Quatre devoirs d'arithmétique

Martine Bühler

Vous trouverez dans cette rubrique plusieurs problèmes d'arithmétique appuyés sur des textes historiques, qui ont été donnés en devoirs à la maison à des élèves de Terminale S, spécialité mathématiques.

- Tout d'abord un problème d'exploration des puissances de 7 modulo 641, qui utilise les propriétés élémentaires de compatibilité des congruences avec la somme et le produit. Cet exercice permet de lire un extrait d'un texte d'Euler : celui-ci s'intéresse aux puissances d'un nombre modulo un nombre premier, afin de démontrer le théorème de Fermat. Mais cette étude des puissances a été faite en classe au tout début du cours d'arithmétique, bien avant d'aborder ce théorème. L'étude des puissances d'un nombre est un « classique » de la spécialité en Terminale S et l'exercice permet une première approche. La partie II essaie une généralisation des résultats constatés sur les exemples des modules 641 et 63 ; les élèves ont trouvé cette deuxième partie difficile et ne pensent pas spontanément à utiliser le principe des tiroirs.
- Le deuxième problème porte sur le théorème chinois des restes. J'étais motivée par la présence dans ma classe de nombreux élèves étudiant le chinois en deuxième ou troisième langue. De plus, j'ai emmené un peu plus tard dans l'année une partie de la classe (volontaire) à une conférence à la Cité des Sciences et de l'Industrie faite par Karine Chemla sur les mathématiques dans la Chine Ancienne. L'équivalence de la question 3b a posé problème et a été l'occasion de discussion sur équivalence, implication et réciproque. Il est à noter qu'un bon nombre d'élèves a reconnu le théorème chinois des restes dans l'exercice de spécialité du bac national 2006.
- Le troisième problème s'occupe de nombres parfaits et nombres de Mersenne. Il est lié à une lettre de Fermat à Frénicle de juin 1640. Il utilise de manière subtile le théorème de Fermat pour trouver la forme des diviseurs d'un nombre de Mersenne. La partie III permet de tester la compréhension des résultats de l'exercice par les élèves. La question a de la partie I donne là encore lieu à des discussions sur théorèmes direct et réciproque.
- Le quatrième problème est une deuxième version d'un problème paru dans un numéro antérieur de *Mnémosyne*, sur la factorisation des grands nombres, à partir d'une idée de Fermat et de l'étude de la machine de Carissan (Voir le numéro 17 de *Mnémosyne*). Ce problème est déjà paru dans le numéro 446 du *Bulletin Vert* de l'APMEP, consacré au calcul. Un film sur le fonctionnement de la machine de Carissan peut être consulté à l'IREM Paris 7 et téléchargé sur le site de l'IREM Paris 7.

Problème 1 *Puissances de 7 modulo 641*

Dans un article publié en 1758, Euler s'intéresse aux restes des puissances de 7 modulo 641.

Préambule : lire le texte ci-dessous en vérifiant tous les calculs d'Euler. Vous écrirez sur la copie tous les calculs nécessaires à cette vérification, sans justification. Tous les calculs d'Euler sont-ils nécessaires pour obtenir le reste de 7^{160} (expliquez votre réponse)?

« Voici donc une méthode assez rapide pour trouver les restes qui proviennent de la division d'une puissance quelconque par un nombre quelconque. Par exemple si nous voulons chercher le reste qui provient de la division de 7^{160} par le nombre 641

Puissances	Restes
7^1	7
7^2	49
7^3	343
7^4	478
7^8	288
7^{16}	255
7^{32}	284
7^{64}	-110
7^{128}	-79
7^{160}	-1

En effet puisque la première puissance 7 donne le reste 7 les puissances 7^2,7^3,7^4 donnent 49,343, et 478, c'est-à-dire –163, dont le carré 7^8 donne le reste 163^2 c'est-à-dire 288, et le carré de celui-ci 7^{16} donne le reste 288^2, c'est-à-dire 255. De même la puissance 7^{32} donne le reste 255^2 c'est-à-dire 284 et le reste de la puissance 7^{64} sera –110 et pour 7^{128} il vient 110^2 c'est-à-dire –79, reste qui multiplié par 284 donnera le reste de $7^{128+32} = 7^{160}$ qui sera 640 c'est-à-dire –1.

