Un problème de restes et sa résolution par Qin Jiushao au 13e siècle(*)

Arnaud Gazagnes(**)

Résumé. Les calculs en astronomie ont donné lieu très probablement à la naissance des congruences. Qin Jiushao, au XIIIe siècle, résolut (ou, du moins, trouva une solution à) un problème de répartition de grains, basé sur un système de congruences. On s'intéressera aussi à une réduction de modules pour les rendre premiers entre eux deux à deux et à une résolution d'une équation avec congruence, faites dans son *Shushu Jiuzhang*, ces procédés intervenant dans sa résolution.

1. Des problèmes de restes

1.1. Une origine possible du « théorème des restes chinois »

Selon les textes dont disposent les historiens, une source de ce type de problème (de restes) pourrait être d'ordre astronomique. En effet, pour être plus précis, l'un des thèmes centraux dans la construction d'un calendrier est la détermination de l'origine de certaines périodes cycliques comme l'année, le mois ou l'(artificiel) cycle de 60 jours(1). Cette « recherche inverse de l'origine » est une difficulté longtemps rencontrée(2).

Le problème général pour dresser un calendrier est l'incommensurabilité entre les révolutions solaires (par année et par jour) et le mois lunaire. Ainsi interviennent le nombre de jours écoulés entre un moment donné et le début des cycles annuel, lunaire ou sexagésimal en cours. En posant x le nombre de jours entre le début des cycles d'un instant pendant lequel n_1 jours du cycle annuel (désigné par A), n_2 jours du cycle du mois lunaire (L) et n_3 jours du cycle sexagésimal (S) se sont écoulés depuis le dernier commencement de ces cycles, le problème s'énonce ainsi :

(*) Cet article est tiré de la brochure *Promenades mathématiques en Chine Ancienne*, en cours de rédaction et qui sera publiée par l'IREM de Reims.

(**) IREM de Reims. Mél : a.gazagnes@voila.fr

(1) L'année chinoise était divisée en 24 périodes de 15 jours. Ce cycle de 60 jours provient de la combinaison d'un cycle de 10 jours et d'un cycle de 12 jours (le plus petit commun multiple de 10 et 12 étant 60). Le premier cycle définit les *dix troncs célestes* (*tian gan*) ; le second, les *douze rameaux terrestres* (*dizhu*). L'usage de cette méthode remonterait à Huangdi, l'Empereur Jaune, dont le règne légendaire aurait débuté en – 2697. Depuis notre VIe siècle, est associé à chaque rameau terrestre un des douze animaux du zodiaque : rat, bœuf, tigre, dragon, … Pour déterminer un élément du cycle, on note un élément du tronc suivi d'un des rameaux. Pour le compte des années, les Chinois utilisaient les années de règne de leurs empereurs et le cycle de 60 était utilisé pour contrôler. Par exemple, la première année du règne Tianhan de l'empereur Wudi correspond à notre année – 100 ; pour désigner l'année – 99, on parlera de la deuxième année de ce règne. Depuis 1949, on n'utilise plus en Chine officiellement que les millésimes grégoriens.

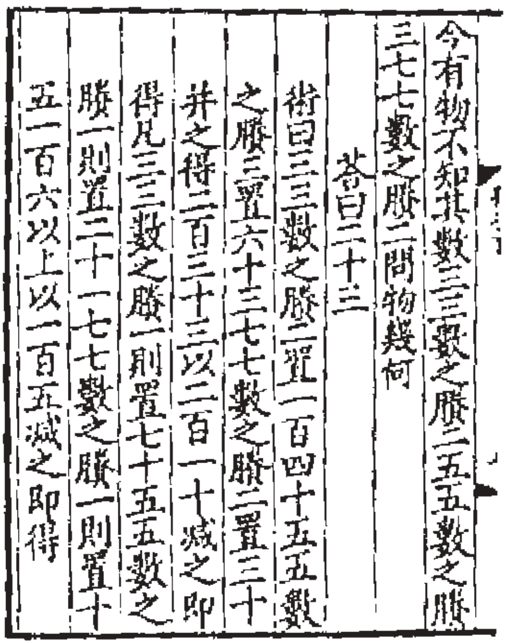
(2) Cette recherche remonte à la période des Han (– 206, 220).

$$x \equiv n_1 \text{ (mod A)} \equiv n_2 \text{ (mod L)} \equiv n_3 \text{ (mod S)}.$$

La façon dont les auteurs chinois (tout comme ceux d'autres civilisations, au Moyen Âge) traitent ce problème des restes n'apporte rien sur leur raisonnement arithmétique. Toutefois, les solutions sont expliquées par des règles, non justifiées, et sont correctes.

