A SIMPLE SOLUTION TO ARCHIMEDES' CATTLE PROBLEM

ANTTI NYGRÉN

Department of Mathematical Sciences,
University of Oulu

OULU 2001

ANTTI NYGRÉN

A SIMPLE SOLUTION TO ARCHIMEDES' CATTLE PROBLEM

OULUN YLIOPISTO, OULU 2001

Manuscript received 12 March 2001
Manuscript accepted 19 March 2001

ISBN 951-42-5932-7 (URL: http://herkules.oulu.fi/isbn9514259327/)

ALSO AVAILABLE IN PRINTED FORMAT
ISBN 951-42-5931-9
ISSN 0355-3191 (URL: http://herkules.oulu.fi/issn03553191/)

OULU UNIVERSITY PRESS
OULU 2001

Nygrén, Antti, A simple solution to Archimedes' cattle problem
Department of Mathematical Sciences, University of Oulu, P.O.Box 3000, FIN-90014 University of Oulu, Finland

2001
Oulu, Finland
(Manuscript received 12 March 2001)

Abtract

A simple solution to the classical Archimedes' cattle problem is given. Unlike the previous ones, this is mainly based on elementary mathematics which, at least in principle, would have been available to the mathematicians of the classical era. The solution applies linear transformation and infinite descent in solving quadratic Diophantine equations in a manner which does not explicitly take advantage of continued fractions. The idea is to create a sequence of transformed equations, until an equation is obtained which can be solved easily. It turns out that this greatly simplifies the problem. The method of solving the Diophantine equations is especially suitable for a computer. The result can be easily used to produce several numerical solutions to the cattle problem.

Keywords: Diophantine equations, quadratic and bilinear equations, Archimedes' cattle problem

Acknowledgements

The author is grateful to K. Väänänen and L. Päivärinta for discussions and advice, and to T. Nygrén for assistance in the preparation of the manuscript and carrying out the computer calculations. Thanks are also due to I. Vardi for sending a preprint of his manuscript and to C. Rorres for his excellent Archimedes www-pages which have been a valuable source of information during the preparation of this work.

Contents

1 Introduction

The origin and the precise age of the famous Archimedes' cattle problem is not known for certainty, but it is generally believed to originate at least partly from Archimedes himself. The task given in the problem is to calculate the number of cattle of the Sun god Helios, starting from a few simple relations. An English translation of the original wording is shown in Appendix A.

The difficulty of the cattle problem is reflected by the fact that the first acceptable mathematical solution was given as late as 1880 by Amthor [1]. Amthor was then able to show that the total number of cattle consists of 206545 digits and he also calculated the first few of them. The complete calculation of the numerical result could not be performed at that time. This was only possible after the advent of computers and, for the first time, it was performed in 1965 by Williams, German and Zarnke [2]. These authors, however, only describe their calculations, but do not give the result in numbers. The smallest number of cattle was published in 1981 by Nelson [3], who also calculated several other solutions by means of a CRAY-1 supercomputer. Quite recently, Vardi [4] made a major step by presenting the first general solution to the problem in closed form and calculating the two smallest numerical results by means of a relatively slow workstation.

In this paper, a novel solution to the cattle problem is given. A key part of this work is a method of solving quadratic Diophantine equations of the type $Ax^2 + Bxy + Cy^2 = 1$, where $AC < 0$. The method does not directly rely on continued fractions, it is both explicitly and implicitly strictly limited to integer calculus, and it makes solving the equation into a routine-like procedure which is especially suitable for a computer. It can probably be applied to equations of other types (e.g. of higher orders) as well, but this has not yet been investigated.

The new solutions are expressed in terms of simple formulas by means of two parameters, which can be divided into two groups. The values of the first type are calculated by means of matrix multiplication, and the parameters of the second type are obtained from those of the first type using only basic arithmetic operations.

The present work is independent of the paper by Vardi [4]. There is also a fundamental difference between these two works: Vardi's formalism carries the irrational number $\sqrt{4729494}$ with it, whereas the present theory contains only integer numbers. This is probably the reason why the expressions derived in this paper are more straightforward and give the numerical results more quickly when programmed into a computer.

2 The first part of the problem

The first part of the cattle problem is simple. It gives the relations of bulls of each colour, which can be written in terms of three equations

$$\begin{aligned}
\mathfrak{W} &= \left(\frac{1}{2}+\frac{1}{3}\right)\mathfrak{B}+\mathfrak{Y} \\
\mathfrak{B} &= \left(\frac{1}{4}+\frac{1}{5}\right)\mathfrak{D}+\mathfrak{Y} \\
\mathfrak{D} &= \left(\frac{1}{6}+\frac{1}{7}\right)\mathfrak{W}+\mathfrak{Y}.
\end{aligned} \tag{1}$$

Here $\mathfrak{W}$, $\mathfrak{B}$, $\mathfrak{D}$ and $\mathfrak{Y}$ are the unknown numbers of white, black, dappled and yellow bulls, respectively. Since the unknowns must be positive integers, the solution of eq. (1) is

$$\begin{aligned}
\mathfrak{W} &= 2\cdot 3\cdot 7\cdot 53\cdot Q \\
\mathfrak{B} &= 2\cdot 3^2\cdot 89\cdot Q \\
\mathfrak{D} &= 2^2\cdot 5\cdot 79\cdot Q \\
\mathfrak{Y} &= 3^4\cdot 11\cdot Q,
\end{aligned} \tag{2}$$

where Q is an arbitrary positive integer.

The corresponding equations for the cows of each colour are

$$\begin{aligned}
\mathfrak{w} &= \left(\frac{1}{3}+\frac{1}{4}\right)(\mathfrak{B}+\mathfrak{b}) \\
\mathfrak{b} &= \left(\frac{1}{4}+\frac{1}{5}\right)(\mathfrak{D}+\mathfrak{d}) \\
\mathfrak{d} &= \left(\frac{1}{5}+\frac{1}{6}\right)(\mathfrak{Y}+\mathfrak{y}) \\
\mathfrak{y} &= \left(\frac{1}{6}+\frac{1}{7}\right)(\mathfrak{W}+\mathfrak{w}).
\end{aligned} \tag{3}$$

Here, again, $\mathfrak{w}$, $\mathfrak{b}$, $\mathfrak{d}$ and $\mathfrak{y}$ refer to the numbers of white, black, dappled and yellow cows. By solving the number of cows from these equations and using the results in eq. (2), we obtain

$$\begin{aligned} \mathfrak{w} &= 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 23 \cdot 373 \cdot Q' \\ \mathfrak{b} &= 2 \cdot 3^2 \cdot 17 \cdot 15991 \cdot Q' \\ \mathfrak{d} &= 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 761 \cdot Q' \\ \mathfrak{y} &= 3^2 \cdot 13 \cdot 46489 \cdot Q', \end{aligned} \tag{4}$$

where $Q' = Q/4657$. In order to make the numbers of the different cows into integers, Q' must be a positive integer as well. Now the common factor Q in eqs. (2) can no longer be quite arbitrary, but necessarily $Q = 4657Q'$.

3 Diophantine equations for the second part of the problem

The additional conditions in the second part of the problem state that the total number of white and black bulls is a square number and that of the dappled and yellow bulls is a triangular number. This can be written as

$$\begin{aligned} \mathfrak{W}+\mathfrak{B} &= m^2 \\ \mathfrak{D}+\mathfrak{Y} &= \frac{1}{2}n(n+1), \end{aligned} \tag{5}$$

where m and n are unknown integers. Here one can notice that $\mathfrak{W} = \mathfrak{B} = \mathfrak{D} = \mathfrak{Y} = \mathfrak{w} = \mathfrak{b} = \mathfrak{d} = \mathfrak{y} = 0$ satisfy all the above conditions. This trivial solution is not acceptable, however, since it is in contradiction with the problem, which states that the herds of bulls are 'mighty in number'.

Using eq. (2), eq. (5) gives

$$\begin{aligned} \mathfrak{W}+\mathfrak{B} &= 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot Q = m^2 \\ \mathfrak{D}+\mathfrak{Y} &= 7 \cdot 353 \cdot Q = \frac{1}{2}n(n+1), \end{aligned} \tag{6}$$

and because $Q = 4657Q'$,

$$\begin{aligned} \mathfrak{W}+\mathfrak{B} &= 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657 \cdot Q' = m^2 \\ \mathfrak{D}+\mathfrak{Y} &= 7 \cdot 353 \cdot 4657 \cdot Q' = \frac{1}{2}n(n+1). \end{aligned} \tag{7}$$

In principle, it would now be possible to solve eqs. (7) for Q'. Then the final solutions would be obtained by inserting each root Q' in eq. (4) and $Q = 4657Q'$ in eq. (2). This leads to considerable difficulties, however, because even the smallest root is a very large number. It is easier to obtain the sequence of roots Q by solving eqs. (6), since this sequence starts from an essentially smaller number. For the final solution, one then only accepts those roots Q which are divisible by 4657.

The first equation in (6) indicates that

$$Q = 3 \cdot 11 \cdot 29 \cdot \tilde{m}^2, \tag{8}$$

where $\tilde{m}$ is a new unknown positive integer. Then

$$m = 2 \cdot 3 \cdot 11 \cdot 29 \cdot \tilde{m} \tag{9}$$

and, inserting Q in the second equation in (6), we obtain

$$n(n+1) = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot \tilde{m}^2. \tag{10}$$

It is now easily seen that

$$\begin{aligned} n &= pu^2 \\ n+1 &= qv^2, \end{aligned} \tag{11}$$

where u, v, p and q are also positive integers and

$$\begin{aligned} uv &= \tilde{m} \\ pq &= 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353. \end{aligned} \tag{12}$$

Hence the Diophantine equation we have to solve is of the form

$$pu^2 + 1 = qv^2. \tag{13}$$

This equation must be investigated using separately all values of p and q which satisfy the condition in eq. (12). For each pair of roots u and v, the corresponding value of Q can then be calculated using eqs. (12) and (8).

