QUOI DE NEUF CONCERNANT LES TRIANGLES RECTANGLES?

(2e partie)

Alain ROBERT

3.— NOMBRES CONGRUENTS

FERMAT a démontré que l'aire d'un triangle rectangle à côtés entiers n'est jamais un carré parfait $S \neq \square$. Il l'a fait par "*descente infinie*" dans la fameuse marge de son exemplaire du DIOPHANTE …(une démonstration élémentaire se trouve dans J. ITARD, (cf. Bibliographie).

Similairement,

$$S \neq 2 \ \square \qquad \text{(VIÈTE, BACHET)},$$
$$S \neq 3 \ \square \qquad \text{(LUCAS)}.$$

Considérons maintenant le triangle rectangle obtenu par la méthode de PYTHAGORE avec

$$a = 9, \quad a^2 = 81 = 2 \times 40 + 1, \quad b = 40 \text{ et } c = 41.$$

Son aire est

$$S = 9 \times 20 = 5 \times 36 = 5 \times \square \ .$$

En divisant par 6 les dimensions linéaires de ce triangle, on aboutit au triangle rationnel

$$a = 3/2, \quad b = 20/3 \quad et \quad c = 41/6$$

d'aire entière $S = 5$. Ce triangle avait déjà été construit par FIBONACCI (Leonardo PISANO) (1220). Comme on l'a vu, l'aire d'un triangle rectangle entier est un nombre pair, donc $S = 5$ ne peut être l'aire d'un triangle rectangle entier. Le résultat de FERMAT montre que $S \neq 1$ pour tout triangle rectangle rationnel (donc aussi $S \neq 4$ pour tout triangle rectangle rationnel). Avec les résultats de BACHET, VIÈTE et LUCAS, on voit donc que

5 est le plus petit entier qui apparaît comme aire d'un triangle rectangle à côtés rationnels.

Quels sont les entiers qui apparaissent comme aires possibles de tels triangles?

Classiquement, ces entiers sont appelés **nombres congruents**. Donnons-en une caractérisation arithmétique. La relation

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

montre que

$$c^2 \pm 2ab = (a \pm b)^2.$$

En travaillant avec des nombres rationnels a, b et c, on peut diviser par 4 cette relation et obtenir

$$(c/2)^2 \pm S = [(a \pm b)/2]^2.$$

Les nombres congruents sont les entiers $S > 0$ tels qu'il existe trois nombres rationnels α, β et γ avec

$$\gamma^2 - S = \alpha^2 \quad \text{et} \quad \gamma^2 + S = \beta^2.$$

Les trois carrés rationnels α^2, γ^2 et β^2 sont à égale distance S l'un de l'autre. Léonardo PISANO écrivait par exemple

$$(3 + \frac{1}{4} + \frac{1}{6})^2 + 5 = (4 + \frac{1}{12})^2,$$
$$(3 + \frac{1}{4} + \frac{1}{6})^2 - 5 = (2 + \frac{1}{3} + \frac{1}{4})^2.$$

On sait aujourd'hui que les équations :

$$\gamma^2 - 5 = \alpha^2 \quad \text{et} \quad \gamma^2 + 5 = \beta^2$$

n'ont que quatre solutions en nombres rationnels ayant des numérateurs et dénominateurs à moins de 50 chiffres! D'autre part, ces équations ont une infinité de solutions rationnelles. Depuis plusieurs siècles, les mathématiciens ont essayé de trouver les plus petits nombres congruents et EULER semble avoir été le premier à donner un triangle rectangle rationnel d'aire 7 : il s'agit de

