. Fermat se réduit à ce que le produit de deux nombres premiers de ces formes $20n + 3$, $20n + 7$ est toujours de la forme $y^2 + 5z^2$. Or notre Théorème 5^o nous apprend que tous les nombres premiers des formes $20n + 3$, $20n + 7$ sont nécessairement de la forme $2y^2 \pm 2yz + 3z^2$. Donc il n'y a qu'à prouver que le produit de deux nombres de la forme

$2y^2 \pm 2yz + 3z^2$ est de la forme $y^2 + 5z^2$; ce qui est facile, car on trouve que

$$(2y^2 + 2yz + 3z^2)(2y'^2 + 2y'z' + 3z'^2) = (2yy' + yz' + zy' + 3zz')^2 + 5(yz' - zy')^2.$$

A l'égard des autres Théorèmes de M. Fermat qui concernent les nombres premiers de la forme $4n + 1$, on en trouvera la démonstration ci-après.

47. Les Théorèmes du n^o 45 ne regardent que les nombres premiers de la forme $4n - 1$. Pour avoir de pareils Théorèmes sur les nombres premiers de la forme $4n + 1$, il faudrait pouvoir démontrer que les nombres premiers de la forme $4na + b$, lorsque b est de la forme $4m + 1$, peuvent toujours être diviseurs de quelque nombre de la forme $t^2 + au^2$ ou $t^2 - au^2$; car nous avons déjà prouvé (40) que tout nombre premier de la forme $4n + 1$ qui est un diviseur de $t^2 \pm au^2$ l'est aussi de $t^2 \mp au^2$. Or quoique l'induction paraisse prouver que les nombres premiers des formes qui conviennent aux diviseurs de $t^2 \pm au^2$ peuvent toujours être effectivement des diviseurs de pareils nombres, cette proposition ne peut être démontrée rigoureusement par rapport aux nombres premiers de la forme $4n + 1$ que pour un très-petit nombre de cas; du moins toutes les tentatives que j'ai faites pour en venir à bout ont été jusqu'à présent inutiles; de sorte que je me bornerai ici à rapporter les résultats de mes Recherches dans quelques cas particuliers où j'ai réussi à trouver la démonstration de la proposition dont il s'agit; ce sont ceux où $b = 1$ et où $a = 1, 2, 3, 5, 7$ ou = au produit de quelques-uns de ces nombres, et où $b = 9$ et $a = 5, 10$.

THÉORÈMES SUR LES NOMBRES PREMIERS DE LA FORME $4n + 1$.

48. Nous avons vu (Lemmes I et II) qu'on peut toujours trouver une valeur de x telle que $x^{p-1} - 1$, ou un quelconque des facteurs rationnels et entiers de ce binôme soit divisible par p . Soit donc $p = 4na + 1$, on aura

$$x^{p-1} - 1 = x^{4na} - 1 = (x^{2na} - 1)(x^{2na} + 1);$$

ainsi $x^{2na} + 1$ pourra être divisible par $4na + 1$, lorsque c'est un nombre premier. Faisons $x^a = r$, et l'on aura le binôme $r^{2a} + 1$ qui pourra être divisible par $4na + 1$; faisons de plus $r^2 + 1 = s$, et le binôme $r^{2a} + 1$ pourra se réduire à cette forme

$$s^a - a s^{a-2} r^2 + \frac{a(a-3)}{2} s^{a-4} r^4 - \frac{a(a-4)(a-5)}{2 \cdot 3} s^{a-6} r^6 + \frac{a(a-5)(a-6)(a-7)}{2 \cdot 3 \cdot 4} s^{a-8} r^8 - \dots,$$

quantité que nous appellerons R pour plus de simplicité. Ainsi tout nombre premier de la forme $4na + 1$ pourra être un diviseur du polynôme R, ou même d'un facteur quelconque entier et rationnel de ce polynôme. Il faut seulement remarquer, à l'égard de la série qui représente ce polynôme, qu'elle ne doit être poussée que jusqu'aux termes exclusivement qui contiendraient des puissances négatives de s; c'est de quoi il est facile de se convaincre par la nature même de cette série, laquelle, en y substituant $r^2 + 1$ à la place de s, doit se réduire à $r^{2a} + 1$.