This solution method differs from that by Amthor [1] or Vardi [4], who derived a single equation of the form $Ax^2 + 1 = y^2$, known as Pell's equation. The reasons for this procedure will be explained later in the Discussion section.

When all possible values of p and q are taken into account, the present approach leads to 64 equations altogether. Nevertheless, the situation is not so complicated as it might look at first sight since, by means of a simple procedure, one can quickly show that 60 of them do not have solutions.

The method of rejecting most of the equations in (13) is as follows. We forget for a while the condition for pq in eq. (12). Let p_0 be one of the prime numbers $2, 3, 7, 11, 29$ or 353. If p is divisible by p_0, the existence of a solution implies the existence of $v \in N$ such that $qv^2 - 1$ is divisible by p_0. Then, neither q nor v is divisible by p_0, so that their remainders rem$[q]$ and rem$[v]$ may have values $1, 2, \ldots, p_0 - 1$. Thus, $qv^2 - 1$ cannot be divisible by p_0, unless $\mathrm{rem}[q] \cdot (\mathrm{rem}[v])^2 - 1$ is divisible by p_0, at least with a single pair of the possible values of rem$[q]$ and rem$[v]$. Correspondingly, if q is divisible by p_0, there must exist $u \in N$ such that $pu^2 + 1$ is divisible by p_0, and the remainders rem$[p]$ and rem$[u]$ must satisfy the condition that $\mathrm{rem}[p] \cdot (\mathrm{rem}[u])^2 + 1$ is divisible by p_0. If, therefore, these conditions are broken for some pair p and q with any value of p_0, the corresponding eq. (13) does not have solutions.

The amount of the work necessary in calculating the possible remainders of p and q can be diminished with the following reasoning. Let t be a primitive root of p_0 and put $p_0 = 2k + 1$ (we can omit the trivial case $p_0 = 2$). If s is a positive integer, then the Fermat little theorem shows that $t^s \equiv 1(p_0) \Leftrightarrow s = 2kr$, where r

is a positive integer. Next, let $q \equiv t^{s_1}(p_0)$ and $v \equiv t^{s_2}(p_0)$. Now $qv^2 - 1$ is divisible by p_0, if and only if $s_1 + 2s_2 = 2kr$, which means that s_1 must be even.

The case where $pu^2 + 1$ is divisible by p_0 is similar. Let $p \equiv t^{s_1}(p_0)$ and $u \equiv t^{s_2}(p_0)$. Because $t^k \equiv -1(p_0)$ the necessary and sufficient condition for the divisibility of $pu^2 + 1$ by p_0 is $s_1 + 2s_2 = k + 2kr$. This means that s_1 must be even if k is even, and s_1 must be odd, if k is odd.

In summary, the possible non-zero remainders of q are the remainders of $t^{2s_1'}$, where $0 < s_1' \leq k$. The non-zero remainders of p are the same as for q if k is even. This means that p_0 has the form $4h + 1$, where h is a non-negative integer. If $p_0 = 4h + 3$, the possible non-zero remainders of p are those among the numbers $1, 2, \ldots, p_0 - 1$ which are not remainders of q.

For each value of p_0, it is now easy to check which values of the remainders rem[p] and rem[q] do not break the above conditions. These are shown in Table 1 for $p_0 = 2, 3, 7, 11$ and 29. Then, because eq. (12) implies that either p or q must be divisible by p_0, one can test all possible pairs p and q to see which of them give the allowed remainders for each value of p_0. If a calculated remainder does not appear on the appropriate row in the table, eq. (13) does not have solutions with these values of p and q. The checking is not tedious, since nearly one half of the equations will already be rejected by the test $p_0 = 3$.

In this manner, one can find out that, out of the original 64 equations, only the following four are left for further study:

$$2 \cdot 11 \cdot 353 \cdot u^2 + 1 = 3 \cdot 7 \cdot 29 \cdot v^2 \tag{14}$$
$$11 \cdot 29 \cdot 353 \cdot u^2 + 1 = 2 \cdot 3 \cdot 7 \cdot v^2 \tag{15}$$
$$3 \cdot 7 \cdot 11 \cdot 353 \cdot u^2 + 1 = 2 \cdot 29 \cdot v^2 \tag{16}$$
$$2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot u^2 + 1 = v^2. \tag{17}$$

The last one is the same as Pell's equation, which was solved in the previous solutions of the cattle problem.

When $p_0 = 353$, the above testing procedure is too laborious. A corresponding check for $p_0 = 353$ can also be done by means of the reasoning presented in Appendix B. However, this does not lead to any more rejections and therefore eqs. (14)–(17) remain for solving. A similar reasoning would have been possible for the other values of p_0 as well, but testing the remainders is quicker. One should finally notice that the above arguments do not prove that those equations we have left would necessarily have solutions.

Table 1. Allowed remainders of p and q when divided by p_0.

p_0	Remainders of p	Remainders of q
2	0, 1	0, 1
3	0, 2	0, 1
7	0, 3, 5, 6	0, 1, 2, 4
11	0, 2, 6, 7, 8, 10	0, 1, 3, 4, 5, 9
29	0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28

4 The smallest solutions of the Diophantine equations

The main difficulty in the cattle problem is in finding the solutions of the Diophantine equations. Previously this has been carried out by means of continued fractions. In this work, a different formalism is introduced which does not explicitly use continued fractions, although the two methods seem to have a close relationship.

Let us investigate the equation

$$A_1x_2^2 + B_1x_1x_2 + C_1x_1^2 - 1 = 0, \tag{18}$$

where A_1, B_1 and C_1 are integers and x_1 and x_2 are unknowns. Our purpose is not to develop a method of solving Diophantine equations of the form (18) in a general case. Rather, the problem is considered as an individual exercise so that all possibilities are not considered which may be encountered in analysing eq. (18). We restrict ourselves to a case where $A_1C_1 < 0$ and $(B_1^2 - 4A_1C_1)^{1/2} \notin Z$. In addition, we consider the roots x_1 and x_2 to be positive integers and $x_2 \leq x_1$. When $A_1C_1 < 0$, one can easily see from eq. (18) which one of the unknowns is greater, and therefore the latter condition is not a limitation but only a choice in notation.

The basic idea is to replace the greater unknown by a new smaller non-negative unknown in such a manner that the form of the equation remains the same and the above restrictions are preserved. Then the procedure can be repeated until the roots of the transformed equation are so small that they are directly seen.

When x_1 is replaced by

$$x_1 = h_1x_2 + x_3, \tag{19}$$

where h_1 is an arbitrary integer and x_3 a new unknown, eq. (18) will be transformed as

$$A_2x_3^2 + B_2x_2x_3 + C_2x_2^2 - 1 = 0. \tag{20}$$

The coefficients in eq. (20) are given by

$$\begin{aligned} A_2(h_1) &= C_1 \\ B_2(h_1) &= B_1 + 2h_1C_1 \\ C_2(h_1) &= A_1 + h_1B_1 + h_1^2C_1. \end{aligned} \tag{21}$$

Hence, we have shown that the form of eq. (18) remains the same in transformation (19). It is also easy to show by direct calculation that $B_2^2 - 4A_2C_2 = B_1^2 - 4A_1C_1$, so that this expression of coefficients remains invariant in transformation (19). Since $(B_1^2 - 4A_1C_1)^{1/2} \notin Z$, $C_2(h_1) \neq 0$ for any integer h_1.

Because the roots are non-negative, the value of h_1 can be chosen in such a way that $0 \leq x_3 \leq x_2$ (the reason for having the two equalities in this relation will be explained later). The value of h_1 satisfying this condition is obtained in the following manner.

Eq. (18) has a solution $x_2 = 0$ only when $C_1 = 1$. Then $x_1 = 1$. When $x_2 > 0$, there is such a real number $k_1 \geq 1$ that $x_1 = k_1x_2$. By inserting x_1 in eq. (18) we obtain

$$C_2(k_1) = A_1 + k_1B_1 + k_1^2C_1 = \frac{1}{x_2^2} \leq 1. \tag{22}$$

Next, we consider two different cases. In the first one, $A_1 \geq 1$ and $C_1 \leq -1$. Because $C_2(k)$ is a polynomial of second degree and $C_2(0) = A_1 \geq 1$, it is easy to see that $C_2(k) > C_2(k_1) > 0$, when $0 < k < k_1$ and $C_2(k) < C_2(k_1)$ when $k > k_1$. In the case $x_2 < x_1$, we have $k_1 > 1$. Then, for each natural number $h_1 < k_1$, $C_2(h_1) > 0$ and, since $C_2(h_1)$ is an integer, necessarily $C_2(h_1) \geq 1$. In the case $k_1 = 1$, obviously $C_2(k_1)$ is an integer, so that $x_2 = x_1 = 1$ and $C_2(k_1) = 1$. Hence, there is in any case a natural number k_2 such that $C_2(k_2) \geq 1$.

We choose h_1 to be the largest natural number for which $C_2(h_1) \geq 1$. Because $C_2(h_1 + 1) \neq 0$, necessarily $C_2(h_1 + 1) \leq -1$. This means that $h_1 \leq k_1 < h_1 + 1 \Rightarrow h_1x_2 \leq k_1x_2 = x_1 = h_1x_2 + x_3 < h_1x_2 + x_2$, which gives $0 \leq x_3 < x_2$. Hence, it has been possible to choose h_1 in the desired way.

