7ème année.– n°6.– Juin 1912.–

SPHINX-ŒDIPE

Directeur Fondateur A. Gérardin

32 quai Claude-le-Lorrain, Nancy, France.

Mensuel, Théorie et Décomposition des Nombres, Analyse Indéterminée, Magie, Astronomie, Curios., Art. inéd. et rares, Trad., Quest., Rép., Concours Mens...

Abonnt annuel (Janv. Déc.) sans suppléments, France 7 frs, Etranger 8 frs (12 n°s)

" " avec tous les suppléments, France 12 frs, Etranger 13 frs 50.

Solution de quelques questions d'analyse indéterminée

par E. Aubry.

Th. I.– Si l'on a $pA^2 = qB^2 + rC^2 + sD^2 + tE^2 \ldots$

$Ba \equiv k$, $Ca \equiv l$, $Da \equiv m$, $Ea \equiv n \ldots$ (mod. A)

$$P = \frac{qk^2 + rl^2 + sm^2 + tn^2 \ldots}{A}\,; \quad Q = \frac{2(qBk + rCl + sDm + tEn \ldots)}{A}$$

l'équation $pX^2 = qY^2 + rZ^2 + sU^2 + tV^2 \ldots$ est satisfaite en entiers pour

$X = P$, $Y = \frac{BP - kQ}{A}$, $Z = \frac{CP - lQ}{A}$, $U = \frac{DP - mQ}{A}$, $V = \frac{EP - nQ}{A}$ ...

On a en effet, quels que soient a, b, c, d, e

$$p(Ax + ay)^2 = q(Bx + by)^2 + r(Cx + cy)^2 + s(Dx + dy)^2 + t(Ex + ey)^2 \ldots$$

en prenant $x = qb^2 + rc^2 + sd^2 + te^2 \ldots - pa^2$

$y = 2(pAa - qBb - rCc - sDd - tEe \ldots)$

Posons en particulier $b = \frac{Ba - k}{A}$, $c = \frac{Ca - l}{A}$, $d = \frac{Da - m}{A}$, $e = \frac{Ea - n}{A}$.

b, c, d, e, sont entiers, puisque, d'après l'énoncé, $Ba - k$, $Ca - l$, $Da - m$, $Ea - n \ldots \equiv 0$ (mod. A); par suite $Ax + ay$, $Bx + by$, $Cx + cy$, $Dx + dy$, $Ex + ey \ldots$ sont également entiers, et en y remplaçant x, y, b, c, d, e, par les valeurs précédentes, on trouve bien, après simplification, les valeurs données dans l'énoncé pour X, Y, Z, U, V.

Th. II.– Si $pA^2 = B^2 + C^2 + D^2$, on a aussi $p = Y^2 + Z^2 + U^2$

(E. Lemoine, I.M. quest. 45; 1894, 19)

On peut supposer A, B, C, D premiers entre eux dans leur ensemble, sinon on les diviserait par leur facteur commun; et si dans le Th. I, on fait $q = r = s = 1$, $t = 0$, $a = 1$, et k, l, m positifs ou négatifs $\leq \frac{A}{2}$ en valeur absolue, ce qui est toujours possible, k, l et m ne sont pas tous les 3 égaux à zéro, puisque A, B, C, D, sont premiers entre eux dans leur ensemble, et l'on a $P = \frac{k^2 + l^2 + m^2}{A} \leq \frac{3}{A} \cdot \frac{A^2}{4} < A$, mais ≥ 1.

Par suite, si l'équation (1) $pX^2 = Y^2 + Z^2 + U^2$ est satisfaite pour $X = A$, il résulte du Th. I qu'elle est également satisfaite pour $X = P = A_2 < A$ mais ≥ 1, puis, en continuant le même raisonnement, on verrait de même que l'équation (1) est encore satisfaite pour $X = A_3 < A_2$ et ≥ 1 ; $X = A_4 < A_3$ et ≥ 1, .. et enfin pour $X = 1$, puisque les nombres $A_1, A_2, A_3, A_4 \ldots$ diminuent de plus en plus, mais sont cependant toujours ≥ 1.