Cela posé, soit d'abord $a = 1$; on aura

$$R = s = r^2 + 1;$$

donc tout nombre premier de la forme $4n + 1$ pourra être un diviseur d'un nombre de la forme $t^2 + u^2$; donc (18) :

1^o Tout nombre premier de la forme $4n + 1$ est aussi de la forme $y^2 + z^2$.

Soit ensuite $a = 2$, on aura

$$R = s^2 - 2r^2;$$

d'où il s'ensuit que tout nombre premier de la forme $8n + 1$ peut être un diviseur d'un nombre de la forme $t^2 - 2u^2$, et par conséquent aussi d'un nombre de la forme $t^2 + 2u^2$ (Lemme IV); donc (18 et 20) :

2^o Tout nombre premier de la forme $8n + 1$ est en même temps de ces trois formes $y^2 + 2z^2$, $y^2 - 2z^2$ et $2z^2 - y^2$.

Soit en troisième lieu $a = 3$, on aura

$$R = s^3 - 3sr^2 = s(s^2 - 3r^2);$$

donc tout nombre premier de la forme $12n + 1$ pourra être diviseur d'un nombre de la forme $t^2 - 3u^2$, et par conséquent aussi d'un nombre de la forme $t^2 + 3u^2$ (Lemme IV); donc (18 et 20) :

3^o Tout nombre premier de la forme $12n + 1$ sera en même temps de la forme $y^2 + 3z^2$ et de l'une de ces deux $y^2 - 3z^2$ et $3z^2 - y^2$; mais on voit par la Table IV que la forme $-y^2 + 3z^2$ ne donne que des nombres de la forme $12n - 1$; donc tout nombre premier $12n + 1$ sera nécessairement de ces deux formes $y^2 + 3z^2$ et $y^2 - 3z^2$.

Soit en quatrième lieu $a = 5$, on aura

$$R = s^5 - 5s^3r^2 + 5sr^4 = s(s^4 - 5s^2r^2 + 5r^4);$$

donc tout nombre premier de la forme $20n + 1$ pourra être un diviseur de $s^4 - 5s^2r^2 + 5r^4$, par conséquent aussi de

$$4s^4 - 20s^2r^2 + 20r^4 = (2s^2 - 5r^2)^2 - 5r^4,$$

c'est-à-dire d'un nombre de la forme $t^2 - 5u^2$; donc il pourra l'être aussi d'un nombre de la forme $t^2 + 5u^2$ (Lemme IV); donc (18 et 20) :

4^o Tout nombre premier de la forme $20n + 1$ est en même temps de ces trois formes $y^2 + 5z^2$, $y^2 - 5z^2$ et $5z^2 - y^2$.

En cinquième lieu, soit $a = 7$, on aura

$$R = s^7 - 7s^5r^2 + 14s^3r^4 - 7sr^6 = s[s^6 - 7(s^4 - r^2)^2r^2];$$

donc tout nombre premier de la forme $28n + 1$ pourra être un diviseur de $s^6 - 7(s^4 - r^2)^2r^2$, et par conséquent d'un nombre de la forme $t^2 - 7u^2$, comme aussi d'un nombre de la forme $t^2 + 7u^2$ (Lemme IV); donc (18 et 20) :

5^o Tout nombre premier de la forme $28n + 1$ sera en même temps de la

forme $y^2 + 7z^2$ et de l'une de ces deux-ci $y^2 - 7z^2$, $7z^2 - y^2$; mais la Table IV montre que la forme $-y^2 + 7z^2$ ne peut donner des nombres de la forme $28n + 1$; donc tout nombre premier $28n + 1$ sera nécessairement de ces deux formes $y^2 + 7z^2$ et $y^2 - 7z^2$.

