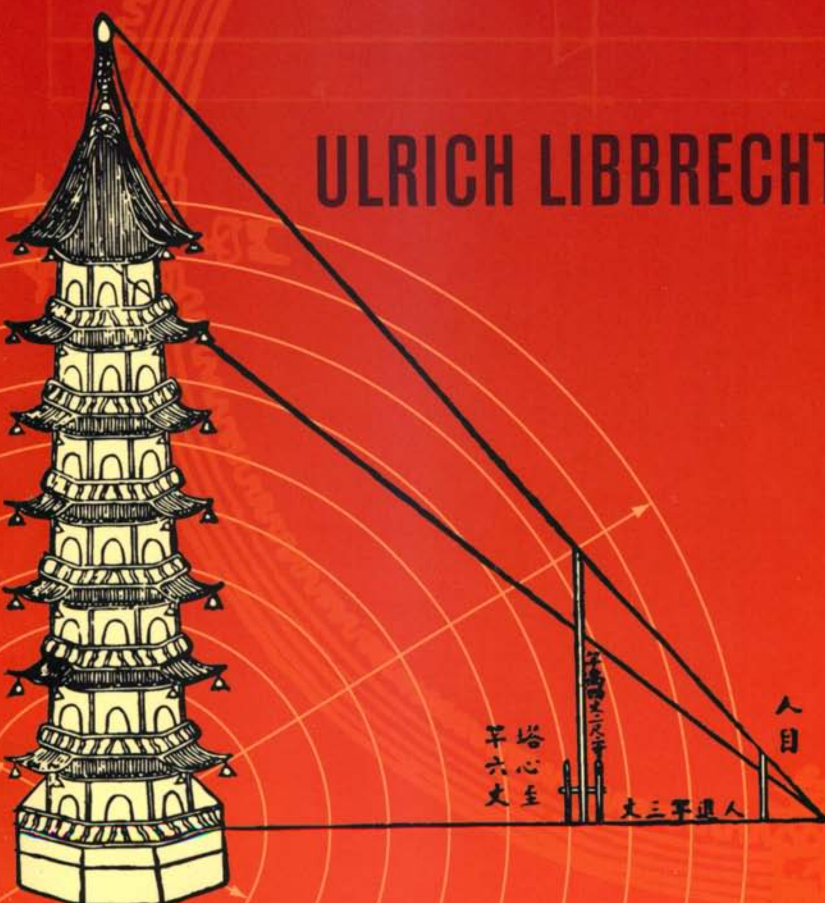
# Chinese Mathematics in the Thirteenth Century

ULRICH LIBBRECHT



# Contents

# 14

# Indeterminate Analysis of the First Degree outside China: General Historical Survey

A general algebraic rule states that in order to solve a system of equations one needs as many equations as there are unknowns. If there are $n$ equations with more than $n$ variables, we can in general find an infinite number of solutions. These solutions form a set which can be expressed by a simple formula.

Indeterminate equations of the first degree, which are the simplest form, have attracted much attention from the Chinese scholars. These equations of the form $ax+by=c$ are not dealt with in the works of Diophantos of Alexandria (active about the middle of the third century), who treats only equations of higher degree. Linear indeterminate equations are dealt with in the works of Âryabhaṭa, Brahmagupta, Mâhavîra, and Bhâskara in India. The *remainder problem* is a special form of simultaneous indeterminate linear equations with the general structure $N \equiv r_1 \pmod{a} \equiv r_2 \pmod{b} \equiv r_3 \pmod{c} \equiv \ldots \equiv r_n \pmod{n}$. It was developed in China, as well as in India, the Arabic world, and Europe. Since indeterminate equations of higher degree are not dealt with in China, we will restrict our historical survey to linear indeterminate equations and the remainder problem.[1]

## Summary

### SOLUTION OF $AX + BY = C$

The earliest attempts to solve this linear equation by a general procedure are to be found in India from about the fifth century on in the works mentioned in the preceding paragraph. In China there were attempts in the *Chang Ch'iu-chien suan-ching*

[1] For a modern algebraical representation of the remainder theorem, see Chapter 17, section on "Theoretical Representation of Ch'in Ch'in-shao's Method."

(the "hundred fowls" problem), which gives exact results but a very incomplete expression of the method. In Europe it was only from the seventeenth century on that this kind of problem was studied.

THE REMAINDER PROBLEM

This problem, also known as "the Chinese remainder theorem," first appears in the *Sun Tzŭ suan-ching* in the fourth century and finds its culminating point in the work of Ch'in Chiu-shao (1247). In India there were Brahmagupta (c. 625) and Bhâskara (twelfth century), who developed the *kuṭṭaka* method. In the Islamic world, Ibn al-Haitham treats this kind of problem, and he may have influenced Leonardo Pisano (Fibonacci) in Italy. After the thirteenth century we do not find much further investigation in China, India, or the Islamic world. But from the fifteenth century on there is a marked increase in European research, which reached its apogee in the studies of Lagrange, Euler, and Gauss. This problem still appears in all our modern books on theory of numbers and is called the Chinese remainder problem.[2]

The reader may wish in the course of this section to refer to Table 3, which summarizes the chronology of indeterminate analysis.

## History of the Development of Indeterminate Analysis of the First Degree outside China

INTRODUCTORY NOTE

With this outline of the evolution of the remainder problem, we

[2] A list of the most recent works that mention the remainder problem would include Le Veque (1), pp. 35 f; Rademacher (1), pp. 22 f; J. Hunter (1), p. 55; Grosswald (1), pp. 49 ff. In the last work Dickson's mistake about the Sun Tzŭ problem in Nichomachus (see note 13) is repeated. In China, studies of ancient mathematics, begun at the end of the eighteenth century, have resulted in new investigations of indeterminate problems. But their interest is merely historical, since they give us access to the older works but no new insights into indeterminate analysis that are on the same level as European studies at that time.

Table 3. Chronology of Indeterminate Analysis

| Year | Europe | China | India | Islam |
|---|---|---|---|---|
| 100 | | | | |
| 200 | | | | |
| | Diophantos of Alexandria | | | |
| 300 | | | | |
| | | *Sun Tzŭ suan-ching (?)* | | |
| 400 | | | | |
| | | Ho Ch'êng-t'ien | | |
| | | Tsu Ch'ung-chih | | |
| | | Hsia-hou Yang | | |
| 500 | | Chang Ch'iu-chien | | |
| | | | Âryabhaṭa | |
| | | | Bhâskara I | |
| | | Chên Luan | | |
| 600 | | Liu Hsiao-sun | | |
| | | | Brahmagupta | |
| | | Li Shun-fung | | |
| 700 | | | | |
| | | I-hsing | | |
| | | Lung Shou-i | | |
| 800 | | | | |
| | | | Mahâvîra | |
| | | | | Abû-Kâmil |
| 900 | | | | |
| 1000 | | | | Ibn al-Haitham |
| | | Hsieh Ch'a-wei | | Abû Bakr al-Farajî |
| | | Shên Kua | | |
| 1100 | | | | |
| | | | Bhâskara II | |
| 1200 | Leonardo Pisano (Fibonacci) | | | |
| | | Ch'in Chiu-shao | | |
| | | Yang Hui | | |
| | | Chou Mi | | |
| 1300 | | | | |
| | Isaac Argyros | | | |
| | | Ku Hêng | | |
| | | Yen Kung | | |
| 1400 | | | | |
| | Regiomontanus | | | |
| | Elia Misrachi | | | |
| | Munich MS | | | |
| 1500 | | | | |
| | Michael Stifel | | | |
| | Göttingen MS | Chou Shu-hsüeh | | |
| | | Ch'êng Ta-wei | | |
| 1600 | | | | |
| | Van Schooten | | | |
| | Beveridge | | | |

are going beyond the scope of this work. But there are several reasons for doing so.

First, we can evaluate Ch'in Chiu-shao's method only if we compare it with other works treating the same problem. Many of these works are not easily accessible, and for the greater part there is no analysis of the contents. A scientific comparison is possible only if we are able to compare the original texts, without any translation into modern algebraical (and thus general) language. For such translation always gives an inaccurate idea of the original text.[3]

A comparison need not be historical; it can also be a comparison of patterns. In setting up a pattern, it is not legitimate to make use of interpretations of the original texts, particularly if they are intended to give evidence that a certain people have developed an idea and cannot be considered inferior to another people, and so on—all relics of an unscientific nationalism.[4]

From the logical point of view a pattern must be built up in a certain structure. A comparison can be made only if we have knowledge of a general set of possibilities for solving the

[3] A distinction must be made between rhetorical algebra and algorithmic algebra. Rhetorical algebra can be general, even without a general notation. From the methodological point of view we are reminded of what Nesselmann (1) said more than a century ago: "The rule that a historian, with respect to his documentation and authorities, will cite them correctly and accurately in the first place, and secondly quote only *what he has actually seen,* seems so obvious that it can be easily considered superfluous to waste any words over such trivial matters. And yet, how often and how thoroughly are both rules violated!" (Die Regel, dass ein historischer Schriftsteller, was seine Belege und Autoritäten anlangt, erstens dieselben richtig und genau, zweitens aber *nur das citirt, was er gesehen hat,* scheint so natürlich zu sein, dass man es leicht für überflüssig halten kann, über einen so trivialen Gegenstand noch Worte zu machen. Und doch, wie oft und wie vielfach wird gegen beide Regeln gefehlt!) (p. 35); and "Nothing is more common and more natural, when reading ancient books, than that we substitute our own point of view for that of the old author whom we are reading." (Nichts is also bei der Lektüre alter Werke gewöhnlicher und natürlicher, als dass wir unsern eigenen Standpunkt dem alten Schriftsteller, den wir lesen, substituiren) (p. 37).

[4] Many studies of the last century in particular display this characteristic, having as their aim "national glory" or "glory of the true religion" and an extreme historicism as their foundation.

problem.[5] Each of the solutions given for the problem in the course of ages can be considered as a subset of this general set. There is evolution only if subset *A* (the first in time) is a subset of a subset *B*. Such comparison is impossible without real insight into the specific structure of each subset. For this reason we need access to the original texts.[6]

### GREECE[7]

The oldest indeterminate problems known in Europe are all of higher degree and are mostly of the form $Ay^2+1=x^2$, known as the Pell equation.[8] Of these problems the so-called Cattle Problem, doubtfully attributed to Archimedes, is most famous,[9] and "the solution is more complicated than that of any in the extant works of Diophantos."[10] It is supposed that Diophantos of Alexandria (active A.D. 275) may have treated of the problem in one of his lost books.[11] But as D. E. Smith pointed out, the

[5] At least as far as this specific mathematical knowledge has developed.
[6] This logical comparison is worked out in Chapter 21.
[7] In this section we have to restrict ourselves to the remainder theorem, although mention will be made of the greatest mathematicians who have done general studies of indefinite analysis.
[8] For further information, see Smith (1), vol. 2, pp. 452 ff and bibliographical notes.
[9] See also Archibald (1), pp. 411 ff with bibliographical notes; Smith (1), vol. 2, p. 453 and p. 584; and Heath (1), pp. 142 ff.
[10] Archibald (1), p. 414.
[11] Smith (1), vol. 2, p. 453, and Tannery (1), p. 370. Diophantos treated only indeterminate equations of higher degree. Needham (1), vol. 3, p. 122 writes: "Curiously, the algebra of Diophantos, in so far as it touches this subject, deals with indeterminate quadratic equations almost solely." There is however a very simple explanation for this fact. Diophantos did not require whole numbers as solutions for his indeterminate problems, and with this condition the solving of indeterminate equations of the first degree has no sense: " . . . After all, they present no difficulties so long as no integral solutions are required." (Sie machen ja, wenn die Ganzzahligkeit der Lösungen nicht verlangt wird, gar keine Schwierigkeit). Tropfke (1), vol. 3, p. 101. Those who disdain oriental mathematics should read Hankel (1), pp. 164 f, where there is a realistic evaluation of Diophantos: "With our author not the slightest trace of a general, comprehensive method is discernible; each problem calls for some special method which refuses to work even for the most closely related problems. For this reason it is difficult for the modern scholar to solve the 101st problem even after having

solution of indeterminate problems as a form of recreation must be very old in Greece.[12] The greatest of the mathematicians, however, who applied themselves to indeterminate analysis was undoubtedly Diophantos of Alexandria.[13] After Diophantos, however, the decline of mathematics in Europe had begun and there was nothing more until the time of Fibonacci (c. 1202). For a millennium the Dark Ages covered Europe, but evolution was going on in China and India.

## INDIA

The study of India's contribution to the solution of indeterminate equations is very important, because many scholars assume an Indian origin for a considerable part of Chinese mathematical knowledge. A later chapter will attempt to compare the *ta-yen* rule and the Indian *kuṭṭaka*,[14] but for the moment we shall restrict ourselves to a description of the Indian methods.

The general purpose of this branch of algebra[15] seems to be astronomical.[16] Datta and Singh distinguish three varieties of indeterminate problems[17], namely,

1. $N=ax+R_1=by+R_2$. Putting $|R_1-R_2|=c$, we can reduce the problem to: $by-ax=\pm c$.

---

studied 100 of Diophantos's solutions." (Von allgemeineren umfassenden Methoden ist bei unserem Autor keine Spur zu entdecken; jede Aufgabe erfordert eine ganz besondere Methode, die oft selbst bei den nächstverwandten Aufgaben ihren Dienst versagt. Es ist deshalb für einen neueren Gelehrten schwierig, selbst nach dem Studium von 100 Diophantischen Lösungen, die 101. Aufgabe zu lösen).

[12] Smith (1), vol. 2, p. 584.

[13] Dickson, in (1), vol. 2, p. 58, mistakenly says that Nicomachus of Gerasa (active c. 90) dealt with the famous Sun Tzŭ problem. Needham (1), vol. 3, p. 34, note *a*, discusses this question and shows that the problem must be derived from Isaac Argyros (middle fourteenth century), a Byzantine monk. For further information, the reader is referred to Needham. Dickson's error is reproduced in Ganguli (1), p. 113; Sen (1), p. 495; and Grosswald (1), pp. 49 f.

[14] On the name *kuṭṭaka*, see Datta and Singh (1), pp. 89 ff.

[15] "The *kuṭṭaka* was considered so important by the ancient Hindu algebraists that the whole science of algebra was once named after it." Datta and Singh (1), p. 88.

[16] See the very important paper by Van Der Waerden (1).

[17] Datta and Singh (1), p. 89.

2. $(\alpha x \pm \gamma)/\beta = y$ ($x$ and $y$ must be positive integers).[18]
3. $by + ax = \pm c$. The general problem is $by \pm ax = \pm c$, which can be reduced to four kinds of equations:

$$by - ax = +c \quad \text{(a)}$$
$$by - ax = -c \quad \text{(b)}$$
$$by + ax = +c \quad \text{(c)}$$
$$by + ax = -c \quad \text{(d)}$$

A general condition of solvability is that $a$, $b$, and $c$ be prime to each other.[19]

Âryabhaṭa I[20] solves only equations (a) and (b). In his work, now commonly known as the *Âryabhaṭîya,* there is a section on mathematics,[21] containing two stanzas (32–33) on indeterminate analysis.[22] There has been much discussion about the real meaning of the text, and a correct interpretation is not easy.