2h. III.- Si $pA^2 = B^2 + C^2 + D^2 + E^2$, on a aussi $p = Y^2 + Z_1^2 + U^2 + V^2$.
On démontre exactement comme ci-dessus que l'on a, avec X égal à 1 ou 2, $pX^2 = Y^2 + Z_1^2 + U^2 + V^2$; si $X = 2$, Y, Z_1, U, V sont impairs, et l'on a $p = Y'^2 + Z_1'^2 + U'^2 + V'^2$, en posant
$4Y' = Y \pm Z_1 \pm U \pm V$, $4Z_1' = Y \pm Z_1 \mp U \pm V$, $4U' = Y \mp Z_1 \pm U \pm V$, $4V' = Y \mp Z_1 \mp U \mp V$.
Y', Z', U', V' sont entiers en prenant le signe convenable.
Corollaire.- Tout nombre est décomposable en 4 carrés entiers (2h. de Bachet).
Soit, s'il est possible, un nombre N non décomposable en 4 carrés ; on peut démontrer que N divise la forme $X^2 + Y^2 + Z_1^2 + U^2$ dans laquelle X, Y, Z, U sont $< \frac{1}{2}N$. On a donc $\frac{1}{N}(X^2 + Y^2 + Z^2 + U^2) = N_2 < \frac{4}{N} \cdot \frac{N^2}{4} < N$.
On ne peut avoir $N_2 = a^2 + b^2 + c^2 + d^2$; sinon, on aurait au moyen de l'identité d'Euler

$$N N_2^2 = (X^2 + Y^2 + Z_1^2 + U^2)(a^2 + b^2 + c^2 + d^2) = X'^2 + Y'^2 + Z_1'^2 + U'^2$$

d'où, par suite du th. ci-dessus, N serait décomposable en 4 carrés.
Donc il existait un nombre N non décomposable en 4 carrés, il y en aurait un plus petit N_2 de même nature, puis un autre $N_3 < N_2$ et ainsi de suite, puis finalement le nombre 1, ce qui serait absurde.

2h. IV.- Si $pA^2 = B^2 + rC^2$, on a aussi $pX^2 = Y^2 + rZ_1^2$; $X \leqq 2\sqrt{\frac{r}{3}}$ pour r positif, ou $X \leqq \sqrt{r}$ pour r négatif ; $Y \equiv Ba$, $Z_1 \equiv Ca \pmod{p}$
Soit $d \geqq 1$ le plus grand commun diviseur de A et C ; on a $A = A'd$, $C = C'd$ A' premier avec C' ; on a nécessairement aussi $B = B'd$, d'où $pA'^2 = B'^2 + rC'^2$, et en posant $f \equiv \frac{1}{d} \pmod{p}$, on a aussi $B' = \frac{B}{d} \equiv Bf$, $C' = \frac{C}{d} \equiv Cf \pmod{p}$. A' étant premier avec C', on peut déterminer a tel que $C'a \equiv l \equiv 1 \pmod{A'}$, et prendre $k \leqq \frac{1}{2}A'$ et $\equiv B'a \pmod{A'}$. Par suite, d'après le 2h. I, l'équation $pX^2 = Y^2 + rZ_1^2$ est satisfaite pour les valeurs suivantes

$$X = A_2 = \frac{k^2 + rl^2}{A'} = \frac{k^2 + r}{A'}, \text{ puisque } l = 1$$

$$Y = B_2 = \frac{B'P - kQ}{A'} = \frac{B'}{A'^2}\left(rl^2 - k^2 - 2\frac{C'}{B'}rkl\right)$$

$$Z = C_2 = \frac{C'P - lQ}{A'} = \frac{C'}{A'^2}\left(k^2 - rl^2 - 2\frac{B'}{C'}kl\right)$$