$$a = 24/5, \quad b = 35/12 \quad \text{et} \quad c = 337/60.$$

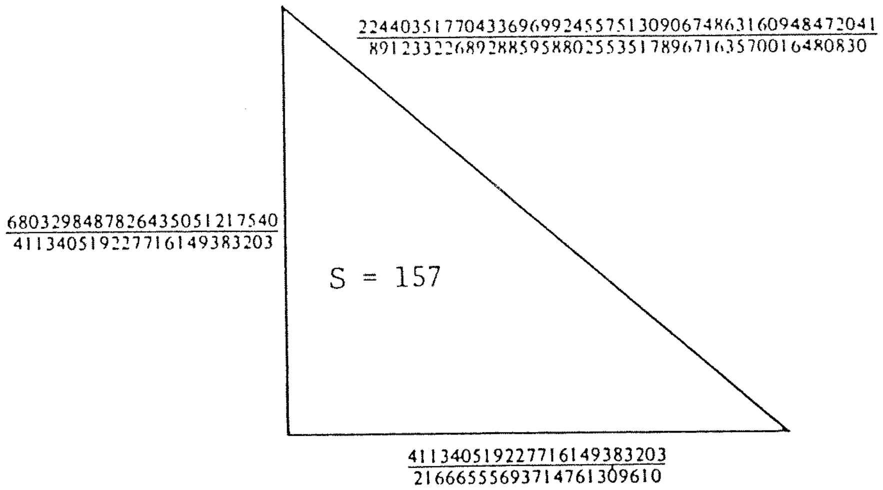
Les premiers nombres congruents sont ainsi

$$5, \quad 6, \quad 7, \ldots$$

Voici un triangle rectangle

$$a = 6 + \frac{3}{20}, \quad b = 13 + \frac{1}{3} \quad \text{et} \quad c = 14 + \frac{41}{60}$$

dont l'aire est $S = 41$. Donc 41 est un nombre congruent! On peut montrer que 157 est un nombre congruent : le triangle rectangle rationnel le plus simple ayant pour aire 157 a été déterminé par D. ZAGIER.



On conçoit bien maintenant la difficulté de déterminer les nombres congruents! On appréciera donc d'autant mieux le critère fourni par TUNNEL (Princeton) en 1983. Voici comment il s'énonce. Considérons les deux séries

$$\begin{aligned}\theta(x) &= \Sigma_{-\infty}^{\infty} x^{n^2} = 1 + 2\Sigma_{n>1} x^{n^2} = \\ &= 1 + 2x + 2x^4 + 2x^9 + \cdots \\ g(x) &= x\Pi_{n>1}(1 - x^{8n})(1 - x^{16n})\end{aligned}$$

puis les deux développements

$$\begin{aligned}g(x)\theta(x^2) &= x + 2x^3 + x^9 - 2x^{11} - \ldots = \Sigma_{n>1} a_n x^n, \\ g(x)\theta(x^4) &= x + 2x^5 - x^9 - 2x^{13} + \cdots \\ &= \Sigma_{n>1} b_n x^n.\end{aligned}$$

Alors TUNNEL démontre le résultat suivant.

THÉORÈME. *Soit n un entier positif sans facteur carré. Alors :*

$$\begin{aligned}a_n \neq 0 &\Longrightarrow n \textit{ n'est pas congruent}, \\ b_n \neq 0 &\Longrightarrow 2n \textit{ n'est pas congruent}.\end{aligned}$$

Ainsi, par exemple, $a_1 = 1$ montre que 1 n'est pas congruent (FERMAT). De même $b_1 = 1 \Longrightarrow 2$ n'est pas congruent, $a_3 = 2 \Longrightarrow 3$ n'est pas congruent. Comme $4 = \square$ ce n'est pas un nombre congruent non plus!

Pour démontrer ce théorème, TUNNEL se base sur des résultats récents obtenus dans la théorie des courbes cubiques (aussi appelées courbes elliptiques (cf. ci-dessous)) par différents mathématiciens (SHIMURA, WALDSPURGER, GROSS, ...). Une célèbre conjecture formulée par BIRCH et SWINNERTON-DYER permettrait de démontrer que les conditions données par TUNNEL caractérisent entièrement les nombres congruents, justifiant l'appellation de "*critère*" parfois donnée au théorème de TUNNEL. Précisément cette conjecture permettrait de montrer qu'inversement

$$n \text{ impair sans facteur carré et } a_n = 0 \Longrightarrow n \text{ congruent},$$
$$n \text{ pair sans facteur carré et } b_{n/2} = 0 \Longrightarrow n \text{ congruent}.$$

Remarquons encore que l'ensemble des triangles rectangles rationnels est dénombrable. On peut donc en dresser une liste exhaustive en établissant pour chacun d'entre eux la surface. On obtiendra ainsi une liste de tous les nombres congruents ...Mais si n est un entier donné (positif sans facteur carré, par exemple 157) on se sait pas a priori combien de temps attendre pour le voir apparaître ou pour décider qu'il n'apparaîtra plus! A cet égard, le théorème de TUNNEL donne une condition extrêmement simple pour démontrer qu'un entier n'est pas congruent. Pour un entier n grand, on peut même remarquer qu'il existe un logiciel "*MacSyma*" permettant d'effectuer des calculs littéraux et qui serait capable de donner rapidement les coefficients a_n et b_n.