The translation of the text is roughly as follows:[23]

1. Divide the divisor having the greater *agra*[24] by the divisor having the smaller *agra* (*Adhikâgrabhâgahâram chindyât ûnâgrabhâgahâreṇa*).

[18] This problem could be reduced to (1).
[19] This rule was known to the greater part of the Indian mathematicians. See Datta and Singh (1), p. 92.
[20] For a general account of Âryabhaṭa's life and work, see Smith (1), vol. 1, pp. 153 ff.
[21] Called *Ganita.*
[22] The text was lost for a long time. Colebrooke (1) tells us that "a long and diligent research in various parts of India failed of recovering the algebraic and other works of Âryabhaṭa" (p. v). It was after its rediscovery published by Kern; there are translations by Rodet (1), Kaye (1), and Clark (1). Other studies (much more valuable than the European ones), most including a translation, are Ganguli (1) and (2); Datta and Singh (1), pp. 93 - 101; Sen Gupta (1); Mazumdar (1); Datta (1) and (2); Sen (1).
[23] As all the existing translations must include many interpolations in order to make sense, I have avoided translating anything more than the text itself. I am much indebted to Dr. J. Deleu (University of Ghent), who examined this translation and gave me much information about the grammatical structure of the text. The division of the text is mine, and is made only to facilitate references.
[24] I have not translated the technical term *agra,* because it gave rise to very different interpretations, which will be explained later. As in Chinese, many technical terms are not to be taken in their general meaning.

2. Mutually divide the remainders (*śeṣaparasparabhaktaṃ*).
3. Multiply by the *mâti* and add to the difference between the *agras* (*mâtiguṇam agrântare kṣiptam*).
4. Multiply the one below by the one above and add the ultimate [or the lowest] one (*adha upariguṇitaṃ antyayuk*).
5. Divide by the divisor having the smaller *agra* (*ûnâgracchedabhâjite*).
6. Multiply the remainder by the divisor having the greater *agra* (*śeṣam adhikâgracchedagunaṃ*).
7. Add the *agra* which divides both to the greater *agra* (*dvicchedâgraṃ adhikâgrayutam*)

ANALYSIS

The translations differ from each other in many points. L. Rodet and W. Clark both rely on the explanation given by the commentator Parameśvara (sixteenth century);[25] Clark also relies on the parallel text in Brahmagupta, XVIII, 3–5.[26] Ganguli interprets the text starting from the mathematical formulae; Datta follows "the interpretation of the rule by Bhâskara I (525), a direct disciple of Âryabhaṭa I."[27]

There is disagreement about the meaning of the term *agra*. Ganguli and Datta translate it as "remainder," while for Clark it is a specific technical term. This enables us to distinguish the interpretations from each other. As the translations of Rodet and Kaye[28] do not seem to be based on an understanding of the real meaning of Âryabhaṭa's rule, they may be ignored. The translations of Ganguli and Datta differ from each other, as the former adds the term "quotient" in (3), whereas the latter adds "residue" (see below).

As a thorough analysis of the interpretations would be beyond the scope of this study, we give an example of each interpretation together with some notes.

[25] Kern's edition of 1875 contains Parameśvara's commentary; other editions are U. N. Singh, Muzaffapur, 1906, with commentary by Nilakaṇṭha (1500); and K. Sastri, Trivandrum, 1930/31.
[26] Colebrooke (1), p. 325.
[27] Datta and Singh (1), pp. 93 ff.
[28] Kaye's translation of *mâtiguṇam agrântare kṣiptam* as "an assumed number

Clark's translation is as follows: "Divide the divisor which gives the greater *agra* by the divisor which gives the smaller *agra*. The remainder is reciprocally divided (that is to say, the remainder becomes the divisor of the original divisor, and the remainder of this second division becomes the divisor of the second divisor, etc.). (The quotients are placed below each other in the so-called chain.) (The last remainder) is multiplied by an assumed number and added to the difference between the *agras*.[29] Multiply the penultimate number by the number above it and add the number which is below it. (Continue this process to the top of the chain.) Divide (the top number) by the divisor which gives the smaller *agra*. Multiply the remainder by the divisor which gives the greater *agra*. Add this product to the greater *agra*. The result is the number which will satisfy both divisors and both *agras*."[30]

Parameśvara's example, quoted by Clark, is the following:

$$\begin{cases} 8x \equiv 4 \pmod{29} \\ 17x \equiv 7 \pmod{45}. \end{cases}$$

Find x.

$$8x-29y=4 \qquad \text{(a)}$$

*(mâti)* together with the original difference is thrown in" makes no sense, even from the grammatical point of view. See Clark (1), p. 44: "It omits altogether the important word *guṇam* (multiplied)." Moreover, as Kaye was dominated by the idea that all Indian mathematical knowledge must be of Greek origin, he tried to prove that the basis of Âryabhaṭa's method was to be found in Euclid's method for finding the greatest common divisor. It may show some relation with Âryahbaṭa's method, but the application of the results is quite different. Kaye's statement is indeed very shallow, and as he failed entirely to give the correct explanation of Âryabhaṭa's text, his importance is only historical. Kaye's interpretation is followed by Mazumdar (1). For a general criticism of Kaye's work, see Ganguli (2).

29 The text given by Brahmagupta is very close to Âryabhaṭa's, but here Brahmagupta has: "The residue [of the reciprocal division] is multiplied by an assumed number such that the product, having added to it the difference of the remainders, may be exactly divisible [by the residue's divisor]. That multiplier is to be set down [underneath] the quotient last." Clark (1), p. 42.

30 Ibid. p. 43.

Applying the Euclidean algorithm for finding the G.C.D. to 29 and 8 (until the remainder is 1), we have:

| | | | | |
|---|---|---|---|---|
| | 3 | 1 | 1 | 1 |
| 29 | 8 | 5 | 3 | 2 |
| 24 | 5 | 3 | 2 | |
| 5 | 3 | 2 | 1 | |

This allows us to draw up the following "chain" of equations:

$$8x = 29y + 4$$
$$8x_1 = 5y + 4 \qquad \text{with } x_1 = x - 3y$$
$$3x_1 = 5y_1 + 4 \qquad \text{with } y_1 = y - 1x_1$$
$$3x_2 = 2y_1 + 4 \qquad \text{with } x_2 = x_1 - 1y_1$$
$$1x_2 = 2y_2 + 4 \qquad \text{with } y_2 = y_1 - 1x_2.$$

The last equation can easily be solved by inspection:[31]

$$x_2 = 2y_2 + 4; \qquad y_2 = \frac{x_2 - 4}{2}.$$

It is obvious that the smallest positive solution is $x_2=6$, giving $y_2=1$. According to Âryabhaṭa's rule the following chain is to be drawn up:

| | | | in general: |
|---|---|---|---|
| 3 | $73 = 3 \times 20 + 13$ | $q_1$ | $x = q_1 y + x_1$ |
| 1 | $20 = 1 \times 13 + 7$ | $q_2$ | $y = q_2 x_1 + y_1$ |
| 1 | $13 = 1 \times 7 + 6$ | $q_3$ | $x_1 = q_3 y_1 + x_2$ |
| 1 | $7 = 1 \times 6 + 1$ | $q_4$ | $y_1 = q_4 x_2 + y_2$ |
| 6 | | $x_2$ | |
| 1 | | $y_2$ | |

One of the solutions of the problem (but not the smallest one) is $x=73$, $y=20$. For finding the smallest solution, we divide 73 by 29 to find $x_0$; the remainder is the *agra* required:[32]

[31] A method still used in our mathematical textbooks.

[32] This agrees with the general solution of $Ax-By = C$, being $x = x_0 + Bt$ and $y = y_0 + At$ ($x_0$ and $y_0$ are the smallest solutions). From which: $x_0 = X - Bt$, if $X$ is any solution of the equation.

$73-29n=15$ (*agra*$_1$).

In the same way we can find *agra*$_2$$=11$ as the smallest solution of

$17x-45y=7.$ (b)

According to Clark's interpretation, *agra* is the smallest solution for $x$ in an equation with two unknowns.[33] In fact, "the rule [given by Âryabhaṭa] applies only to the third process. . . . The solution of the single indeterminate equation is taken for granted and is not given in full."[34]

Thus,

$p=15$ is the *agra* of $8x=29y+4$;
$q=11$ is the *agra* of $17x=45z+7$.

We must now find a value of $x$ satisfying both equations. The general solution[35] of (a) is $x=15+29t$; of (b), $x=11+45t'$. Thus, $29t+15=45t'+11$ and $45t'-29t=4$.

We solve in the same manner as above, and find $t'=22$, $t=34$. The general solution is

$x=29t+15,$
$x=29\times 34+15=1{,}001.$

This equation that Clark gives, following Parameśvara's commentary, is very close to the original text. Ganguli, however, holds that Âryabhaṭa's method is not identical with Brahmagupta's and that "for the same reason the interpretation given by the Sanskrit commentator Parameśvara cannot be accepted as correct."[36] This matter is by no means decided, and I do not want to enter an arena that is not mine.

[33] Clark defines *agra* as "the remainders which constitute the provisional values of $x$, that is to say, values one of which will satisfy one condition, one of which will satisfy the second condition of the problem." This statement is somewhat confusing, but one will find the explanation in the mathematical representation. Anyhow, the "values of $x$" are the smallest values, a fact that is not pointed out by Clark.
[34] Clark (1), p. 47.
[35] This explanation is neither in Âryabhaṭa, nor in Clark. Clark says only: "Then in accordance with the rule $34\times 29 = 986$ and $986+15 = 1{,}001$."
[36] Ganguli (1), p. 115.

Ganguli gives a very different explanation. In his opinion the problem closely resembles the Sun Tzŭ problem[37] and should have the general form

$$N \equiv R_1 \pmod{A} \equiv R_2 \pmod{B}.$$

The treatment, however, seems to be very different from that of the *ta-yen* rule,[38] as Ganguli states:

"Âryabhaṭa's problem in indeterminate analysis appears to be exactly similar to the one given by Sun Tzŭ. Âryabhaṭa considers only *two* divisors, while Sun Tzŭ contemplates any number of divisors.[39] This difference may, at first sight, appear to be of no importance. But it is fundamental. Accordingly Âryabhaṭa's solution cannot be extended so as to give a solution of Sun Tzŭ's problem."[40]

Ganguli's explanation is very extensive, and it is impossible to give more than a summary of it here. The general problem is[41] $N=Ax+R_1=By+R_2$, or $Ax+R_1=By+R_2$, from which $Ax=By+R_2-R_1$. Putting $R_2-R_1=C$, we have $Ax=By+C$. There are two possibilities: $B>A$ or $A>B$. Let us take an example:[42]

$$N \equiv 4 \pmod{29} \equiv 7 \pmod{45}.$$

We apply the Euclidian algorithm:[43]

[37] It is a pity that Ganguli is also a victim of the "disease of historicism"; his chief purpose seems to be to prove that Âryabhaṭa owed his methods neither to Greece nor to China.

[38] As Matthiessen (1) already explained. It is difficult to understand Needham (1), vol. 3, p. 122, note *e*: "The argument of Matthiessen that they were very different does not carry conviction." This matter will be discussed again in Chapter 18. See also Yushkevitch (1), p. 145: "At any rate, the Indian method is quite different from the Chinese one. (Allerdings ist die indische Methode von der chinesischen verschieden)."

[39] This is not entirely true, because there is only one problem having three divisors. But the method is applicable to any number of divisors.

[40] Ganguli (1), p. 114. See Chapter 15.

[41] Ganguli equates the term *agra* with the remainders of the problem.

[42] Ganguli gives only a theoretical explanation without any example.

[43] Clark stops this mutual division when the remainder becomes 1, Ganguli when it becomes 0.

| | | | | | |
|---|---|---|---|---|---|
| | 1 | 1 | 1 | 4 | 3 |
| 45 | 29 | 16 | 13 | 3 | 1 |
| 29 | 16 | 13 | 12 | 3 | |
| 16 | 13 | 3 | 1 | 0 | |

From the chain[44]

| | | | | | | |
|---|---|---|---|---|---|---|
| | $q_1$ | $q_2$ | $q_3$ | $q_4$ | t | $r_3$ |
| or | 1 | 1 | 1 | 4 | 1 | 3 |

we compute[45]

$t = y_2 = 1$ $\qquad x_2 = 3\times 1 + 3 = 6$
$y_1 = 4\times 6 + 1 = 25$ $\qquad x_1 = 1\times 25 + 6 = 31$
$y = 1\times 31 + 25 = 56$ $\qquad x = 1\times 56 + 31 = 87.$

Take $\alpha$ and $\beta$ as the smallest solutions.

