Séminaire de philosophie et mathématiques

Roger Cuculière

Mille ans de chasse aux nombres congruents

Séminaire de Philosophie et Mathématiques, 1988, fascicule 2
« Mille ans de chasse aux nombres congruents », , p. 1-17

<http://www.numdam.org/item?id=SPHM_1988___2_A1_0>

MILLE ANS

DE CHASSE AUX NOMBRES

CONGRUENTS

---

par Roger CUCULIERE

Tout le monde sait, ou à peu près, ce que font les biologistes; les physiciens ou les chimistes. Mais il n'en va pas de même pour les mathématiciens. Au contraire, beaucoup de gens pensent qu'en mathématiques tout a été déjà découvert et que le seul problème qui demeure est d'apprendre le contenu de ces découvertes et de l'appliquer à divers domaines scientifiques ou techniques.

Il faut dire que de nos jours les mathématiques explosent en une incroyable variété de spécialités différentes et que les travaux d'un mathématicien risquent de n'être pas même intelligibles pour la plupart de ses confrères, et a fortiori pour le reste de l'humanité pensante.

Pourtant, une discipline mathématique échappe à cette loi commune, et c'est la mère de toutes les autres, la Théorie des Nombres. Ici, les chercheurs travaillent parfois sur des questins posées plusieurs siècles auparavant, des questions qui concernent des objets familiers tels que les nombres entiers ou les fractions ordinaires, des questions formulées si simplement qu'un élève des collèges peut les entendre, mais qui résistent aux assauts répétés de générations de savants, armés pourtant des ultimes ressources de la science de leur temps.

C'est ainsi que l'on a assité récemment à un nouvel épisode d'une aventure mathématique pluri-séculaire : la quête des nombres congruents. Nous allons en retracer les principales étapes.

*

* *

Ces nombres doivent leur nom à Léonardo Bigello, surnommé Fibonacci (figlio di Bonnaci) et appelé aussi Léonard de Pise, né vers1179, mort vers 1250, connu surtout aujourd'hui par la suite "de Fibonacci". Il a été le plus grand

mathématicien du Moyen-Age. Dans sa jeunesse, il a appris des Arabes, au cours de divers voyages, les méthodes de calcul e que ceux-ci avaient enpruntées aux Hindous. Revenu à Pise, il composa cinq ouvrages et c'est le dernier qui nous intéresse aujourd'hui, le "Liber Quadratorum" ou "Livre des Nombres Carrés", écrit en 1225, qui a eu une origine et un destin des plus curieux.

Fibonacci fut présenté à l'empereur Frédéric II de Hohenstaufen qui tenait momentanément sa cour à Pise et il fut engagé dans une espèce de tournoi mathématique avec Jean de Palerme, mathématicien attaché à la cour impériale. C'est de là qu'est sorti cet ouvrage, qui n'est pas un recueil systématique des propriétés des nombres carrés, mais une sélection de celles qui ont trait au problème proposé en défi à l'auteur.

Mais ce livre, trop en avance sur son temps, tomba dans un oubli profond, ne bénéficia pas de l'invention de l'imprimerie et fut supposé perdu jusqu'au XIXe siècle.

Le prince Baldassare Boncompagni, mathématicien et mécène romain, en retrouva une copie et en donna une première édition en 1854, et c'est en 1952 que Paul Ver Eicke le traduisit en français.

Voici le texte du prologue, adressé à l'empereur, et qui décrit l'objet de l'ouvrage :

"Lorsque, ô Seigneur Frédéric, prince très glorieux, maître Dominique m'amena à Pise, aux pieds de Votre Excellence, maître Jean de Palerme, m'ayant rencontré, me proposa la question, qui n'appartient pas moins à la géométrie qu'au nombre, de trouver un nombre carré qui, augmenté ou diminué de cinq, fait toujours naître un nombre carré. Après avoir réfléchi sur la solution de cette question que j'avais déjà trouvée, j'ai constaté que cette solution prenait sa source dans les choses multiples qui se présentent dans les nombres carrés et entre ces nombres. Ayant d'ailleurs appris par des propos tenus à Pise, et par d'autres qui me sont revenus de la Cour Impériale, que Votre Majesté avait daigné lire le livre que j'avais écrit sur les nombres, et qu'il Lui plaisait parfois d'entendre les subtilités relatives à la géométrie, je me suis rappelé la question que je viens d'énoncer et qui m'avait été proposée à Votre Cour par Votre philosophe. J'en ai pris le sujet, ai entrepris de composer le présent ouvrage, et ai voulu l'intituler *Le livre des nombres carrés*. Je viens donc réclamer Votre indulgence en cas où il contiendrait quelque chose de plus ou moins exact ou nécessaire; car il appartient à la divinité plutôt qu'à l'humanité d'avoir la mémoire de tout et de ne se tromper en rien, et personne n'est exempt de défauts ni de toutes parts sur ses gardes".

Le carré cherché est un carré rationnel, c'est-à-dire le carré d'une fraction dont le numérateur et le dénominateur sont des nombres entiers. De nos jours, nou dirions qu'il s'agit de résoudre, dans le corps Q des nombres rationnels, le système d'équations :

$$\begin{cases} x^2 + 5 = y^2 \\ x^2 - 5 = z^2 \end{cases}$$

Dans son ouvrage, Fibonacci généralise ce problème, s'intéressant plus généralement à tous les nombres qui pourraient remplacer 5 dans la question de Jean de Palerme :

"Trouver un nombre qui ajouté à un nombre carré et retranché de celui-ci, forme toujours un nombre carré".