Nous savions donc que, si la puissance 7^{160} était divisée par 641, le reste était 640 c'est-à-dire –1, d'où nous concluons que le reste de la puissance 7^{320} est +1. Donc en général le reste de la puissance 7^{160n} divisée par 641 sera soit +1 si *n* est un nombre pair, soit –1, si *n* est un nombre impair. »

Partie I : étude du texte d'Euler.

1. Justifiez le remplacement de 478 par –163 et expliquez l'intérêt pratique de cette démarche.
2. Citez le résultat du cours utilisé pour le calcul du reste de 7^8.
3. Justifiez le résultat donné pour le reste de la division de 7^{320} par 641 ainsi que celui de la division de 7^{160n} par 641 ?
4. Quel est le reste de la division de 7^{320n} par 641 ? Déterminer, en utilisant les résultats d'Euler et sans calculs supplémentaires, le reste de la division de 7^{648} par 641.
5. On appelle r_N le reste de la division de 7^N par 641. Montrer que cette suite est périodique.
6. Donner une méthode pour le calcul du reste de la division de 7^N par 641.

Partie II : et pour d'autres modules que 641 ?

1. Calculer les restes de $7, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7$ dans la division par 63.
2. Montrer que la suite (r_N) des restes de la division de 7^N (pour *N* entier strictement positif) par 63 est périodique. Quel est le reste de la division de 7^9 par 63 ?
3. On considère un nombre entier strictement positif *m*. La suite des restes de la division de 7^N par *m* est-elle toujours périodique ?
4. Euler constate que le reste de la division de 7^{320} par 641 est égal à 1. Existe-t-il un entier *h* strictement positif tel que le reste de la division de 7^h par *m* est égal à 1 pour tout entier *m* strictement positif ?

Vous justifierez soigneusement vos réponses aux questions 3 et 4.

Partie III : un résultat général

1. Programmez votre tableur pour obtenir les restes de 7^n dans la division par différents entiers *a*. Pour cela, vous écrirez « *n* » dans la cellule A1 et vous obtiendrez dans la colonne A les entiers de 1 à 100 ; vous écrirez « a = » dans la cellule D1 et choisirez une valeur de *a* dans la cellule E1. Dans la colonne B, obtenez les restes de 7^n dans la division par *a*. Dans la colonne C, programmez un test pour écrire « gagné » lorsque ce reste est 1.
2. **Conjecture :** après avoir essayé suffisamment de valeurs de *a* pour avoir une idée convaincante, conjecturez une condition nécessaire et suffisante portant sur 7 et *a* pour qu'il existe un entier *n* strictement positif tel que $7^n \equiv 1 \pmod{a}$.
3. **Démontrez votre conjecture** (dans un sens) : commencez par montrer : s'il existe un entier *n* strictement positif tel que $7^n \equiv 1 \pmod{a}$, alors …
4. La réciproque est plus difficile. Commencez par démontrer que, sous la condition trouvée, il existe un nombre *u* tel $7u \equiv 1 \pmod{a}$. Justifier alors l'existence de deux entiers naturels distincts *m* et *k* (avec $k > m$) tels que $7^k \equiv 7^m \pmod{a}$. En multipliant cette congruence par u^m, concluez.
5. Pouvez-vous conjecturer ce qui se passe pour les restes de la division de b^n par un entier *a* dans le cas général.

Problème 2 *Le théorème chinois des restes*

Le but de l'exercice est de déterminer les entiers naturels x vérifiant le système :

$$\begin{cases} x \equiv 2 (\text{mod}\, 3) \\ x \equiv 3 (\text{mod}\, 5) \\ x \equiv 2 (\text{mod}\, 7) \end{cases}$$

On pose $M_1 = 5\times7 = 35$; $M_2 = 3\times7 = 21$; $M_3 = 3\times5 = 15$.