As $x = Bm + \alpha \longrightarrow \alpha = x - Bm = 87 - 45\times 1 = 42$
$y = Am + \beta \longrightarrow \beta = y - Am = 56 - 29\times 1 = 27$
$N = B\beta + R_2 = 45\times 27 + 7 = 1{,}222.$

44 This $t$ or *mâti* is any assumed number (zero or any positive integer). The value of $y_2 = t$.
The general rule is: $B = AQ_1 + r_1 \rightarrow A(x - Q_1 y) = r_1 y + C \rightarrow Ax_1 = r_1 y + C$ with $x_1 = x - Q_1 y$. Indeed,
$Ax = By + C$
$Ax = (AQ_1 + r_1)\, y + C$
$Ax = AQ_1 y + r_1 y + C$
$A(x - Q_1 y) = r_1 y + C.$
$A = Q_2 r_1 + r_2 \rightarrow r_2 x_1 = r_1(y - Q_2 x_1) \rightarrow$
$r_2 x_1 = r_1 y_1 + C$ with $y_1 = y - Q_2 x_1$
$r_1 = Q_3 r_2 + r_3 \rightarrow r_2(x_1 - Q_3 y_1) = r_3 y_1 + C \rightarrow$
$r_2 x_2 = r_3 y_1 + C$ with $x_2 = x_1 - Q_3 y_1$
$r_2 = Q_4 r_3 + r_4 \rightarrow r_4 x_2 = r_3\,(y_1 - Q_4 x_2) + C \rightarrow$
$r_4 x_2 = r_3 y_2 + C$ with $y_2 = y_1 - Q_4 x_2$.
Suppose that $r_4 = 1$; $r_4 x_2 = r_3 y_2 + C \rightarrow x_2 = r_3 y_2 + C$. Take $y_2 = t \rightarrow x_2 = r_3 t + C$ giving the solution of the last equation.
45 In general:

| | | |
|---|---|---|
| $x = Q_1 y + x_1$ | from | $x_1 = x - Q_1 y$ |
| $y = Q_2 x_1 + y_1$ | from | $y_1 = y - Q_2 x_1$ |
| $x_1 = Q_3 y_1 + x_2$ | from | $x_2 = x_1 - Q_3 y_1$ |
| $y_1 = Q_4 x_2 + y_2$ | from | $y_2 = y_1 - Q_4 x_2$ |
| $x_2 = r_3 t + C$ | from | $x_2 = r_3 y_2 + C$ |
| $y_2 = t.$ | | |

The working out of the problem is not greatly different from Clark's. But this is true only of the method. The problem to which it is applied is quite different:[46]

| Ganguli | Clark |
|---|---|
| $N=Ax+R_1$ | $mx=Ay+R_1$ |
| $N=By+R_2$ | $nx=Bz+R_2$. |

Clark criticizes Ganguli's explanation of the text and states: "I cannot help feeling that the Sanskrit is stretched in order to make it fit the formula."[47]

Datta and Singh[48] rely on the interpretation of Bhâskara I (525), who was a direct disciple of Âryabhaṭa I.[49] The translation is as follows:

"Divide the divisor corresponding to the greater remainder by the divisor corresponding to the smaller remainder. The residue (and the divisor corresponding to the smaller remainder) being mutually divided (*) the last *residue* should be

[46] Of course, Clark's representation can be reduced to Ganguli's, but $A$, $B$, $R_1$, $R_2$ cannot be positive integers. This method was worked out by Mahâvîra (850) and Śrîpati (1039). See Datta and Singh (1), p. 137.
[47] Clark (1), p. 50. Ganguli also gives an explanation of the case in which $A>B$.
[48] Strictly speaking, this is Datta's interpretation, first published in Datta (1), and takee np in Datta and Singh (1).
[49] This seems to be a reliable reference. I have not seen this commentary. The following translation is given by Datta and Singh (1), p. 99: "Set down the dividend above and the divisor below. Write down successively the quotients of their mutual division, one below the other, in the form of a chain. Now find by what number the last remainder should be multiplied, such that the product being subtracted by the (given) residue (of the revolution) will be exactly divisible (by the divisor corresponding to the remainder). Put down that optional number below the chain and then the (new) quotient underneath. Then multiply the optional number by that quantity which stands just above it and add to the product the (new) quotient (below). Proceed afterwards also in the same way. Divide the upper number (i.e., the multiplier) obtained by this process by the divisor and the lower one by the dividend; the remainders will respectively be the desired *ahargana* and the revolutions." And note 1: "The above rule has been formulated with a view to its application in astronomy." Srinivasiengar [(1), pp. 96 ff] accepts Datta's explanation, which is very clear.

multiplied by such an optional integer that the product being added (in case the number of quotients of the mutual division is even) or subtracted (in case the number of quotients is odd) by the difference of the remainders (will be exactly divisible by the last but one remainder. Place the quotients of the mutual division successively one below the other in a column; below them the optional multiplier and underneath it the quotient just obtained) (**). Any number below (i.e., the penultimate) is multiplied by the one just above it and then added to that just below it. Divide the last number (obtained by doing so repeatedly) by the divisor corresponding to the smaller remainder; then multiply the residue by the divisor corresponding to the greater remainder and add the greater remainder. (The result will be) the number corresponding to the two divisors."

According to Datta, the part from (*) to (**) can also be rendered as follows: ". . . (until the remainder becomes zero), the last quotient[50] should be multiplied by an optional integer and then added (in case the number of quotients of the mutual division is even) or subtracted (in case the number of quotients is odd) by the difference of the remainders. (Place the other quotients of the mutual division successively one below the other in a column: below them the result just obtained and underneath it the optional integer.) . . ."

The problem is $N=ax+R_1=by+R_2$. If $R_1-R_2=c$, and $R_1>R_2$, we have $by=ax+c$. If $R_2>R_1$, we have $ax=by+c$. Suppose that $R_1>R_2$. The equation is $ax+c=by$. There are four subcases:

1. The last $r=0$

a) The number of quotients is even[51]

b) The number of quotients is odd

2. The mutual division is stopped at a remainder $r_p \neq 0$

a) The number of quotients is even

b) The number of quotients is odd.

[50] As we have seen, Ganguli agrees with "quotient."

[51] The first quotient must be neglected, as is usual with Âryabhaṭa.

The result is exactly the same as in Ganguli's explanation in case (1), but the difference between the interpretations lies in the subdivision of the cases,[52] all corresponding to the general rule.

It seems very likely that Âryabhaṭa's problem is indeed $N \equiv R_1 \pmod{A} \equiv R_2 \pmod{B}$ and that it in some way resembles the Sun Tzŭ problem. But as Clark states, "The general method of solution by reciprocal division and formation of a chain is clear,[53] but some of the details are uncertain and we do not know to what sort of problems Âryabhaṭa applied it."[54] The last question is not difficult to answer; they were chronological problems, as is demonstrated in a very important paper by Van Der Waerden.[55]

Which were the problems Âryabhaṭa was able to solve? They were all of the type

$$by - ax = \pm c. \qquad (1)$$

If $R_1 > R_2$, solve the equation $by = ax + c$, or $y = (ax + c)/a$ $(c > 0)$. If $R_1 < R_2$, solve the equation $ax = by + c$, or $x = (by + c)/a$ $(c < 0)$. Equation (1) is arranged so that $c$ is always positive.

Bhâskara I extends this rule[56] to a direct solution of $y = (ax - c)/b$ $(c < 0)$. Brahmagupta provides some improvements on Âryabhaṭa's rule. The most important is: ". . . it is not necessary to continue the operations of mutual division until the remainder becomes zero. We may stop at any stage if we can solve the resulting reduced equation [by inspection]."[57] An-

[52] Clark's interpretation being a more general and more complicated case of the same problem.

[53] This is very important because it gives a general rule, indispensable for solving indeterminate equations, especially when the moduli are very large, as in chronological problems.

[54] Clark (1), p. 50.

[55] As early as 1874, Hankel (1) wrote: "[it] owes its origin probably to the very same chronological-astrological problems to which it is so frequently applied. (. . . verdankt ihren Ursprung vermuthlich denselben chronologisch-astrologischen Aufgaben, auf welche sie von ihnen vielfach angewandt wird. . .)" (p. 197).

[56] See Datta and Singh (1), pp. 99 f, where some secondary rules are given.

[57] Ganguli (1), p. 130.

other is that we can transform the equation $by=ax+c$ to $ax=by-c$ "so that we shall have to start with the division of $b$ by $a$,"[58] which makes it unnecessary to have $c>0$.[59]

Bhâskara I was the first to state the rule for solving the special indeterminate equation $by=ax\pm1$, the so-called "constant pulverizer."[60] If the equation $(ax\pm1)/b=y$ is solved,[61] the solution of $(ax\pm c)/b=y$ can easily be derived. Suppose the solutions of $(ax\pm1)/b=y$ are $x=\alpha$ and $y=\beta$. Then $b\beta=a\alpha\pm1$. If we multiply by $c$, we get $b(c\beta)=a(c\alpha)\pm c$, and $x=c\alpha$, $y=c\beta$ is a solution of $(ax\pm c)/b=y$.

Almost the same rule is given by Brahmagupta and Bhâskara II.[62] For example

$$\frac{17x+5}{15}=y.$$

Solving the equation $\frac{17x+1}{15}=y$,[63] we find that $x=7$, $y=8$. Multiply by 5:

$$x=7\times5=35 \quad -n\times15=5$$
$$y=8\times5=40 \quad -n\times17=6.$$

This method is adopted by Âryabhaṭa II (950) as the general rule. As he always assumes that $t=0$, this is an important simplification. Moreover, he was the first to formulate clearly the general solutions $x=x_0+bt$ and $y=y_0+at$. Finally, he

58 Datta and Singh (1), p. 103.

59 There was little change in the general rule after Âryabhaṭa; Brahmagupta and Mahâvîra are only links in the historical chain. Brahmagupta's work was for a long time the oldest one known, because Âryabhaṭa's work was lost. Colebrooke (1) translated it in 1817; Mahâvîra's work was edited and translated by M. Rangacarya (1); see also Aiyar (1). It is impossible to treat these works in detail, because our purpose is only to make an objective comparison between Indian and Chinese methods.

60 Or *sthira-kuṭṭaka*. For an explanation of this term, see Datta and Singh (1), pp. 117 f. This explanation of the "constant pulverizer" follows Datta and Singh (1), pp. 118 ff.

61 This equation is solved in the same way as the general equation.

62 See also Ayyangar (1).

63 Given by Bhaskara II. See Datta and Singh (1), p. 120; Taylor (1), p. 112; Gurjar (1), pp. 115 f.

provided an interesting series of reducing rules, also applied by Bhâskara II.[64]

Brahmagupta, Bhâskara II, and Nârâyana (1350) give rules for the solution of the equation $by+ax=\pm c$.[65] We shall pass over all the special cases the Indian mathematicians have solved and investigate the "general problem of remainders."[66]

$$N=a_1x_1+r_1=a_2x_2+r_2=a_3x_3+r_3= \ . \ . \ . \ =a_nx_n+r_n.$$

The general solution is given by Bhâskara I and Bhâskara II:

$$a_1x_1+r_1=a_2x_2+r_2. \qquad (1)$$

Suppose that $\alpha_1$ is the smallest value for $x_1$; the general solution is $x_1=\alpha_1+a_2t$,

and

$$N=a_1(\alpha_1+a_2t)+r_1=(a_1\alpha_1+r_1)+a_1a_2t.$$

We can equalize to the third equation:

$$N=(a_1\alpha_1+r_1)+a_1a_2t=a_3x_3+r_3,$$

or

$$a_1a_2t+(a_1\alpha_1+r_1)=a_3x_3+r_3.$$

Suppose that $\alpha_2$ is the smallest solution for $t$; the general solution is $t=\alpha_2+a_3u$, and

$$N=a_1a_2a_3u+(a_1a_2\alpha_2+a_1\alpha_1+r_1).$$

We can proceed in the same way:

$$N=a_1a_2a_3a_4v+(a_1a_2a_3\alpha_3+a_1a_2\alpha_2+a_1\alpha_1+r_1) \ . \ . \ . \ ,$$

until all the equations are used.[67]

EXAMPLES

1. To solve the equations[68]

[64] All these rules are included in Datta and Singh (1), pp. 111 ff; Gurjar (1), p. 115 ff gives the same rules with examples.
[65] See Datta and Singh (1), pp. 120 ff.
[66] See Datta and Singh (1), 131 ff; Yushkevitch (1), pp. 145 f.
[67] A thorough analysis suffices to prove Yushkevitch correct in his statement that the Indian and Chinese methods are completely different.
[68] Given by Bhâskara I. See Datta and Singh (1), p. 133.

$N=8x+5=9y+4=7z+1.$

For solving $N=8x+5=9y+4$, we use the pulverizer to find that $x=1, y=1$, and $N=13$.[69] The general solutions are $x=1+9t$ and $y=1+8t$. Substituting in the original equations, we get:

$8(1+9t)+5=7z+1$
or $72t+13=7z+1$.

The solution for $t$ is 36, or in general $t=36=a+7u$, from which $t_0=1$ $(a+7u=36 \longrightarrow a=1)$. $N=72\times 1+13=85$ is the general solution of the problem.

2. $N=2x+1=3y+1=4z+1=5u+1=6v+1=7w$.[70] Bhâskara I gives the answer 721.

3. $N\equiv 5 \pmod 6 \equiv 4 \pmod 5 \equiv 3 \pmod 4 \equiv 2 \pmod 3$.[71]

Were the Indian mathematicians aware of the conditions of solvability? In his commentary on Brahmagupta, Pṛthûdakaswâmî investigates the case where the moduli are not rela-

[69] Following Bhâskara II's method. Here the equation is reduced to $8x+1=9y$.

$\frac{8}{9}=(0, 1, 8)$

| | |
|---|---|
| 0 | 1 |
| 1 | 1 |
| 1 | |
| 0 | |

In the same way, we treat $72t+12=7z$

$\frac{72}{7}=(10, 3, 2)$

| | |
|---|---|
| 10 | |
| 3 | $3\times 12+0=36=t.$ |
| 12 | |
| 0 | |

[70] Also from Bhâskara I. This problem is also treated by Ibn al-Haitham (c. 1000). See Dickson (1), p. 59, and Wiedemann (1), p. 83; Fibonacci includes it in his *Liber Abacci*, p. 281.

[71] See Datta and Singh (1), pp. 134 f.

tively prime.[72] The text says: "Wherever the reduction of two divisors by a common measure is possible, there 'the product of the divisors' should be understood as equivalent to the product of the divisor corresponding to the greater remainder and quotient of the divisor corresponding to the smaller remainder as reduced (i.e. divided) by the common measure. . . ."

Suppose that $N=a_1x_1+r_1=a_2x_2+r_2$, and that the greatest common denominator of $a_1$ and $a_2=g$.[73] Then $N=(a_1\alpha_1+r_1)+a_1a_2t$ can be written as

$$N=(a_1\alpha_1+r_1)+\frac{a_1a_2}{g}t.$$

We shall conclude this treatment of Indian methods with an evaluation.

1. There is a striking continuity in mathematical works on indeterminate analysis, which puts any study of their contents on a sure basis. This is not the case in China.
2. The methods are on a very high level,[74] and a large number of them are still used in our mathematical textbooks.
3. Modern Indian scholars are of the opinion that all knowledge of indeterminate analysis must have been derived from Indian works. Historical influence seems to have been very great, but internal analysis gives a more reliable basis for comparison than vague historical statements. Chapter 18 of this work is devoted to a comparison of the Indian *kuṭṭaka* and the Chinese *ta-yen* rule. For this reason a thorough analysis of the Indian methods was a necessity.[75]

[72] See Datta and Singh (1), p. 132 (the text) and Yushkevitch (1), p. 146 (interpretation).
[73] Where $r_2-r_1$ is divisible by G.C.D. $(a_1, a_2)$. This general condition is not expressed.
[74] "... As for methods, the Indian works have an aspect of generality that brings them close to the works of modern authors, something that neither Greek nor Arab mathematics succeeded in attaining." ( . . . Quant aux méthodes, les travaux des Indiens ont un caractère de généralité qui les rapproche de ceux des modernes, et auquel ni les mathématiques des Grecs, ni celles des Arabes n'ont réussi à s'élever.) Woepcke (1), p. 32.
[75] For all the sources relied on in this study, the reader is referred to the general bibliography.

## ISLAM

Little information concerning the Chinese remainder problem is to be found in Islamic mathematical works. Abû Kâmil al-Miṣrî[76] (c. 850–930) treats of indeterminate problems, but they are all of the "hundred fowls" type. "Abû Kâmil's procedure in this work, however, is less systematic, and he finds his solutions by trial."[77] As we shall see in the next chapter, the "hundred fowls" problem is to be found for the first time in the work of Chang Ch'iu-chien (c. 475). Similar problems appear in the works of Mahâvîra (ninth century) and Bhâskara II (twelfth century).