Autrement dit, trouver R pour que le systèpe d'équations

$$\begin{cases} x^2 + R = y^2 \\ x^2 - R = z^2 \end{cases}$$

ait des solutions rationnelles.

Un tel nombre est dénommé par l'auteur "congru" ou "congruent". Si l'on envisage que les carrés en question soient entiers, alors le plus petit nombre R qui convienne est 24, avec les égalités : $5^2 + 24 = 7^2$, $5^2 - 24 = 1^2$. Mais si l'on accepte des fractions, alors le nombre 6 est aussi congruent car on peut diviser par 4 les deux nombres de chacune de ces égalités, et l'on obtient :

$$\left(\frac{5}{2}\right)^2 + 6 = \left(\frac{7}{2}\right)^2, \left(\frac{5}{2}\right)^2 - 6 = \left(\frac{1}{2}\right)^2$$

On voit qu'un nombre congruent R reste congruent lorsqu'on le multiplie ou qu'on le divise par un carré. C'est pourquoi on ne s'intéresse aux nombres congruents qu'entiers et sans diviseurs carrés. Nous venons de voir que 6 est un tel nombre. Le problème posé par Jean de Palerme revient à demander si 5 en est un aussi. Dans son ouvrage, Fibonacci répond affirmativement, en exhibant les carrés qui constituent une solution :

$$\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2, \left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2$$

*

* *

*

Nous avons choisi de partir de l'oeuvre de Fibonacci pour esposer les nombres congruents, mais la question n'est pas apparue ex nihilo en 1225. On peut lui trouver une origine dans l'antiquité babylonienne, avec des problèmes tels que celui qui est posé sur la figure 1.a) : deux frères doivent se partager équitablement un champ trapézoïdal; trouver les longueurs x,y,z qui rendront cela possible.

La solution est donnée par la figure 1.b. Si a et b désignent les hauteurs des deux trapèzes qui constituent les parts des deux frères, la similitude des triangles hachurés donne : $(x - z)/a = (y - x)/b$ et l'équivalence des parts des deux frères s'écrit : $(x + z)a/2 = (y + x)b/2$. Le produit de ces égalités conduit à $x^2 - z^2 = y^2 - x^2$. Autrement dit, il faut trouver trois carrés z^2, x^2, y^2 formant une progression arithmétique. C'est exactement le problème posé par Jean de Palerme, à ceci près que la raison de cette progression est prescrite : elle doit être égale à 5. C'est pourquoi Fibonacci dit dans son introduction que ce problème "n'appartient pas moins à la géométrie qu'au nombre".

Dans la "préhistoire" de notre problème, il nous faut surtout citer Diophante d'Alexandrie, mathématicien du IIIe siècle de notre ère, comme le grand

pourvoyeur de ce type de questions consistant à chercher des nombres entiers ou fractionnaires astreints à vérifier certaines relations. De nos jours, on représente ces problèmes par des équations appelées "diophantiennes" lorsqu'on veut les résoudre en nombres entiers ou rationnels.

On peut citer dans l'oeuvre de Diophante trois problèmes qui annoncent celui dont nous traitons aujourd'hui.

Premier énoncé :

"Trouver trois nombres qui soient en égale différence et tels que, pris deux à deux, ils forment un carré".

Si nous appelons a, b, c nos trois nombres, le fait qu'ils sont "en égale différence" signifie qu'ils suivent une progression arithmétique de raison R, soit : $c - b = b - a = R$. Et dire que "deux à deux ils forment un carré" signifie : $a+ b = z^2$, $b + c = y^2$, $c + a = x^2$. Par soustraction, on obtient : $y^2 - x^2 = b - a$ et $x^2 - z^2 = c - b$, soit : $y^2 - x^2 = x^2 - z^2 = R$. Et l'on retrouve exactement le problème babylonien.

Second énoncé :

"Trouver quatre nombres tels que le carré de la somme de ces quatre nombres, augmenté ou diminué de chacun de ces nombres, forme un carré".

Troisième énoncé :

"Trouver trois nombres tels que le carré de chacun d'eux, augmenté ou diminué de la somme de ces trois nombres, forme un carré".

Sans entrer dans les détails, nous voyons bien encore la parenté avec le problème posé par Jean de Palerme : ces énoncés mettent en jeu des carrés qui restent carrés lorsqu'on les augmente ou qu'on les diminue d'une même quantité. Dans la solution du second problème, Diophante utilise un auxiliaire extrêmement fécond, le triangle rectangle. Exprimé en langage algébrique actuel, ceci revient à partir des identités remaquables bien connues :

$$a^2 + b^2 + 2ab = (a + b)^2 \text{ , et :}$$

$$a^2 + b^2 - 2ab = (a - b)^2 .$$

Si d'aventure le nombre $a^2 + b^2$ était égal à un carré x^2, ce serait bien un carré qui resterait tel lorsqu'on l'augmenterait ou qu'on le diminuerait de la quantité 2ab. Mais il est parfaitement possible que l'on ait $a^2 + b^2 = x^2$, il suffit (et il faut) que a,b,x soient les côtés d'un triangle rectangle, le côté x étant l'hypoténuse.

Observons que, si a et b sont les côtés de l'angle droit d'un triangle rectangle à côtés rationnels, alors 2ab est un nombre congruent. Par suite $\frac{2ab}{4}$ l'est aussi puisque 4 est un carré. Mais $\frac{2ab}{4}$ c'est $\frac{ab}{2}$ c'est-à-dire l'aire de notre triangle.

Ici apparaît un autre procédé de fabrication des nombres congruents, en liaison avec une figure fondamentale de la géométrie arithmétique, le triangle rectangle à côtés rationnels : un nombre congruent, c'est tout simplement l'aire d'un tel triangle.