1. Justifier l'existence d'un entier relatif u tel que $uM_1 \equiv 1 (\text{mod}\, 3)$, puis déterminer un entier naturel u_1 (le plus petit possible) tel que $u_1 M_1 \equiv 1 (\text{mod}\, 3)$.
5. Déterminer le reste de M_2 dans la division par 5 et celui de M_3 dans la division par 7.
6. Soit l'entier $x_0 = 2u_1 M_1 + 3M_2 + 2M_3$. (Ne pas calculer x_0 avant c.)

a. Quels sont les restes de la division de x_0 par 3, 5 et 7 ?

b. Montrer que : x solution du problème $\Leftrightarrow x \equiv x_0 (\text{mod}\, 3\times5\times7)$ (on pourra commencer par montrer que, si le nombre entier x est solution, alors 3×5 divise $x - x_0$).

c. Donner la plus petite solution entière positive du problème.

7. Lire le texte suivant et expliquer chaque phrase à l'aide de l'exercice précédent :

Extrait de *Histoire des mathématiques chinoises* de J.-C. Martzloff (Masson)

Dans le **Sunzi suanjing** (Classique arithmétique de Sunzi, probablement écrit vers le $4^{ème}$ –$5^{ème}$ siècle de notre ère), on rencontre le problème suivant :

Soit des objets en nombre inconnu : si on les compte par 3, il en reste 2 ; par 5, il en reste 3 et par 7, il en reste 2. Combien y a-t-il d'objets ?

Règle : « En comptant par 3, il en reste 2 » : poser 140 ; « en comptant par 5, il en reste 3 » : poser 63 ; « en comptant par 7, il en reste 2 » : poser 30. Faire la somme de ces trois nombres, obtenir 233. Soustraire 210 de ce total, d'où la réponse.

En général, pour chaque unité restante d'un décompte par 3, poser 70 ; pour chaque unité restante d'un décompte par 5, poser 21 ; pour chaque unité restante d'un décompte par 7, poser 15. Si (la somme ainsi obtenue) vaut 106 ou plus, ôter 105 pour trouver la réponse.

8. Résoudre le système de congruences suivant, d'inconnues x entier relatif et où a, b et c sont des entiers relatifs donnés :

$$\begin{cases} x \equiv a (\text{mod}\, 3) \\ x \equiv b (\text{mod}\, 5) \\ x \equiv c (\text{mod}\, 7) \end{cases}$$

(vous justifierez votre réponse).

9. Question facultative :

a. donner une procédure permettant de résoudre le système de congruences suivant :

$$\begin{cases} x \equiv a (\text{mod}\, m_1) \\ x \equiv b (\text{mod}\, m_2) \\ x \equiv c (\text{mod}\, m_3) \end{cases}$$

où les entiers relatifs a, b et c sont donnés, et les entiers naturels m_1, m_2, m_3 sont premiers entre eux deux à deux.

b. Justifier cette procédure.

Ce type de problème et cette procédure de résolution apparaissent à plusieurs reprises dans la littérature mathématique chinoise. Voici un extrait de «*une histoire des mathématiques chinoises* de Kiosy Yabuuti (Belin 2000) :

> « Dans son *Livre des nombres en neuf chapitres*, Qin Jiushao, des Song du Sud, lui donne le nom de « *procédure de la grande expansion de recherche de l'unité* » et expose en détail une méthode de résolution. Qin Jiushao applique sa méthode à des problèmes calendaires. Comme nous l'avons mentionné, le lien entre ce type de problème et les problèmes calendaires remonte aux Han. Le problème du *Classique Mathématique de Maître Sun* est précurseur de la « *procédure de la grande expansion de recherche de l'unité* » ; celle-ci constitue l'une des grandes recherches de l'époque des Song du Sud, et l'un des résultats remarquables des mathématiques chinoises. »