4.— RELATION AVEC LES COURBES ELLIPTIQUES

Le problème de savoir si un entier S (positif, sans facteur carré) est un nombre congruent se ramène à un problème diophantien sur une cubique. Voici pourquoi. Dire que S est congruent revient à dire que le système d'équations

$$x = \square \ , \quad x + S = \square \quad \textit{et} \quad x - S = \square$$

possède une solution rationnelle $x \in \mathbb{Q}$. Lorsque ceci est le cas, il est clair que

$$x(x+S)(x-S) = x(x^2 - S^2)$$

est un carré rationnel > 0 et donc on peut trouver un couple (x, y) formé de nombres rationnels satisfaisant

$$y^2 = x(x^2 - S^2) \quad \textit{et} \quad y > 0.$$

Autrement dit, on peut trouver un point à coordonnées rationnelles sur la cubique d'équation

$$y^2 = x(x^2 - S^2),$$

point qui ne soit pas sur l'axe des x. Inversement, tout point (x, y) à coordonnées rationnelles et $y > 0$ sur cette cubique fournit un triangle rectangle rationnel d'aire S selon les formules

$$a = \frac{|S^2 - x^2|}{y}, \quad b = \frac{2|x|S}{y} \quad \text{et} \quad c = \frac{S^2 + x^2}{y}.$$

Résumons

THÉORÈME. *Soit $S > 0$ un entier sans facteur carré. Alors les propriétés sont équivalentes :*

i) Il existe un triangle rectangle à côtés rationnels et d'aire S.

ii) S est un nombre congruent, i.e. il existe trois nombres rationnels α, β et γ avec

$$\gamma^2 - S = \alpha^2 \quad \text{et} \quad \gamma^2 + S = \beta^2.$$

iii) Sur la cubique d'équation

$$y^2 = x(x^2 - S^2)$$

il y a un point $P = (x, y)$ à coordonnées x et y rationnelles avec $y \neq 0$.

Par exemple, le point de coordonnées

$$x = 41^2/7^2, \quad y = 2^4 \times 3^2 \times 5 \times 41/7^3$$

est sur la cubique

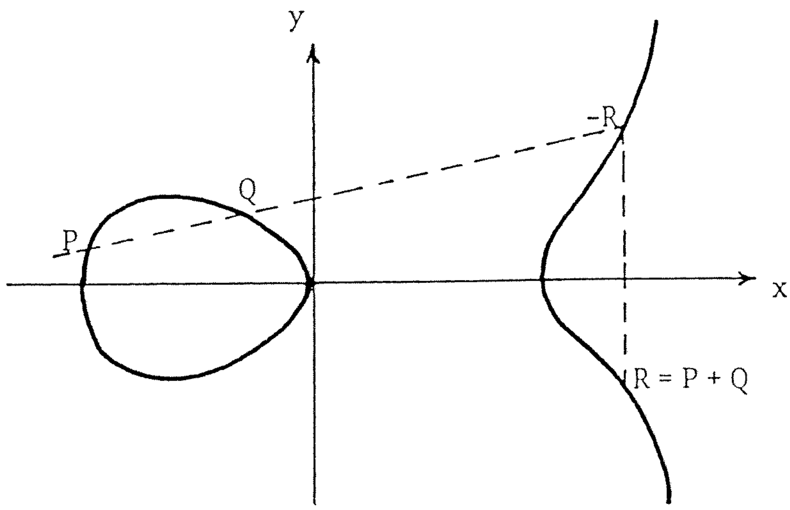
$$y^2 = x(x^2 - 31^2).$$

Donc 31 est un nombre congruent!

Revenons à l'étude d'une cubique de la forme

$$y^2 = x(x^2 - S^2)$$

où S est fixé. Il est facile de se faire une idée de l'ensemble des couples $P = (x, y)$ à coordonnées réelles sur cette cubique. Cette courbe est symétrique relativement à l'axe des x et on trouve deux points $(x, \pm y)$ au-dessus des valeurs de x rendant strictement positive $x(x^2 - S^2)$. On trouve donc des valeurs au-dessus des valeurs de $x \in [-S, 0]$ et $x \in [S, \infty]$.