1.2. Du « problème de Sunzi »…

Dans le troisième chapitre du S*unzi suanjing*(3) (datant sans doute de l'époque des Six Dynasties (de 220 à 589)), on trouve(4) le problème suivant, appelé traditionnellement « problème de Sunzi » ; c'est le plus ancien problème de restes (ou, dit de façon moderne, de congruence) dont nous ayons la trace. Comme dans tout manuel mathématique ancien, il est donné l'énoncé, sa réponse, puis sa règle de résolution (sans justification).


今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

Problème de Sunzi, reproduit dans la Collection *Tianlu linlang* (1932).

<u>*Problème 3-26 du* Sunzi suanjing.</u>

Suppose que l'on ait un nombre inconnu d'objets. S'ils sont comptés par 3, il en reste 2, s'ils sont comptés par 5, il en reste 3 et s'ils sont comptés par 7, il en reste 2. Combien d'objets y a-t-il ?

(3) Littéralement : *Classique mathématique de Sunzi*. Ce mathématicien, dont on ignore beaucoup, voire s'il a réellement existé, comme Pythagore en Occident, n'est pas à confondre avec un général du même nom (« en français ») qui a écrit *L'art de la guerre*.

(4) Le texte original est perdu ; la version existante est composée d'extraits inclus dans la grande encyclopédie *Yongle dadian* [*Grande Encyclopédie de la période de règne Yongle*] (1407). Cette même encyclopédie contient aussi le *Shushu Jiuzhang* de Qin Juishao : c'est pour cette raison principale qu'on le connaît.

Réponse : 23.

Règle : S'ils sont comptés par 3, il en reste 2 : soit 140. S'ils sont comptés par 5, il en reste 3 : soit 63. S'ils sont comptés par 7, il en reste 2 : soit 30. Prends la somme [de ces trois nombres] pour obtenir 233. Soustrais 210 de ce total ; cela donne la réponse.

Il s'agit donc de déterminer le plus petit entier positif N tel que :

$$\mathrm{N} = 3x + 2 = 5y + 3 = 7z + 2,$$

ou encore

$$\mathrm{N} \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 2 \pmod 7.$$

La valeur de N cherchée est $70 \times 2 + 21 \times 3 + 15 \times 2 - 210$.

La seconde partie de la méthode indique comment trouver N lorsque les restes (pourvu que les modules soient 3, 5 et 7) sont a, b et c :

En général : Pour chaque unité restante en comptant par 3, soit 70(5)*. Pour chaque unité restante en comptant par 5, soit 21. Pour chaque unité restante en comptant par 7, soit 15. Si [la somme obtenue ainsi] vaut 106 ou plus, soustrais 105 pour obtenir la réponse.*

On calcule

$$\mathrm{N} = 70a + 21b + 15c - 105n.$$

La méthode de résolution, explicitée ci-dessus, est appelée « soustraction de 105 » (d'où le n), 105 étant le plus petit commun multiple des trois modules donnés, 3, 5 et 7.

Le petit poème suivant, correspondant au calcul

$$((2 \times 70) + (3 \times 21) + (2 \times 15)) - 105 - 105 = 23$$

a été écrit entre les dynasties Han et Ming et servait de moyen mnémotechnique pour la méthode :

« Trois septuagénaires dans la même famille ? Rare ! | Cinq pruniers avec vingt-et-une branches en fleurs | Sept mariés en parfaite harmonie ? | [C'est] précisément le milieu du mois ! | Cent cinq soustrait ? Et voilà le résultat ! ».

Petites explications… Les trois septuagénaires se rapportent aux nombres 70 et 3 du premier regroupement. De même, les cinq pruniers avec vingt-et-une branches se rapportent aux nombres 21 et 5. Le troisième vers parle du nombre 7. Le quatrième vers parle indirectement du nombre 15 : le “milieu du mois” fait allusion à la date de la fête de mariage ayant lieu le quinzième jour du mois lunaire et, ce jour-là, les filles mariées retournent chez leurs parents leur rendre hommage. La suite se comprend sans peine.