Repères chronologiques :

- Han : de 206 avant J.-C. à 220 après J.-C.
- Tang : 618-907 (c'est l'époque du juge Ti, héros des romans policiers de Robert Van Gulik, Collection 10/18 ; lisez donc, si ce n'est déjà fait, le premier de la série : *Trafic d'or sous les Tang*).
- Song :
  Song du Nord : 960-1127
  Song du Sud : 1127-1279

Le résultat donnant de façon générale l'existence et la forme des solutions d'un système de congruences de premier degré dont les modules sont premiers entre eux deux à deux s'appelle « théorème chinois des restes » (« chinese remainders theorem » pour les Anglo-Saxons).

Problème 3 *Etude des diviseurs des nombres de Mersenne à l'aide du théorème de Fermat*

Depuis l'Antiquité, les mathématiciens se sont préoccupés de nombres appelés *parfaits* : un nombre *N* est dit parfait lorsqu'il est égal à la somme de ses diviseurs stricts (c'est-à-dire différents de *N* ; les Grecs et leur successeurs parlaient de *parties aliquotes*).

7. Déterminer les diviseurs de 6 et 28. Sont-ils parfaits ?
8. Soit *n* un entier naturel non nul. Le nombre $M_n = 2^n - 1$ est appelé *nombre de Mersenne*. montrer que, si M_n est un nombre premier *p*, alors le nombre $N = 2^{n-1}\left(2^n - 1\right)$ est un nombre parfait (pour écrire tous les diviseurs de *N* différents de *N*, demandez-vous quelle est la décomposition en produit de facteurs premiers de *N* et employez la méthode du cours).
9. Montrez que, si le nombre *n* est composé, alors M_n est composé. Que peut-on alors dire de *n* si M_n est premier ?
10. Le nombre M_{11} est-il premier ?

II. Nombres de Mersenne.

Le problème des nombres parfaits nous amène alors à chercher un moyen de savoir si , pour un nombre premier donné *n*, le nombre M_n est premier ou composé. *A priori*, cela nécessite de chercher si M_n est divisible par un nombre premier inférieur ou égal à sa racine carrée. Nous allons, comme Fermat au dix-septième siècle, chercher un « abrégé ».

1. Soit un nombre **premier** *n* différent de 2 et un nombre premier *p*. On suppose que *p* divise M_n. On a donc $2^n \equiv 1 \pmod{p}$. On appelle *d* le plus petit entier strictement positif tel que $2^d \equiv 1 \pmod{p}$.

d. On a donc : $d \leq n$. Montrer que *d* divise *n* (on pourra écrire l'égalité de division euclidienne de *n* par *d*).
e. En déduire : $d = n$.
f. Rappeler le théorème de Fermat. Que peut-on en déduire pour 2^{p-1} ?
g. Montrer que *n* divise $p - 1$.
h. En déduire qu'il existe un entier naturel *a* tel que : $p = 2an + 1$.

2. On considère le nombre de Mersenne $M_{37} = 2^{37} - 1$.

2. Soit *p* un nombre premier. Expliquez pourquoi, si *p* divise M_{37}, il existe un entier naturel *a* tel que : $p = 74a + 1$.
3. M_{37} est-il un nombre premier ?

III. Une lettre de Fermat.

Dans le texte de Fermat ci-joint (extrait de *Œuvres* de Fermat, éditées par Tannery et Henry, Tome II), Fermat appelle *progression double* la suite géométrique de terme général 2^n.

- Il appelle ainsi *radicaux des nombres parfaits* les nombres $2^n - 1$. Pourquoi ?
- A quelle question de l'exercice précédent correspond le 1°) de Fermat ?
- A quelle question de l'exercice précédent correspond le 3°) de Fermat ?
- Ecrire le 2°) avec nos notations (par exemple, le radical est $2^n - 1$) et énoncer le résultat du cours correspondant à ce 2°).
- Lire le numéro 7.