In the second case, $A_1 \leq -1$ and $C_1 \geq 1$. Then $C_2(k) < C_2(k_1) \leq 1$ when $0 < k < k_1$, and $C_2(k) > C_2(k_1)$ when $k > k_1$. In the case $x_2 < x_1$, we have $k_1 > 1$. Then, since $C_2(h_1)$ is a non-zero integer for each natural number h_1, necessarily $C_2(h_1) < 0$ when $h_1 < k_1$. If $x_1 = x_2$, then $k_1 = 1 \Rightarrow C_2(1) = 1 \Rightarrow x_2 = x_1 = 1$. In addition, $C_2(0) = A_1 < 0$. Hence, there is such an integer $k_2 \geq 0$ that $C_2(k_2) < 0$.

Let h_1 be the greatest integer, for which $C_2(h_1) < 0 \Rightarrow C_2(h_1 + 1) \geq 1$. Now $h_1 < k_1 \leq h_1 + 1 \Rightarrow h_1x_2 < k_1x_2 = x_1 = h_1x_2 + x_3 \leq h_1x_2 + x_2 \Rightarrow 0 < x_3 \leq x_2$. Therefore this h_1 is such a number that $0 < x_3 \leq x_2$.

When h_1 is chosen in the way described above, one can show that eq. (20) fulfills similar basic assumptions as those (i.e. $0 \leq x_2 \leq x_1$ and $A_1C_1 < 0$) made in eq. (18). It was shown above that x_2 and x_3 are non-negative and $x_3 \leq x_2$. Because $A_2 = C_1$, A_1 and A_2 have different signs. It was also shown above that the assumption $C_1 \leq -1$ led to $C_2(h_1) \geq 1$ and the assumption $C_1 \geq 1$ to $C_2(h_1) < 0$. Hence also C_1 and C_2 have different signs so that the signs of A_2 and C_2 must be opposite. The original assumptions are therefore also valid for eq. (20).

The above criterion of choosing h_1 can be expressed in a very brief and clear form: h_1 is the greatest integer which changes the sign of C, i.e. the signs of $C_2(h_1)$ and C_1 are opposite. The restriction $0 \leq x_3 \leq x_2$ in transformation (19) was made in order to obtain such a clear criterion. In the case $A_1 \leq -1$, $C_1 \geq 1$ the criterion led to the relation $0 < x_3 \leq x_2$, so that $x_3 = x_2$ is also possible.

Since the form of the equation, as well as the assumptions on the relative signs of the coefficients have been preserved in the transformation from eq. (18) to eq.

(20), the transformation can be repeated to eq. (20) in a similar way. Therefore the transformation can be repeated infinitely. The choice of h_1 can always be made, also in the case when the equation has no solutions. If solutions exist, the calculation must, after a finite number of transformations, lead to a situation where $x_i = 1$ and $x_{i+1} = 0$. These numbers are the roots of the equation $A_i x_{i+1}^2 + B_i x_i x_{i+1} + C_i x_i^2 - 1 = 0$ if and only if $C_i = 1$. Because in all calculated transformations $x_j = h_j x_{j+1} + x_{j+2}$, $j = i-1, \ldots, 1$, the values of the coefficients h_j are known, this sequence allows a simple calculation of the values of the unknowns x_1 and x_2. If the equation has no solutions, none of the transformations leads to the value $C_i = 1$. Namely, if this would happen, one could calculate the solution according to the lines explained above.

Next, we carry out the above process on eqs. (14)–(17). The values of the coefficients A_i, B_i, C_i and h_i for eqs. (14) and (15) are written in Tables 2 and 3, respectively. In the table captions, the equations are rewritten in the form where $x_1 > x_2$ as in the above theory.

The calculations indicate that the algorithm makes a loop so that, after a certain number of operations, the same numbers will reappear. However, the loop does not close at the starting equation but at its first transformation. The length of the loop is the same in both cases, it is observed that $A_{94} = A_2$, $B_{94} = B_2$ and $C_{94} = C_2$.

A second feature in the algorithm is that, after 47 transformations, the same numbers appear in the return part of the loop in such a way that A and C have exchanged their values and also the sign of B is changed. In order to show this more clearly, the loops are presented in two sets of columns; the right hand columns contain the return part.

When the same calculations are made in eqs. (16) and (17), it is noticed that their loops are the same as those in Tables 3 and 2, respectively. The difference is that these equations enter the loops at their turning points. Therefore the values of A_1, B_1, C_1 and h_1 of these equations are written below the right hand columns. The algorithm starting from these values continues up the right hand columns and back down the left hand columns.

Inside the loops, one can find two values of i, 47 and 93, such that B_i is divisible by C_i. Then, based on eqs. (21), one can choose such an $\tilde{h}_i$ that $\tilde{B}_{i+1} = 0$. If this choice is made at $i = 93$, the original equation will be restored both in Table 2 and Table 3. If the same procedure is made at $i = 47$, the loop of eq. (14) will give Pell's equation (17) and, correspondingly, the loop of eq. (15) will give eq. (16). All this suggests that Diophantine equations of the form (13) are joined together in pairs. Therefore the equations may have deep connections which would not be visible without this algorithm, but the connection is not investigated any further here.

Because the length of both loops is 92 steps, this suggests that the length only depends on the product of p and q, although this has not been studied.

It is seen that, in Table 2, $C_i = 1$ at $i = 47$ but, in Table 3, C_i is never unity. This means that eqs. (14) and (17) have solutions, but eqs. (15) and (16) have no solutions at all.

It is now a simple matter to calculate the smallest positive roots of eq. (14). Since the numerical values of the coefficients h_i are known, x_1 and x_2 can be calculated recursively using the transformation $x_i = h_i x_{i+1} + x_{i+2}$, starting from $x_{i+1} = x_{47} =$

1, $x_{i+2} = x_{48} = 0$ and $h_i = h_{46} = 1$. The result is that the smallest positive roots of eq. (14) are

$$\begin{aligned} v = r_1 &= 30042660791428171336 5 \\ u = r_2 &= 84129507677858393258. \end{aligned} \tag{23}$$

The smallest non-negative solutions of eq. (17) are readily seen and they are

$$\begin{aligned} v &= 1 \\ u &= 0. \end{aligned} \tag{24}$$

Table 2. Eq. (14): $-7766x_2^2 + 609x_1^2 - 1 = 0$.

i	A_i	B_i	C_i	h_i		i	A_i	B_i	C_i	h_i
1	-7766	0	609	3						
2	609	3654	-2285	1	$\Longleftarrow$	93	-2285	-3654	609	6
3	-2285	-916	1978	1		92	1978	916	-2285	1
4	1978	3040	-1223	3		91	-1223	-3040	1978	1
5	-1223	-4298	91	47		90	91	4298	-1223	3
6	91	4256	-2210	1		89	-2210	-4256	91	47
7	-2210	-164	2137	1		88	2137	164	-2210	1
8	2137	4110	-237	17		87	-237	-4110	2137	1
9	-237	-3948	3514	1		86	3514	3948	-237	17
10	3514	3080	-671	5		85	-671	-3080	3514	1
11	-671	-3630	2139	1		84	2139	3630	-671	5
12	2139	648	-2162	1		83	-2162	-648	2139	1
13	-2162	-3676	625	6		82	625	3676	-2162	1
14	625	3824	-1718	2		81	-1718	-3824	625	6
15	-1718	-3048	1401	2		80	1401	3048	-1718	2
16	1401	2556	-2210	1		79	-2210	-2556	1401	2
17	-2210	-1864	1747	1		78	1747	1864	-2210	1
18	1747	1630	-2327	1		77	-2327	-1630	1747	1
19	-2327	-3024	1050	3		76	1050	3024	-2327	1
20	1050	3276	-1949	1		75	-1949	-3276	1050	3
21	-1949	-622	2377	1		74	2377	622	-1949	1
22	2377	4132	-194	21		73	-194	-4132	2377	1
23	-194	-4016	3595	1		72	3595	4016	-194	21
24	3595	3174	-615	6		71	-615	-3174	3595	1
25	-615	-4206	499	8		70	499	4206	-615	6
26	499	3778	-2327	1		69	-2327	-3778	499	8
27	-2327	-876	1950	1		68	1950	876	-2327	1
28	1950	3024	-1253	2		67	-1253	-3024	1950	1
29	-1253	-1988	2986	1		66	2986	1988	-1253	2
30	2986	3984	-255	16		65	-255	-3984	2986	1
31	-255	-4176	1450	2		64	1450	4176	-255	16
32	1450	1624	-2807	1		63	-2807	-1624	1450	2
33	-2807	-3990	267	15		62	267	3990	-2807	1
34	267	4020	-2582	1		61	-2582	-4020	267	15
35	-2582	-1144	1705	1		60	1705	1144	-2582	1
36	1705	2266	-2021	1		59	-2021	-2266	1705	1
37	-2021	-1776	1950	1		58	1950	1776	-2021	1
38	1950	2124	-1847	1		57	-1847	-2124	1950	1
39	-1847	-1570	2227	1		56	2227	1570	-1847	1
40	2227	2884	-1190	3		55	-1190	-2884	2227	1
41	-1190	-4256	169	25		54	169	4256	-1190	3
42	169	4194	-1965	2		53	-1965	-4194	169	25
43	-1965	-3666	697	5		52	697	3666	-1965	2
44	697	3304	-2870	1		51	-2870	-3304	697	5
45	-2870	-2436	1131	2		50	1131	2436	-2870	1
46	1131	2088	-3218	1		49	-3218	-2088	1131	2
47	-3218	-4348	1	4348	$\Longrightarrow$	48	1	4348	-3218	1
							-4729494	0	1	2174