(5) $70 = 2 \times 5 \times 7$; $21 = 3 \times 7$; $15 = 3 \times 5$. 21 (respectivement 15) a été choisi parce qu'il est congru à 1 modulo 5 (respectivement 7) et à 0 modulo 3 et 7 (respectivement 3 et 5). 35 est congru à 0 modulo 5 et 7 mais pas à 1 modulo 3 ; c'est pourquoi il est pris $2 \times 35 = 70$, qui convient, quant aux congruences. On s'approche de l'équation du paragraphe 3…

1.3. … au problème de Qin Jiushao

Ce problème des restes connaît son apogée en Chine avec Qin Jiushao, à travers son *Shushu Jiuzhang*(6), en 1247.

Celui-ci résout des congruences du premier degré par une méthode qu'il appelle *dayan qiu yi shu* [*procédure de la grande expansion pour la recherche de l'unité*], tout en se contentant d'une seule solution, la plus petite valeur positive. Il ne prétend pas être l'auteur de sa règle *dayan*(7), mais l'avoir apprise par les travaux sur les calendriers. Dans son introduction, Qin Jiushao écrit : « Toutefois, la méthode *dayan* n'est pas contenue dans le *Jiuzhang*(8) car, pour l'instant, personne n'a été capable de le tirer [d'autres procédures]. Ceux qui construisent les calendriers en ont fait une utilisation considérable tout en affinant leurs méthodes »(9). Un problème ayant pour thème une répartition de grains sera traité dans le paragraphe 4. Toutefois, il nous faut aborder auparavant les paragraphes 2 et 3. Dans cette même introduction, il fait mention des calendriers *dayan li et huangji li*(10). Il est possible que Qin Jiushao relie le problème du calendrier avec le problème de Sunzi, bien que ne le mentionnant pas, contrairement à la plupart des mathématiciens de son époque. De plus, Qin Jiushao ne semble pas avoir été intéressé par les problèmes de calendrier en tant que tels : ils n'ont été pour lui qu'une source d'inspiration. En effet, seul un de ses dix problèmes de restes (le deuxième) traite de calendrier ; les neuf autres traitent de divination, finances, logistique militaire, architecture et travaux d'excavation.

La question de l'origine de cette règle reste ouverte… Sa règle permet de résoudre le problème des restes sous sa forme la plus générale, ce qui présente une formidable avancée mathématique.

Qin Jiushao n'a cependant pas été le seul à se pencher sur ce problème. En Chine, le mathématicien Yang Hui en 1275 (soit près de huit siècles plus tard) écrit un ouvrage(11) contenant cinq versions d'un même problème de restes. Nous pouvons citer, hors de Chine, en Inde Brahmagupta (vers 625) et Bhâskara (au XIIe siècle), en

(6) Littéralement : « Le livre des nombres en neuf chapitres ».
(7) Needham (cité dans l'ouvrage référencé de Libbrecht) donne l'explication de ce terme : « Au cours du temps, les méthodes sur les problèmes indéterminés prirent le nom de *dayan shu*, dérivé d'une obscure phrase dans le *Yijing* affirmant que le “ nombre de la grande expansion ” est 50. […] La raison de l'adoption de ce terme technique est assez claire. Dans la méthode classique de consultation des oracles que le *Yijing* [*Livre des mutations*] décrit […], l'une des 50 tiges ou baguettes est mise de côté avant que les 49 soient divisées en deux tas aléatoires symbolisant le *ying* et le *yang*. Il était très naturel, par conséquent, que les mathématiciens, cherchant les restes de l'un par des divisions continues, se soient souvenus de cela. »
(8) Nom abrégé d'un ouvrage fondamental dans les mathématiques chinoises.
(9) Il prétend donc qu'une source de ce type de problèmes se trouve dans les problèmes chronologiques.
(10) Le *dayan li* [*Calendrier de la grande expansion*] a été construit par le moine Yixing en −727, le *huangji li* [*Calendrier du faîte impérial*], par Liu Zhou au milieu du VIe siècle.
(11) *Xugu zhaiqi suanga* [*Continuation d'un choix de méthodes mathématiques anciennes curieuses*].