In the work of Ibn al-Haitham there is a real remainder problem,[78] identical in every respect to a problem of Bhâskara I[79] and a problem in Fibonacci (1202).[80]

Ibn al-Haitham's problem reads as follows: "Find a number, that divided by 2, 3, 4, 5, 6 has the remainder 1, and divided by 7 has no remainder." The author gives two methods. The first is $N=2\times3\times4\times5\times6+1=721$, the solution used by Bhâskara I. However, this is not the smallest solution, because Ibn al-Haitham does not take into account the fact that some of the divisors are not relatively prime.[81] This method is of course not a general one.

The second method is the equation $N=\frac{3}{4}(6+2n\times7)20+1$, where $n$ is an integer such that $6+2n\times7$ is a multiple of 4. If $n=1$, then $N=\frac{3}{4}\times20\times20+1=301$. If $n=2$, then $N=721$, and

[76] His full name is Sogâ ben Aslam ben Muhamet ben Sogâ, Abû Kâmil. For a general description of his work, see Suter (2), p. 43. His algebraic work is translated by J. Weinberg (1), with the exception of the indeterminate problems. These have been translated by Suter (1) *(Das Buch der Seltenheiten der Rechenkunst.)* According to Weinberg (1), the Staatsbibliothek München has another work of Abû Kâmil on indeterminate problems. See also A. Mieli (1), p. 108. There is a discussion of some of Abû Kâmil's problems in Loria (1), p. 147, and (3), p. 153; Yushkevitch (4), pp. 232 ff; Tropfke (1), vol. 3, pp. 103 f; other articles on the algebra of Abû Kâmil are Karpinski (2) and (3).

[77] Martin (1), p. 8.

[78] Translated by Wiedemann (1). See Dickson (1), vol. 2, p. 59. There is a general description of his life and work in Suter (2), pp. 91–95.

[79] Datta and Singh (1), p. 133.

[80] (1), vol. 1, p. 281.

[81] See Yushkevitch (4), p. 146.

so on. It is obvious that $\frac{3}{4}(6+2n\times 7)20$ is divisible by 2, 3, 4, 5, and 6. That $\frac{3}{4}(6+2n\times 7)20+1$ is divisible by 7 follows from $\frac{3}{4}(6+2n\times 7)20+1=90+30n\times 7+1=91+30n\times 7=(13+30n)\times 7$.[82] The solutions are 301, 721, . . . .

The work of Abû Bakr al-Farajî[83] is entirely within Diophantos's sphere of influence.[84] Abû Bakr includes some indeterminate problems of the first degree,[85] but as Woepcke states: "Actually, it is only the statement of these problems that is indeterminate; the author makes them determinate at the outset by arbitrarily choosing the values of one or more unknowns. In most cases, however, he points out what is arbitrary in the solution provided. Like Diophantos, from whom several of these problems are borrowed, the author does not exclude fractional values. Thus we cannot think of this as a method for the solution of indeterminate equations of the first degree similar to those of Indian or modern mathematicians."[86] Consequently this kind of problem is not of use in our inquiry.[87]

82 The same result, 301, was found in India by Sûryadeva Yajvâ. See Datta and Singh (1), p. 133. Fibonacci gives the following solution:
$N-1\equiv 0 \pmod 2 \equiv 0 \pmod 3 \equiv 0 \pmod 4 \equiv 0 \pmod 5 \equiv 0 \pmod 6$.
Take $N-1 = \text{L.C.M.}(2, 3, 4, 5, 6) = 60$; $60 \equiv 4 \pmod 7$.
We have to find $N-1\equiv 6 \pmod 7$.
$N-1 = 120 \equiv 1 \pmod 7$
$N-1 = 180 \equiv 4 \pmod 7$
$N-1 = 240 \equiv 5 \pmod 7$
$N-1 = 300 \equiv 6 \pmod 7$
The solution is $N = 300+1 = 301$.
Fibonacci gives the general solution
$N = 301+n\times 2\times 3\times 4\times 5\times 6\times 7 = 301+n\times 420$.

83 Muh. b. el-Hasan, Abû Bekr, el-Karchî (died c. 1029).

84 Diophantos's work was translated by Abu'l Wafâ (940–998) into Arabian.

85 See Woepcke (1), p. 10.

86 Ibid. ("En vérité, ce ne sont que les énoncés de ces problèmes qui soient indéterminés; l'auteur rend ces problèmes tout de suite déterminés, en choisissant arbitrairement la valeur d'une ou de plusieurs inconnues. Cependant, il fair ressortir, dans la plupart des cas, ce qu'il y a d'arbitraire dans la solution donnée. Comme Diophante, auquel plusieurs de ces problèmes sont empruntés, l'auteur n'exclut pas des valeurs fractionnaires. Il ne s'agit donc pas ici d'une méthode semblable à celle des Indiens ou des modernes, pour la résolution des équations indéterminées du Ier degré.")

87 It is very likely that there still exist other Arabian works on indeterminate

## EUROPE

### INTRODUCTORY NOTE

If one were to write a detailed history of indeterminate analysis in Europe, it would be necessary to examine all the existing works on arithmetic before modern times.[88] Some of these writers treat the remainder problem, for example, Peurbach, Koebel, Jacob, Rudolff, Cardano, and Tartaglia. However, since a large number of these works say nothing new about the matter, we must, in order to keep this outline within reasonable limits, restrict ourselves to the works mentioned in Dickson (1), who omits only the important Göttingen manuscript. It is necessary to remember that the purpose of this survey is to gather material for a comparison with the Chinese *ta-yen* rule.

The oldest example of an indeterminate problem in Europe appears in the *Propositiones ad acuendos juvenes,* attributed to Alcuin (730?–804);[89] however, as this problem has nothing to do with the remainder problem, it is important only for the investigation of possible historical relationships.

### LEONARDO PISANO (FIBONACCI)

In the *Liber Abbaci* (1202) of Leonardo Pisano (c. 1170–c. 1250), a contemporary of Ch'in Chiu-shao, there are two problems in which the *ta-yen* rule is used.[90] Because the solution of the problems is of help in making a truly scientific comparison,[91] the whole text is provided here:

"Dividat excogitatum numerum per 3, et per 5, et per 7; et

---

analysis. One need only examine Suter (2), where there is a list of 528 names of authors on Arabian mathematics and astronomy. Most of their works exist only in manuscript form, and the greater part have never been studied or translated.

[88] A list of some of them is given in Hofmann (1), pp. 142–145.

[89] The text is published in Migne (1). See Vogel (3), p. 223.

[90] Vol. 1, p. 304.

[91] And not the sort of comparison Van Hee makes, between Ch'in Chiu-shao (1247) and Gauss (1801): "The operations are the same. But what a difference in theory! In the mind of the great German mathematician a sure, methodical progression, stripped of useless details; in the case of the yellow algebraists, obscurity, repetition, fumbling, and, it seems, no idea of uni-

semper interroga, quot ex unaquaque divisione superfuerit. Tu vero ex unaquaque unitate, que ex divisione ternarii superfuerit, retine 70; et pro unaquaque unitate, que ex divisione quinarii superfuerit, retine 21; et pro unaquaque unitate, que ex divisione septenarii superfuerit, retine 15. Et quotiens numerus super excreverit tibi ultra 105, eicias inde 105; et quod tibi remanserit, erit excogitatus numerus. Verbi gratia: ponatur, quod ex divisione ternarii remaneant 2; pro quibus retineas bis septuaginta, id est 140; de quibus tolle 105, remanent tibi 35. Et ex divisione quinarii remanent 3; pro quibus retine ter 21, id est 63, que adde cum predictis 35, erunt 98. Et ex divisione septenarii remaneant 4; pro quibus quater 15 retinebis, id est 60; que adde cum 98 predictis, erunt 158; ex quibus eice 105, remanebunt tibi 53; que erant excogitatus numerus.

"Procedit enim ex hac regula pulchrior divinatio, videlicet ut si quis tecum noverit hanc regulam; et aliquis ei privatim dixerit aliquem numerum, tunc ille tuus consocius, non interrogatus, tacite dividat numerum sibi dictum per 3, et per 5, et per 7, predicta ratione; et quod ex qualibet divisione remanserit, per ordinem tibi dicat; et sic poteris scire numerum sibi privatim dictum."[92]

---

formity capable of tying this most interesting system under discussion to the general principles of numbers." (Ce sont les mêmes opérations. Mais quelle différence dans la théorie! Chez le puissant mathématicien allemand une marche méthodique, sûre, et sobre de détails inutiles; chez les algébristes jaunes, des obscurités, des redites, des tâtonnements et, semble-t-il, aucune idée d'ensemble capable de relier l'intéressant système en discussion aux principes généraux des nombres.) (12), p. 448. It is a pity that Van Hee never saw the "Chinese" solution Fibonacci gives for the remainder problem.

92 "Let a contrived number be divided by 3, also by 5, also by 7; and ask each time what remains from each division. For each unity that remains from the division by 7, retain 70; for each unity that remains from the division by 5, retain 21; and for each unity that remains from the division by 7, retain 15. And as much as the number surpasses 105, subtract from it 105; and what remains to you is the contrived number. Example: suppose from the division by 3 the remainder is 2; for this you retain twice 70, or 140; from which you subtract 105, and 35 remains. From the division by 5, the remainder is 3; for which you retain three times 21, or 63, which

The second problem is as follows:[93]

"Precipe ut numerum, quem in corde suo posuerit, dividat per 5, et per 7, et per 9 ad modum antecedentis regule: et singulariter interroga, quid ex unaquaque divisione remaneat; et pro unaquaque unitate, que ex divisione quinarii remanserit, retine 126; et pro qualibet unitate, ex septenario remanente, 225; et pro qualibet ex novenario, 280; et semper cum summa excreverit, ita ut possit inde extrahere 315, eice ea inde quotienscumque poteris; et quod tibi in fine remanserit, erit quesitus numerus."[94]

The first problem is $\mathcal{N} \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 4 \pmod 7$.[95] The solution is:

| | r=1 | r | | |
|---|---|---|---|---|
| mod 3 | 70 | 2 | $2 \times 70 = 140 - 105 =$ | 35 |
| mod 5 | 21 | 3 | $3 \times 21 =$ 63 | 63 |
| mod 7 | 15 | 4 | $4 \times 15 =$ 60 | 60 |
| | | | | 158 |
| | | | | −105 |
| | | | | 53 |

you add to the above 35; you get 98; and from the division by 7, the remainder is 4, for which you retain four times 15, or 60; which you add to the above 98, and you get 158; from which you subtract 105, and the remainder is 53, which is the contrived number.

"From this rule comes a more pleasant riddle [game], namely if someone has learned this rule with you; if somebody should say some number privately to him, then your companion, not interrogated, should silently divide the number for himself by 3, by 5, and by 7 according to the abovementioned rule; the remainders from each of these divisions, he says to you in order; and in this way you can know the number said to him in private."

[93] Vol. I, p. 304.

[94] "Bid someone to divide a number of which he is thinking by 5, by 7, and by 9 according to the preceding rule; and separately ask for the remainder from each division; and for each unity that remains from the division by 5, retain 126; for each unity that remains from the division by 7, retain 225; and for each unity that remains from the division by 9, retain 280; and each time as the sum should become too large, so that you can subtract 315, subtract it as many times as you can; and what finally remains should be the number asked for."

[95] The Sun Tzŭ problem is $\mathcal{N} \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 2 \pmod 7$. The two problems are not entirely identical, as we find in Tropfke (1), vol. 3, p. 103; Cantor (2), vol. 2, p. 26.

For the second problem, only the *yen-shu*[96] are given:

| | |
|---|---|
| mod 5 | 126 |
| mod 7 | 225 |
| mod 9 | 280 |

The *yen-mu* = 315.

On page 231 of the *Liber Abbaci* the following problems are given:

1.
$N \equiv 1 \pmod 2 \equiv 1 \pmod 3 \equiv 1 \pmod 4 \equiv 1 \pmod 5 \equiv 1 \pmod 6 \equiv 0 \pmod 7$

The solution can be obtained as follows:[97]

$$
\begin{aligned}
N-1 &= \text{L.C.M. } (2, 3, 4, 5, 6) = 60 \\
60 &= 7 \times 8 + 4 \\
2 \times 60 &= 7 \times 17 + 1 \\
3 \times 60 &= 7 \times 25 + 5 \\
4 \times 60 &= 7 \times 34 + 2 \\
5 \times 60 &= 7 \times 42 + 6
\end{aligned}
$$

and $N = 5 \times 60 + 1 = 7 \times 42 + 7$ or $N = 301$.
The general solution is $N = 301 + 420n$.[98]

2.
$N \equiv 1 \pmod n \equiv 0 \pmod{11}$, where $n = 2, 3, \ldots, 10$.

3.
$N \equiv 1 \pmod n \equiv 0 \pmod{23}$, where $n \equiv 2, 3, \ldots, 22$.

[96] In the terminology of Ch'in Chiu-shao; for the explanation of this term, and of *yen-mu*, see Chapter 17.

[97] "Eritque numerus ille 60; quem divide per 7, superant 4, qui vellent esse 6. Ideo quia totus numerus per 7 dividatur; ergo numerus, qui fuerit unum minus eo, cum per 7 dividatur, 6 inde superare necesse est, hoc est 1, minus septenario numero: quare duplicetur 60, vel triplicetur, vel multiplicetur per alium quemlibet numerum, donec multiplicatio ascendat in talem numerum, qui cum dividatur per 7, remaneant inde 6, etc." (p. 282).

[98] The same problem appears in Bhâskara I (522) and Ibn al-Haitham (c. 1000). This last or another Arabian mathematical work may have been Fibonacci's source.

4.
$N \equiv 1 \pmod 2 \equiv 2 \pmod 3 \equiv 3 \pmod 4 \equiv 4 \pmod 5 \equiv 5 \pmod 6 \equiv 0 \pmod 7$.[99]

5.
$N \equiv 1 \pmod 2 \equiv 2 \pmod 3 \equiv 3 \pmod 4 \equiv 4 \pmod 5 \equiv 5 \pmod 6 \equiv 6 \pmod 7 \equiv 7 \pmod 8 \equiv 8 \pmod 9 \equiv 9 \pmod{10} \equiv 0 \pmod{11}$.[100]

Fibonacci does not give the slightest theoretical or general explanation of his method for the solution of the remainder problem, and for this reason his whole treatment is on a level no higher than that of Sun Tzŭ.[101] He does indeed state the *ta-yen* rule, but there is no evidence that he was able to apply it generally. Perhaps he knew only the *yen-shu* of the moduli 3, 5, 7, and 9. In any case his work includes no problem with moduli that are not relatively prime. His algebraical language is entirely rhetorical,[102] according to the custom of his time; and for the purposes of comparison with Ch'in Chiu-shao this fact is very important.

There are several investigations of Fibonacci's sources, and it seems to be beyond all doubt that the greater part of his problems were derived from Arabian mathematicians, namely Al-Khwârizmî and Abû-Kâmil.[103] The latter's work also contains indeterminate problems,[104] and perhaps the *ta-yen*

[99] Comes also from Bhâskara I. See Datta and Singh (1), p. 134. Bhâskara's methods, however, are not the same.