Par exemple, le triangle le plus connu, de côtés 3, 4, 5, donne le nombre congruent $\frac{3x4}{2} = 6$.

Le triangle de côtés 5, 12, 13 conduit au nombre $\frac{5x12}{2} = 30$. Et ainsi de suite.

Mais le plus important, c'est que l'on obtient ainsi tous les nombres congruents. En effet, si l'on suppose que le nombre R vérifie : $x^2 + R = y^2$ et $x^2 - R = z^2$, l'identité bien connue : $(y + z)2 + (y - z)2 = 2(y2 + z2)$ conduit finalement à l'égalité :

$$(y + z)^2 + (y - z)^2 = (2x)^2$$

ce qui revient à dire que les nombres y + z et y - z, sont les côtés de l'angle droite d'un triangle rectangle dont l'hypoténuse est 2x . Et quelle est l'aire de ce triangle rectangle ? C'est $\frac{1}{2}$ (y+z) (y-z) soit $\frac{1}{2}(y^2 - z^2)$, nombre égal à R : ce que nous voulions démontrer.

Par exemple, le nombre congruent 5 est l'aire du triangle rectangle dont les côtés mesurent :

$$\frac{49}{12} - \frac{31}{12} = \frac{3}{2} \ , \ \frac{49}{12} + \frac{31}{12} = \frac{20}{30} \ , \ 2.\frac{41}{12} = \frac{41}{6} .$$

Soit en réduisant au même dénominateur : $\frac{9}{6}$, $\frac{40}{6}$, $\frac{41}{6}$.

Ce deuxième visage des nombres congruents explique leur importance dans l'histoire de la science des nombres, car la figure du triangle rectangle dont les côtés sont nombres entiers ou fractions est sans doute le plus ancien objet d'étude des mathématiques spéculatives, comme nous l'avons déjà observé.

A ce stade, il nous faut expliquer comment on obtient les triplets pythagoriciens, c'est-à-dire les triplets de nombres entiers ou fractionnaires a,b,c, tels que : $a^2 + b^2 = c^2$. Pour traiter cette antique question, nous utiliserons une méthode "moderne". L'équation $a^2 + b^2 = c^2$ s'écrit : $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$, soit $x^2 + y^2 = 1$ en posant $x = \frac{a}{c}$ et $y = \frac{b}{c}$.

Mais x2 + y2 = 1 , c'est l'équation d'un cercle dans un système d'axes perpendiculaires (figure 2) . Les points M dont les coordonnées x et y vérifient cette relation constituent le cercle de centre O et de rayon 1 . C'est Henri Poincaré qui a eu le premier l'idée de cette nouvelle interprétation géométrique des problèmes disphantiens et qui consiste à rechercher les points à coordonnées entières ou rationnelles sur certaines courbes algébriques. Pour l'instant, il s'agit donc de trouver tous les poinst M du cercle d'équation x2 + y2 = 1 dont les coordonnées x et y sont des nombres rationnels, des fractions. Pour ce faire, on considère la droite AM qui joint le point M au point A de coordonnées (-1,0). La pente de cette droite est $\frac{y}{x+1}$, un rationnel que nous désignerons par $\frac{n}{m}$, fraction supposée irréductible dont les termes m et n sont donc des entiers sans diviseurs communs. Les équations paramétriques de la droite AM sont donc : Y = nt , X+1 = mt . En reportant ceci dans l'équation du cercle, on exprime t en fonction de m et n, soit $t = \frac{2m}{m^2+n^2}$, et l'on en déduit : $Y = \frac{2mn}{m^2+n^2}$, $X = \frac{m^2 - n^2}{m^2 + n^2}$.

Il en résulte que les solutions en nombres entiers de l'équation $a^2 + b^2 = c^2$ sont données par les formules :

$$a = m^2 - n^2 \ , \ b = 2mn \ , \ c = m^2 + n^2 \ ,$$

ou bien tout autre triplet obtenu en multipliant, ou si possible en divisant ces trois entiers par un même nombre.

Nous avons obtenu un procédé automatique de fabrication des triangles rectangles entiers, connu depuis l'Antiquité. Chacun de ces triangles fournit un nombre congruent égal à $\frac{1}{2}$ ab, soit : $mn(m^2 - n^2)$.

Si ce nombre est divisible par un carré, le quotient est encore un nombre congruent. Le tableau de la figure 3 présente une liste de quelques uns de ces triangles et des nombres congruents correspondants. Nous nous sommes bornés à des triangles dits "primitifs", dont les côtés sont sans diviseur commun. Tous les autres triangles possibles en découlent en multipliant ces trois côtés par un même nombre.

Pour être certain d'obtenir tous les triangles primitifs sans répétitions, il suffit de prendre m et n sans diviseurs communs, l'un pair et l'autre impair, avec $m > n$.

*

* *

Revenons aux nombres congruents. La formule $R = mn(m^2 - n^2)$ nous les donne tous, éventuellement après division par les facteurs carrés qui pourraient diviser R. En 1855, Genocchi a trouvé d'autres formules donnant des nombres congruents.

Reprenant les égalités : $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$, nous avons vu que l'on a : $a^2 + b^2 = c^2$ et le nombre congruent correspondant est $R = mn(m^2 - n^2)$.