Table 3. Eq. (15): $-112607x_2^2 + 42x_1^2 - 1 = 0$.

i	A_i	B_i	C_i	h_i		i	A_i	B_i	C_i	h_i
1	-112607	0	42	51						
2	42	4284	-3365	1	$\Longleftarrow$	93	-3365	-4284	42	102
3	-3365	-2446	961	3		92	961	2446	-3365	1
4	961	3320	-2054	1		91	-2054	-3320	961	3
5	-2054	-788	2227	1		90	2227	788	-2054	1
6	2227	3666	-615	6		89	-615	-3666	2227	1
7	-615	-3714	2083	1		88	2083	3714	-615	6
8	2083	452	-2246	1		87	-2246	-452	2083	1
9	-2246	-4040	289	14		86	289	4040	-2246	1
10	289	4052	-2162	1		85	-2162	-4052	289	14
11	-2162	-272	2179	1		84	2179	272	-2162	1
12	2179	4086	-255	16		83	-255	-4086	2179	1
13	-255	-4074	2275	1		82	2275	4074	-255	16
14	2275	476	-2054	1		81	-2054	-476	2275	1
15	-2054	-3632	697	5		80	697	3632	-2054	1
16	697	3338	-2789	1		79	-2789	-3338	697	5
17	-2789	-2240	1246	2		78	1246	2240	-2789	1
18	1246	2744	-2285	1		77	-2285	-2744	1246	2
19	-2285	-1826	1705	1		76	1705	1826	-2285	1
20	1705	1584	-2406	1		75	-2406	-1584	1705	1
21	-2406	-3228	883	4		74	883	3228	-2406	1
22	883	3836	-1190	3		73	-1190	-3836	883	4
23	-1190	-3304	1681	2		72	1681	3304	-1190	3
24	1681	3420	-1074	3		71	-1074	-3420	1681	2
25	-1074	-3024	2275	1		70	2275	3024	-1074	3
26	2275	1526	-1823	1		69	-1823	-1526	2275	1
27	-1823	-2120	1978	1		68	1978	2120	-1823	1
28	1978	1836	-1965	1		67	-1965	-1836	1978	1
29	-1965	-2094	1849	1		66	1849	2094	-1965	1
30	1849	1604	-2210	1		65	-2210	-1604	1849	1
31	-2210	-2816	1243	2		63	1243	2816	-2210	1
32	1243	2156	-2870	1		63	-2870	-2156	1243	2
33	-2870	-3584	529	7		62	529	3584	-2870	1
34	529	3822	-2037	2		61	-2037	-3822	529	7
35	-2037	-4326	25	173		60	25	4326	-2037	2
36	25	4324	-2210	1		59	-2210	-4324	25	173
37	-2210	-96	2139	1		58	2139	96	-2210	1
38	2139	4182	-167	25		57	-167	-4182	2139	1
39	-167	-4168	2314	1		56	2314	4168	-167	25
40	2314	460	-2021	1		55	-2021	-460	2314	1
41	-2021	-3582	753	5		54	753	3582	-2021	1
42	753	3948	-1106	3		53	-1106	-3948	753	5
43	-1106	-2688	2643	1		52	2643	2688	-1106	3
44	2643	2598	-1151	3		51	-1151	-2598	2643	1
45	-1151	-4308	78	55		50	78	4308	-1151	3
46	78	4272	-2141	2		49	-2141	-4272	78	55
47	-2141	-4292	58	74	$\Longrightarrow$	48	58	4292	-2141	2
							-81543	0	58	37

5 The general solutions of the Diophantine equations

In the previous section, the smallest non-negative solutions of eqs. (14) and (17) were derived. Once these are known, it is a fairly simple task to calculate all the other roots. We first investigate eq. (14).

Let us assume that x_1 and x_2 are roots of eq. (14), different from the roots r_1 and r_2 in eq. (23). Therefore, when the algorithm in Table 2 is carried out, necessarily at $i = 47$, where $C_i = 1$, $x_i \neq 1$ and $x_{i+1} \neq 0$. Since $C_i \neq 1$ within the range $48 \leq i \leq 93$, also $x_{i+1} > 0$ within this range. If we next choose a transformation coefficient $\tilde{h}_{93} = 3$ instead of $h_{93} = 6$, eqs. (21) will lead to a transformed equation

$$-7766\tilde{x}_{94}^2 + 609\tilde{x}_{95}^2 - 1 = 0, \tag{25}$$

where $\tilde{x}_{94} = x_{94}$ and $x_{93} = 3\tilde{x}_{94} + \tilde{x}_{95}$. Also, $\tilde{x}_{94} > 0$ and $\tilde{x}_{95} > 0$.

Since the transformation in eq. (19) is linear at each step of the cycle, the linear relations

$$\begin{array}{rcl} x_1 & = & a_1\tilde{x}_{95} + a_2\tilde{x}_{94} \\ x_2 & = & a_3\tilde{x}_{95} + a_4\tilde{x}_{94} \end{array} \tag{26}$$

must be valid. When the numeric values of the transformation coefficients $h_i, i = 1, \ldots, 92$ and $\tilde{h}_{93}$ are known, the coefficients $a_i, i = 1, \ldots 4$ can be easily calculated. The results are

$$\begin{array}{rcl} a_1 & = & 109931986732829734979866232821433543901088049 \\ a_2 & = & 392567302329690546856394748066206816187916440 \\ a_3 & = & 30784636507697855142356992218944109072681060 \\ a_4 & = & a_1. \end{array} \tag{27}$$

By inserting eqs. (27) and (26) in eq. (14), it is observed that x_1 and x_2 are roots of eq. (14), if and only if $v = \tilde{x}_{95}$ and $u = \tilde{x}_{94}$ are roots of eq. (14). Then the roots (x_1, x_2) can be expressed in terms of smaller roots $(\tilde{x}_{95}, \tilde{x}_{94})$

$$\left(\begin{array}{c} x_1 \\ x_2 \end{array} \right) = \mathbf{L} \left(\begin{array}{c} \tilde{x}_{95} \\ \tilde{x}_{94} \end{array} \right), \tag{28}$$

where the matrix $\mathbf{L}$ is

$$\mathbf{L} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_1 \end{pmatrix}. \tag{29}$$

The above reasoning can be repeated for the roots $(\tilde{x}_{95}, \tilde{x}_{94})$. This will give a new pair of smaller roots. The algorithm can be continued in the similar way, until it leads to such roots $(\tilde{r}_1, \tilde{r}_2)$ that the algorithm in the next loop gives $x_{47} = 1$, $x_{48} = 0$. By calculating backwards from these values one can obtain $(\tilde{r}_1, \tilde{r}_2)$ and, since the calculation is the same as in calculating the smallest roots in Section 4, also $(\tilde{r}_1, \tilde{r}_2) = (r_1, r_2)$. This indicates that the above reasoning, started from any pair of roots, necessarily leads to the same pair of smallest roots. Therefore all roots of eq. (14) can be derived from the smallest roots and the nth pair of roots (r_{2n-1}, r_{2n}) is given by

$$\begin{pmatrix} r_{2n-1} \\ r_{2n} \end{pmatrix} = \mathbf{L}^{n-1} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}. \tag{30}$$

When $n = 1$, $\mathbf{L}^0$ is a unit matrix. Hence all positive roots of eq. (14) are given by eq. (30), where r_1 and r_2 are the numbers in eq. (23).

Next we investigate eq. (17) which is of the form $pqu^2 + 1 = v^2$, where $p = 7766$ and $q = 609$. Then $pqu^2 = (v-1)(v+1)$. We only consider non-trivial solutions $u \neq 0$, $v \neq 1$. Because pq is divisible by 2, but not by 4, v must be odd and u must be even so that

$$\begin{aligned} v &= 2v' + 1 \\ u &= 2u', \end{aligned} \tag{31}$$

where v' and u' are unknown integers. Then, obviously

$$pqu'^2 = v'(v'+1). \tag{32}$$

Since eq. (32) is similar to eq. (10), the analysis in Section 3 applies here also. This means that there are only two alternatives, corresponding to eqs. (14) and (17), respectively:

1. In the first case $v' = pu_0^2$ and $v' + 1 = qv_0^2$. This leads to eq. (14) so that also $u = u_0$ and $v = v_0$ are roots of eq. (14). By inserting v' and $v' + 1$ in eq. (32), we obtain $u' = u_0 v_0$. Then eq. (17) has a solution $v = 2pu_0^2 + 1 = 2qv_0^2 - 1$, $u = 2u_0 v_0$, where u_0 and v_0 are arbitrary roots of eq. (14).

2. In the second case $v' = pqu_1^2$, $v' + 1 = v_1^2$, which leads back to eq. (17). Hence $v = v_1$, $u = u_1$ are roots of eq. (17). Also in this case, eq. (32) gives $u' = u_1 v_1$. This means that eq. (17) has a solution $v = 2pqu_1^2 + 1 = 2v_1^2 - 1$, $u = 2u_1 v_1$, where u_1 and v_1 are smaller roots of eq. (17).

Because, in the second case, u_1 and v_1 are not the trivial solution 0 and 1, the above reasoning can be repeated. This leads to smaller numbers u_2 and v_2, which are roots of either eq. (14) or eq. (17). If u_2 and v_2 are roots of eq. (17), the same process can be repeated again. There are necessarily a finite number of steps in this process, because it gives two number sequences which are bounded from below. Therefore the sequence must finally end in such a solution of eq. (17) that the following pair is a solution of eq. (14).