Voici trois propositions que j'ai trouvées, sur lesquelles j'espère de faire un grand bâtiment :

Les nombres moindres de l'unité que ceux qui procèdent de la progression double, comme

1	2	3	4	5	6	7	8	9	10	11	12	13	
1	3	7	15	31	63	127	255	511	1023	2047	4095	8191	etc.,

soient appelés les radicaux des nombres parfaits, pource que, toutes les fois qu'ils sont premiers, ils les produisent. Mettez, au dessus de ces nombres, autant en progression naturelle : 1, 2, 3, 4, 5, etc. qui soient appelés leurs exposants.

Cela supposé, je dis que :

1° Lorsque l'exposant d'un nombre radical est composé, son radical est aussi composé. Comme, parce que 6, exposant de 63, est composé, je dis que 63 est aussi composé.

2° Lorsque l'exposant est nombre premier, je dis que son radical moins l'unité est mesuré par le double de l'exposant. Comme, parce que 7, exposant de 127, est nombre premier, je dis que 126 est multiple de 14.

3° Lorsque l'exposant est nombre premier, je dis que son radical ne peut être mesuré par aucun nombre premier que par ceux qui sont plus grands de l'unité qu'un multiple du double de l'exposant ou que le double de l'exposant. Comme, parce que 11, exposant de 2047, est nombre premier, je dis qu'il ne peut être mesuré que par un nombre plus grand de l'unité que 22, comme 23, ou bien par un nombre plus grand de l'unité qu'un multiple de 22 : en effet 2047 n'est mesuré que par 23 ou par 89, duquel, si vous ôtez l'unité, reste 88, multiple de 22.

Voilà trois fort belles propositions que j'ai trouvées et prouvées non sans peine : je les puis appeler les fondements de l'invention des nombres parfaits. Je ne doute pas que M. Frenicle ne soit allé plus avant, mais je ne fais que commencer, et sans doute ces propositions passeront pour très belles dans l'esprit de ceux qui n'ont pas beaucoup

épluché ces matières, et je serai bien aise d'apprendre le sentiment de M. de Roberval.

7. Au reste, vous ou moi avons équivoqué de quelques caractères au nombre que j'avois cru parfait (1), ce que vous connoîtrez aisément puisque je vous baillois 137 438 953 471 pour son radical, lequel j'ai pourtant depuis trouvé, par l'abrégé tiré de ma troisième proposition, être divisible par 223; ce que j'ai connu à la seconde division que j'ai faite, car, l'exposant dudit radical étant 37, duquel le double est 74, j'ai commencé mes divisions par 149, plus grand de l'unité que le double de 74; puis, continuant par 223, plus grand de l'unité que le triple de 74, j'ai trouvé que ledit radical est multiple de 223.

De ces abrégés j'en vois déjà naître un grand nombre d'autres et *mi par di veder un gran lume.*

Je vous entretiendrai un jour de mon progrès, si M. Frenicle me vient au secours et m'abrège par ce moyen ma recherche des abrégés. En tout cas, je vous conjure de faire en sorte que M. de Roberval joigne son travail au mien, puisque je me trouve pressé de beaucoup d'occupations qui ne me laissent que fort peu de temps à vaquer à ces choses.

Je suis etc.

Problème 4 *Factorisation de grands nombres et machine de Carissan*

En 1643, Fermat répond à Mersenne qui lui a lancé le défi de factoriser 100 895 598 169. Il trouve cette factorisation (898 423 x 112 303), mais indique dans une lettre ultérieure une méthode générale. C'est cette lettre que nous allons lire ensemble.

I. DIFFERENCE DE DEUX CARRES ET FACTORISATION

Soit N un nombre entier naturel impair.
1°) On suppose que $N=a^2-b^2$ avec a et b entiers naturels. Déterminer deux entiers naturels p et q tels que N=pq.
2°) On suppose que N=pq avec p et q entiers naturels et p > q.

a) Quelle est la parité de p et q ?

b) Montrer qu'il existe deux entiers naturels a et b tels que $N=a^2-b^2$.

c) Démontrer que :
« p et q sont premiers entre eux » équivaut à « a et b sont premiers entre eux ».
3°) Fermat utilise les définitions suivantes :

Les nombres compositeurs sont les facteurs d'un nombre composé.