Si dans cette dernière égalité nous remplaçons m par c et n par a, nous avons comme nouveau nombre congruent : $ca(c^2 - a^2)$. Mais $c^2 - a^2$ est égal à b^2, et nous pouvons supprimer ce facteur carré b^2, donc ac est encore un nombre congruent. Il en est de même pour bc. Par ailleurs, le produit ac est égal à $(m^2 - n^2)(m^2 + n^2) = m^4 - n^4$; tout nombre de cette forme est congruent, quels que soient m et n. Si nous remplaçons m par a et n par b, nous montrons que $(a^2 - b^2)(a^2 + b^2)$ est congruent et comme $a^2 + b^2 = c^2$ est un carré, alors $a^2 - b^2$ est congruent. On peut continuer ainsi, on trouve que sont aussi congruents a2 + c2 et $b^2 + c^2$, de même que $m^4 + 4n^4$, $2(m^4 + n^4)$, $2mn(m^2 + n^2)$, etc. Mais attentin, dans ces formules les entiers m et n doivent être distincts.

Toutes ces formules permettent de construire des listes de nombres congruents, et d'autant plus facilement que les moyens de calcul sont évolués : un simple programme BASIC de quelques lignes vous permettra d'en réunir une belle collection.

A des époques plus reculées, des hommes de science avaient déjà constitué de telles listes. Un manuscrit arabe du 10e siècle en avait donné déjà trente. Au 15e siècle, Fra Luca Pacioli a repris l'oeuvre de Fibonacci et poussé plus avant l'investigation en produisant cinquante-deux nombres congruents.

Pourtant un simple coup d'oeil sur la figure 3 nous fait évaluer les limites de l'entreprise. Certes, on dresse une table de nombres congruents et l'on peut même en rassembler beaucoup. Mais ils apparaissent dans un ordre quelconque et l'on ne peut prévoir si un nombre donné, par exemple 3, se trouvera ou non dans cette table. Nous n'avons aucun moyen algorithmique de déterminer si un nombre donné est ou non congruent, ou de contruire la liste des nombres congruents compris entre deux limites prescrites, par exemple entre 1 et 100. A ce

niveau, les progrès ne peuvent se faire par calculs mais par l'étude théorique des nombres et de leurs propriétés.

Et tout d'abord, le nombre 1 est-il congruent ? Ceci reviendait à dire qu'il existe un triangle rectangle à côtés entiers dont l'aire est un carré parfait. Fermat, au 17e siècle, a montré dans ses "observations sur Diophante" qu'un tel triangle n'existe pas. Cette démonstration se fait par l'absurde. Si un tel triangle existait, dit Fermat, on aurait deux carrés entiers dont la somme et la différence seraient des carrés : ce qui serait l'autre manière d'exprimer que le nombre 1 est congruent.

On aurait donc une solution en entiers non nuls pour le système d'équations :

$$\begin{cases} x^2 + y^2 = z^2 \\ x^2 - y^2 = t^2 \end{cases}$$

Système qui s'écrit aussi :

$$\begin{cases} z^2 = t^2 + 2y^2 \\ x^2 = t^2 + y^2 \end{cases}$$

La démonstration de Fermat est très intéressante, car c'est le seul endroit où le génial Toulousain révèle les ressorts de ses méthodes. Mais il le fait dans un langage courant, sans le secours de la notation algébrique. Ainsi, le système que nous venons d'écrire est énoncé par lui comme suit :

"Par conséquent, on aurait un nombre carré (z^2) somme d'un carré (t^2) et du double d'un carré ($2y^2$) avec la condition que la somme des carrés qui servent à le composer ($t^2 + y^2$) soit également un carré (x^2) ".

A lire ces lignes, on ne doute plus que le succès de la notation algébrique soit le fruit d'un choix conscient dû au souci de simplification et de libération de l'esprit !

Et il poursuit :

"Mais si un nombre carré est somme d'un carré et du double d'un carré, sa racine est également somme d'un carré et du double d'un carré, ce que je puis prouver sans difficulté".

Autrement dit, Fermat prend l'équation disphantienne $z^2 + t^2 + 2y^2$ toute seule et nous dit que sa solution exige que $z = m^2 + 2n^2$, du moins si x,y,z sont sans diviseurs communs.

Ceci peut se prouver par des manipulations calculatoires qui constituaient sans doute la démonstration de Fermat, mais aussi par une méthode géométrique analogue à celle qui nous a fait trouver le triplets pythagoriciens comme points rationnels du cercle $X^2 + Y^2 = 1$. Dans le cas présent, on diviserait par z^2 les deux membres de l'équation $z^2 = t^2 + 2y^2$ et le résultat s'écrirait $X^2 + 2Y^2 = 1$ qui est l'équation, non plus d'un cercle, mais d'une ellipse, dont on chercherait de même les points à coordonnées rationnelles. On trouverait : $z = m^2 + 2n^2$ $t = n^2 - 2n^2$, $y = 2mn$.

Et Fermat nous annonce l'apparition d'un nouveau triangle rectangle car si l'on pose $u = m^2$ et $v = 2n^2$, il s'ensuit : $u^2 + v^2 = m^4 + 4n^4 = t^2 + y^2 = x^2$. Or, l'aire de ce nouveau triangle est $\frac{1}{2}uv = (mn)^2$: c'est un carré !

S'il existait un triangle rectangle dont l'aire soit un carré, il en existerait un autre, plus petit qui aurait la même propriété. Donc il y en aurait encore un autre, encore plus petit, et ainsi de suite, ce qui est manifestement impossible.

C'est la méthode dite de "descente infinie" imaginée par Fermat et appliquée par lui à diverses questions.

Notons que Fermat a démontré du même coup que l'équation $x^4 - y^4 = z^2$ ne saurait avoir de solutions entières non nulles et par voie de conséquence son "grand théorème" pour l'exposant 4 : l'équation $x^4 + y^4 = z^4$ n'a pas de solutions entières non nulles.