Si l'on faisait encore $a = 11$, on aurait

$$R = s^{11} - 11s^9r^2 + 11.4s^7r^4 - 11.7s^5r^6 + 11.5s^3r^8 - 11s r^{10};$$

de sorte que tout nombre premier de la forme $44n + 1$ pourra être un diviseur de

$$s^{11} - 11(s^8 - 4s^6r^2 + 7s^4r^4 - 5s^2r^6 + r^8)r^3;$$

mais je ne vois pas comment cette quantité pourrait se réduire à la forme $t^2 - 11u^2$; c'est pourquoi il me paraît que l'usage de la méthode précédente est borné aux seuls cas que nous venons d'examiner; d'autant plus que ces cas sont les seuls où l'on ait pu jusqu'ici déterminer les racines de l'équation $r^{2a} + 1 = 0$, en supposant a un nombre premier; en effet, si l'on pouvait trouver, pour une valeur quelconque de a , l'expression de la racine r , et que cette expression contint d'une manière quelconque le radical $\sqrt{a}$ ou $\sqrt{-a}$, il est facile de voir qu'on pourrait toujours avoir un facteur de $r^{2a} + 1$ qui serait de la forme $t^2 \pm au^2$, et qui pourrait par conséquent être divisible par tout nombre premier de la forme $4na + 1$.

Ayant trouvé jusqu'ici que tout nombre premier de la forme $4na + 1$ est toujours un diviseur de $t^2 \pm au^2$ lorsque $a = 2, 3, 5, 7$, il s'ensuit du Lemme VI que cela sera vrai aussi lorsque a sera égal au produit de quelques-uns des nombres 2, 3, 5, 7. Ainsi, faisant successivement

$$a = 6, 10, 14, 15, 21, 30,$$

on trouvera, d'après les Tables I et II combinées avec les Tables III et IV, les Théorèmes suivants :

6° Tout nombre premier de la forme $24n + 1$ est en même temps de l'une et de l'autre de ces deux formes $y^2 + 6z^2$ et $y^2 - 6z^2$.

7° Tout nombre premier de la forme $40n + 1$ est en même temps de chacune de ces trois formes $y^2 + 10z^2$, $y^2 - 10z^2$ et $10z^2 - y^2$.

8° Tout nombre premier de la forme $56n + 1$ est de la forme $y^2 + 14z^2$ ou $2y^2 + 7z^2$, et en même temps de la forme $y^2 - 14z^2$.

9° Tout nombre premier de la forme $60n + 1$ est à la fois de l'une et de l'autre de ces formes $y^2 + 15z^2$ et $y^2 - 15z^2$.

10° Tout nombre premier de la forme $84n + 1$ est à la fois de l'une et de l'autre de ces formes $y^2 + 21z^2$ et $y^2 - 21z^2$.

11° Tout nombre premier de la forme $120n + 1$ est à la fois de l'une et de l'autre de ces formes $y^2 + 30z^2$ et $y^2 - 30z^2$.

Considérons maintenant les nombres premiers de la forme $20n + 9$, et je dis que ces nombres sont nécessairement diviseurs de quelques nombres de la forme $t^2 - 5u^2$. Car si on le nie, il faudra qu'on admette (Lemme VII, n° 45) que le nombre

$$\frac{(t + u\sqrt{5})^{20n+9} - (t - u\sqrt{5})^{20n+9}}{2t\sqrt{5}},$$

et même qu'un facteur quelconque de ce nombre est divisible par le nombre premier $20n + 9$. Or l'expression précédente a évidemment ce facteur

$$\frac{(t + u\sqrt{5})^5 - (t - u\sqrt{5})^5}{2\sqrt{5}},$$

c'est-à-dire, en développant les termes,

$$5(t^4 + 10t^2u^2 + 5u^4) = 25(t^2 + u^2)^2 - 5(2t^3);$$

donc le nombre $20n + 9$ sera nécessairement diviseur d'un nombre de la forme $t^2 - 5u^2$. De là et des Tables citées résulte d'abord ce Théorème :

12° Tout nombre premier de la forme $20n + 9$ est en même temps de ces trois formes $y^2 + 5z^2$, $y^2 - 5z^2$ et $5z^2 - y^2$.