Or, puisque $k \geqq \frac{A'}{2}$, il est facile de démontrer que $A_2 = \frac{k^2 + r}{A'}$ est $< A'$ ou que $A' \leqq 2\sqrt{\frac{1}{3}r}$ pour r positif ou $\leqq \sqrt{r}$ pour r négatif.
De $pA'^2 = B'^2 + rC'^2$, on déduit $\frac{B'}{C'} \equiv -r\frac{C'}{B'} \pmod{p}$; on a donc

$$C_2 = \frac{C'}{A'^2}\left(k^2 - rl^2 - 2\frac{B'}{C'}kl\right) \equiv \frac{C'}{A'^2}\left(k^2 - rl^2 + 2\frac{C'}{B'}rkl\right) \pmod{p}$$

et en posant $\frac{1}{A'^2}\left(k^2 - rl^2 + 2\frac{C'}{B'}rkl\right) \equiv g \pmod{p}$, on a
$B_2 \equiv B'g \equiv Bfg$, $-C_2 \equiv C'g \equiv Cfg \pmod{p}$.
Si l'équation (1) est satisfaite pour $X = A$, $Y = B$, $Z_1 = C$, on voit donc qu'elle est satisfaite également pour $X = A_2 < A$, $Y = B_2 \equiv Bfg$, $Z_1 = -C_2 \equiv Cfg \pmod{p}$, ou pour $X = A' \leqq 2\sqrt{\frac{1}{3}r}$ pour r positif, ou $\leqq \sqrt{r}$ pour r négatif ; $Y = B' \equiv Bf$, $Z_1 = C' \equiv Cf \pmod{p}$
En continuant le même raisonnement, on verrait de même que l'équation (1) est encore satisfaite pour $X = A_3 < A_2$,
$Y = B_3 \equiv B_2 f_2 g_2 \equiv Bfgf_2g_2$, $Z_1 = C_3 \equiv C_2 f_2 g_2 \equiv Cfgf_2g_2 \pmod{p}$

ou pour $A'_2 \leqq 2\sqrt{\frac{1}{3}r}$ pour r positif ou $\leqq \sqrt{r}$ pour r négatif,
$Y = B'_2 \equiv B_2 f_2 \equiv B f g f_1$, $Z_1 = C'_2 \equiv C_2 f_2 \equiv C f g f_2$ (mod. p)
puis pour $X = A_4 < A_3$ etc. et l'on voit finalement que l'équation (1) est bien satisfaite pour $X \leqq 2\sqrt{\frac{r}{3}}$ pour r positif ou $\leqq \sqrt{r}$ pour r négatif, puisque dans la suite $A_1 A_2 \dots A_i$, on a $A_i < A_{i-1}$ ou $A_{i-1} \leqq 2\sqrt{\frac{1}{3}r}$ pour r positif ou $\leqq \sqrt{r}$ pour r négatif, et l'on a bien aussi $Y \equiv Ba$, $Z_1 \equiv Ca$ (mod. p), puisque $Y \equiv B f g f_2 g_2 \dots$ $Z_1 \equiv C f g f_2 g_2 \dots$ (mod. p)

Corollaire 1.— Si $pA^2 = B^2 + rC^2$ pour $r = 1, 2$ ou 3, on a aussi

$$p = Y^2 + rZ_1^2 \qquad Y \equiv Ba, \quad Z_1 \equiv Ca \pmod{p}$$

Si $r = 1$ ou 2, on a d'après le Th. précédent $X \leqq 2\sqrt{\frac{2}{3}} < 2$, d'où $X = 1$; si $r = 3$, on a $X = 1$ ou 2 ; pour $X = 2$, on a $p \cdot 2^2 = Y^2 + 3Z_1^2$, d'où $p = Y'^2 + 3Z'^2$ en posant $4Y' = Y \pm 3Z_1$, $4Z'_1 = Z_1 \mp Y$; en prenant le signe convenable, Y' et Z'_1 sont entiers, et l'on a, en remarquant que $\frac{Y}{Z_1} \equiv -3\frac{Z_1}{Y} \pmod{p}$ et en posant $\frac{a}{4}\left(1 \pm 3\frac{Z_1}{Y}\right) \equiv a' \pmod{p}$,