*

* *

Nous avons tenu à présenter la démonstration de Fermat pour souligner que le cas du nombre 1, qui est le plus simple des nombres non-congruents, s'il n'est pas hors de portée d'un raisonnement de difficulté moyenne, n'est pas tout de même totalement trivial. Le sort du nombre 2 se règle de manière analogue, en relation avec l'équation impossible $x^4 + y^4 = z^2$. Le nombre 3 n'est pas non plus congruent, mais c'est déjà moins simple à démontrer.

Le nombre 4 se ramène à 1 comme tous les carrés, après division par les facteurs carrés, et 5 apparaît comme le plus petit nombre congruent. Mais ensuite ?
Divers résultats partiels ont été trouvés, en 1855 par Genocchi, et en 1879 par Samuel Roberts, en utilisant la méthode de descente de Fermat.
Ne sont pas congruents :

- les nombres premiers de la forme $8k + 3$
- les nombres $2p$, où p est premier de la forme $8k + 5$
- les nombres pq où p et q sont premiers de la forme $8k + 3$
- les nombres $2pq$ où p et q sont premiers de la forme $8k + 5$

Pour la première centaine, ceci nous donne la liste suivante de non-congruents assurés : 3,11,19,43,59,67 et 83 d'après le premier critère, le quatrième ne fournissant des nombres qu'à partir de $2x5x13 = 130$.

Mais c'et surtout depuis une vingtaine d'années que la théorie des nombres congruents a connu d'importants progrès.
Rappelons qu'un nombre R est congruent s'il existe des entiers m,n,q tels que :

$$mn(m^2 - n^2) = q^2R .$$

Si l'on pose $X = \frac{Rn}{m}$ et $Y = \frac{qR^2}{m^2}$, cette égalité s'écrit : $Y^2 = X^3 - R^2X$.

On peut se demander : quel progrès attendre d'un tel changement de variable ? C'est que l'égalité $Y^2 = X^3 - R^2X$ peut être considérée comme l'équation d'une certaine courbe algébrique, enemble des points qui vérifient la dite équation, de la même manière que nous avons fait intervenir ci-dessus le cercle d'équation $X^2 + Y^2 = 1$. Mais ici, la courbe

d'équation $Y^2 = X^3 - R^2X$ s'appelle une cubique parce que son équation est degré 3. Son allure est donnée par la figure 4. Ce type de courbe est bien connu, on peut la paramétrer par des fonctions spéciales nommées fonctions elliptiques, de même que le cercle $X^2 + Y^2 = 1$ peut être paramétré par les fonctions trigonométriques : $X = \cos\theta$, $Y = \sin\theta$. C'est pourquoi notre cubique s'appelle une courbe elliptique.

L'étude de ces courbes s'est fort développée depuis les années 60 avec les travaux des mathématiciens anglais Birch et Swinnerton-Dyer, et le Français Jean Lagrange en a tiré d'importantes conséquences, notamment en ce qui concerne la liste des nombres congruents de 1 à 1000. Dans cet intervalle, il y a 608 nombres sans facteurs carrés. En 1977, Jean Lagrange y trouvait 322 nombres congruents, 227 nombres non congruents et il restait 59 nombres sur lesquels on ne savait se prononcer.

C'est en 1983 que l'Américain J.B. Tunnell a découvert un critère décisif permettant de discriminer les nombres congruents. Voici ce critère.

Soit R un entier impair, sans diviseurs carrés.

. Supposons R congruent. Alors, le nombre de triplets d'entiers (x,y,z) vérifiant : $2x^2 + y^2 + 8z^2 = R$ vaut deux fois le nombre de triplets d'entiers (x,y,z) vérifiant : $4x^2 + y^2 + 32z^2 = R$.

. Supposons que 2R est congruent. Alors, le nombre de triplets d'entiers vérifient : $2x^2 + y^2 + 8z^2 = R$ vaut deux fois le nombre de triplets d'entiers vérifiant : $4x^2 + y^2 + 32z^2 = R$.

De plus, il est probable que les réciproques de ces assertions sont vraies. Pour le prouver, il faudrait que soit établie une certaine conjecture de Birch et Swinnerton-Dyer sur les courbes elliptiques. Dans de nombreux cas particuliers, les mathématiciens savent prouver ces réciproques, et c'est ce qui a permis de dresser la table complète des nombres congruents de 1 à 1000 (figure 5).

Ce critère est très important sur le plan algorithmique, car il permet de vérifier en un temps fini si un nombre R donné est congruent. Ce n'était pas le cas des critères précédents, parce qu'ils reposaient sur l'existence de solutions d'équations disphantiennes qui, pour chaque nombre R donné, pouvaient nécessiter une infinité de vérifications.

De plus, les vérifications fondées sur cette méthode n'exigent pas, quand le nombre est congruent, que l'on exhibe un triangle rectangle à côtés rationnels dont il mesure l'aire, et qui a parfois des côtés fort compliqués, exemple le nombre congruent 157 : voir la figure 6.

Une page vient d'être tournée, par des voies inattendues, dans l'étude d'un problème pluriséculaire dans l'histoire duquel se mêlent la géométrie arithmétique des Anciens et les découvertes les plus modernes de la Théorie des nombres, en relation avec les courbes elliptiques.

Mais tout n'est pas dit pour autant. D'abord, nous avons vu que les critères de Tunnell, pour être vraiment concluants, exigent la démonstration d'une certaine propriété dont la véracité n'est point à ce jour assurée.