In conclusion, all positive solutions of eq. (17) are obtained in the following manner. Starting from an arbitrary solution v_0, u_0 of eq. (14), one can first make use of item 1 and calculate

$$\begin{aligned} v_1 &= 2 \cdot 609 v_0^2 - 1 \\ u_1 &= 2 u_0 v_0, \end{aligned} \tag{33}$$

which are roots of eq. (17). Then item 2 indicates that a sequence of other roots of eq. (17) is obtained recursively from the equations

$$\begin{aligned} v_n &= 2 v_{n-1}^2 - 1 \\ u_n &= 2 u_{n-1} v_{n-1}, \end{aligned} \tag{34}$$

where $n = 2, 3, \ldots$. By a direct substitution, one can easily see that all pairs v_i and u_i are indeed roots of eq. (17). The smallest non-trivial solution of eq. (17) is obtained from eq. (33) using $v_0 = r_1$ and $u_0 = r_2$.

The above discussion means that every pair of roots of eq. (17) can be calculated by means of eqs. (33) and (34) starting from some pair of roots of eq. (14). Hence the solutions of eqs. (14) and (17) make a two-dimensional system in the following way. The solutions of eq. (14) make a sequence as indicated by eq. (30), and a sequence of solutions of eq. (17) emerges from every element in this sequence. One should also notice that applying eqs. (34) to the trivial solution $u = 0$, $v = 1$, gives the same trivial solution.

Although this method gives all positive roots of eqs. (14) and (17), it does not reveal all relations between the roots. These relations become clearer in the following analysis.

When moving from one equation to another along the algorithmic chain, a linear transformation

$$\begin{aligned} x_i &= b_1 x_{j+1} + b_2 x_j \\ x_{i+1} &= b_3 x_{j+1} + b_4 x_j \end{aligned} \tag{35}$$

will be formed, where the coefficients b_1, b_2, b_3 and b_4 are non-negative. Inserting the expressions of x_i and x_{i+1} in $A_i x_{i+1}^2 + B_i x_i x_{i+1} + C_i x_i^2$ gives $A_j x_{j+1}^2 + B_j x_j x_{j+1} + C_j x_j^2$, so that the quadratic form remains in transformation (35). One should notice that the transformation can also be applied if one or both of the equations is (14) or (17).

Let $b_i, i = 1, \cdots, 4$ be the coefficients by which we move from $p' x^2 + 1 = q' y^2$ to $p' \tilde{x}^2 + 1 = q' \tilde{y}^2$. This means going around one or more full loops starting either from eq. (14) or from eq. (17). Hence

$$\begin{aligned} y &= b_1 \tilde{y} + b_2 \tilde{x} \\ x &= b_3 \tilde{y} + b_4 \tilde{x}. \end{aligned} \tag{36}$$

The expression $q'y^2 - p'x^2$ remains invariant in this transformation and the coefficients b_1, b_2, b_3 and b_4 are all non-zero. Therefore, if $\tilde{y} = 1$ and $\tilde{x} = 0$, $q'b_1^2 - p'b_3^2 = q'$. If $\tilde{y} = 0$ and $\tilde{x} = 1$, $q'b_2^2 - p'b_4^2 = -p'$. If $\tilde{x} = \tilde{y} = 1$, $q'(b_1+b_2)^2 - p'(b_3+b_4)^2 = q' - p'$.

It is easy to see that $q'b_1b_2 = p'b_3b_4$. On the other hand, $q'^2b_2^2 - p'^2b_3^2 = q'^2b_1^2b_2^2 - p'^2b_3^2b_4^2 = 0 \Rightarrow q'b_2 = p'b_3$. Hence $b_1 = b_4$. This gives $q' = q'b_1^2 - p'b_3^2 = q'b_1^2 - q'b_2b_3 \Rightarrow b_1^2 - b_2b_3 = 1$. Because the coefficients b_2 and b_3 are of the form $b_2 = p'b'$ and $b_3 = q'b' \Rightarrow b_1^2 - p'q'b'^2 = 1$, where b' is the greatest common divisor of b_2 and b_3. Hence we have shown that the coefficients of the transformation are of the form $b_1, b_2 = p'b', b_3 = q'b'$ and $b_4 = b_1$, where $v = b_1$, $u = b'$ are roots of equation $v^2 - p'q'u^2 = 1$.

If, conversely, we assume that, in eqs. (36), $b_1 = b_4$, $b_2 = p'b'$ and $b_3 = q'b'$, where b_1 and b' satisfy the conditions $p'q'b'^2 + 1 = b_1^2$ and $p'\tilde{x}^2 + 1 = q'\tilde{y}^2$, an easy calculation shows that $p'x^2 + 1 = q'y^2$. Therefore two arbitrary pairs of roots (r, r') and $(\tilde{r}, \tilde{r}')$ of equation $p'x^2 + 1 = q'y^2$ have a relation

$$\begin{pmatrix} \tilde{r} \\ \tilde{r}' \end{pmatrix} = \begin{pmatrix} b_1 & p'b' \\ q'b' & b_1 \end{pmatrix} \begin{pmatrix} r \\ r' \end{pmatrix}, \tag{37}$$

where b_1 and b' are certain roots of eq. (17).

In the case of eq. (14), $q' = q = 609$ and $p' = p = 7766$. By applying eq. (37) one can then see that the nth pair of roots of eq. (14) is given by

$$\begin{pmatrix} r_{2n-1} \\ r_{2n} \end{pmatrix} = \begin{pmatrix} b_1 & pb' \\ qb' & b_1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \tilde{\mathbf{L}}_{n-1} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}. \tag{38}$$

Since the linear transformation $\mathbf{L}$ is equivalent to a single loop (back to the original equation) in the transformation sequence, expression $q'y^2 - p'x^2$ remains invariant in this transformation. Hence the expression also remains invariant in the transformation $\mathbf{L}^{n-1}$. It was shown above that $q'y^2 - p'x^2$ remains invariant in the transformation $\tilde{\mathbf{L}}_{n-1}$ and therefore, according to eq. (30), $\tilde{\mathbf{L}}_{n-1} = \mathbf{L}^{n-1}$. The elements of matrix $\mathbf{L}$ can be calculated using eq. (33) in the following way: $a_1 = a_4 = 2 \cdot 609 r_1^2 - 1$, $a_2 = 7766 \cdot 2r_1r_2$ and $a_3 = 609 \cdot 2r_1r_2$.

In the case of eq. (17), $q' = 1$ and $p' = pq = 7766 \cdot 609$. In the same way as above, the relation of the roots (r_{2n-1}, r_{2n}) and the smallest non-negative solution $(1, 0)$ is

$$\begin{pmatrix} r_{2n-1} \\ r_{2n} \end{pmatrix} = \begin{pmatrix} b_1 & pqb' \\ b' & b_1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \tilde{b}_1 & pq\tilde{b}' \\ \tilde{b}' & \tilde{b}_1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{39}$$

Here $\tilde{b}_1$ and $\tilde{b}'$ are the smallest positive roots of eq. (17).

6 Choosing the solutions of the Diophantine equations

The solution of the cattle problem implies the choice of such roots of the Diophantine equations that Q in eqs. (2) will be divisible by 4657. Eqs. (8) and (12) indicate that this condition is fulfilled if and only if one of the roots of eq. (14) or (17) is divisible by 4657. Since, in the continuation, we only investigate divisibility by a single prime number $t_0 = 4657$, we adopt a convention that remainders and congruences always refer to t_0. Also, the remainder of u and the matrix composed of the remainders of the elements of $\tilde{\mathbf{L}}_n$ are denoted by rem$[u]$ and rem$[\tilde{\mathbf{L}}_n]$, respectively.

We first investigate eq. (14). All its solutions are obtained from eq. (30), where matrix $\mathbf{L}^{n-1}$ is the same as matrix $\tilde{\mathbf{L}}_{n-1}$ in eq. (38). From eq. (38) we see that the pairs of roots (r_{2n_1-1}, r_{2n_1}) and (r_{2n_2-1}, r_{2n_2}) of eq. (14) satisfy the condition $r_{2n_1-1} \equiv r_{2n_2-1}$ and $r_{2n_1} \equiv r_{2n_2}$, when the remainders rem$[\tilde{\mathbf{L}}_{n_1-1}]$ and rem$[\tilde{\mathbf{L}}_{n_2-1}]$ are the same.

Next we investigate how many different remainder matrices rem$[\tilde{\mathbf{L}}_{n-1}]$ exist. The remainders of the elements of $\tilde{\mathbf{L}}_{n-1}$ depend only on b_1 and b' which are also roots of eq. (17). First we find out how many different remainders rem$[v]$ and rem$[u]$ exist which satisfy the condition

$$609 \cdot 7766(\mathrm{rem}[u])^2 + 1 \equiv (\mathrm{rem}[v])^2. \tag{40}$$

The factor $609 \cdot 7766$ in congruence (40) can of course be replaced by its remainder $t_1 = 2639$. According to the Fermat little theorem, $t_1^{4656} \equiv 1$ and, because $4656 = 16 \cdot 3 \cdot 97$, it is easy to show that t_1 is a primitive root of 4657. Hence, each non-zero remainder is congruent with t_1^s, where s is a positive integer.

Let now rem$[u]$ be an arbitrary remainder and s_1 such a number that $1 \leq s_1 \leq 4656$ and $t_1^{s_1} \equiv$ rem$[u]$. The problem is whether such a remainder rem$[v]$ exists that $t_1(\mathrm{rem}[u])^2 + 1 \equiv (\mathrm{rem}[v])^2$. We first assume that rem$[v]$ exists.