Enfin puisque les nombres de la forme $40n + 9$ sont aussi de la forme

$8n+1$, et que nous avons déjà vu que les nombres premiers de cette dernière forme sont toujours diviseurs de quelques nombres de la forme t^2-2u^2 ; il s'ensuit du Lemme VI qu'en faisant $a=2.5$, les nombres premiers de la forme $4na+9$, c'est-à-dire $40n+9$, seront toujours diviseurs de quelques nombres de la forme u^2-at^2 , c'est-à-dire de u^2-10t^2 . Donc :

13° Tout nombre premier de la forme $40n+9$ est en même temps de ces trois formes y^2+10z^2 , y^2-10z^2 et $10z^2-y^2$.

49. SCOLIE I. — Au reste, si l'on combine les Théorèmes que nous avons démontrés jusqu'ici avec le Lemme III, on en pourra déduire un grand nombre d'autres Théorèmes d'Arithmétique qui seraient peut-être bien difficiles à démontrer directement.

Ainsi, si p est un nombre premier d'une de ces formes $8n \pm 1$, $2^{\frac{p-1}{2}}-1$ sera divisible par p , et si p est de la forme $8n \pm 3$, $2^{\frac{p-1}{2}}+1$ sera alors divisible par p .

De même, si p est de la forme $12n \pm 1$, $3^{\frac{p-1}{2}}-1$ sera divisible par p , et si p est de la forme $12n \pm 5$, $3^{\frac{p-1}{2}}+1$ sera alors divisible par p .

Si p est d'une de ces formes $20n \pm 1$, $20n \pm 9$, $5^{\frac{p-1}{2}}-1$ sera divisible par p ; et si p est d'une de ces formes $20n \pm 3$, $20n \pm 7$, alors $5^{\frac{p-1}{2}}+1$ sera divisible par p . Et ainsi de suite.

50. SCOLIE II. — Les nombres premiers de la forme $4n+1$ sont toujours la somme de deux carrés (48); mais les nombres premiers de la forme $4n-1$ ne pouvant jamais être la somme de deux carrés, seront nécessairement la somme de trois ou de quatre carrés, puisqu'il est démontré que tout nombre entier est ou carré ou la somme de deux ou trois ou quatre carrés [voyez les *Mémoires* pour 1770 (*).]. Or je remarque que la forme $4n-1$ se réduit à ces deux-ci $8n-1$ et $8n+3$;

(*) *Oeuvres de Lagrange*, t. III, p. 189.

à l'égard des nombres premiers de la forme $8n+3$ on a prouvé qu'ils sont toujours la somme d'un carré et du double d'un carré (45); et quant à ceux de la forme $8n-1$, M. Fermat assure que le double de chacun de ces nombres est toujours aussi la somme d'un carré et du double d'un carré (voyez la *Lettre* à M. Digby citée ci-dessus, n° 36); mais ce dernier Théorème est du nombre de ceux qui restent encore à démontrer. On peut observer que la forme $8n-1$ se réduit à ces trois-ci $24n-1$, $24n+7$, $24n+15$, dont il n'y a que les deux premières qui puissent convenir à des nombres premiers; or il est déjà démontré (45) que tout nombre premier de la forme $24n+7$ est de la forme y^2+6z^2 ; donc le double d'un nombre premier de la même forme sera de la forme

$$2y^2+12z^2=(y+2z)^2+(y-2z)^2+(2z)^2,$$

c'est-à-dire la somme de trois carrés. Ainsi le Théorème dont il s'agit est démontré pour tous les nombres premiers de la forme $8n-1$ lorsque n n'est pas un multiple de 3; et il ne reste plus qu'à le démontrer pour les nombres de la forme $24n-1$; mais je ne vois pas, quant à présent, comment on y pourrait parvenir.

J'ajouterai, en finissant, que j'ai remarqué que tout nombre premier de la forme $4n-1$ est la somme d'un nombre premier de la forme $4n+1$ et du double d'un nombre premier de la même forme; ainsi

$$\begin{aligned} 3 &= 1+2.1, & 7 &= 5+2.1, & 11 &= 1+2.5, & 19 &= 17+2, \\ 23 &= 13+2.5=1+2.11, & 31 &= 29+2, & 43 &= 41+2, \\ 47 &= 37+2.5=1+2.23, \dots \end{aligned}$$

mais ce n'est que par induction que j'ai trouvé ce Théorème.