$$Y' \equiv Ba', \quad Z' \equiv Ca' \pmod{p}$$

Corollaire 2.— Si $p = 1$, la méthode ci-dessus permet d'obtenir une solution de l'équation $Y^2 - rZ_1^2 = 1$ (équation de Fermat) en partant de $B^2 - r = 1 \cdot A^2$ ou, si r est simplement pair, de $B^2 - 4r = 1 \cdot A^2$. Si, en particulier, r est un nombre premier de la forme $4n+1$, on en déduit facilement que l'équation $ru^2 = v^2 + 1$ est toujours possible, et par suite du th. ci-dessus que r est de la forme $x^2 + y^2$.

Th. V.— Si l'on a $p = a^2 + rb^2 = c^2 + rd^2$, r positif
$a \equiv Bh$, $b \equiv Ch$, $c \equiv Bg$, $d \equiv Cg \pmod{p}$, on a $b = d$, $a = c$, ou si $r = 1$, on peut avoir aussi $a = \pm d$, $b = \mp c$.

On a, en effet, $ad - bc \equiv Bh \cdot Cg - Ch \cdot Bg \equiv 0 \pmod{p}$, d'où puisque a, b, c, d sont $< \sqrt{p}$, $ad - bc = 0$ ou $\pm p$. Si l'on a
(α) $ad - bc = 0$, on trouve

$$p^2 = (a^2 + rb^2)(c^2 + rd^2) = (ac + rbd)^2 + r(ad - bc)^2 = (ac + rbd)^2$$

d'où (β) $ac + rbd = p$; on déduit de (α) et (β)
$pd = b(c^2 + rd^2)$ d'où $d = b$, puisque $c^2 + rd^2 = p$, puis $a = c$, à cause de (α). — Avec $ad - bc = \pm p$, on a

$$p^2 = (ac + rbd)^2 + r(ad - bc)^2 = (ac + rbd)^2 + rp^2$$

ce qui est impossible pour $r > 1$ et qui exige si $r = 1$,
$ac + bd = 0$, d'où $a = \pm d$, $b = \mp c$.

Th. VI.— Si l'on a $A = k^2 + rl^2$, $A^3 = B^2 + rC^2$ pour $r = 1, 2$ ou 3, on a
$-B = k^3 - 3krl^2$, $-C = 3k^2 l - rl^3$

Si dans le Th. 4, Coroll. 1, on fait $p = A$, on a
$A = Y^2 + rZ_1^2$, $Y \equiv Ba$, $Z_1 \equiv Ca$. (mod. $p = A$)
Soient donc $Y = k$, $Z_1 = l$; on a $A = k^2 + rl^2$, $k \equiv Ba$, $l \equiv Ca$ (mod. A) ; on déduit donc du Th. I que l'équation $AX^2 = y^2 + rZ_1^2$ est satisfaite pour $X = \frac{k^2 + rl^2}{A} = 1$,

$$Y = \frac{B(k^2 + rl^2) - 2k(kB + rCl)}{A^2} = k' \qquad (\gamma)$$

$$Z_1 = \frac{C(k^2 + rl^2) - 2l(kB + rCl)}{A^2} = l' \qquad (\delta)$$

et par un raisonnement identique à celui du Th. IV, on déduit aussi que $k' \equiv Bf$, $-l' \equiv Cf$ (mod. A) ; on a donc ainsi