Let rem$[v] \equiv t_1^{s_2}$, where $1 \leq s_2 \leq 4656$. This gives

$$t_1^{2s_1+1} + 1 \equiv t_1^{2s_2} \equiv t_1^{3 \cdot 4656 + 2s_2}. \tag{41}$$

Here $3 \cdot 4656$ was added to the exponent to make sure that it is greater than $2s_1 + 1$. For the same reason we put $1 \equiv t_1^{3 \cdot 4656}$. Thus congruence (41) gives

$$t_1^{3 \cdot 4656 - (2s_1+1)} + 1 \equiv t_1^{3 \cdot 4656 + 2s_2 - (2s_1+1)}. \tag{42}$$

The exponent on the right hand side is odd and the exponent on the left hand side is of the form $1 + 2[3 \cdot 2328 - (s_1 + 1)]$, so that we have found such a remainder $\mathrm{rem}[u'] \equiv t_1^{3 \cdot 2328 - (s_1+1)}$ that congruence (40) does not have a solution $\mathrm{rem}[v]$.

On the other hand, if $\mathrm{rem}[u]$ is such a remainder that congruence (40) does not have a solution $\mathrm{rem}[v]$, there is such an s_2 within the range $0 \leq s_2 \leq 2327$ that

$$t_1^{2s_1+1} + 1 \equiv t_1^{2s_2+1}. \tag{43}$$

In the same way as above,

$$t_1 t_1^{2[3 \cdot 2328 - (s_1+1)]} + 1 \equiv t_1^{3 \cdot 4656 + 2s_2 - 2s_1}. \tag{44}$$

Because the exponent on the right hand side is even, we have found remainders $\mathrm{rem}[u']$ and $\mathrm{rem}[v']$ which satisfy congruence (40).

If s_1 is replaced by $s_1' = 3 \cdot 2328 - (s_1 + 1)$ in eq. (44), it will be noticed that $3 \cdot 2328 - (s_1' + 1) = s_1$. Then the remainders $\mathrm{rem}[u] \equiv t_1^{s_1}$ and $\mathrm{rem}[u'] \equiv t_1^{s_1'}$ are joined together in pairs. In addition, we notice that no value of $\mathrm{rem}[u]$ can make $\mathrm{rem}[v]$ zero, because in such a case we would have $t_1(\mathrm{rem}[u])^2 \equiv -1 \equiv t_1^{2328}$. This congruence cannot be valid since the exponent on one side is even and on the other side odd.

It was shown above that the remainders of u can be arranged in pairs in such a way that one remainder in each pair has a $\mathrm{rem}[v]$ which satisfies congruence (40) and the other remainder does not. Because the number of these pairs is $(t_0 - 1)/2$ and because there are two values of $\mathrm{rem}[v] \neq 0$ for each $\mathrm{rem}[u]$ satisfying congruence (40), we have found $t_0 - 1$ pairs of remainders $(\mathrm{rem}[u], \mathrm{rem}[v])$ satisfying congruence (40). In addition, the pairs $(\mathrm{rem}[u], \mathrm{rem}[v]) = (0, 1)$ and $(\mathrm{rem}[u], \mathrm{rem}[v]) = (0, 4656)$ satisfy (40), so that the total number of pairs is $t_0 + 1$.

Hence we have shown that there are at most $t_0 + 1$ different remainder matrices for the matrices $\tilde{\mathbf{L}}_{n-1}$ in eq. (38). It is easily calculated that $\mathrm{rem}[\tilde{\mathbf{L}}_{4658}] = \mathrm{rem}[\mathbf{L}^{4658}] = \mathbf{I}$ (a unit matrix). If n' is the smallest positive integer which makes $\mathrm{rem}[\mathbf{L}^{n'}]$ into a unit matrix, then 4658 is divisible by n'. Because $4658 = 2 \cdot 17 \cdot 137$, it can be easily shown that $n' = 4658$. Similarly, one can show that the smallest positive integer n'' which makes $\mathrm{rem}[\mathbf{L}^{n''}] = -\mathbf{I}$ is equal to 2329. In these calculations one can make use of the fact that $\mathbf{L}^{n_1}\mathbf{L}^{n_2} = \mathbf{L}^{n_1+n_2}$ and $(\mathbf{L}^{n_1})^{n_2} = \mathbf{L}^{n_1 n_2}$.

Let

$$\tilde{\mathbf{L}} = \begin{pmatrix} b_1 & pb' \\ qb' & b_1 \end{pmatrix}$$

be a coefficient matrix in eq. (37), such that the remainders of the roots (r, r') and $(\tilde{r}, \tilde{r}')$ of eq. (14) are the same. Hence $b_1 r + pb'r' \equiv r$ and $qb'r + b_1 r' \equiv r'$. Thus $[(b_1 - 1)^2 - pqb'^2]r \equiv 0 \Rightarrow 2(1 - b_1)r \equiv 0$. Also, $[(b_1 - 1)^2 - pqb'^2]r' \equiv 0$. Because r and r' are not both divisible by t_0, $b_1 - 1$ is divisible by 4657. Then $pb'r'$ and $qb'r$ are divisible by t_0 so that b' is divisible by 4657. The remainders of the roots of eq. (14) will be identical only when rem$[\tilde{\mathbf{L}}]$ is a unit matrix. Because rem$[\mathbf{L}^{4658}]$ is a unit matrix, eq. (30) indicates that the remainders of the roots of eq. (14) are periodic and the length of the period is 4658. The same pair of residuals cannot appear more than once within a single period.

The inverse of

$$\tilde{\mathbf{L}} = \left(\begin{array}{cc} b_1 & pb' \\ qb' & b_1 \end{array} \right)$$

is

$$\tilde{\mathbf{L}}^{-1} = \left(\begin{array}{cc} b_1 & -pb' \\ -qb' & b_1 \end{array} \right).$$

Therefore

$$\mathbf{L}^{-1} = \left(\begin{array}{cc} 2qr_1^2 - 1 & -2pr_1r_2 \\ -2qr_1r_2 & 2qr_1^2 - 1 \end{array} \right).$$

Then

$$\mathbf{L}^{-1} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} r_1 \\ -r_2 \end{pmatrix},$$

so that

$$\text{rem} \left[\mathbf{L}^{4657} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \right] = \begin{pmatrix} \text{rem}[r_1] \\ t_0 - \text{rem}[r_2] \end{pmatrix}.$$

Because rem$[\mathbf{L}^{2329}]$ = rem$[\mathbf{L}^{-2329}] = -\mathbf{I}$, also

$$\text{rem} \left[\mathbf{L}^{2328} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \right] = \begin{pmatrix} t_0 - \text{rem}[r_1] \\ \text{rem}[r_2] \end{pmatrix}.$$

This information allows us to find the roots of eq. (14), which are divisible by t_0. Let us assume that v_0 is divisible by t_0 in the pair of roots (v_0, u_0). There is an integer n that

$$\begin{pmatrix} v_0 \\ u_0 \end{pmatrix} = \mathbf{L}^n \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}.$$

We know that

$$\mathbf{L}^n = \left(\begin{array}{cc} c_1 & pc' \\ qc' & c_1 \end{array} \right)$$

and

$$\mathbf{L}^{-n} = \left(\begin{array}{cc} c_1 & -pc' \\ -qc' & c_1 \end{array} \right),$$

where c_1 and c' are certain roots of eq. (17). Because

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \mathbf{L}^{-n} \begin{pmatrix} v_0 \\ u_0 \end{pmatrix}$$

and rem$[v_0] = 0$, we have rem$[r_1]$ = rem$[-pc'u_0]$ and rem$[r_2]$ = rem$[c_1u_0]$. Since

$$\mathbf{L}^{2n} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \mathbf{L}^n \begin{pmatrix} v_0 \\ u_0 \end{pmatrix},$$

it follows that

$$\begin{aligned}\mathrm{rem}\left[\mathbf{L}^{2n}\begin{pmatrix}r_1\\ r_2\end{pmatrix}\right] &= \begin{pmatrix}\mathrm{rem}[pc'u_0]\\ \mathrm{rem}[c_1u_0]\end{pmatrix} = \begin{pmatrix}t_0-\mathrm{rem}[r_1]\\ \mathrm{rem}[r_2]\end{pmatrix}\\ &= \mathrm{rem}\left[\mathbf{L}^{2328}\begin{pmatrix}r_1\\ r_2\end{pmatrix}\right] = \mathrm{rem}\left[\mathbf{L}^{2328+k\cdot 4658}\begin{pmatrix}r_1\\ r_2\end{pmatrix}\right].\end{aligned}$$

Hence, necessarily $n = 1164 + 2329 \cdot k$, where k is a non-negative integer.

By a direct calculation one can easily show that v_0 is divisible by t_0, when

$$\begin{pmatrix}v_0\\ u_0\end{pmatrix} = \mathbf{L}^{1164}\begin{pmatrix}r_1\\ r_2\end{pmatrix}.$$

Because

$$\mathrm{rem}\left[\mathbf{L}^{2329}\begin{pmatrix}r_1\\ r_2\end{pmatrix}\right] = \begin{pmatrix}t_0-\mathrm{rem}[r_1]\\ t_0-\mathrm{rem}[r_2]\end{pmatrix},$$

the divisibility is also valid when k is a positive integer. Therefore v_0 is divisible by t_0 if and only if $n = 1164 + 2329 \cdot k$.

Further, if we assume that u_0 is divisible by t_0, a similar reasoning shows that $2n = 4657 + k \cdot 4658$. Then n cannot be an integer and therefore u_0 cannot be divisible by t_0.