Occident, Léonard de Pise (Fibonacci)[12] et, dans la civilisation arabe, Ibn al Haytham (965-1040)[13]. Il n'y aura plus guère de travaux dans ces civilisations sur ce thème après le XIII^{e} siècle ; le monde attendra le XV^{e} siècle pour voir naître de nouveaux travaux, puis viendront ceux de Lagrange, Euler et Gauss.

2. Recherche de modules premiers entre eux

On va exhiber la méthode de Qin Jiushao à l'aide du problème 1-3 du *Shushu Jiuzhang*, dans lequel il faut chercher les modules réduits de 54, 57, 75 et 72, c'est-à-dire des modules premiers entre eux deux à deux (ou encore : PGCD $(m_i, m_j) = 1$ pour tous $i \neq j$)[14].

- Le procédé commence par trouver le PGCD de ces quatre nombres, soit 3, calculé par soustractions successives.

  Par exemple, calculons PGCD (57, 72) :

$72 - 57 = 15$	$15 - 12 = 3$
$57 - 15 = 42$	$12 - 3 = 9$
$42 - 15 = 27$	$9 - 3 = 6$
$27 - 15 = 12$	$6 - 3 = 3$

  Le résultat 3 est apparu au moins deux fois, donc PGCD (57, 72) = 3. (On comprend ainsi pourquoi les mathématiciens chinois appelèrent très tôt le PGCD « l'égal », *deng*.)

- Puis les trois plus grands nombres sont divisés par ce PGCD.

  (54, 57, 75, 72) est remplacé par (54, 19, 25, 24).

- La réduction est suivie par la recherche du PGCD des nouveaux nombres en étudiant successivement tous les couples de nombres dont le premier élément est 24, puis 25, puis 19.

  Lorsque PGCD $(m, n) = d \neq 1$, le couple est remplacé par $\left(m, \dfrac{n}{d}\right)$.

  PGCD (24, 25) = 1   PGCD (24, 19) = 1   PGCD (24, 54) = 6
  (24, 54) est remplacé par (24, 9) puis (54, 19, 25, 24), par (9, 19, 25, 24).

- Ensuite, chaque couple obtenu (p, q) est revu et une autre manipulation est faite :

  si PGCD $(p, q) = \mathrm{D} \neq 1$, le couple est remplacé par $\left(\dfrac{p}{\mathrm{D}}, q\mathrm{D}\right)$.

  PGCD (25, 19) = 1   PGCD (25, 9) = 1   PGCD (24, 19) = 1
  PGCD (24, 9) = 3
  (24, 9) est remplacé par (8, 27), puis (9, 19, 25, 24), par (27, 19, 25, 8).

---

(12) L'un de ses énoncés dans son *Liber Abaci* (1202) est très similaire à celui de Sunzi. Il s'agit de résoudre N ≡ 2 (mod 3), N ≡ 3 (mod 5), N ≡ 4 (mod 7).

(13) Il résout le problème $x \equiv 1 \pmod{m_i}$ et $x \equiv 0 \pmod{p}$, avec p premier et $1 < m_i < p$.

(14) La résolution de ce problème demande de trouver une solution de N ≡ 0 (mod 54) ≡ 0 (mod 57) ≡ 51 (mod 75) ≡ 18 (mod 72).

Les valeurs des modules réduits sont donc **27**, **19**, **25** et **8**.

À titre d'exemple, voici les étapes successives pour 300, 240 et 180 (ces nombres sont énoncés dans le problème 6 de ce même chapitre).

- 300 240 180
- 300 4 3
- 100 4 9
- 25 16 9

Ceci écrit, il faut signaler que Qin Jiushao distingue quatre types de nombres : les nombres entiers (*yuanshu*), les nombres décimaux (*shoushu*), les nombres fractionnaires (*tongshu*) et les multiples des puissances de 10 (*fushu*). Pour chaque type, il y a une règle qui amène à travailler sur des nombres entiers. Voici les étapes successives dans le cas des trois nombres(15) $365+\frac{1}{4}$, $29+\frac{499}{940}$ et 60 :

- $365+\frac{1}{4}=\frac{1\,461}{4}$ $\qquad 29+\frac{499}{940}=\frac{27\,759}{940}$ $\qquad 60=\frac{60}{1}$
- $\frac{1\,461 \quad 940 \quad 1}{940 \quad 4 \quad 1}$ $\qquad \frac{27\,759 \quad 4 \quad 1}{940 \quad 4 \quad 1}$ $\qquad \frac{60 \quad 940 \quad 4}{940 \quad 4 \quad 1}$
- 1 373 340 111 036 225 600
- PGCD (1 373 340, 111 036, 225 600) = 12
- $\frac{1\,373\,340}{12}=114\,445$ $\qquad \frac{111\,036}{12}=9\,253$ $\qquad 225\,600$

Le mathématicien travaille alors avec les trois nombres 114 445, 9 253 et 225 600.