Ensuite, considérez la table de la figure 5, où l'on a classé les nombres sans facteurs carrés, selon leur reste dans la division par 8 : vous constatez que les colonnes des restes 5,6,7 sont pleines. Alter, Curtz et Kubota ont conjecturé en 1972 qu'il en était de même

pour tous les nombres, autrement dit que tout entier, qui donne un reste de 5,6 ou 7 quand on le divise par 8, est congruent. Mais pour l'instant, on ne sait pas démontrer ceci.

En 1975, Stephens a ramené cette conjecture à une autre qui concerne les courbes elliptiques et il en a trouvé une démonstration dans le cas où le nombre considéré est premier ou le double d'un nombre premier.

Et enfin, si l'on sait qu'un nombre R est congruent, il reste à trouver un triangle rectangle numérique dont il soit l'aire, il reste à trouver un carré rationnel qui, augmenté ou diminué de R, reste carré. Et quand on en a trouvé un, il reste à en trouver d'autres et, pourquoi pas les trouver tous.

Sur toutes ces questions, des hommes de l'art continuent de se pencher, des découvertes ont été acquises, d'autres sont à venir. En mathématiques comme ailleurs, l'histoire n'est pas finie, elle se fait tous les jours. Nous aurons peut-être l'occasion de relater de nouveaux succès dans la chasse millénaire aux nombres congruents.

BIBLIOGRAPHIE

R. Alter, T.B. Curtz, K.K. Kubota : remarks & results on congruent numbers, Proc. 3rd S.-E. Conf. Combinatoris, graphs theory & computing, 1972.

J. Lagrange : construction d'une table de nombres congruents, Bull. Soc. maths. France, mémoire 4750, 1977.

J.B. Turnell : A classical Disphantine problem and modular forms of weight 3/2, Invent. math., 1983.

Serge Lang : une activité vivante : faire des mathématiques, Revue du Palais de la Découverte, janvier 1983. Republié en "Serge Lang fait des maths en public", Berlin 1984.

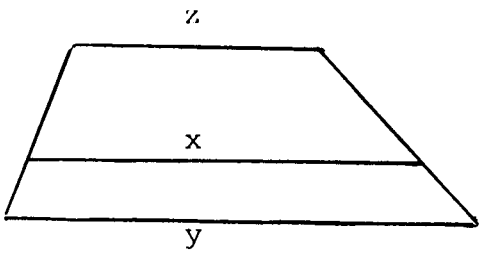

Figure 1.a : problème babylonien : partager équitablement un champ trapézoïdal

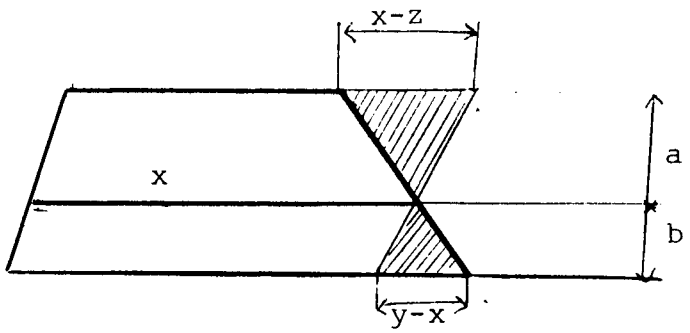

Figure 1.b : Solution : les triangles hachurés sont semblables

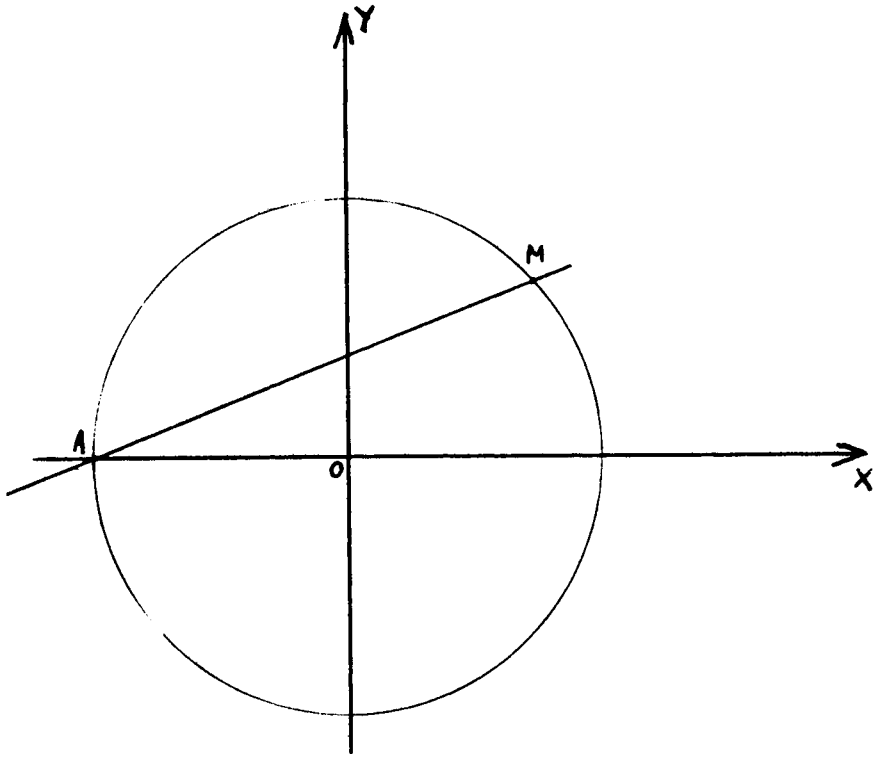

Figure 2. Paramétrisation du cercle d'equation $X^2 + Y^2 = 1$ par intersection avec une droite variable passant par le point A(-1,0).