Next, we investigate eq. (17) and assume that (v_n, u_n) are its roots. In investigating congruence (40), it already became clear that the root v_n of eq. (17) cannot be divisible by t_0. Therefore it is sufficient to investigate the divisibility of u_n. We remember that either eq. (33) or (34) is valid for u_n. In the latter case, $u_n = 2u_{n-1}v_{n-1}$, where (v_{n-1}, u_{n-1}) are also roots of eq. (17). Then, if u_n is divisible by t_0, u_{n-1} must also be divisible by t_0. By repeating this reasoning, we finally meet $u_1 = 2u_0v_0$, where (v_0, u_0) are roots of eq. (14). Since u_1 is divisible by t_0 and u_0 is not, necessarily v_0 is divisible by t_0. It is now easy to see that every u_n, calculated according eqs. (33) and (34) from a v_0 which is divisible by t_0, is also divisible by t_0. Hence the solutions of eq. (17) we are searching for are those which are derived using eqs. (33) and (34) from the chosen solutions of eq. (14).

7 The complete solution to Archimedes' cattle problem

According to the preceding theory, all solutions of Archimedes' cattle problem can be calculated according to the following procedure:

Constants r_1 and r_2 are defined in eqs. (23) and $\mathbf{L}$ is the matrix defined in eqs. (29) and (27). Let k be an arbitrary non-negative integer and

$$\begin{pmatrix} v_0(k) \\ u_0(k) \end{pmatrix} = \mathbf{L}^{1164+2329k} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}. \tag{45}$$

According to eqs. (33) and (34), we next calculate $v_n(k)$ and $u_n(k)$ from the formulas

$$\begin{array}{rcll} v_n(k) & = & \left\{ \begin{array}{l} 2 \cdot 609\, v_0(k)^2 - 1 \\ 2\, v_{n-1}^2(k) - 1 \end{array} \right. & \begin{array}{l} \text{when } n = 1 \\ \text{when } n = 2, 3, \ldots \end{array} \\ u_n(k) & = & \quad 2\, u_{n-1}(k)\, v_{n-1}(k) & \text{when } n = 1, 2, \ldots \end{array} \tag{46}$$

Next eqs. (12) and (8) give the value of $Q = 3 \cdot 11 \cdot 29 \cdot u^2 v^2$, where u and v are accepted solutions of eq. (14) or (17). Hence the solutions $v_n(k)$ and $u_n(k)$ define the coefficient

$$Q_n(k) = 3 \cdot 11 \cdot 29 \cdot u_n^2(k)\, v_n^2(k), \tag{47}$$

and

$$Q'_n(k) = Q_n(k)/4657. \tag{48}$$

Finally, the numbers of bulls and cows of different colours are obtained by inserting $Q_n(k)$ in eqs. (2) and $Q'_n(k)$ in eqs. (4).

The smallest solution of the Cattle Problem is now obtained by first calculating a vector

$$\begin{aligned} \begin{pmatrix} v \\ u \end{pmatrix} = & \left(\begin{array}{l} 109931986732829734979866232821433543901088049 \\ 30784636507697855142356992218944109072681060 \end{array} \right. \\ & \left. \begin{array}{l} 392567302329690546856394748066206816187916440 \\ 109931986732829734979866232821433543901088049 \end{array} \right)^{1164} \times \\ & \begin{pmatrix} 300426607914281713365 \\ 84129507677858393258 \end{pmatrix}. \end{aligned} \tag{49}$$

The total number of cattle is then given by

$$T = 6299 \cdot 957 \cdot u^2 v^2 + 21054639 \cdot 957 \cdot u^2 v^2 / 4657. \tag{50}$$

Here the first and second term give the number of bulls and cows, respectively.

8 Calculation of h_i and its connection to continued fractions

In Section 4, the necessary conditions for the coefficients h_i were given, but no method was presented for calculating their values. In the following, such a calculation method is derived. Connections between the theory and continued fractions are also examined.

Our task is to determine the value of h_i for the equation $A_i x_{i+1}^2 + B_i x_{i+1} x_i + C_i x_i^2 = 1$, where $A_i C_i < 0$ and $(B_i^2 - 4A_i C_i)^{1/2} \notin Z$. Then equation

$$A_i + B_i z + C_i z^2 = 0 \tag{51}$$

has one and only one positive irrational real root z_i. We denote the integer part of a number by $\lfloor \cdot \rfloor$. Because the expression on the left-hand side of eq. (51) has opposite signs for $z = h_i$ and $z = h_i + 1$, necessarily $h_i = \lfloor z_i \rfloor$.

We can now obtain a formula for determining the value of h_i. We adopt the notations Δ and δ for the integer and decimal parts of $(B_i^2 - 4A_i C_i)^{1/2}$, respectively, and notice that Δ and δ are constants, because $(B_i^2 - 4A_i C_i)^{1/2}$ is invariant. The positive root of eq. (51) is

$$z_i = \frac{-B_i \pm (\Delta + \delta)}{2C_i}, \tag{52}$$

where the sign in the numerator is chosen to be the same as the sign of C_i. If $C_i > 0$, $(-B_i + \Delta)/(2C_i) = \lfloor (-B_i + \Delta)/(2C_i) \rfloor + \mu/(2C_i)$, where $\mu \in Z$ and $0 \leq \mu < 2C_i$. Because $0 < \delta < 1$, we see that $0 < (\mu + \delta)/(2C_i) < 1$ and therefore

$$h_i = \lfloor z_i \rfloor = \left\lfloor \frac{-B_i + \Delta}{2C_i} \right\rfloor . \tag{53}$$

In the case of $C_i < 0$, we have $(-B_i - \Delta)/(2C_i) = \lfloor (-B_i - \Delta)/(2C_i) \rfloor + \mu/(2C_i)$, where $\mu \in Z$ and $2C_i < \mu \leq 0$. Because $-1 < -\delta < 0$, obviously $0 < (\mu - \delta)/(2C_i) < 1$, so that

$$h_i = \lfloor z_i \rfloor = \left\lfloor \frac{-B_i - \Delta}{2C_i} \right\rfloor . \tag{54}$$

Depending on the sign of C_i, the value of h_i can always be calculated either from eq. (53) or (54).

The connection of the theory to continued fractions is revealed by the following line of thought. Inserting $z_i = h_i + 1/z'_{i+1}$ in eq. (51), we obtain

$$C_i + (B_i + 2h_iC_i)z'_{i+1} + (A_i + h_iB_i + h_i^2C_i)(z'_{i+1})^2 = 0. \tag{55}$$

According to eq. (21) this can be written in the form

$$A_{i+1} + B_{i+1}z'_{i+1} + C_{i+1}(z'_{i+1})^2 = 0, \tag{56}$$

were A_{i+1}, B_{i+1} and C_{i+1} are the coefficients of the next quadratic equation in the algorithmic chain. This indicates that $z'_{i+1} = z_{i+1}$, i.e. a root of eq. (51) for the index $i+1$. Starting from $i = 1$, it is now easy to see that the choice of the numbers $h_i = \lfloor z_i \rfloor$ is equivalent to finding a continued fraction expansion of the positive root of equation $A_1 + B_1z + C_1z^2 = 0$. Then it is also clear that the coefficients h_i, obtained in solving Pell's equation $y^2 - Ax^2 = 1$ with the present method, create the continued fraction expansion of $A^{1/2}$.

Finally, we compare the usual method of calculating the continued fraction expansion of a quadratic irrational number z_1 with the present theory. Unconventionally, we start the indexing from 1 instead of 0, and denote the terms of the expansion by h'_i. Let z_1 be the positive root of equation $A_1 + B_1z + C_1z^2 = 0$ with $C_1 > 0$. Now $z_1 = (m_1 + \sqrt{D})/q_1$, where $m_1 = -B_1$ and $q_1 = 2C_1$ and D is the discriminant of the quadratic equation. In calculating continued fractions the first term is given by $h'_1 = \lfloor z_1 \rfloor$, i.e. $h_1 = h'_1$.

The next step in the usual method is to calculate $m_2 = h'_1q_1 - m_1$ and $q_2 = (D - m_1^2)/q_1$. In the present algorithm, the corresponding step is to carry out the transformation to equation $A_2 + B_2z + C_2z^2 = 0$ using the coefficient $h = h_1 = h'_1$. Then it is noticed that $m_2 = 2h_1C_1 + B_1 = B_2$ and $q_2 = [B_1^2 - 4A_1C_1 - (2h_1C_1 + B_1)^2]/(2C_1) = -2C_2$. In calculating continued fractions, the following task is to create a new irrational number $z'_2 = (m_2 + \sqrt{D})/q_2$. The same step in the present algorithm is to solve the positive root of equation $A_2 + B_2z + C_2z^2 = 0$. Since $C_2 > 0$, this gives $z_2 = (B_2 + \sqrt{D})/(-2C_2)$ and, obviously, $z'_2 = z_2$.

Now, of course, $h'_2 = \lfloor z'_2 \rfloor = \lfloor z_2 \rfloor = h_2$. By repeating the above operations, we see that $m_3 = B_3$ and $q_3 = 2C_3$ and, in general,$m_i = B_i$ and $q_i = (-1)^{i+1} \cdot 2C_i$. Hence, the same auxiliary quantities are actually calculated in both methods. The standard method is clearly better in calculating the continued fraction expansion of a number, since it does not imply finding a quadratic equation with integer coefficients, which would have the number as its root.

9 Computer calculations

The algorithm was programmed using *Mathematica 3.0* on a laptop Macintosh PowerBook 3400c computer with a PowerPC 603ev processor at 240 MHz, 144 MB RAM and 2.8 GB disk.