3. Résolution d'une équation avec congruence

3.1. Présentation de la méthode

L'équation générique à résoudre est : $ax \equiv 1 \pmod{m}$, avec a et m donnés.

Qin Jiushao appelle « surplus » (*qi*) le coefficient a et « mère de l'expansion » (*yanmu*) le coefficient m. Le terme de « surplus » est utilisé parce que a est un reste modulo m. Le terme *yanmu* rappelle que nous sommes dans le domaine de travail de la règle *dayan*. Le terme de « mère » (*mu*) est issu du calcul fractionnaire. En effet, le numérateur est usuellement appelé « le fils » et le dénominateur, « la mère »(16). Les mathématiciens ont voulu exprimer le fait que les calculs de restes ont un lien avec les calculs de fractions. Pourtant, même si les érudits chinois ne s'en sont pas aperçus, la méthode résolutoire de Qin Jiushao correspond à la détermination sous

(15) Qin Jiushao utilise les données du *Sifen li* [*Calendrier au quart*], datant d'avant la dynastie des Han (donc avant − 206), où l'année compte 365 jours 1/4 (ce quart explique le nom du titre), le mois, 29 jours 499/940 et le cycle sexagésimal est utilisé.

(16) Probablement parce que l'auteur de ces expressions pensait à une mère enceinte et son enfant, soulignant à la fois la différence en taille et le lien intime entre les deux termes. Les numérateurs représentent un certain nombre de parts produites par le dénominateur…

forme de fractions continues de $\frac{m}{a}$[17].

La partie I ci-dessous est en fait ce que nous nommons « algorithme d'Euclide ». Cet algorithme apparaît déjà dans le *Jiuzhang Suanshu* (*Les neuf chapitres de techniques de calcul*, écrit sous la dynastie des Han) sous la forme de « soustractions alternées ». Les notations sont celles de Vinogradrov[18].

Ce type de solution correspond à ce qui est expliqué dans pratiquement tout livre de théorie élémentaire des nombres. Une chose est toutefois essentielle à voir : Qin Jiushao ne connaît pas la notion de nombres premiers et il procède **uniquement** à l'aide de cet algorithme d'Euclide (ou des généralisations et variantes de celui-ci), mais jamais par décompositions d'un nombre en un produit de nombres premiers[19]. Il n'en demeure pas moins que sa démarche est la même que celle qui repose sur les fractions continues. Cependant, Qin Jiushao ne travaille qu'avec des nombres positifs : c'est pourquoi il donne deux résultats, suivant que le nombre de divisions dans son algorithme d'Euclide est pair ou non.

Selon l'historien Qian Baocong, Qin Jiushao résout[20] le problème ainsi :

Partie I	Partie II	Partie III
$m = aq_1 + r_2$ $a = r_2q_2 + r_3$ $r_2 = r_3q_3 + r_4$ … $r_{n-2} = r_{n-1}q_{n-1} + r_n$ (avec $r_n = 1$ et $q_n = r_{n-1}$)	$P_0 = 1$ $P_1 = q_1$ $P_2 = q_2P_1 + P_0$ $P_3 = q_3P_2 + P_1$ … $P_{n-1} = q_{n-1}P_{n-2} + P_{n-3}$ (et $P_n = m$)	• si n est impair, $x = P_{n-1}$, • si n est pair, $x = (r_{n-1} - 1)P_{n-1} + P_{n-2}$

La solution x ainsi obtenue est **la plus petite solution positive**.

3.2. Application à une équation particulière

Qin Jiushao résout l'équation $\boxed{377\,873\,x \equiv 1 \pmod{499\,067}}$.

Le tableau ci-dessous donne les calculs successifs de la résolution. (Les différents calculs des trois parties ont été regroupés.)

(17) Cette détermination implique, d'une part, la recherche du PGCD de a et de m par la méthode des soustractions alternées et, d'autre part, la détermination d'une solution positive de l'équation $ax - my = 1$ (équivalente à l'équation $ax \equiv 1 \pmod{m}$).