Ex : 45 = 9x5 ; 9 et 5 sont les compositeurs du nombre composé 45.

Les parties d'un nombre sont ses diviseurs, c'est-à-dire les compositeurs.

a) Lire le texte lignes 1 à 14 (attention, à la ligne 2, traduire « *ou* » par « *c'est-à-dire* »).

b) Quelle est la phrase du texte de Fermat correspondant aux questions 1°) et 2°)b) ?

c) Quelle est la phrase du texte de Fermat correspondant à la question 2°)c) ?

d) Que se passe-t-il si N est un carré ?

e) Lire les lignes 15 et 16 et les traduire avec des notations algébriques.

II. FACTORISATION DE GRANDS NOMBRES

Le but de cette partie est la factorisation de N = 250 507. Cela revient à déterminer deux entiers naturels x et y tels que $x^2 - y^2 = N$ (équation notée (E) dans la suite). Une telle équation s'appelle « équation diophantienne ».

1°)Travail modulo 7.

a)Compléter le tableau suivant par le reste de X^2 modulo 7 suivant les valeurs de X.

X	0	1	2	3	4	5	6
X^2				2			

Le nombre 7 × 113 + 3 peut-il être un carré ? Pourquoi ? (Il est impératif d'utiliser le tableau précédent et son cerveau, mais surtout pas la calculatrice !)[1].

b) On cherche à résoudre $x^2 - y^2 = 250\,507$, c'est-à-dire $x^2 - 250\,507 = y^2$. Donc, si le nombre entier x est solution, alors le nombre $x^2 - 250\,507$ doit être un carré. A l'aide du tableau précédent, déterminer les valeurs possibles modulo 7 de $x^2 - 250\,507$. En déduire les valeurs possibles modulo 7 de x^2.

[1] Les nombres 0, 1, 2, 4 s'appellent résidus quadratiques modulo 7.

c) Mais x^2 doit être un carré, donc le même tableau permet de restreindre encore les valeurs possibles de x^2 modulo 7. Le faire, puis en déduire les valeurs possibles de x modulo 7. Le nombre 778 peut-il être solution de l'équation (E) ?

2°) Faire un travail analogue modulo 9.

3°) Faire un travail analogue modulo 15.

4°) Résolution de l'équation (E) : $x^2 - y^2 = 250\,507$.

a) Justifier : si x est solution de (E), alors $x \geq \sqrt{250507}$. Quelle est la plus petite valeur possible de x ?

b) Soit $x_0 = 501$. Calculer les restes de x_0 modulo 7, modulo 9 et modulo 15. Le nombre x_0 est-il solution de l'équation (E) ?

c) Remplir le tableau suivant jusqu'à trouver une valeur de x compatible avec les conditions trouvées dans les questions 1°), 2°), 3°).

x	501	502	503	504	...
mod7					
mod9					
mod15					

Est-on sûr que la valeur ainsi trouvée est solution de l'équation (E) ?
Vérifier que cette valeur est bien une solution et en déduire une factorisation de 250 507.

Extrait de : Fermat *Œuvres* éd. Tannery et Henry, tome II, 1894, Lettre de 1643, pp. 257-258

LVII.

FRAGMENT D'UNE LETTRE DE FERMAT (²).

< 1643 >

(A, f° 74.)

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres, et, si les quarrés sont premiers entre eux, les nombres compositeurs le sont aussi. Mais si les quarrés ont entre eux un commun diviseur, le nombre en question sera aussi divisible par le même commun diviseur, et les nombres compositeurs seront divisibles par le côté de ce commun diviseur.