TABLE DES MATIÈRES

DU TOME TROISIÈME.

DEUXIÈME SECTION.

(SUITE.)

MÉMOIRES EXTRAITS DES RECUEILS DE L'ACADÉMIE ROYALE DES SCIENCES
ET BELLES-LETTRES DE BERLIN.

	Pages.
VII. Nouvelle méthode pour résoudre les équations littérales par le moyen des séries.	5
VIII. Sur la force des ressorts pliés.....	77
IX. Sur le Problème de Képler.....	113
X. Sur l'élimination des inconnues dans les équations.....	141
XI. Nouvelles réflexions sur les Tautochrones.....	157
XII. Démonstration d'un Théorème d'Arithmétique.....	189
XIII. Réflexions sur la résolution algébrique des équations.....	205
XIV. Démonstration d'un Théorème nouveau concernant les nombres premiers.....	425
XV. Sur une nouvelle espèce de calcul relatif à la différentiation et à l'intégration des quantités variables.....	441
XVI. Sur la forme des racines imaginaires des équations.....	479
XVII. Sur les réfractions astronomiques.....	519
XVIII. Sur l'intégration des équations à différences partielles du premier ordre.....	549
XIX. Nouvelle solution du Problème du mouvement de rotation d'un corps de figure quelconque qui n'est animé par aucune force accélératrice.....	579
XX. Sur l'attraction des Sphéroïdes elliptiques.....	619
XXI. Solutions analytiques de quelques Problèmes sur les pyramides triangulaires...	661
XXII. Recherches d'Arithmétique.....	695