On sait depuis le XIX$^{\text{e}}$ siècle que si on ajoute un point à l'infini jouant le rôle d'élément neutre, l'ensemble des points (réels) sur la cubique est un groupe abélien pour la loi d'addition donnée par
a) $P_1 + P_2 + P_3 = e = (\infty) \Longleftrightarrow P_1, P_2$ et P_3 alignés,
b) $P = (x, y) \Longleftrightarrow -P = (x, -y)$.

En d'autres termes, la somme de deux points P et Q sur la cubique s'obtient en prenant le symétrique R du troisième point d'intersection avec la droite reliant P et Q (cf. dessin). Lorsque $P = Q$, la droite les reliant est naturellement remplacée par la tangente en P à la cubique : le point $2P = P + P$ est donc le symétrique du troisième point d'intersection de la tangente en P à la cubique.

Remarque. Lorsque S est un nombre rationnel, il est facile de voir que si P et Q ont des coordonnées rationnelles, il en est de même de $P + Q$ (même si $P = Q$) et l'ensemble des points à coordonnées rationnelles forme un sous-groupe de l'ensemble des points à coordonnées réelles sur la cubique. On a vu comment à tout point rationnel $P = (x, y)$ avec $y > 0$, on peut associer un triangle rectangle rationnel d'aire S. De plus, on a aussi montré comment à ce triangle rectangle rationnel, on peut associer un point rationnel sur la cubique. Les calculs montrent qu'on obtient en fait le point $2P$.

Résultats. *Supposons que S est un entier sans facteur carré. Alors le groupe des points rationnels sur la cubique $y^2 = x(x^2 - S^2)$ est un groupe de type fini isomorphe au produit du groupe d'ordre 4 : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par un groupe libre $\mathbb{Z}^r$ (r entier > 0).*

Le sous-groupe d'ordre 4 est constitué du point à l'infini (également neutre) et des trois points d'intersection avec l'axe des x. On trouvera donc un point rationnel sur la cubique avec $y > 0$ précisément lorsque $r > 0$, i.e. lorsque le groupe formé des points rationnels est infini. Les trois conditions du théorème ci-dessus sont donc encore équivalentes à :

iv) Sur la cubique d'équation $y^2 = x(x^2 - S^2)$ il y a une infinité de points à coordonnées x et y rationnelles.

C'est la détermination de l'invariant r, rang du groupe des points à coordonnées rationnelles sur la cubique, qui est si difficile. On ne connaît pas d'algorithme effectif pour calculer r en fonction de S ... autre que celui donné par la conjecture de BIRCH et SWINNERTON-DYER (et qu'il serait même trop difficile d'expliquer ici ...).

Il est aussi très intéressant de considérer les points $P(x, y)$ à coordonnées complexes sur la cubique