(18) *Elements of Number Theory*, Vinogradov, I. M., New York : Dover, 1954. Cité dans l'ouvrage anglais de J.-Cl. Martzloff.

(19) On ne traitera donc pas des conditions algébriques modernes (de facto anachroniques) comme (1) a et m sont premiers entre eux ou (2) le cas $m \equiv 1 \pmod{a}$…

(20) Les étapes suivantes se prêtent très bien à un travail sur tableur… Il y a néanmoins des cas pathologiques comme ceux de la note précédente qui demanderont un approfondissement !

s	0	1	2	3	4	5	6	7	8	9	10
q_s		1	3	8	2	12	3	1	1	6	12
r_s			121 194	14 291	6 866	559	158	85	73	12	1
P_s	1	1	4	33	70	873	2 689	3 562	6 251	41 068	499 067

On a $r_s = 1$ pour $s = 10$ et 10 est pair.

La solution est $x = (r_9 - 1)\,P_9 + P_8 = (12 - 1) \times 41\,068 + 6\,251 = 457\,999$.

4. Résolution d'un système de congruences

On va s'intéresser maintenant à la résolution complète par Qin Jiushao du problème 2-1 du *Shushu Jiuzhang* :

Suppose que nous ayons trois paysans de première classe. Les productions respectives de leurs rizières(21) *sont toutes égales entre elles (on le constate en se servant de la mesure de capacité (hu)). Sachant que A (jia) a vendu son riz au marché officiel de sa propre préfecture, sachant aussi (qu'après cela) il lui en est resté 3 dou 2 sheng*(22)*, que B (yi) a vendu son riz aux villageois d'Anji*(23) *et (en fin de compte) il lui en est resté 7 dou, C (bing) a vendu son riz à un intermédiaire de Pingjiang et il lui en est resté 3 dou, on demande quelle était la quantité initiale de riz que possédait chacun des paysans et quelle quantité chacun d'entre eux a vendue. (Nota : Le hu du pavillon de Wensi vaut 83 sheng, celui d'Anji, 110 et celui de Pingjiang, 135).*

Réponse. Quantité totale de riz : 738 dan à répartir entre 3 hommes soit 246 dan chacun. Quantité de riz vendue par A : 296 dan, par B : 223 dan, par C : 182 dan.

Avec nos notations modernes, Qin Jiushao cherche à trouver la plus petite solution du système

$\boxed{\begin{cases} x \equiv 32 \pmod{83} \\ x \equiv 70 \pmod{110} \\ x \equiv 30 \pmod{135} \end{cases}}$, où x est le montant de riz en sheng de chaque paysan.

Qin Jiushao présente sa méthode ainsi(24) :
Utiliser la méthode dayan :

(21) Le riz est cultivé dans la Chine du Sud (région chinoise la plus ensoleillée et humide) tandis que le blé et le millet sont cultivés dans la Chine du Nord (où les régions sont plus sèches). Les villes citées après se placent dans des provinces du Sud.
(22) Unités utilisées : 1 *dou* = 10 *sheng* (mesure de capacité - boisseau) et 1 *dan* = 10 *dou*.
(23) Anji est une préfecture de la province Zhejiang, Pingjiang est une préfecture de le province Hunan. Le pavillon de Wensi (*wensi yuan*) est une agence gouvernementale sous les Song, où les ouvriers eunuques produisent de la joaillerie, des brocarts, … pour l'Empereur et ses femmes.
(24) Les trois valeurs numériques, placées à côté de la terminologie, correspondent à chacune des trois équations. On se ramène au système lorsqu'il n'y a qu'une valeur écrite. Un calcul est présenté lorsque cela éclaire la méthode.

- *Poser les modules des administrations locales en tant que nombres primordiaux.*

Yuanshu Nombres primordiaux y_i	83	110	135

- *Joindre tout d'abord les nombres par 2 et chercher leur égal commun.*

  Qin Jiushao calcule le PGCD de ces trois nombres et trouve 1.