TABLE DES MATIÈRES

DE TOME TROISIÈME

DEUXIÈME SECTION

MEMOIRES PRESENTES PAR MEMBRES DE L'ACADEMIE ROYALE DES SCIENCES

ET DE L'INSTITUT NATIONAL DE FRANCE

1793

1794

1795

1796

1797

1798

1799

1800

1801

1802

1803

1804

1805

1806

1807

1808

1809

1810

1811

1812

1813

1814

1815

1816

1817

1818

1819

1820

1821

1822

1823

1824

1825

1826

1827

1828

1829

1830

1831

1832

1833

1834

1835

1836

1837

1838

1839

1840

1841

1842

1843

1844

1845

1846

1847

1848

1849

1850

1851

1852

1853

1854

1855

1856

1857

1858

1859

1860

1861

1862

1863

1864

1865

1866

1867

1868

1869

1870

1871

1872

1873

1874

1875

1876

1877

1878

1879

1880

1881

1882

1883

1884

1885

1886

1887

1888

1889

1890

1891

1892

1893

1894

1895

1896

1897

1898

1899

1900

1901

1902

1903

1904

1905

1906

1907

1908

1909

1910

1911

1912

1913

1914

1915

1916

1917

1918

1919

1920

1921

1922

1923

1924

1925

1926

1927

1928

1929

1930

1931

1932

1933

1934

1935

1936

1937

1938

1939

1940

1941

1942

1943

1944

1945

1946

1947

1948

1949

1950

1951

1952

1953

1954

1955

1956

1957

1958

1959

1960

1961

1962

1963

1964

1965

1966

1967

1968

1969

1970

1971

1972

1973

1974

1975

1976

1977

1978

1979

1980

1981

1982

1983

1984

1985

1986

1987

1988

1989

1990

1991

1992

1993

1994

1995

1996

1997

1998

1999

2000

2001

2002

2003

2004

2005

2006

2007

2008

2009

2010

2011

2012

2013

2014

2015

2016

2017

2018

2019

2020

2021

2022

2023

2024

2025

2026

2027

2028

2029

2030

2031

2032

2033

2034

2035

2036

2037

2038

2039

2040

2041

2042

2043

2044

2045

2046

2047

2048

2049

2050

2051

2052

2053

2054

2055

2056

2057

2058

2059

2060

2061

2062

2063

2064

2065

2066

2067

2068

2069

2070

2071

2072

2073

2074

2075

2076

2077

2078

2079

2080

2081

2082

2083

2084

2085

2086

2087

2088

2089

2090

2091

2092

2093

2094

2095

2096

2097

2098

2099

2100

2101

2102

2103

2104

2105

2106

2107

2108

2109

2110

2111

2112

2113

2114

2115

2116

2117

2118

2119

2120

2121

2122

2123

2124

2125

2126

2127

2128

2129

2130

2131

2132

2133

2134

2135

2136

2137

2138

2139

2140

2141

2142

2143

2144

2145

2146

2147

2148

2149

2150

2151

2152

2153

2154

2155

2156

2157

2158

2159

2160

2161

2162

2163

2164

2165

2166

2167

2168

2169

2170

2171

2172

2173

2174

2175

2176

2177

2178

2179

2180

2181

2182

2183

2184

2185

2186

2187

2188

2189

2190

2191

2192

2193

2194

2195

2196

2197

2198

2199

2200

2201

2202

2203

2204

2205

2206

2207

2208

2209

2210

2211

2212

2213

2214

2215

2216

2217

2218

2219

2220

2221

2222

2223

2224

2225

2226

2227

2228

2229

2230

2231

2232

2233

2234

2235

2236

2237

2238

2239

2240

2241

2242

2243

2244

2245

2246

2247

2248

2249

2250

2251

2252

2253

2254

2255

2256

2257

2258

2259

2260

2261

2262

2263

2264

2265

2266

2267

2268

2269

2270

2271

2272

2273

2274

2275

2276

2277

2278

2279

2280

2281

2282

2283

2284

2285

2286

2287

2288

2289

2290

2291

2292

2293

2294

2295

2296

2297

2298

2299

2300

2301

2302

2303

2304

2305

2306

2307

2308

2309

2310

2311

2312

2313

2314

2315

2316

2317

2318

2319

2320

2321

2322

2323

2324

2325

2326

2327

2328

2329

2330

2331

2332

2333

2334

2335

2336

2337

2338

2339

2340

2341

2342

2343

2344

2345

2346

2347

2348

2349

2350

2351

2352

2353

2354

2355

2356

2357

2358

2359

2360

2361

2362

2363

2364

2365

2366

2367

2368

2369

2370

2371

2372

2373

2374

2375

2376

2377

2378

2379

2380

2381

2382

2383

2384

2385

2386

2387

2388

2389

2390

2391

2392

2393

2394

2395

2396

2397

2398

2399

2400

2401

2402

2403

2404

2405

2406

2407

2408

2409

2410

2411

2412

2413

2414

2415

2416

2417

2418

2419

2420

2421

2422

2423

2424

2425

2426

2427

2428

2429

2430

2431

2432

2433

2434

2435

2436

2437

2438

2439

2440

2441

2442

2443

2444

2445

2446

2447

2448

2449

2450

2451

2452

2453

2454

2455

2456

2457

2458