$$y^2 = x(x^2 - S^2).$$

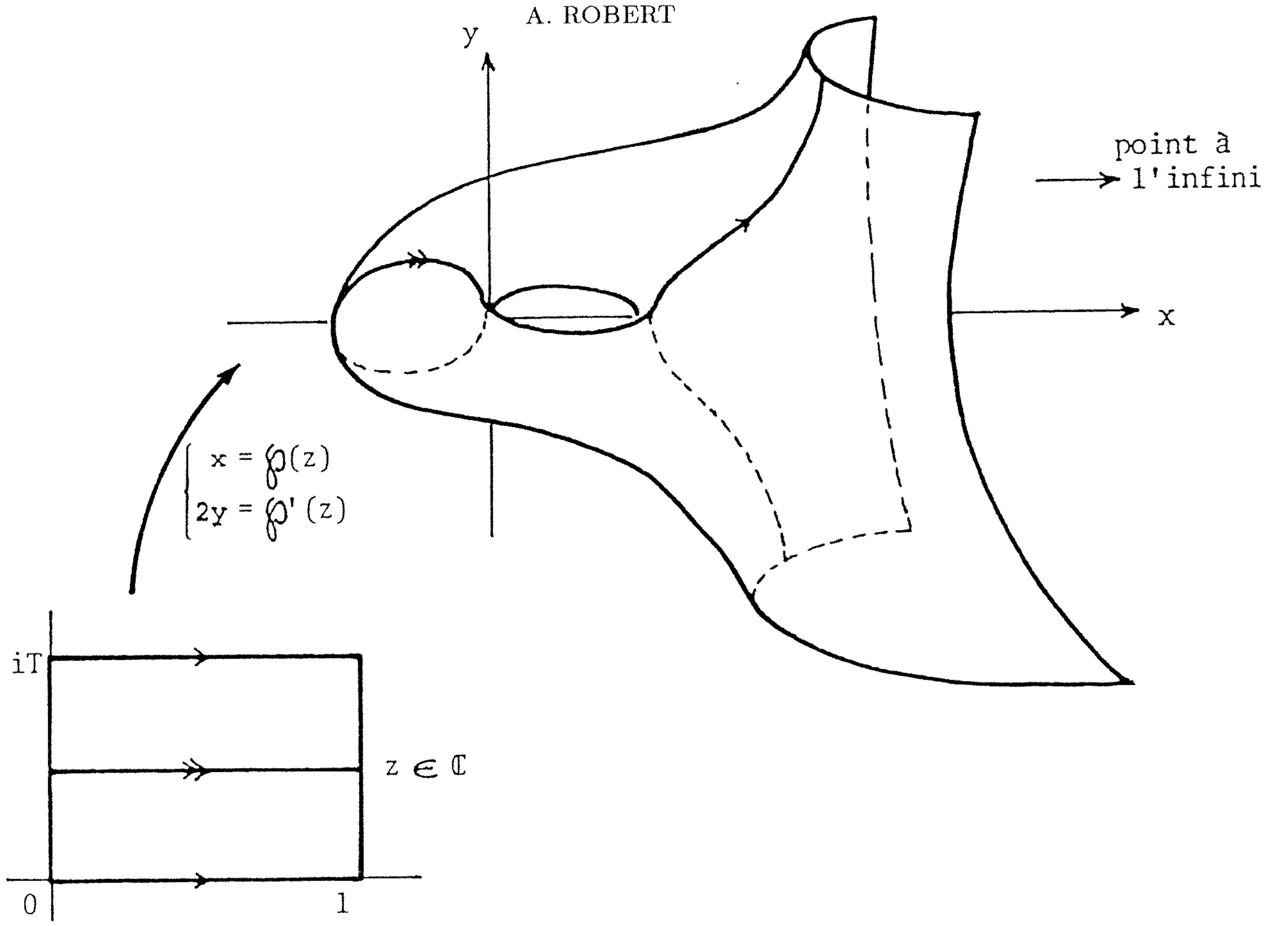
Ces points forment aussi un groupe dont la structure peut se déterminer par la paramétrisation suivante. Pour chaque $T > 0$, WEIERSTRASS a construit une fonction transcendante, classiquement dénotée par $\mathcal{P}$ qui est bi-périodique dans le sens suivant

$$\mathcal{P}(z+1) = \mathcal{P}(z) = \mathcal{P}(z+iT)$$

et qui présente un pôle double en chaque point du réseau $\mathbb{Z} + iT\mathbb{Z} \subset \mathbb{C}$ (on devrait donc dénoter $\mathcal{P} = \mathcal{P}_T$). La dérivée de $\mathcal{P}$ a les mêmes propriétés de périodicité que $\mathcal{P}$ (mais présente des pôles triples où $\mathcal{P}$ avait des pôles doubles!). Il se trouve que

$$z \longmapsto (\mathcal{P}(z), \frac{1}{2}\mathcal{P}'(z)) = (x, y)$$

est une paramétrisation des points complexes sur une cubique $y^2 = x(x^2 - S^2)$ où S est une fonction de T. Dans cette paramétrisation, le point $z = 0$ (ou n'importe quel point z du réseau $\mathbb{Z} + iT\mathbb{Z}$) est envoyé sur le point à l'infini de la cubique et la somme dans $\mathcal{C}$ correspond à la somme sur la cubique par cette paramétrisation! Le groupe des points complexes sur la cubique est ainsi isomorphe au groupe additif $\mathcal{C}$ modulo le réseau $\mathbb{Z} + iT\mathbb{Z}$. C'est donc un tore (produit du cercle $\mathbb{R}/\mathbb{Z}$ par lui-même $i\mathbb{R}/iT\mathbb{Z}$). On peut même se représenter la situation intuitivement. L'ensemble des points complexes $(x, y) \in \mathbb{C}^2$ situés sur la cubique est une surface réelle dans $\mathbb{C}^2 \cong \mathbb{R}^4$. Par une projection convenable sur un sous-espace $\mathbb{R}^3$, on peut voir que cette surface est un tore topologique. On peut même prendre un sous-espace de dimension 3 contenant les deux axes réels $\mathbb{R} \times \{0\}$ et $\{0\} \times \mathbb{R}$ dans $\mathbb{C}^2$ et contenant donc le sous-espace $\mathbb{R}^2$ dans lequel on trouve les points à coordonnées réelles. Voici une illustration :