[100] There are some other indeterminate problems in the *Liber Abacci*, on p. 281 and p. 282, but as the method has nothing to do with the *ta-yen* rule, they are not discussed here. These problems can be found also in Dickson (1), vol. 2, p. 59.

[101] See Chapter 15. See also Tropfke (1), vol. 3, p. 105, who says of the indeterminate problem on p. 281 of the first part: "The type of solution does not exceed guessing by very much. Leonardo in a different place...is also familiar with the *ta-yen* rule." (Die Art der Lösung geht nicht viel über Raten hinaus. Leonardo kennt aber auch...an anderer Stelle die Regel *Ta Yen*.)

[102] As is that of Ch'in Chiu-shao; but the latter gives clear diagrams.

[103] Smith (1), vol. 2, p. 382; Yushkevitch (1), pp. 371 ff; see also Bartolotti (1).

[104] However, the *ta-yen* rule is not given in the extant work of Abû-Kâmil.

rule may be derived from an Arabian source. Several scholars have noticed the remarkable similarity between the *ta-yen* rule and the problems dealt with in the work of European mathematicians.[105] Perhaps it is not possible to settle this question until the relationships among the Chinese, Indian, and Islamic worlds have been studied in more detail and the role of Central Asia has been elucidated.[106]

ISAAC ARGYROS (1318–1372)

In some editions of the *Εισαγωγη Αριθμητικη (Eisagogè Arithmètikè)* of Nichomachus of Gerasa[107] there is an appendix entitled *προβληματα Αριθμητικα (Problèmata Arithmètika)*, of which the fifth problem is the same as the one in Sun Tzŭ's work. Needham discusses the matter[108] and on the basis of convincing arguments attributes the problem to Isaac Argyros.[109] Moreover, an analysis of the text seems to justify this interpretation, since the context highly resembles that of the problems in

105 See Cantor (1), vol. 2, p. 26; Tropfke (1), vol. 3, p. 103; Yushkevitch (1), p. 380.

106 Extreme historicism should be avoided. From a logical point of view, one can try to find a chronological relationship, laying stress on the historical dimension of ideas; but this kind of relationship is very difficult to prove and involves much supposition and conjecture. Moreover, cultural nationalism sometimes obstructs a scientific judgment, as has often happened in the case of this particular problem. Another approach is to try to give as objective a description as possible, in order to discern a pattern. The validity of the pattern can be determined from comparison. Such an approach lays stress on the mathematical dimension. For this reason, it should be pointed out that Fibonacci's knowledge of indeterminate analysis is far beneath that of Ch'in Chiu-shao, in spite of the fact that he might have been a greater mathematician than Ch'in and the fact that his work was an important link in the evolution of world mathematics, which was perhaps not the case for Ch'in. Curtze in (3), p. 82, concludes from Fibonacci's text: "Thereby the *ta-yen* rule is proven to have been known to Leonardo to the extent that it was known to the Chinese, albeit without proof." (Damit ist also die Regel *ta-yen* in dem Umfange, welchen die Chinesen kannten, aber ohne Beweis, als Leonardo bekannt nachgewiesen.) This is true if we accept only the Sun Tzŭ problem for comparison, but Ch'in Chiu-shao was Fibonacci's contemporary.

107 So in the *Codex Cizensis*, a Byzantine manuscript of the late fourteenth–early fifteenth centuries.

108 (1), vol. 3, p. 34, note *a*.

109 Ibid.

Fibonacci's *Liber Abbaci*. The title of the problem is "*Μεθοδος, δι'ης αστειως ευρησεις, οιον αριθμον εχει τις επι νουν*" (Method for finding out successfully of which number somebody is thinking). This reminds one of the "*excogitatus numerus*" (contrived number) and the "*Precipe ut numerum, quem in corde suo posuerit . . .*" (bid someone to divide a number of which he is thinking . . .) of Fibonacci.

The translation of the text is as follows:[110]

"If you wish to know no matter what number between 7 and 105 which somebody has in mind, you will find it by the following method. Let the man who has the number in mind mentally subtract 3 as many times as possible, and let him say aloud the remainder under 3—if there is one of course. When he has said it, keep in mind the number 70 for each unity. Thus, if 1 remains, only 70; if 2 remains, two times 70 or 140; if zero remains, you keep nothing. You must pay attention, with the subsequent remainders of subtractions, to this fact whereby there remains no unity. After that let him in the same way subtract 5 as many times as possible and let him say to you this remainder under 5, and take 21 for each unity, and add this number by yourself to the first one, if there is any. After that let him subtract the number 7 in the same manner and let him say the remainder under 7; take 15 for each unity, add all the numbers you have and subtract 105 from the sum as many times as possible—if it is possible of course; and what remains from this is the number you are searching for."

After this, Isaac Argyros gives the example $N=28$:

$$\begin{array}{lrl} 28-9\times 3=1 \longrightarrow & 70 & \\ 28-5\times 5=3 \longrightarrow & 3\times 21=63 & \\ 28-4\times 7=0 \longrightarrow & \underline{0} & \\ & 133 & -105=28. \end{array}$$

THE MUNICH MANUSCRIPT OF THE FIFTEENTH CENTURY (C. 1450)

After Leonardo Fibonacci, no studies on the remainder problem are known to have been produced in Europe until, in the

[110] See Hoche (1), pp. 152 f. I am much indebted to Drs. van Ommeslaeghe for giving me this translation of the Greek text.

fifteenth and sixteenth centuries, mainly in Germany, interest was awakened again. In 1870 Gerhardt published a part of a manuscript kept in the Staatsbibliothek at Munich,[111] and Curtze published another part of it (problems 268–272) in 1895.[112] A recent publication of the whole text is Vogel (3).

The text seems to have been written by more than one author, but the major part was from the hand of a certain Frater Fredericus.[113]

One of the indeterminate problems says:[114]

"Quidam dominus dives habet 4 bursas denariorum, in unaquaque tantum quantum in alia de denariis, quos vult distribuere in viam eleosine quator ordinibus scilicet czeilen [sic] pauperum. In primo ordine pauperum sunt 43 pauperes, in secundo sunt 39 pauperes, in tercio sunt 35 pauperes, in quarto sunt 31 pauperes. Primam bursam distribuit equaliter primo ordini, in fine tamen remanent sibi 41, ita quod ad complendum ordinem deficiunt sibi 2 denarii. Secundam bursam distribuit equaliter secundo ordini, in fine tamen non potest complere, sed habet in residuo 33, sicque ad complendum ordinem deficiunt ei 6 denarii. Terciam bursam distribuit equaliter tercio ordini, in fine tamen remanent sibi 25, sicque ad complendum ordinem deficiunt ei 10 denarii. Quartam bursam distribuit quarto ordini equaliter, in fine tamen est residuum 17 denariorum, sicque ei 14 denarii deficiunt ad complendum ordinem. Queritur nunc, quod fuerunt denarii in una bursa?

"In summa questio habet hoc: invenias usum numerum, qui dum dividitur per 43, post integra quocientis manent in residuo 41; item dum dividitur per 39, manent in residuo 33; item dum dividitur per 35, manent in residuo 25; item dum dividitur per

111 (1). pp. 141 ff.
112 (1), pp. 31–74 ("Ein Beitrag zur Geschichte der Algebra in Deutschland im fünfzehnten Jahrhundert").
113 For more details about this work, see Curtze (1), and Tropfke (1), vol. 3, p. 105.
114 Curtze (1), p. 64.

31, in residuo manent 17; licet autem non sit solum unus numerus, qui talis est, verum infiniti sunt signabiles. 5458590."[115]

There is not the slightest indication of any method. Curtze[116] supposes, however, that the author was familiar with the *ta-yen* rule, but it is very peculiar that he did not find the smallest solution.[117] Indeed, the solution of $N \equiv 41 \pmod{43} \equiv 33 \pmod{39} \equiv 25 \pmod{35} \equiv 17 \pmod{31}$ is $N = 1{,}819{,}500 + 1{,}819{,}545\, n$.

In the same manuscript there is also a German text, which is much more interesting.[118] "I wish also to know how many

[115] "A certain rich man has 4 purses of silver coins; in each of them there is the same amount, which he wishes to distribute on the way...[?]. In the first group of poor men there are 43 paupers, in the second there are 39 paupers, in the third there are 35 paupers, in the fourth there are 31 paupers. The first purse he distributes equally to the first group; in the end he has a remainder of 41 coins, or he lacks 2 coins to complete the first group. The second purse he distributes equally to the second group, in the end, he cannot complete the distibution, but he has a remainder of 33, or a shortage of 6 coins. The third purse he distibutes equally to the third group; in the end, however, he has a remainder of 25, or a shortage of 10 coins. The fourth purse he distributes equally to the fourth group; in the end, however, he has a remainder of 17 coins, or a shortage of 14 coins. Find the amount of coins in one purse. In résumé this is the problem: find a number that, divided by 43, after you get the whole quotient, has a remainder of 41; when divided by 39, has a remainder of 33; when divided by 35, has a remainder of 25; when divided by 31, has a remainder of 17. Although there should not be only one number that is like that—indeed the solutions are of an infinite number—[a solution is] 5458590."

[116] (1), p. 67.

[117] Curtze (1) gives the solution by the *ta-yen* rule, and says: "The fact that we are justified in assuming that the solution was arrived at in this manner derives from the evidence that later teachers of arithmetic, such as Rudolf (active 1525), Koebel (active 1520), and Simon Jacob (active 1550) taught the extension into four simultaneous equations, without however indicating how they have found the 'use numbers' [Hülfszahlen, or Chinese *yen-shu*] for certain numbers." (Dass wir berechtigt sind, die Auflösung als in dieser Weise erfolgt anzunehmen, ergiebt sich daraus, dass spätere Rechenlehrer wie Rudolf (n. fl. 1525), Koebel (n. fl. 1520) und Simon Jacob (n. fl. 1550) die Erweiterung auf 4 gleichzeitige Gleichungen lehren, ohne jedoch anzugeben, wie sie die für bestimmte Zahlen mitgetheilten Hülfszahlen gefunden haben.)" (p. 67). Anyhow, if it was a Chinese problem, nobody should agree with Curtze's conclusion.

[118] Curtze (1), pp. 65 f; Gerhardt (1), p. 141; Vogel (3), p. 138 (no. 311).

coins he has in his purse or in his mind.[119] Do it so. Let him count the coins he has by threes, then by fives, then by sevens, and as often as there remains 1 with 3, note 70; and as often as there remains 1 with 5, note 21, and with 7, note 15. After that, add up these numbers, and from this sum subtract the radix;[120] that is, multiply 3 by 5 and 7; this will be 105, as many times as you can [subtract], and what remains, so much he has in mind or in his purse.[121] This example does not go higher[122] than as far as the radix goes, that is, to 105, and one does not have to take more than that."

The last sentence seems to mean that the number asked for must be smaller than 105, and thus only the smallest solution is kept.

The following passage is the most interesting one on the remainder problem that has been preserved from this period, and the first European explanation of the rule.

"You ask, why does one take 70 for 3, and 21 for 5, etc. Do it in this way. If you want the number for 3, multiply 5 by 7, and what you find, divide it by 3; and if the remainder is 1, this number is right;[123] however, if the remainder is more than 1, double the same number, and after that divide by 3, and if the remainder is more than 1, add the same number. Do it as long as the remainder becomes 1.[124] In the same manner, if you want the number for 5, multiply 3 by 7; you get 21; divide it by 5; the remainder is 1; for this reason 21 is the right num-

---

As the text has been published only in medieval German, it is translated here into English.

119 The text says: "Wie vil pfenning in dem peutel oder im 'synn' hast." "*Synn*" is in another place spelled as "*sinn*." I think it means "mind"; it recalls the "contrived number" (*excogitatus numerus*) of Fibonacci.

120 A part of this text is in Latin; here the text says: "et ab ista summa subtrahe radicem."

121 To this point, this is exactly the same problem as the one in the *Sun Tzŭ suan-ching* and in the *Liber Abacci*.

122 "Item das exempel get nit höher."

123 $5 \times 7$ is the *yen-shu* of 3.

124 2: $35 \equiv 2 \pmod 3$
$\underline{35 \equiv 2 \pmod 3}$
$70 \equiv 4 \pmod 3 \equiv 1 \pmod 3$.

ber for 5.[125] If you want the number for 7, multiply 3 by 5; you get 15; divide this by 7; the remainder is 1; thus 15 is the right number for 7.[126] The same way for the others [he indicates the accompanying diagram]."

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 70 | 21 | 15 | 15 | 10 | 6 | 40 | 45 | 36 | 28 | 21 | 36 |
| 3 | 5 | 7 | 2 | 3 | 5 | 3 | 4 | 5 | 3 | 4 | 7 |
| | 105 | | | 30 | | | 60 | | | 84 | |
| 21 | 28 | 36 | 63 | 36 | 28 | 128 | 175 | 120 | 216 | 225 | 280 |
| 2 | 3 | 7 | 2 | 7 | 9 | 5 | 6 | 7 | 5 | 8 | 9 |
| | 42 | | | 126 | | | 210 | | | 360 | |
| 1144 | 936 | 1782 | | | | | | | | | |
| 9 | 11 | 13 | | | | | | | | | |
| | 1287 | | | | | | | | | | |

This text seems to be of great importance for the history of indeterminate analysis in Europe. The author does indeed know a general procedure for solving the problem; and he is far beyond the level of Fibonacci, since he is surely making use of more than conjecture. Whether this is an example of "*die reine Regel*" (the pure rule), as Curtze says, is another question. The author indeed solves the congruences, but he does not solve them in a general way, as Ch'in Chiu-shao does. He has to build up his "congruence factors" with great patience, looking always for the remainder 1. That seems to be the only reason why his moduli go no higher than 13.[127] The second characteristic of his method is that the moduli must always be relatively prime in pairs. It is difficult to understand why Curtze wishes to prove that there is absolutely no Chinese influence in Europe.[128] In the first place, this is without real

[125] $3 \times 7$ is the *yen-shu* of 5.
$21 \equiv 1 \pmod 5$.
[126] $3 \times 5$ is the *yen-shu* of 7.
$15 \equiv 1 \pmod 7$.
[127] For that reason, one could consider this as an example of the rule ("die Regel"), but not of the pure rule ("die reine Regel"). For comparison: instead of multiplying 2,345 with 8,457, one can also add up 2,345 times 8,457; this is also a rule, but not a pure rule.
[128] Curtze (1), p. 66.

importance, because it is beyond all doubt that in 1247 Ch'in Chiu-shao solved indeterminate problems in which the moduli are not relatively prime in pairs. On the other hand, the remainder problem became known in Europe through Fibonacci's work (1202), no matter from where he learned it. The Italian works were very well known in Germany, as one can see from the use of several words belonging to Italian mathematical terminology.[129] Is it unreasonable to suppose that the manuscript of Munich derived (perhaps over many links) from Fibonacci? It is in any case to the credit of the author of the manuscript that he was the first to understand the problem in a more general way than his predecessors.