Ceci permet de determiner les points de ce cercle qui ont leurs coordonnées rationnels.

m	n	$a = m^2 - n^2$	$b = 2mn$	$c = m^2 + n^2$	$R = mn(m^2 - n^2)$	R débarrassé de ses diviseurs carrés
2	1	3	4	5	6	6
3	2	5	12	13	30	30
4	1	15	8	17	60	15
4	3	7	24	25	84	21
5	2	21	20	29	210	210
5	4	9	40	41	180	5
6	1	35	12	37	210	(210)
6	5	11	60	61	330	330
7	2	45	28	53	630	70
7	4	33	56	65	924	231
7	6	13	84	85	546	546
8	1	63	16	65	504	16
8	3	55	48	73	1320	(330)
8	5	39	80	89	1560	390
8	7	15	112	113	840	(210)
9	2	77	36	85	1386	154
9	4	65	72	97	2340	154
9	8	17	144	165	1224	34
10	1	99	20	101	990	110
10	3	91	60	109	2730	2730
10	7	51	140	149	3570	3570
10	9	19	180	181	1710	190
11	2	117	44	125	2574	286
11	4	165	88	137	4620	1155
11	6	85	132	157	5610	5610
11	8	57	176	185	5016	1254
11	10	21	220	221	2310	2310
12	1	143	24	145	1716	429
12	5	119	120	169	7140	1785
12	7	95	168	193	7280	1995
12	11	23	264	265	2036	759

Figure 3 : quelques nombres congurents.
on a porté entre parenthèses les nombres congurents déjà trouvés.

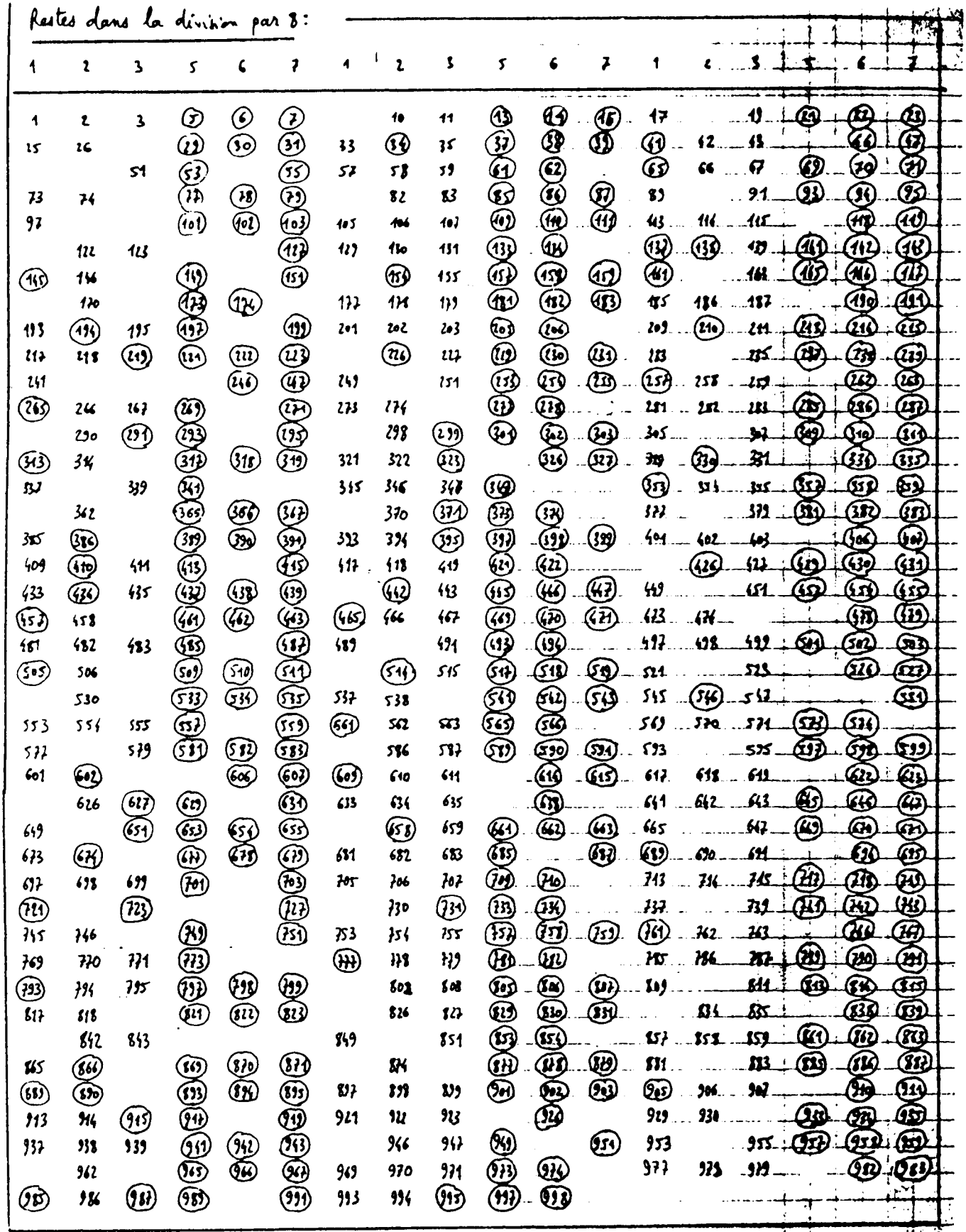

Figure 5. Les nombres congruents de 1 à 1000

Tableau des nombres entiers de 1 à 1000 qui n'ont pas de diviseur carré (autre que 1), classés selon leur reste dans la division par 8 : on a entouré les nombres congruents à