Par exemple : 45 est composé de 5 et de 9, de 3 et de 15, de 1 et de 45. Partant, il sera trois fois la différence de deux quarrés : savoir de 4 et de 49, qui sont premiers entre eux, comme aussi sont les compositeurs correspondants 5 et 9; plus, de 36 et de 81, qui ont 9 pour commun diviseur, et les compositeurs correspondants, 3 et 15, ont le côté de 9, savoir 3, pour commun diviseur; enfin 45 est la différence de 484 et 529, qui ont 1 et 45 pour compositeurs correspondants.

Il est fort aisé de trouver les quarrés satisfaisants, quand on a le nombre et ses parties, et d'avoir les parties lorsqu'on a les quarrés.

Dans l'article de la page suivante, Eugène Carissan présente une machine à résoudre des équations diophantiennes selon le principe de la partie II du problème ; cette machine peut donc servir à factoriser de grands nombres, ce qu'a effectivement fait Eugène Carissan. Par exemple :

3 570 537 526 921 = 841 249 x 4 244 329

(18 minutes d'utilisation de la machine)

L'idée est de mécaniser les recherches des valeurs possibles de *x* selon les différents modules (14 modules différents dans la machine de Carissan : 19 ; 21 = 3 x 7 ; 23 ; 26 = 2 x 13 ; 29 ; 31 ; 34 = 2 x 17 ; 37 ; 41 ; 43 ; 53 ; 55 = 5 x 11 ; 59).

Extrait d'un article d'Eugène Carissan paru en 1920 dans le *Bulletin de la Société d'Encouragement à l'Industrie Nationale*

MACHINE A RÉSOUDRE LES CONGRUENCES[1]

But. — Cet appareil, qui a figuré à l'Exposition de machines à calculer organisée par la Société d'Encouragement du 5 au 13 juin 1920, a pour but la résolution mécanique, en nombres entiers, des équations indéterminées à deux variables.

Principe. — La machine est une application de la théorie des congruences, et des méthodes d'utilisation de cette théorie qu'a instituées M. André Gérardin, de Nancy (2), pour la résolution des équations indéterminées.

Soit, à titre d'exemple simple, à résoudre en nombres entiers l'équation :

$$x^2 - 6y^2 = 1\,324\,801 = A$$

ou

$$6y^2 + A = x^2. \qquad (1)$$

On envisage successivement les diverses hypothèses possibles : $y =$ mult. de $m + 0, 1, 2, \ldots (m-1)$, pour un certain nombre de diviseurs ou modules m, et on examine dans chacune de ces hypothèses s'il y a compatibilité entre le premier et le deuxième membre de l'équation (1), en tenant compte de ce fait que x^2 ne peut avoir, pour un module déterminé, que certaines valeurs connues à l'avance (résidus quadratiques).

Soit à appliquer le module 5; on a, en remarquant que A est un mult. de $5 + 1$, et que les résidus quadratiques (valeurs de x^2) ne peuvent être, en module 5, que 0, 1, 4 :

1re hypothèse :
$y =$ mult. de $5+0$; $6y^2 =$ mult. de $5+0$; $6y^2 + A =$ mult. $5+1$ . . . combinaison *possible*.
2e et 5e hypothèses :
$y =$ mult. de 5 ± 1; $6y^2 =$ mult. de $5+1$; $6y^2 + A =$ mult. $5+2$ . . . — *impossible*.
3e et 4e hypothèses :
$y =$ mult. de 5 ± 2; $6y^2 =$ mult. de $5+4$; $6y^2 + A =$ mult. $5+0$ . . . — *possible*.

En résumé, y ne peut être que mult. de $5 + 0$; mult. de $5 + 2$; mult. de $5 + 3$, ce que nous exprimons par la *bande modulaire* 0I00I, dans laquelle : le signe 0 marque la possibilité, le signe I l'impossibilité.

(1) Communication faite en séance publique par l'auteur le 26 juin 1920.
(2) Directeur de la revue : *Le Sphinx-Œdipe*, 32, Quai Claude-Le-Lorrain, Nancy.

Portrait de Marin Mersenne