There is another problem in the same manuscript: $N \equiv 2 \pmod 3 \equiv 2 \pmod 5 \equiv 3 \pmod 7$. Here again we have the problem of Fibonacci (and of Sun Tzŭ). The author calls his method the "*regula posicionis, et dicitur regula falsa*" (the rule of position, also called the false rule, i.e., the rule of false position). This is of course entirely wrong.[130]

REGIOMONTANUS[131]

From the correspondence between Regiomontanus and Bianchini we know something about the knowledge of indeterminate analysis in the fifteenth century. In 1463 Regiomontanus posed the following problem in one of his letters: "Quero numerum, qui si dividatur per 17 manent in residuo 15, eo autem diviso per 13, manent 11 residua, et ipso diviso per 10 manent tria residua: quero, quis sit numerus ille."[132] Bian-

[129] Ibid., p. 33.

[130] It is strange to find the same in China. In the *Ssŭ-k'u ch'üan-shu chien-ming mu-lu* of 1782, one can read that the *ta-yen* rule relies on the *t'ien-yüan* algebra, but that the rule of false position, a European method, is much better. Even the *Tzŭ Yüan* gives the same information about the origin of the rule of false position, while it is clear that it was transmitted from China to Europe. See Needham (1), vol. 3, p. 118, and Ch'ien Pao-tsung (11′).

[131] Zinner (1) has an extensive study on the life and work of Regiomontanus.

[132] De Murr (1), p. 99; Curtze (2), p. 219. "I ask for a number that divided by 17 has the remainder 15; divided by 13 has the remainder 11; divided by 10 has the remainder 3. I ask you, which is this number."

chini's answer (1464) says: ". . .Huic quesito multe responsiones dari possent cum diversis numeris, qui propositionem concluderunt, ut 1103, 3313 et alii multi. Sed in hoc non curo laborem expendere, in aliis numeris invenire."[133] From the last sentence, it is obvious that Bianchini did not know the general rule.[134] Regiomontanus wrote in reply: ". . .bene reddidistis numerum quesitum minimum 1103, secundum autem 3313. Satis est, nam infiniti sunt tales, quorum minimus est 1103. Huic si addiderimus numerum numeratum ab ipsis tribus divisoribus, scilicet 17, 13 et 10, habebitur secundus, item eodem addito resultat tertius, etc."[135]

In the margin Regiomontanus drew the diagram

$$\begin{array}{ll} 17 & 170 \\ 13 & \underline{\ \ 13} \\ 10 & 510 \\ & \underline{\ 17\ } \\ & 2210 \end{array}$$

[133] "To this problem many solutions can be given with different numbers, which agree with the problem, such as 1,103, 3,313, and many others. However I do not want to go to the the trouble of finding out other numbers."

[134] Curtze (2), p. 237, n. 1; Tropfke (1), vol. 3, p. 105; Cantor (1), vol. 2, p. 287: "...and even though Bianchini makes it known, through his next remark to the effect that he does not want to go to the trouble of finding further solutions, that he was not aware of the general solution 2,210 $n$ + 1,103, it can under no circumstances be assumed that such questions can find their answers through the mere fumbling of researchers unfamiliar with such matters."(...Und wenn auch Bianchini durch die nachfolgenden Worte, er wolle sich die Mühe nicht geben, weitere Lösungen zu suchen, zu erkennen gibt, dass er die allgemeine Auflösung 2210 $n$ + 1103 nicht besass, so ist doch keineswegs anzunehmen, dass solche Fragen durch blosses Herumtasten ihre Beantwortung finden konnten, ohne dass den Bearbeitern jemals vorher ähnliche Gegenstände vorgelegen hätten.) In any case, it is fortunate for Bianchini that he was not Chinese.

[135] "You have rightly given the smallest number asked for as 1,103, and the second one as 3,313. This is enough, because such numbers, of which the smallest is 1,103, are infinite. If we should add a number computed [by multiplying] these three divisors, namely 17, 13, and 10, we should have the second; in the same manner, by adding the same, the third one results, and so on."

Curtze concludes: ". . . this, together with the marginal notation, makes it obvious that Regiomontanus possessed a complete solution of this problem, as during his lifetime a great many such problems were widely circulated."[136] This is possible, but Regiomontanus does not explain how he found the first solution. And this was indeed not so simple. If we solve the problem according to the *ta-yen* rule, we get

| | | | |
|---|---|---|---|
| *ting-mu* | 17 | 13 | 10 |
| *yen-shu* | 130 | 170 | 221 |
| *yen-mu* | | 2210 | |
| *chi-shu* | 11 | 1 | 1 |
| *ch'êng-lü* | 14 | 1 | 1 |

$$14 \times 130 = 1820 \quad \times 15 = 27{,}300$$
$$1 \times 170 = 170 \quad \times 11 = 1{,}870$$
$$1 \times 221 = 221 \quad \times 3 = 663$$
$$29{,}883 - 13 \times 2{,}210 = 1{,}103$$

According to Curtze, Regiomontanus performed all these computations by mental arithmetic; but in the margin he did a simple multiplication. And how did he solve the congruences? Curtze's allegation "that he also knew thoroughly the remainder problem, the *ta-yen* rule of the Chinese . . ."[137] is not at all convincing. If we reject all unprovable suppositions, Regiomontanus says only that the numbers Bianchini found[138] are right, but that all the other numbers can easily be found by adding the least common multiple of 17, 13, and 10 to the first number. To pretend that he knew a general method simply because it was known elsewhere in his time[139] is not at all scientific. It is of course impossible to prove the contrary; without texts to rely on, all is mere conjecture.

136 "Hieraus in Verbindung mit der Randglosse ist klar, dass Regiomontan die vollständige Lösung dieses Problems besass, wie denn zu seiner Lebenszeit dergleichen Aufgaben vielfach umliefen." (2), p. 254, *n*. 1.

137 ". . . dass er auch das Restproblem, die Regel *ta-yen* der Chinesen, vollständig beherrschte." (2), p. 189.

138 And, as we read, by "going to trouble" (*laborem expendere*), that is, without a general method.

139 That is, to the author of the Munich manuscript.

ELIA MISRACHI

Elia Misrachi (1455–1526), a Jewish mathematician, included some remainder problems[140] in his *Sefer-Hamispar*.[141]

1. "What number has the remainder 1 when divided by 2, the remainder 2 when divided by 3, the remainder 3 when divided by 4, the remainder 4 when divided by 5, the remainder 5 when divided by 6 and the remainder 0 when divided by 7?"[142] It is beyond all doubt that this problem is derived from Leonardo Pisano; the method is also entirely the same.

2.
$N \equiv 1 \pmod 2 \equiv 2 \pmod 3 \equiv 3 \pmod 4 \equiv 0 \pmod 5$ (variant of 1).

3.
$N \equiv 1 \pmod 2 \equiv 1 \pmod 3 \equiv 1 \pmod 4 \equiv 1 \pmod 5 \equiv 1 \pmod 6 \equiv 0 \pmod 7$.[143]

4.
$N \equiv 1 \pmod 2 \equiv 1 \pmod 3 \equiv 1 \pmod 4 \equiv 0 \pmod 5$.

5.
$N \equiv 1 \pmod 2 \equiv 2 \pmod 3 \equiv 3 \pmod 4 \equiv 1 \pmod 5 \equiv 5 \pmod 6 \equiv 1 \pmod 7 \equiv 7 \pmod 8 \equiv 8 \pmod 9 \equiv 1 \pmod{10}$.

6.
$N \equiv 0 \pmod 2 \equiv 2 \pmod 3 \equiv 0 \pmod 4 \equiv 0 \pmod 5 \equiv 2 \pmod 6 \equiv 3 \pmod 7 \equiv 4 \pmod 8 \equiv 5 \pmod 9 \equiv 0 \pmod{10}$.

The methods Elia Misrachi used in solving these problems do not include anything new.

MICHAEL STIFEL[144]

Dickson says: "Michael Stifel gave the correct result that if $x$ has the remainders $r$ and $s$ when divided by $a$ and $a+1$, respectively, then $x$ has a remainder $(a+1)r+a^2s$ when divided by $a(a+1)$."[145]

140 Wertheim (1), pp. 60 f; Steinschneider (1), p. 477.
141 Not to be confused with the *Sefer-Hamispar* by Abraham ibn Esra (1093–1167).
142 The same problem is given by Bhâskara I, with a slight variation. See Datta and Singh (1), pp. 134 f. It appears in Fibonacci (1), vol. 1, p. 282.
143 The same in Bhâskara I, Ibn al Haitham, and Fibonacci.
144 For the life and works of Stifel, see Müller (1) and Hoppe (1).
145 Dickson (1), vol. 2, p. 60.

In the *Arithmeticae Liber I* (1544), fol. 38, the rule is of course stated in full. However, everything about this work gives the impression that even for Stifel, the problem was a kind of game.[146] Dickson's modern representation is not correct; the last clause should read: ". . . then $(a+1)r+a^2s$ has the remainder $x$ when divided by $a(a+1)$."[147]

Euler discusses Stifel's problem and demonstrates that this particular case can be deduced from his own general rule.[148]

THE MANUSCRIPT OF GÖTTINGEN (c. 1550)[149]

This is the most interesting study on the remainder problem that we have dealt with so far.[150] The general rule is given in Latin, the rest of the text in medieval German. The text is much too long to translate here, so this account will include only its mathematical explanation.[151] It consists of an entire solution of the remainder problem when the moduli are relatively prime in pairs; even a system for solving the congruences is given. There is also an attempt to solve the problem when the moduli are not relatively prime, but this is not a general rule.

1. With moduli relatively prime in pairs:
$\mathcal{N}\equiv 5 \pmod 7 \equiv 7 \pmod 8 \equiv 6 \pmod 9 \equiv 0 \pmod{11}$.
Solution:

| | |
|---|---|
| (1) | (2) |
| $8\times 9\times 11=792$ | $7\times 9\times 11=693$ |
| $792-n\times 7=1$ | $693-n\times 8=5$ |

146 He writes: "Jam si numerus a te electus, qui mihi sit occultus..." (fol. 38, b).

147 "Et aggregatum illud divido, per numerum qui provenit ex multiplicatione duorum meorum numerorum primo receptorum (...) *tunc apparebit semper numerus a te electus, in residuo divisionis meae.*" (fol. 38, b). See also *Die Coss Christoffs Rudolfs* (1453), fol. 16, b.

148 Euler (1), par. 18, pp. 27 f.

149 The MS was published by Curtze (2), pp. 552–558. It is dated 1524. The German part was written by Andr. Alexander (1545). See Hofmann (1), vol. 1, p. 145.

150 It is rather surprising that we do not find it in Dickson (1).

151 The author calls himself "Initius Algebras," but this is of course only a pseudonym.

(3)
$7 \times 8 \times 11 = 616$
$616 - n \times 9 = 4$

(4)
$7 \times 8 \times 9 = 504$
$504 - n \times 11 = 9.$

For (1) the remainder is 1; the congruence is solved.[152] For (2) the remainder is 5; it is necessary to "reduce"[153] (*reducirn*). The method is as follows:[154]

$$\begin{array}{llllll} 5+5= & 10 & & & & \\ & -\underline{8} & & & & \\ & 2+5= & 7 & & & \\ & & +\underline{5} & & & \\ & & 12-8= & 4 & & \\ & & & +\underline{5} & & \\ & & & 9-8=1. & & \end{array}$$

Count the number of "*loca*":[155] there are five fives. Five is the solution of the congruence.

For (3) we get:

[152] "So wir thailen 729 mit 7, restat 1, davon darf die nicht weither reducirt werden. . .sunder sie pleiben unvorwandelt" (p. 555).

[153] "Aber so wir thailen 693 mit 8, restat 5, die müssen wir reducirn in ein ander zal, so sie in die wirdt gethailt mit 8, das dann unitas pleibt."

[154] This means

$$\begin{array}{rl} & 693 \equiv 5 \pmod 8 \\ & \underline{693 \equiv 5 \pmod 8} \\ 2 \times & 693 \equiv 2 \pmod 8 \\ & \underline{693 \equiv 5 \pmod 8} \\ 3 \times & 693 \equiv 7 \pmod 8 \\ & \underline{693 \equiv 5 \pmod 8} \\ 4 \times & 693 \equiv 4 \pmod 8 \\ & \underline{693 \equiv 5 \pmod 8} \\ 5 \times & 693 \equiv 1 \pmod 8 \end{array}$$

[155] *Loca* means the number of fives added up.

$$\begin{array}{l}
4+4=8 \\
\quad +4 \\
12-9=3 \\
\quad +4 \\
7+4=11 \\
\quad -9 \\
2+4=6 \\
\quad +4 \\
10-9=1.
\end{array}$$

The number of "*loca*" is seven.

For (4) we get:

$$\begin{array}{l}
9+9=18 \\
\quad -11 \\
7+9=16 \\
\quad -11 \\
5+9=14 \\
\quad -11 \\
3+9=12 \\
\quad -11 \\
\quad 1
\end{array}$$

The number of "*loca*" is five.

This method for solving the congruences is naturally suited only for small numbers. However, it must be said that it is very ingenious and simple. Moreover, the author grasped very well the reason why he could solve the congruences in this way: "This is the reason why we examine such 'reductions' by the '*loca.*' If we take the 'reduced number' 504, then the remainder is 9. If we double it (i.e. 504), the 9, as the remainder of it, also doubles. This is the reason why we said 9 and 9 is 18, we have 11 above the remainder, and there is left 7, while two times 504 is 1,008, which divided by 11, has the remainder 7, etc."[156]

156 "Warumb wir aber solche Reductionen durch die loca examinirt haben, propter hoc fit, das ist die ursach. Wann, so wir nemen die reducirte zal eine, als 504, do pleiben 9, so wir zwispalten, duplirn sich auch 9, das residium in ir... etc." (p. 556).

The text gives the entire explanation of the method for finding unity.[157]

We multiply by the congruence factors:

$792 \times 1 = 792$
$693 \times 5 = 3{,}465$
$616 \times 7 = 4{,}312$
$504 \times 5 = 2{,}520.$

We multiply with the remainders:

$$\begin{aligned} 792 \times 5 &= 3{,}960 \\ 3{,}465 \times 7 &= 24{,}255 \\ 4{,}312 \times 6 &= 25{,}872 \\ 2{,}520 \times 0 &= \underline{\quad\quad 0} \\ & \phantom{=} 54{,}087 = N. \end{aligned}$$

The most interesting part of the text gives evidence that the author was far advanced beyond conjecture and understood the system thoroughly: "What is the reason why we add them up and multiply them by the remainders; each of the numbers is divisible by all the divisors except by its own corresponding divisor, [in which case] there remains 1. The same 1 of each number is, in the "reduced numbers," multiplied with its remainder, and becomes the remainder of it; and for this reason each 'reduced number' is divisible by all divisors, except its own, if the division leaves a remainder. Therefore the whole sum 54,087 also leaves a remainder when divided by those divisors."[158]

This means that the author had grasped the following system:

[157] The author says: "Desgleichen mögen wir thun mit 504, wiewol es nicht not, wann sie khein Residuanten hat, darin sie soll gemultiplicirt werden..." [We can do the same (solving the congruence) with 504 although there is no need, because it has no remainder which it must be multiplied with.] He is well aware of the fact that, if the remainder is 0, the congruence must not be solved.