La situation est comparable à celle de la paramétrisation d'une équation $x^2+y^2=1$ (cercle) par les fonctions trigonométriques usuelles $x = \cos z$, $y = \sin z$. Ces dernières présentent aussi une périodicité importante!

WEISTRASS a d'abord rencontré les fonctions $\mathcal{P}$ en essayant de calculer la longueur d'un arc d'ellipse, d'où le nom de "*fonctions elliptiques*" donné à ces fonctions. Le terme "*elliptique*" a ensuite été appliqué aux courbes paramétrées par ces fonctions elliptiques : en particulier, toutes les courbes cubiques planes non singulières sont des courbes elliptiques.

C'est l'étude des courbes elliptiques qui a tant progressé depuis 1960 qui a permis à TUNNEL d'obtenir son critère remarquable!

RÉFÉRENCES

La théorie élémentaire des nombres, triples pythagoriciens entre autres, est remarquablement bien expliquée dans

G.-H. HARDY, E.-M. WRIGHT : *The Theory of Numbers.* Oxford at the Clarendon Press, nouveau tirage (1975).

On trouve une démonstration du fait que l'aire d'un triangle rectangle entier n'est jamais un carré dans
J. ITARD : *Arithmétique et Théorie des Nombres.* Que sais-je? n°: 1093, P.U.F. (1967).

Voici la référence à l'article de base :
J.-B. TUNNEL : *A Classical Diophante Problem and Modular Forms of Weight 3/2.* Invent. Math 72 (1983) pp. 323–334.

Un survol de résultats préliminaires est donné dans
J. COATES : *The Work of Gross and Zagier on ...* Sém. Bourbaki, (Nov. 1984), exposé 635 (à paraître dans "*Astérisque*").

Voici un livre qui expose systématiquement toute la théorie utilisée par TUNNEL :
N. KOBLITZ : *Introduction to Elliptic Curves and Modular Forms*, Springer Verlag (1984), Graduate Text in Math. Nb. 97.

Un autre exposé introductif à la théorie des fonctions et courbes elliptiques est :
A. ROBERT : *Elliptic Curves*, Springer Verlag, Lect. Note in Math. N° 326, 2nd corrected ed. (1985).

MATHS SANS FRONTIÈRES

... ou une recette peu ordinaire pour un menu de compétition.

Recette :

Prenez 30 élèves du Collège Foch de Haguenau, de préférence; mettez-les dans une salle de classe.
Ajoutez-y un brin de compétition et une promesse de récompense. Remuez le tout, en l'assaisonnant d'un semblant de jeu.
Intégrez-y une pincée d'intérêt, un zeste de curiosité, sans oublier un soupçon de liqueur de pensée et une bonne dose de logique.
Vous obtenez alors une pâte enthousiaste, que vous ferez lèver grâce à un professeur de mathématiques stimulant.
Agitez régulièrement la préparation, 4 mois durant, en l'échauffant, le 4 décembre très exactement, à l'aide d'une séance d'essai. Découpez la, pour ce faire, en groupes autonomes. Poursuivez en même temps la cuisine mathématique habituelle.
Le 8 Mars, faites lui subir l'épreuve de la cuisson proprement dite : amenez, d'abord, lentement à l'échauffement, en regroupant bien tous vos ingrédients. Laissez mijoter, en attente, de longues minutes. Incorporez alors d'un coup, 12 exercices plus ou moins salés; l'un d'eux devra être accomodé obligatoirement à la crème anglaise. Laissez frémir puis bouillonner, en surveillant bien pendant deux heures.
Le tout reposera ensuite, durant plusieurs semaines. Le résultat sera servi, le 17 Mai, à la Salle des Douanes, accompagné éventuellement de la coupe de champagne du vainqueur.

(Voir l'article de R. JOST, page 19.)