2459

2460

2461

2462

2463

2464

2465

2466

2467

2468

2469

2470

2471

2472

2473

2474

2475

2476

2477

2478

2479

2480

2481

2482

2483

2484

2485

2486

2487

2488

2489

2490

2491

2492

2493

2494

2495

2496

2497

2498

2499

2500

2501

2502

2503

2504

2505

2506

2507

2508

2509

2510

2511

2512

2513

2514

2515

2516

2517

2518

2519

2520

2521

2522

2523

2524

2525

2526

2527

2528

2529

2530

2531

2532

2533

2534

2535

2536

2537

2538

2539

2540

2541

2542

2543

2544

2545

2546

2547

2548

2549

2550

2551

2552

2553

2554

2555

2556

2557

2558

2559

2560

2561

2562

2563

2564

2565

2566

2567

2568

2569

2570

2571

2572

2573

2574

2575

2576

2577

2578

2579

2580

2581

2582

2583

2584

2585

2586

2587

2588

2589

2590

2591

2592

2593

2594

2595

2596

2597

2598

2599

2600

2601

2602

2603

2604

2605

2606

2607

2608

2609

2610

2611

2612

2613

2614

2615

2616

2617

2618

2619

2620

2621

2622

2623

2624

2625

2626

2627

2628

2629

2630

2631

2632

2633

2634

2635

2636

2637

2638

2639

2640

2641

2642

2643

2644

2645

2646

2647

2648

2649

2650

2651

2652

2653

2654

2655

2656

2657

2658

2659

2660

2661

2662

2663

2664

2665

2666

2667

2668

2669

2670

2671

2672

2673

2674

2675

2676

2677

2678

2679

2680

2681

2682

2683

2684

2685

2686

2687

2688

2689

2690

2691

2692

2693

2694

2695

2696

2697

2698

2699

2700

2701

2702

2703

2704

2705

2706

2707

2708

2709

2710

2711

2712

2713

2714

2715

2716

2717

2718

2719

2720

2721

2722

2723

2724

2725

2726

2727

2728

2729

2730

2731

2732

2733

2734

2735

2736

2737

2738

2739

2740

2741

2742

2743

2744

2745

2746

2747

2748

2749

2750

2751

2752

2753

2754

2755

2756

2757

2758

2759

2760

2761

2762

2763

2764

2765

2766

2767

2768

2769

2770

2771

2772

2773

2774

2775

2776

2777

2778

2779

2780

2781

2782

2783

2784

2785

2786

2787

2788

2789

2790

2791

2792

2793

2794

2795

2796

2797

2798

2799

2800

2801

2802

2803

2804

2805

2806

2807

2808

2809

2810

2811

2812

2813

2814

2815

2816

2817

2818

2819

2820

2821

2822

2823

2824

2825

2826

2827

2828

2829

2830

2831

2832

2833

2834

2835

2836

2837

2838

2839

2840

2841

2842

2843

2844

2845

2846

2847

2848

2849

2850

2851

2852

2853

2854

2855

2856

2857

2858

2859

2860

2861

2862

2863

2864

2865

2866

2867

2868

2869

2870

2871

2872

2873

2874

2875

2876

2877

2878

2879

2880

2881

2882

2883

2884

2885

2886

2887

2888

2889

2890

2891

2892

2893

2894

2895

2896

2897

2898

2899

2900

2901

2902

2903

2904

2905

2906

2907

2908

2909

2910

2911

2912

2913

2914

2915

2916

2917

2918

2919

2920

2921

2922

2923

2924

2925

2926

2927

2928

2929

2930

2931

2932

2933

2934

2935

2936

2937

2938

2939

2940

2941

2942

2943

2944

2945

2946

2947

2948

2949

2950

2951

2952

2953

2954

2955

2956

2957

2958

2959

2960

2961

2962

2963

2964

2965

2966

2967

2968

2969

2970

2971

2972

2973

2974

2975

2976

2977

2978

2979

2980

2981

2982

2983

2984

2985

2986

2987

2988

2989

2990

2991

2992

2993

2994

2995

2996

2997

2998

2999

3000

3001

3002

3003

3004

3005

3006

3007

3008

3009

3010

3011

3012

3013

3014

3015

3016

3017

3018

3019

3020

3021

3022

3023

3024

3025

3026

3027

3028

3029

3030

3031

3032

3033

3034

3035

3036

3037

3038

3039

3040

3041

3042

3043

3044

3045

3046

3047

3048

3049

3050

3051

3052

3053

3054

3055

3056

3057

3058

3059

3060

3061

3062

3063

3064

3065

3066

3067

3068

3069

3070

3071

3072

3073

3074

3075

3076

3077

3078

3079

3080

3081

3082

3083

3084

3085

3086

3087

3088

3089

3090

3091

3092

3093

3094

3095

3096

3097

3098

3099

3100

3101

3102

3103

3104

3105

3106

3107

3108

3109

3110

3111

3112

3113

3114

3115

3116

3117

3118

3119

3120

3121

3122

3123

3124

3125

3126

3127

3128

3129

3130

3131

3132

3133

3134

3135

3136

3137

3138

3139

3140

3141

3142

3143

3144

3145

3146

3147

3148

3149

3150

315