- *Comme on ne peut pas simplifier ces nombres en une seule fois, on les simplifie séparément : (donc) on cherche les égaux deux à deux, en chaîne. Simplifier les impairs et non les pairs*[25] *. Obtenir ainsi les mères déterminées. […]*

  C'est la réduction des modules. Il calcule PGCD (83, 110), PGCD (83, 135) et PGCD (110, 135) par soustractions successives (voir le paragraphe 2) et trouve :

  PGCD (83, 110) = PGCD (83, 135) = 1

  PGCD (110, 135) = 5. 135 ÷ 5 = 27

  Il remplace donc (110, 135) par (110, 27) et obtient un triplet d'entiers premiers entre eux, (83, 110, 27).

Dingmu Mères indéterminées m_i	83	110	27

- *Le produit de ces mères donne la mère du développement.*

  Il calcule le produit des m_i : 83 × 110 × 27 = 246 510

Yanmu Mère du développement M	246 510

- *Les produits mutuels donnent les nombres du développement.*

  110 × 27 = 2 970 83 × 27 = 2 241 83 × 110 = 9 130

Yanshu Nombres du développement M_i	2970	2241	9130

- *Ce qui remplit les mères déterminées, le supprimer.*

  Il réduit modulo m_i, c'est-à-dire qu'il calcule le reste de la division de M_i par m_i.

Qishu Nombres excédentaires N_i	65	41	4

- *Chercher les unités. En déduire les modules multiplicatifs.*

  Il résout (voir le paragraphe 3) les équations $N_i\, x \equiv 1 \pmod{m_i}$ où l'inconnue est μ_i.

(25) Le sens des termes « pair » et « impair » présente un très difficile problème. Libbrecht (op. cit.) pense que le premier signifie que tous les nombres sont divisibles par le même facteur.

Résolvons, par exemple, l'équation $65\,x \equiv 1 \pmod{83}$[26].

$83 = 1 \times 65 + 18$
$65 = 3 \times 18 + 11$
$18 = 1 \times 11 + 7$
$11 = 1 \times 7 + 4$
$7 = 1 \times 4 + 3$
$4 = 3 \times 1 + 1$

Ce qui donne le tableau suivant

i	0	1	2	3	4	5	6	7
q_i		1	3	1	1	1	1	3
r_i			18	11	7	4	3	1
P_i	1	1	4	5	9	14	23	83

On a $r_n = 1$ pour $n = 7$ et 7 est impair : $x = P_6 = 23$.

La présentation des calculs se fait de la façon suivante :

$$\begin{array}{|cc|}\hline P_0 & a \\ & m \\ \hline\end{array} \quad \begin{array}{|cc|}\hline P_0 & a \\ P_1 & r_2 \\ & q_1 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline & q_2 \\ P_2 & r_2 \\ P_1 & r_1 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline P_2 & r_2 \\ P_3 & r_3 \\ & q_3 \\ \hline\end{array} \ \dots \ \begin{array}{|cc|}\hline & q_n \\ P_n = m & r_n = 1 \\ P_{n-1} & r_{n-1} \\ \hline\end{array}$$

Dans le cas de notre équation, on obtient les sept présentations successives suivantes :

$$\begin{array}{|cc|}\hline 1 & 65 \\ & 83 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline 1 & 65 \\ 1 & 18 \\ & 1 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline & 3 \\ 4 & 11 \\ 1 & 18 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline 4 & 11 \\ 5 & 7 \\ & 1 \\ \hline\end{array}$$

$$\begin{array}{|cc|}\hline & 1 \\ 9 & 4 \\ 5 & 7 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline 9 & 4 \\ 14 & 3 \\ & 1 \\ \hline\end{array} \quad \begin{array}{|cc|}\hline & 1 \\ 23 & 1 \\ 14 & 3 \\ \hline\end{array}$$

Chung lü Nombres multiplicatifs μ_i	23	51	7

- *Multiplier ceux-ci par les nombres du développement pour en faire les nombres utiles.*

$2\,970 \times 23 = 68\,310$ $\quad 2\,241 \times 51 = 114\,291$ $\quad 9\,130 \times 7 = 63\,910$

Yongshu Nombres utiles $F_i = M_i\,\mu_i$	68 310	114 291	63 910

(26) On pourra faire le lien entre les différents termes q_i et les termes de la décomposition en fraction continue de $83/65 = (1, 3, 1, 1, 1, 3)$.