Restes dans la division par 8 :																		
1	2	3	5	6	7	1	2	3	5	6	7	1	2	3	5	6	7
1	2	3	5	6	7		10	11	13	14	15	17		19	21	22	23
25	26		29	30	31	33	34	35	37	38	39	41	42	43		46	47
		51	53		55	57	58	59	61	62		65	66	67	69	70	71
73	74		77	78	79		82	83	85	86	87	89		91	93	94	95
97			101	102	103	105	106	107	109	110	111	113	114	115		118	119
	122	123			127	129	130	131	133	134		137	138	139	141	142	143
145	146		149		151		154	155	157	158	159	161		163	165	166	167
	170		173	174		177	178	179	181	182	183	185	186	187		190	191
193	194	195	197		199	201	202	203	205	206		209	210	211	213	214	215
217	218	219	221	222	223		226	227	229	230	231	233		235	237	238	239
241				246	247	249		251	253	254	255	257	258	259		262	263
265	266	267	269		271	273	274		277	278		281	282	283	285	286	287
	290	291	293		295		298	299	301	302	303	305		307	309	310	311
313	314		317	318	319	321	322	323		326	327	329	330	331		334	335
337		339	341			345	346	347	349			353	354	355	357	358	359
	362		365	366	367		370	371	373	374		377		379	381	382	383
385	386		389	390	391	393	394	395	397	398	399	401	402	403		406	407
409	410	411	413		415	417	418	419	421	422			426	427	429	430	431
433	434	435	437	438	439		442	443	445	446	447	449		451	453	454	455
457	458		461	462	463	465	466	467	469	470	471	473	474			478	479
481	482	483	485		487	489		491	493	494		497	498	499	501	502	503
505	506		509	510	511		514	515	517	518	519	521		523		526	527
	530		533	534	535	537	538		541	542	543	545	546	547			551
553	554	555	557		559	561	562	563	565	566		569	570	571	573	574	
577		579	581	582	583		586	587	589	590	591	593		595	597	598	599
601	602			606	607	609	610	611		614	615	617	618	619		622	623
	626	627	629		631	633	634	635		638		641	642	643	645	646	647
649		651	653	654	655		658	659	661	662	663	665		667	669	670	671
673	674		677	678	679	681	682	683	685		687	689	690	691		694	695
697	698	699	701		703	705	706	707	709	710		713	714	715	717	718	719
721		723			727		730	731	733	734		737		739	741	742	743
745	746		749		751	753	754	755	757	758	759	761	762	763		766	767
769	770	771	773			777	778	779	781	782		785	786	787	789	790	791
793	794	795	797	798	799		802	803	805	806	807	809		811	813	814	815
817	818		821	822	823		826	827	829	830	831		834	835		838	839
	842	843				849		851	853	854		857	858	859	861	862	863
865	866		869	870	871		874		877	878	879	881		883	885	886	887
889	890		893	894	895	897	898	899	901	902	903	905	906	907		910	911
913	914	915	917		919	921	922	923		926		929	930		933	934	935
937	938	939	941	942	943		946	947	949		951	953		955	957	958	959
	962		965	966	967	969	970	971	973	974		977	978	979		982	983
985	986	987	989		991	993	994	995	997	998							

Les nombres congruents de 1 à 1000. Tableau des nombres entiers de 1 à 1000 sans diviseur carré (autre que 1), classés selon leur reste dans la division par 8 : on a entouré les nombres congruents.

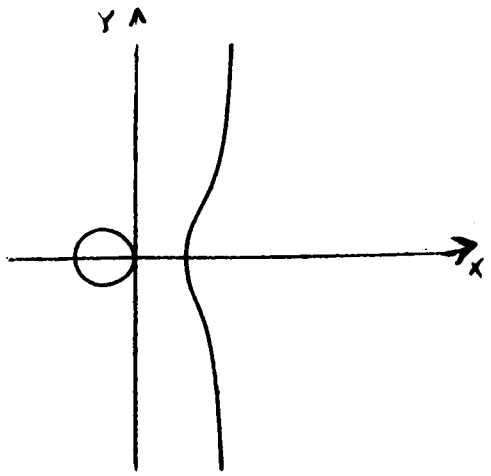

Figure 4 : cubique d'équation $Y^2 = X^3 - R^2X$, courbe elliptique.

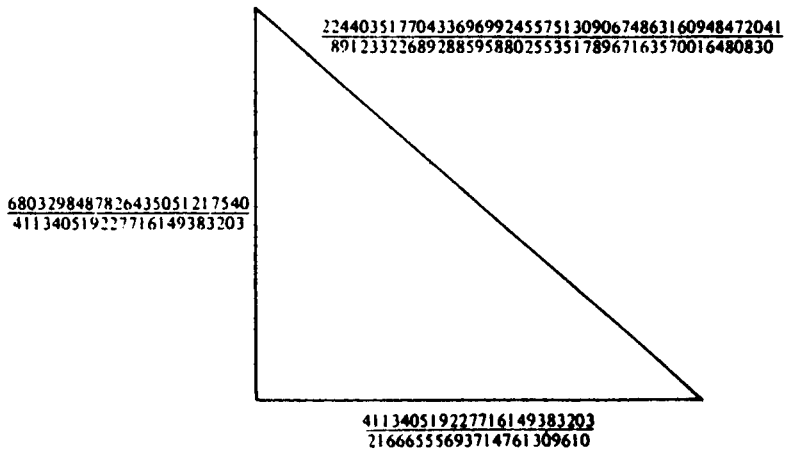

Figure 6 : le triangle rectangle rationnel le plus simple dont l'aire est 157, calculé par D. Zagier.