$A = k^2 + r\ell^2 = k'^2 + r(-\ell')^2$, $k \equiv Ba$, $\ell \equiv Ca$, $k' \equiv Bf$, $-\ell' \equiv Cf$ (mod. A); du Th. V, on déduit donc $k = k'$, $\ell = -\ell'$, et par suite, à cause de (γ) et (δ)

$$B(r\ell^2 - k^2) - C(2rk\ell) = kA^2 = k(k^2 + r\ell^2)^2$$
$$C(k^2 - r\ell^2) - B(2k\ell) = -\ell A^2 = -\ell(k^2 + r\ell^2)^2 \qquad (3)$$

Multiplions (ε) par $k^2 - r\ell^2$, (ζ) par $2k\ell$; on trouve après addition et réduction

$$-B(r\ell^2 - k^2)^2 - B(4rk^2\ell^2) = -B(k^2 + r\ell^2)^2 = (k^3 - 3rk\ell^2)(k^2 + r\ell^2)^2$$

d'où $-B = k^3 - 3kr\ell^2$

On trouverait de même $-C = 3k^2\ell - r\ell^3$, en multipliant (ε) par $2k\ell$ et (ζ) par $r\ell^2 - k^2$.

Corollaire 1.- Le nombre 25 est le seul carré entier qui, augmenté de 2, fasse un cube.

Soit en effet $A^3 = B^2 + 2.1^2$. Puisque $r = 2$, on a d'après le Th. précédent $-1 = 3k^2\ell - 2\ell^3$, $-B = 6k\ell^2 - k^3$

la première égalité exige évidemment $\ell = -1$, $k = 1$, d'où $B = -5$.

Corollaire 2.- Si $x^2 + 3y^2 = z^3$, on a

$x = m^3 - 9mn^2$, $y = 3m^2n - 3n^3$, $z = m^2 + 3n^2$

(É. Dubouis. I.M., q. 3662, 1910, 49)

En faisant $r = 3$ dans le Th. ci-dessus, on retrouve bien les valeurs de x, y, z signalées, et d'ailleurs connues depuis longtemps.

Remarque.- Au moyen de ce corollaire, on démontre par la descente l'impossibilité en entiers de $x^3 + y^3 + z^3 = 0$

(Cf. Legendre, Théorie des Nombres, t. II, p. 9).

Décomposition des grands nombres en leurs facteurs

par Seelhoff, de Brême.

(Extr. du Zeitschrift für Math. u. Physik, 31e année, 3e livr. [1885-1886] trad. par M. Delannoy trouvée dans les archives d'Éd. Lucas que M. C. A. Laisant a eu l'amabilité de me faire parvenir et que nous éditerons pour le plaisir des arithmologues)

La méthode que j'expose ci-après, pour décomposer de grands nombres en leurs facteurs, subsiste jusqu'à $2^{64} + 1$, pour tous les cas où je l'ai employée. Le dernier nombre dont je ne connaissais pas la décomposition par M. Landry, m'a précisément fourni l'occasion de développer la méthode que j'avais employée pour des nombres tels que $2^{47} - 1$, $2^{53} - 1$ etc, et d'arriver à un résultat certain. Je présente cette méthode sous la forme ainsi obtenue.

Appelons N le nombre dont on cherche les facteurs et posons $N = \omega^2 + r$. Admettons que pour un nombre premier p [on a] $N \equiv \rho \pmod{p}$, ρ étant un reste quadratique pour p, de sorte que $\omega_1^2 \equiv \rho \pmod{p}$. On peut alors écrire l'égalité suivante $N \equiv \omega_1^2 + (\omega + \omega_1)(\omega - \omega_1) + r$

Désignons par δ la réunion du 2e et du 3e terme du 2e membre, c.à.d. posons $\delta = \omega^2 + r - \omega_1^2$. On a

$$\omega^2 + r \equiv \rho \pmod{p}$$
$$-\omega_1^2 \equiv -\rho \pmod{p}$$

par conséquent $\delta = \omega^2 + r - \omega_1^2 \equiv 0 \pmod{p}$

Si l'on remplace la racine ω_1 par l'expression plus générale $\omega_1 + py$, on a