- *Multiplier les restes de riz par les nombres qui leur correspondent.*

  $32 \times 68\,310 = 2\,185\,920$ $70 \times 114\,291 = 8\,000\,370$ $30 \times 63\,910 = 1\,917\,300$

Yu Restes initiaux r_i	32	70	30

Zong Totaux $T_i = F_i\, r_i$	2 185 920	8 000 370	1 917 300

- *Ajouter les résultats.*

  $2\,185\,920 + 8\,000\,370 + 1\,917\,300 = 121\,035\,590$

Zong shu Somme S des T_i	121 035 590

- *Ce qui remplit la mère du développement, l'éliminer.*

  Il réduit cette somme modulo M (par additions répétées) :

  $121\,035\,590 = 49 \times 246\,510 + 24\,600$

- *Cela donne les parts de riz (toutes égales entre elles) ; fois le nombre d'hommes, donne la quantité totale de riz.*

  D'où la solution du système donnée dans le texte : $\boldsymbol{x} = \mathbf{24\,600}$.

Épilogue

Quelques siècles plus tard, on trouvera dans les livres d'arithmétique le théorème suivant, appelé « théorème des restes chinois »…

Soit k entiers positifs $m_1, m_2, \ldots, m_k$, premiers entre eux.

Alors le système de congruences

$$x \equiv r_i \pmod{m_i} \qquad \text{(S)}$$

avec $i = 1, 2, \ldots, k$ admet une unique solution modulo M avec $\mathrm{M} = m_1 m_2 \ldots m_k$.

Soit $\mathrm{M}_1, \mathrm{M}_2, \ldots, \mathrm{M}_k$ tels que $\mathrm{M} = m_1\mathrm{M}_1 = m_2\mathrm{M}_2 = \ldots = m_k\mathrm{M}_k$.

Puisque m_i et M_i sont premiers entre eux, on peut trouver k entiers $\mu_1, \mu_2, \ldots, \mu_k$ tels que $\mathrm{M}_1\mu_1 \equiv 1 \pmod{m_1}$, $\mathrm{M}_2\,\mu_2 \equiv 1 \pmod{m_2}$, …, $\mathrm{M}_k\mu_k \equiv 1 \pmod{m_k}$ et la solution générale de (S) est : $x = \mathrm{M}_1\mu_1 r_1 + \mathrm{M}_2\mu_2 r_2 + \ldots + \mathrm{M}_k\mu_k r_k \pmod{\mathrm{M}}$.

Bibliographie.

LIBBRECHT, U., « The Chinese *Ta-yen* Rule : a Comparative Study», Orientalia. Lovaniensa (Louvain), volume 3, 1972.
MARTZLOFF, J.-Cl., *Histoire des mathématiques chinoises*, Masson, 1983.
MARTZLOFF, J.-Cl., *A History of Chinese Mathematics*, Springer, 1997.
STEENS, E., *Dictionnaire de la civilisation chinoise*, Éd. du Rocher, 1996.
YABUUTI, K., *Une histoire des mathématiques chinoises*, Belin Sciences, 2000.

Résumé de la résolution du système

$$\begin{cases} x \equiv 32 \pmod{83} \\ x \equiv 70 \pmod{110} \\ x \equiv 30 \pmod{135} \end{cases}$$

Terminologie	Valeurs numériques			Remarques
Yuanshu Nombres primordiaux y_i	83	110	135	Modules
Dingmu Mères déterminées m_i	83	110	27	Modules m_i premiers deux à deux
Yanmu Mère du développement M	246 510			M = produit des m_i
Yanshu Nombres du développ. M_i	2 970	2 241	9 130	$M_i = \dfrac{M}{m_i}$
Qishu Nombres excédentaires N_i	65	41	4	$N_i =$ reste de la division de M_i par m_i
Cheng lü Nombres multiplicatifs μ_i	23	51	7	Les μ_i sont les plus petites solutions positives des équations $N_i x \equiv 1 \pmod{m_i}$
Yongshu Nombres utiles F_i	68 310	114 291	63 910	$F_i = M_i \mu_i$
Yu Restes r_i	32	70	30	Restes initiaux r_i
Zong Totaux T_i	2 185 920	8 000 370	1 917 300	$T_i = F_i\, r_i$
Zongshu Somme S	121 035 590			Somme des T_i
Réduction	121 035 590 = 49 × 246 510 + 24 600			Réduction de S modulo M

D'où la solution du système donnée dans le texte : $x = 24\,600$.