[158] Pp. 556 f.

$$\begin{array}{r}
3960 \equiv 5 \pmod 7 \equiv 0 \pmod 8 \equiv 0 \pmod 9 \equiv 0 \pmod{11} \\
24255 \equiv 0 \pmod 7 \equiv 7 \pmod 8 \equiv 0 \pmod 9 \equiv 0 \pmod{11} \\
25872 \equiv 0 \pmod 7 \equiv 0 \pmod 8 \equiv 6 \pmod 9 \equiv 0 \pmod{11} \\
2520 \equiv 0 \pmod 7 \equiv 0 \pmod 8 \equiv 0 \pmod 9 \equiv 0 \pmod{11} \\
\hline
54087 \equiv 5 \pmod 7 \equiv 7 \pmod 8 \equiv 6 \pmod 9 \equiv 0 \pmod{11} \\
-n \times 5544 \equiv 0 \pmod 7 \equiv 0 \pmod 8 \equiv 0 \pmod 9 \equiv 0 \pmod{11} \\
\hline
4191 \equiv 5 \pmod 7 \equiv 7 \pmod 8 \equiv 6 \pmod 9 \equiv 0 \pmod{11}.
\end{array}$$

This is the first text in Europe giving evidence that the whole system was known thoroughly, at least for the case in which the moduli are relatively prime in pairs. Only the method for solving the congruences is not ideal, because it is restricted to small numbers.

2. With moduli not relatively prime in pairs:[159]
$\mathcal{N} \equiv 2 \pmod 6 \equiv 6 \pmod 8 \equiv 4 \pmod{10} \equiv 8 \pmod{14}$.
The solution is given as follows:

The L.C.M. $(6, 8, 10, 14) = 840$.
$840 : 6 = 140 \qquad 140 \equiv 2 \pmod 6$[160]
$840 : 8 = 105 \qquad 105 \equiv 1 \pmod 8 \longrightarrow 630 \equiv 6 \pmod 8$
$840 : 10 = 84 \qquad 84 \equiv 4 \pmod{10}$
$840 : 14 = 60 \qquad 60 \equiv 4 \pmod{14} \longrightarrow 120 \equiv 8 \pmod 8$
$140 + 630 + 84 + 120 = 974$
$974 - 840 = 134$.[161]

[159] The author is well aware of the difference between the two methods, for he says: "So do wurden vorgeschlagen divisorés, die do communicirn mit einander..." (p. 557).

[160] It is impossible to solve the congruence $140 \equiv 1 \pmod 6$ "und hierumb, das er nicht khan in die loca khumen, dar inn er aufging an der dritten stadt, darumb lassen wir in reducirt und gemultiplicirt sein mit sein restanten 2." Indeed, $140 = 2 \pmod 6$; $2 \times 140 \equiv 4 \pmod 6$; $3 \times 140 \equiv 0 \pmod 6$.

[161] Ch'in Chiu-shao's rule would give the following solution:

| | | | | |
|---|---|---|---|---|
| | 6 | 8 | 10 | 14 |
| | 3 | 8 | 5 | 7 |
| | 3 × | 8 × | 5 × | 7 = 840 |
| *yen-shu* | 280 | 105 | 168 | 120 |
| *chi-shu* | 1 | 1 | 3 | 1 |
| *ch'êng-lü* | 1 | 1 | 2 | 1 |
| | 280 | 105 | 336 | 120 |
| | ×2 | ×6 | ×4 | ×8 |
| | 560 + | 630 + | 1,344 + | 960 |

$= 3{,}494 - n \times 840 = 134.$

This is not a general method. The reason why the right solution is found is obvious from the following scheme:

$$
\begin{aligned}
140 &\equiv 2 \pmod 6 \equiv \mathit{4\ (mod\ 8)} \equiv 0 \pmod{10} \equiv 0 \pmod{14}\\
630 &\equiv 0 \pmod 6 \equiv 6 \pmod 8 \equiv 0 \pmod{10} \equiv 0 \pmod{14}\\
84 &\equiv 0 \pmod 6 \equiv \mathit{4\ (mod\ 8)} \equiv 4 \pmod{10} \equiv 0 \pmod{14}\\
120 &\equiv 0 \pmod 6 \equiv 0 \pmod 8 \equiv 0 \pmod{10} \equiv 8 \pmod{14}\\
\hline
974 &\equiv 2 \pmod 6 \equiv 6 \pmod 8 \equiv 4 \pmod{10} \equiv 8 \pmod{14}.
\end{aligned}
$$

The second equation $974 \equiv 6 \pmod 8$ is right only because the sum of the two remainders 4 equals 8, being the modulus.[162]

In a last problem, the author gives the reason why this problem is unsolvable:

$$N \equiv 4 \pmod 5 \equiv 3 \pmod 6 \equiv 2 \pmod 8 \equiv 1 \pmod 9.$$

The lowest common multiple of the moduli is 360. The *yen-shu* are 72, 60, 45, and 40. For 60 we have $\alpha \times 6 \equiv 1 \pmod{60}$; this is unsolvable, because 60 is divisible by 6.

The reason for unsolvability can be derived from the problem at first glance. The equation $3 \pmod 6 = 1 \pmod 9$ is impossible, the only possibilities being $3 \pmod 6 = r \pmod 9$, where $r$ is 0, 3, or 6 ; $3 \pmod 6 = 2 \pmod 8$ is also unsolvable, because the first is odd and the second even.

The general condition for solvability when the moduli are not relatively prime was unknown to the author, namely, that $r_i - r_j$ must be divisible by the greatest common divisor of $m_i$ and $m_j$.[163]

C. G. BACHET DE MEZIRIAC[164]

In his *Problèmes plaisans et delectables, qui se font par les nombres* (1612), Bachet de Méziriac gives a solution of the equation

[162] In the system of Ch'in Chiu-shao, this scheme becomes:

$$
\begin{aligned}
560 &\equiv 2 \pmod 6 \equiv 0 \pmod 8 \equiv 0 \pmod{10} \equiv 0 \pmod{16}\\
630 &\equiv 0 \pmod 6 \equiv 6 \pmod 8 \equiv 0 \pmod{10} \equiv 0 \pmod{14}\\
1344 &\equiv 0 \pmod 6 \equiv 0 \pmod 8 \equiv 4 \pmod{10} \equiv 0 \pmod{14}\\
960 &\equiv 0 \pmod 6 \equiv 6 \pmod 8 \equiv 0 \pmod{10} \equiv 8 \pmod{14}\\
\hline
3494 &\equiv 2 \pmod 6 \equiv 6 \pmod 8 \equiv 4 \pmod{10} \equiv 8 \pmod{14}
\end{aligned}
$$

[163] Ch'in Chiu-shao did not know this condition either (see Chapter 17). However, it is fulfilled in his examples.

[164] For the life and works of Bachet de Méziriac, see Itard (1).

$Ax+By=C$. A full description can be found in Dickson.[165] The general treatment is as follows:

The solution of $Ax=By+C$ can be deduced from $Ax=By+1$. Making use of Euclid's algorithm for finding the G.C.D. of $A$ and $B$, we get:

$$A=Bq_1+r_1 \quad (1a)$$
$$B=r_1q_2+r_2 \quad (1b)$$
$$r_1=r_2q_3+r_3 \quad (1c)$$
$$r_2=r_3q_4+r_4 \quad (1d)$$
$$\vdots \quad \vdots \quad \vdots$$

Suppose that $r_4=1$; then $r_2=r_3q_4+1$, and

$$r_2r_3+1-r_2\equiv 0 \pmod{r_3}\equiv 1 \pmod{r_2}. \quad (1)$$

From the first equation,[166] we get $\alpha=q_4r_3-q_4+1$, and

$$\alpha r_3=\beta r_2+1. \quad (2)$$

Multiply (1c) by $\alpha$:

$$r_1=r_2q_3+r_3 \quad (1c)$$
$$\alpha r_1=\alpha r_2q_3+\alpha r_3.$$

Substitute (2):

$$\alpha r_1=\alpha r_2q_3+\beta r_2+1$$
$$\alpha r_1=(\alpha q_3+\beta)r_2+1.$$

Take $\alpha q_3+\beta=\gamma$

$$\alpha r_1=\gamma r_2+1. \quad (3)$$

Multiply (1b) by $\gamma$:

$$B=r_1q_2+r_2 \quad (1b)$$
$$\gamma B=\gamma r_1q_2+\gamma r_2.$$

165 Dickson (1), vol. 2, pp. 44 f.

166 We can prove the first equation by substituting $r_2$ by $r_3q_4+1$; then we have $r_2r_3+1-r_2=r_2(r_3-1)+1=r_3q_4+1$, and $(r_3-1)+1=\alpha\, r_3$, where $\alpha=q_4r_3-q_4+1$.

Substitute (3):

$\gamma B = \gamma r_1 q_2 + \alpha r_1 - 1$
$\gamma B = (\gamma q_2 + \alpha) r_1 - 1.$

Take

$\gamma q_2 + \alpha = \delta$
$\gamma B = \delta r_1 - 1$
$\delta r_1 = \gamma B + 1. \qquad (4)$

Multiply (1a) by $\delta$:

$A = Bq_1 + r_1 \qquad (1a)$
$\delta A = \delta B q_1 + \delta r_1.$

Substitute (4):

$\delta A = \delta B q_1 + \gamma B + 1$
$\delta A = (\delta q_1 + \gamma) B + 1.$

Take $\delta q_1 + \gamma = \varepsilon$. From this we obtain the solutions

$x = \delta$
$y = \delta q_1 + \gamma = \varepsilon.$

Example: [167]

$67x = 60y + 1$
$67 = 60 \times 1 + 7$
$60 = 7 \times 8 + 4$
$7 = 4 \times 1 + 3$
$4 = 3 \times 1 + 1$
$\alpha = q_4 r_3 - q_4 + 1 = 1 \times 3 - 1 + 1 = 3$
$\beta = \frac{\alpha r_3 - 1}{r_2} = \frac{3 \times 3 - 1}{4} = 2$
$\gamma = \alpha q_3 + \beta = 3 \times 1 + 2 = 5$
$\delta = \gamma q_2 + \alpha = 5 \times 8 + 3 = 43 = x$
$\varepsilon = \delta q_1 + \gamma = 43 \times 1 + 5 = 48 = y.$

Matthiessen is quite right in stating: "It [Bachet's method] agrees completely with the *kuṭṭaka* method of the Indian math-

[167] See Dickson (1), vol. 2, p. 44.

ematicians."[168] The only difference is that Bachet does not use "the assumed number $t$,"[169] but the direct formula $\alpha = q_4 r_3 - q_4 + 1$.

In Bachet's work there are other remainder problems that Dickson does not mention. On page 127 we read: "I ask for a number that, when divided by 2, leaves a remainder of 1; when divided by 3, leaves a remainder of 1; and likewise when divided by 4, 5, or 6 every time leaves 1; but, when divided by 7, leaves nothing."[170]

Bachet states that the problem can be changed as follows: $N \equiv 1 \pmod{60} \equiv 0 \pmod{7}$, where 60 = the least common multiple of (2, 3, 4, 5, 6). But the condition of solvability is that 2, 3, 4, 5, 6 be relatively prime with 7. Bachet gives a proof of this condition.

Concerning his method, he says: "But inasmuch as the construction of this problem is rather difficult and the demonstration [of it] too long, I do not wish to include it here. Therefore until my book on elements [*Eléments arithmétiques*] is brought to light, you can by a little trial and error find the number sought for in this manner. You must double, triple, quadruple, and so continue to multiply the number 60, until you find a number that, increased by one, is a multiple of 7. Thus multiplying 60 by 5 will produce 300; adding 1 to this you will have 301, the number sought for."[171]

168 "Sie [Bachet's method] stimmt mit der Cuttaca der Inder vollständig überein." Matthiessen (1), p. 79.

169 See the section on India in this chapter.

170 "Je demande un nombre qui estant divisé par 2, il reste 1; estant divisé par 3, il reste 1; et semblablement estant divisé par 4, ou par 5, ou par 6, il reste tousiours 1; mais estant divisé par 7, il ne reste rien." It is the same problem already met with in the works of Bhâskara I, Ibn al-Haitham, Fibonacci, and Elia Misrachi. This must have been a very popular problem, for it is given in the form of a story: "Une pauvre femme portant un panier d'oeufs pour vendre au marché. . . ."

171 "Mais d'autant que la construction de ce problème est assez difficile, et la démonstration trop longue je ne la veux apporter icy. Parquoy en attendant que mon livre des elemens soit mis en lumière on pourra tastonnant quelque peu trouver le nombre cherché en cette sorte. Il faut doubler,

On page 131 he gives the problem $N \equiv 1 \pmod 2 \equiv 2 \pmod 3 \equiv 3 \pmod 4 \equiv 4 \pmod 5 \equiv 5 \pmod 6 \equiv 0 \pmod 7$,[172] and the solution $N = \alpha \times 60 - 1 = \beta \times 7 + 1$ or $2 \times 60 = 17 \times 7 + 1$, and so $N = 119$.

CASPAR ENS

In his *Thaumaturgus Mathematicus* (Munich, 1636), Caspar Ens gives the problem already met with in Fibonacci, vol.1, p. 281: "Numeros, ex quorum facta per 2.3.4.5.6 divisione unitam residua sit, per 7. vero nihil remaneat, in usum arithmeticum adinvenire."[173] He says that the same problem is treated by C. G. Bachet.[174] His own solution, however, is the same as Fibonacci's; on the other hand, his method does not agree with that of Fibonacci, but with that of Ibn al-Haitham: $N = 2 \times 3 \times 4 \times 5 \times 6 + 1 = 721 - 420 = 301$.

FRANS VAN SCHOOTEN

In his *Exercitationum Mathematicarum liber primus,* published in 1657, there is, beginning on p. 407, a chapter entitled "De modo inveniendi numeros qui per datos divisi certos post divisionem relinquant."[175] The method Van Schooten[176] gives is on a very low mathematical level compared with the Götting-en manuscript of a century before. However, from the work of Van Schooten we can see that knowledge of the (simple) *ta-yen* rule was widespread at this time.

tripler, quadrupler, et ainsi continuellement multiplier le nombre 60, jusques à ce que l'on trouve un nombre qui accreu de l'unité soit mesuré par 7. Ainsi multipliant 60 par 5 viendra 300, auquel adjoustant 1 on aura 301 le nombre cherché."

"Le livre des elemens" was never published; it exists only in manuscript form. See Itard (1), p. 36 and p. 48.

172 The general solution of this kind of problem had not yet been discovered in Bachet's time. He says himself that Sfortunati (c. 1500) and Tartaglia (1500–1557) did not understand the method.

173 Ens (1), p. 70, Problema LIV.

174 "Quaestio a Gasparo Bacheto subtilissime pertractatur."

175 "Method for finding numbers that divided by given numbers leave certain numbers after division." A Dutch translation, *Eerste Bouck der Mathematische Oeffeningen,* was published by Van Schooten in 1660.

176 On the Van Schooten family, see Smith (1), vol. 1, p. 425; on the life and works of Van Schooten, see Hofman (2).

Van Schooten solves two remainder problems. The first is $N \equiv 1 \pmod 2 \equiv 1 \pmod 3 \equiv 1 \pmod 5 \equiv 0 \pmod 7$. He gives the general representation $dz = au + 1 = bx + 1 = cy + 1$, from which $dz - 1 = au + bx + cy$.

He gives the solution[177]

| | | | |
|---|---|---|---|
| | $2 \times 3 \times 5 = 30$ | $30 + 1 = 31$ | indivisible by 7 |
| $(\times 2)$ | $= 60$ | $60 + 1 = 61$ | indivisible by 7 |
| $(\times 3)$ | $= 90$ | $90 + 1 = 91$ | divisible by 7. |

But, he says, as this method is too long, do it thus:

$30 = 4 \times 7 + 2$
$90 = 12 \times 7 + 6 \qquad 91 = 12 \times 7 + 7.$

The other solutions can been found by adding 210, the least common multiple of 2, 3, 5, and 7. This problem is of course a very special one, and the method used cannot be general.

In the second problem,

$N \equiv 2 \pmod 7 \equiv 1 \pmod{11} \equiv 9 \pmod{13}$
or $7x + 2 = 11y + 1 = 13r + 9$. We find
$7x + 1 = 11y = 13z + 8$.

One has to take a multiple of 11 such that

this 11-fold $- 1 =$ 7-fold
this 11-fold $- 8 =$ 13-fold.

Then he takes 99, but he does not say why,[178]

$99 - 1 = 98 = 7 -$ fold
$99 - 8 = 91 = 13 -$ fold

From this, we derive:

$7x + 2 = 98 + 2 = 100$
$11y + 1 = 99 + 1 = 100$
$13r + 9 = 91 + 9 = 100$

[177] "E qua liquet, ad quaesitum numerum obtinendum, opus tantum esse quaerere numerum, qui dividi possit per 2, 3 & 5, et si unitate augeatur, dividi queat per 7" (p. 407).
[178] "Patet, si ad id sumatur 99, non cuplum ipsius 11. . ." (p. 408). "So is openbaer, indien men daer toe neemt 99, 't 9-vout van 11. . ." (p. 380).

and $N=100+n\times 1{,}001$, 1,001 being the L.C.M.(7, 11, 13).

Van Schooten also states the *ta-yen* rule, but he attributes it to a certain Nicolaus Huberti a Persijn.[179] He repeats the two problems with the *ta-yen* method:

1. L.C.M. (2, 3, 5, 7) = 210
210 : 2 = 105; 105 : 2 = 52 with r = 1
210 : 3 = 70; 70 : 3 = 23 with r = 1
210 : 5 = 42; 42 : 5 = 8 with r = 2
210 : 7 = 30; 30 : 7 = 4 with r = 2.

If the remainder is not equal to 1, one has to find how many times the remainder must be taken so that, if divided by 5, the remainder is 1. He finds 3.

He has thus no special method for solving the congruence

$\alpha\times 42\equiv 1 \pmod 5$.

Solving the last congruence $\alpha\times 30\equiv 1 \pmod 7$, he finds 4.[180]

| Divisors | Remainders | "Multiplicators" | Products |
|---|---|---|---|
| 2 | 1 | 105 | 105 |
| 3 | 1 | 70 | 70 |
| 5 | 1 | 126 | 126 |
| 7 | 0 | 120 | 0 |
| | | | 301 |
| | | | $-n\times 210=91$. |

2. L.C.M. (7, 11, 13) = 1,001
1,001 : 7 = 143; 143 : 7 = 20 with r = 3
$\alpha\times 143\equiv 3 \pmod 7 \rightarrow \alpha=5;\ 5\times 143=715$.

1,001 : 11 = 91; 91 : 11 = 8 with r = 3
$\beta\times 91\equiv 3 \pmod{11} \rightarrow \beta=4;\ 4\times 91=364$.
1,001 : 13 = 77; 77 : 13 = 5 with r = 12
$\gamma\times 77\equiv 12 \pmod{13} \rightarrow \gamma=12;\ 12\times 77=924$.

[179] Niclaes Huberts van Persijn. Van Schooten calls Nicolaus Huberti the inventor of the method, and says that the latter communicated it to him.
[180] The solution of this congruence is not necessary, because the remainder is zero. The author of the Göttingen manuscript was well aware of this fact.

| Divisors | Remainders | "Multiplicators" | Products |
|---|---|---|---|
| 7 | 2 | 715 | 1,430 |
| 11 | 1 | 364 | 364 |
| 13 | 9 | 924 | 8,316 |
| | | | 10,110 |
| | | | $-n \times 1{,}001 = 100.$ |

This is indeed the *ta-yen* rule.[181] Van Schooten says: "The well-known arithmetician Symon Jacobs of Coburg[182] also writes on this in his great *Arithmetica,* but he does not show how to find the 'multiplicators.' "[183]

WILLIAM BEVERIDGE

In his *Institutionum chronologicarum libri II* (1669), Beveridge included a full explanation of the remainder problem for the case in which the moduli are relatively prime. It is an important fact that this was the first general proof of the *ta-yen* rule.

His problem reads thus: "Invenire numerum *P,* quo per datos quoscumque *A, B,* inter se primos diviso, residua sunt data *K, L.*"[184] A more general problem is: "Invenire numerum *O* minimum, quo diviso per datos *M, B, A* inter se omnimodo primos, residua sint data *K, L, Z.*"[185]

The rule that is given says: "Primo inveniatur *D* minimus multiplex *B* talis, quo per *A* diviso supersit unitas, et inveniatur etiam *C* minimum numeri *A* multiplex talis, quo per *B* diviso restat unitas."[186] Thus

$$D = \alpha \times B \equiv 1 \pmod{A}$$
$$C = \beta \times A \equiv 1 \pmod{B}.$$

[181] Dickson (1), vol. 2, p. 60.

[182] Died in 1565.

[183] "De his tradidit quoque celebris Arithmeticus Simon Jacobi Coburgensis in Arithmetica sua majori, sed multiplicatores invenire non docet." (p. 410). Simon Jacob (1510?–1565) wrote *Rechenbuch auff den linien und mit Ziffern* (1557).

[184] Beveridge (1), p. 254: "Find a number *P,* of which the remainders are given *K, C,* when divided by some given *A, B,* which are relatively prime."

[185] Beveridge (1), p. 256.

[186] "First there is to be found a number *D* the smallest multiple of *B* such that it leaves unity when divided by *A.* . ."

Here $\alpha$ and $\beta$ are to be as small as possible; no method is given for finding $\alpha$ and $\beta$.

Then find the products $DK$ and $CL$ and "denique summam horum productorum ex $K$ in $D$ et $L$ in $C$, divides per $F$ ex $A$ in $B$ factum, et residuus fiet $P$ . . . ."[187]

$$P=DK+CL-n\times AB.$$[188]

The proof given by Beveridge is roughly as follows:[189]

$$D=\alpha\times B\equiv 1 \pmod{A}$$
$$D-1\equiv 0 \pmod{A}$$
$$DK-K\equiv 0 \pmod{AK}\equiv 0 \pmod{A}$$
$$DK\equiv K \pmod{A}.$$

Also

$$C=\beta\times A\equiv 0 \pmod{A}$$
$$CL\equiv 0 \pmod{A};$$

thus

$$DK+CL\equiv K \pmod{A}+0 \pmod{A}\equiv K \pmod{A}.$$

In the same way $DK+CL\equiv L \pmod{B}$, from which: $DK+CL \equiv K \pmod{A}\equiv L \pmod{B}$. Since $AB\equiv 0 \pmod{A}\equiv 0 \pmod{B}$, we get the least number $P$ while dividing $DK+CL$ by $AB$; the remainder is the smallest solution: $P=DK+CL-m\times AB$ ($m$ being as great as possible). A similar proof is given for the second problem.[190]

In Beveridge's work only the method for solving the congruences is lacking, although the method was known in the sixteenth century, as is obvious from the Göttingen manuscript.

With the work of Beveridge, we come to the end of what might be called the prescientific phase of the remainder problem. That term is not meant to deny that there was real

187 "After that divide the sum of these products $K\times D$ and $L\times C$ by $F$ ($=A\times B$), and the remainder will be $P$."

188 This subtraction is omitted in Dickson (1), vol. 2, p. 61. But without this, $P$ is not the smallest number.

189 In fact, the proof is given in words and is too extensive to reproduce here, where it is stated in a modern algebraical way.

190 See also Dickson (1), vol. 2, p. 61.

insight on the part of some mathematicians. But all of them remained in the arithmetical phase of the problem,[191] and only a few tried to give an arithmetical proof of the particular problems they were solving.[192] But after Beveridge there was a gradual attempt to give a general algebraical proof.[193]

However, the old style arithmetic continued to be studied in Europe,[194] and secondhand proofs of the problem[195] contributed nothing new to a general solution. In Europe the Sun Tzŭ problem was considered as a game, even as late as the nineteenth century.[196]

One of the problems in Fibonacci's work (vol. 1, p. 282), derived in all probability from Ibn al-Haitham, who relied on Bhâskara I, is reproduced by Elia Misrachi;[197] we find the same problem in the works of Caspar Ens[198] and Daniel Schwenter.[199] Euler wrote in *Commentarii academiae scientiarum Petropolitanae 7* (1734/5), 1740:[200]

191 Or algorithmic phase, for the method was used without giving proof, and in the first centuries after Fibonacci, even the *yen-shu* were transmitted without explanation.

192 As in the case of the Göttingen manuscript.

193 In Chapter 21 we shall examine Ch'in Chiu-shao's work in the light of the algebraical works of Euler, Lagrange, and Gauss in order to come to an evaluation of Ch'in's method. Of course, one has to bear in mind that Ch'in's work is algorithmic and that he gives no proof for his method.

194 For instance, the article of De Rocquigny (1) in 1881.

195 Dostor (1), Marchand (1), Domingues (1). Dostor's problem is a very special case, very simple to prove.

196 For example, Schäfer (1), *Die Wunder der Rechenkunst. Eine Zusammenstellung der rätselhaftesten, unglaublichsten und belustigendsten arithmetischen Kunstaufgaben zur Beförderung der geselligen Unterhaltung und des jugendlichen Nachdenkens* (The Miracles of the Art of Arithmetic. A compendium of the most mysterious, unbelievable, and entertaining problems in the art of arithmetic, for the stimulation of social intercourse and youthful reflection), Weimar, 1842. His indeterminate problem is on p. 50 (no. 60).

197 Lived in Constantinople (1455–1526). He also includes the other problems of Fibonacci (*Liber Abacci*, p. 281).

198 *Thaumaturgus Mathematicus*, Munich, 1636, pp. 70–71.

199 *Deliciae Physico-Math. oder Math. -u. Phil. Erquickstunden*, Nürnberg, 1636, p. 41.

200 P. 46. The title of this chapter is: "Solutio problematis arithmetici de inveniendo numero qui per datos numeros divisus relinquat data residua." This chapter is also published in *Commentationes arithmeticae collectae I*, pp. 18–32.

"Reperiuntur in vulgaribus arithmeticorum libris passim huiusmodi problemata, ad quae perfecta resolvenda plus studii et sollertiae requiritur, quam quidem videatur. Quamvis enim plerumque regula sit adjecta, cujus ope solutio obtineri queat, tamen ea vel est insufficiens solique casui proposito convenit, ita ut circumstantiis quaestionis parum immutatis ea nullius amplius sit usus, vel subinde etiam solet esse falsa . . . Simili quoque modo ubique fere occurrit istud problema, ut inveniatur numerus, qui per 2, 3, 4, 5 et 6 divisus relinquat unitatem, per 7 vero dividi queat sine residuo. Methodus vero idonea ad huiusmodi problemata solvenda nusquam exhibetur; solutio enim ibi adjecta in hunc tantum casum competit atque tentando potius absolvitur.

"Si quidem numeri, per quos quaesitus numerus dividi debet sunt parvi, prout in hoc exemplo, tentando non difficulter quaesitus numerus invenitur; difficillima autem foret istiusmodi solutio, si divisores propositi essent valde magni."[201]

This text from Euler may be considered to represent the little that European mathematics had produced in indeterminate analysis until the beginning of the eighteenth century. In India and China, however, this branch of mathematics had already developed to a high level. The idea of *ex oriente lux* is by no means established historically, but there is no doubt about *in oriente lux* where medieval indeterminate analysis is concerned.

201 "In popular books on arithmetic, one can frequently find such problems which require more study and cleverness for solving them correctly than may seem. For although a rule is usually given, with the help of which the solution may be found, nevertheless, either this rule is insufficient and appropriate only for the special case represented, so that, if the circumstances of the problem are slightly changed, it is no longer useful; or it repeatedly shows itself to be false [...]. This problem is found in the same form almost everywhere, namely that a number should be found, that, if divided by 2, 3, 4, 5, and 6 has the remainder 1, but can be divided by 7 without remainder. Nevertheless, a method appropriate for solving such problems is nowhere explained: for the solution given satisfies this case, but it is rather solved by conjecture [by trying]. If the numbers which the number asked for has to be divided by are small, as in this example, the number asked for can be found without much difficulty by conjecture. Such a solution, however, will be very difficult if the divisors given are fairly large."

# Chinese Mathematics in the Thirteenth Century

## ULRICH LIBBRECHT

An exploration of the life and work of the thirteenth-century mathematician Ch'in, this fascinating book examines a range of mathematical issues that reflect Chinese life of a millennium ago. Its first part consists of four closely related studies of Ch'in and his work. The first study brings together what is known of the mathematician's life and of the history of his only extant work, the *Shu-shu chiu-chang.* Subsequent studies examine the entire range of mathematical techniques and problems found within Ch'in's book.

The core of this book consists of an in-depth study of what modern mathematicians still refer to as the Chinese remainder theorem for the solution of indeterminate equations of the first degree. This was Ch'in's most original contribution to mathematics–so original that no one could correctly explain Ch'in's procedure until the early nineteenth century. This volume's concluding study unites information on artisanal, economic, administrative, and military affairs dispersed throughout Ch'in's writings, providing rare insights into thirteenth-century China.

Dover (2005) unabridged republication of the edition published by the MIT Press, Cambridge, Massachusetts, 1973. 71 figures. 85 diagrams. Glossary. Bibliography. Index. 592pp. 5⅜ x 8½. Paperbound.



ISBN 0-486-44619-0
52995
9 780486 446196

Cover design by John M. Alves