The calculation time was measured by means of the *Timing* command. All output was suppressed by means of semicolons, so that the times do not include the conversion of the computer internal presentation into strings of ASCII characters. Only after calculation were the results or parts of the results output in files or on the screen. The results were always checked by studying that they fulfilled the seven equations and the numbers of cows are integers. The latter is needed because the calculation of the numbers of cows involves a division. The conditions of square and triangular numbers were also checked for the first three solutions. This was not done for the longer solutions, because the time and memory consumption in calculating the square roots is too high.

The time needed for a full computation of the smallest result was about 7.6 s. This time can be compared with the time taken by the square and triangular number checks, which was about 225 s each. All the other checks took only a fraction of a second. The time needed to write each number in a file was 190–200 s. Hence the total time is about half an hour. This mainly consists of producing the ASCII output, the actual computing time being only a tiny fraction of it.

A large number of solutions, up to the length of nearly 5 million digits, were calculated. Only the first three of them were completely written in files; of the others, the first and last digits were printed. The lengths and the fifty first and fifty last digits of the total number of cattle for the first 20 solutions as well as the computing times are shown in Table 4. It is seen that the number of digits is approximately a multiple of 206545 or 206546. Also, the last three digits for the first five solutions is 800, 200, 200, 800 and 000, and after this, the cycle is repeated again and again. All the computing times are for complete calculations from the very beginning, i.e. without making use of the previous results. An apparent feature in these times is that, after the fifth solution, every second time is smaller than the previous one. This results from the fact that, once a solution of eq. (14) is found, a sequence of solutions of eq. (17) is easily calculated. For instance, in order to obtain solutions 2, 4, 8 and 16, it is sufficient to calculate only $\mathbf{L}^{1164}$ but, for solutions 3, 5, 7, 9, 11, 13, 15, 17 and 19, higher powers of $\mathbf{L}$ must be computed.

In order to compare the speeds of the two algorithms, a programme for the method used by Vardi [4] was also written. The calculation of $\varepsilon^{4658} = a_1 + b_1\sqrt{4729494}$ in the way described by Vardi took about 10.7 s. Instead of this, however, a complex number $a_1 + ib_1\sqrt{4729494}$ was calculated, which took 20.7 s. This was done because it provides an easy way of extracting a_1, needed in the continuation. The additional 10 s is not an essential increase, because it is only a small part of the total time. The remaining multiplications, divisions and additions increased the total time to 438 s. Hence the numerical efficiency of the two methods is reflected by the times 7 s and 7 min in the same task. The time reported by Vardi for the smallest solution was 1.5 h with a Sun workstation. This must contain writing the nine resulting numbers in a file. With the present laptop computer, the total time of computing and writing in files was about 36 min.

10 Discussion

The most essential point in the above solution of the cattle problem is solving quadratic Diophantine equations of a certain specific type. Unlike some previous methods, the present one does not use continued fractions, although it has a close connection to them. This relationship is reflected by the fact that the coefficients h_i in Table 2 are the same as the partial quotients in the continued fractions presentation of $\sqrt{7766 \cdot 609}$. The reason for this connection was explained in Chapter 8.

The benefits of the new method are evident. Only the basic arithmetic operations of integer numbers are needed in understanding the solution and in making the calculations. No advanced theorems of number theory are applied. The numerical solution is especially suitable for a computer. Another benefit is that, even if the number of steps in the algorithm were very great, the calculation will not get more elaborate when proceeding along the chain. This is because $B_i^2 - 4A_iC_i$ remains constant and A_i and C_i will always have opposite signs so that the numerical values of the coefficients will not grow excessively. Therefore the algorithm is also applicable when the roots are very big.

The method makes use of the well known ideas of linear transformation and infinite descent in a new way. Unlike the old solutions, the present one is based on transformations of Diophantine equations. This leads to the fact that the calculations are limited to integer numbers, and the concepts of irrational numbers or even fractions are not needed at all.

The purpose of this paper is not to create a brief and elegant solution to the cattle problem but, rather, to present it in the form it was originally discovered. It seems probable, for instance, that the discussion associated with the rejection of equations in Chapter 3 could be omitted. The line of thought is roughly as follows. We know that Pell's equation $y^2 - Dx^2 = 1$ always has a solution. Let us suppose that there are two equations $qy^2 - px^2 = 1$ and $q'y^2 - p'x^2 = 1$ such that both equations have a solution and $qp = q'p' = D$. Then one can show that there is an exit to the same Pell equation from the algorithm loop of each of these equations. Conversely, both loops can be developed starting from the same Pell equations, and therefore the loops are identical. Hence the two equations are necessarily identical. This means that, in addition to Pell's equation, there can be at most one equation

Table 4. The number of digits, the 50 first and last digits and the computing times of the twenty first solutions.

No	of digits	The first/last 50 digits	Time/s
1	206545	77602714064868182695302328332138866642323224059233... 05994630144292500354883118973723406626719455081800	7.6
2	413091	44009490043932285816719235169348369864194234934020... 11581193275201859189229977601612293349744397607200	16.6
3	619637	24958343754678123578712999230980999881561136361147... 44919334686973352593735579708551482776099647416200	42.3
4	826183	14154195432731766172032653110432770554478706512805... 29497196996042055318793576061599829319808330908800	44.3
5	1032728	80270249627607350627294754707634710725064411374829... 80699303632338364623950738864748504565921321045000	96.8
6	1239274	45522283522934483532429086649904673863640229366397... 29173911528967704349900291189294413031960053344800	90.5
7	1445820	25816268253259718324690345064768807693002781855400... 77893495392969120303854296342149319432846317888200	167.5
8	1652366	14640735370590271106027979075734871733820823638582... 49782035518048443581883698403835052875802227315200	126.1
9	1858911	83029479740778480390992214567494033971458643169338... 80611991400119558164544000428857887778833160825800	248.4
10	2065457	47087078152320997072282938915190218666297665303416... 86570434640037157265986582633249636788416084180000	203.8
11	2272003	26703683268219368825480577944889988732920773505237... 21017329543901176145353890642532008685065245697800	316.6
12	2478549	15143999756846876938673801002103600654442055000072... 52109101586725248914580549990213380909696848259200	227.6
13	2685094	85883556336335680939605742561053086924100922738733... 87338942332263137435109633401710976139323897304200	429.7
14	2891640	48705661432949561361357338946050302491455632914808... 56066134324557929672530134983582390963742024832800	352.9
15	3098186	27621602514117834486805751043626655217904227982861... 31104306025398924814315115126268750833676689405000	530.7
16	3304732	15664563481972963809538732671608027827276540861217... 69581836924762033719965210978567445461511752140800	373.7
17	3511277	88835739691549075450127051132588835004913462225449... 67523439543398286074167078250401030418369028720200	678.1
18	3717823	50379882309690068540226701421929494094046458818823... 24058601259500490631702992399535840646118017383200	531.3
19	3924369	28571074551199738707258038519334066987791101057040... 05306789951035666709718661605336793986024602929800	816.8
20	4130915	16203021197872170587157008485464224005358445875774... 24538558925624110968323032772706512285357136720000	563.2

which has a solution and satisfies the above conditions. This equation could be found by applying the algorithm to Pell's equation.

Excluding the final results in Chapter 9, all calculations in this work were carried out by a simple pocket calculator. This was done in order to show that no computer is needed in deriving the theory. It also proves that the calculations could actually be done by means of an abacus. The use of an abacus would be even easier since one can always construct an abacus which is big enough for all numbers needed. In this work the small number of digits in the calculator made it necessary to divide the numbers into smaller parts.

The reason why the cattle problem was not solved starting from Pell's equation was to show how Diophantine equations of a more general form can be solved and what happens if no solutions exist. In addition, this procedure revealed the relationship between eqs. (14) and (17) and their roots. The method also gives a simple way of deriving a great number of new solutions to the cattle problem starting from a single solution. A small practical benefit is that eq. (14) leads to roots (r_1, r_2), whereas Pell's equation implies a longer calculation of much greater coefficients a_1, a_2, a_3 and a_4. In the case of eq. (14), the same coefficients are obtained in a simple way from the roots (r_1, r_2).

It is surprising how difficult the cattle problem has turned out to be, although it can indeed be solved by means of simple methods. The only tools used in the present solution which are not known to have been available to ancient Greeks are Fermat little theorem and matrix algebra. The importance of these implements is not so essential in this work that one could not manage without them, although they clearly make the analysis easier.

Because the theory of quadratic forms by Gauss is similar to the treatment of quadratic forms in the present algorithm, Gauss has actually been very close to the solution of the cattle problem. Certainly the reason why he did not do it was, at least partly, that he had no interest in individual problems which seemed to have no wider importance. In addition, he also produced so much mathematical theory and much else that lack of time may be an explanation.

Much consideration has been put on the question whether Archimedes himself had known a solution to the cattle problem. This work overturns at least the argument which states that, at Archimedes' time, mathematics was too undeveloped to allow finding the solution. Also, Archimedes admits the difficulty of the problem but gives to understand that the solution is possible. Because it is not evident that the problem has a solution at all, it is not likely that Archimedes would have made such a statement without knowing the solution.

Vardi [4] proposes that Archimedes would hardly have been able to solve the complete cattle problem due to the tremendous size of the answer, and he would have presented the problem because he believed (without being able to prove it) that all problems leading to Pell's equation do have a solution. However, it is sufficient for a complete solution that one is able to present an algorithm which leads to the answer, the actual numerical answer is not essential. It is remarkable that the wording of the original problem hints in this direction: In the first part of the problem the exact numbers of bulls and cows of various colours are explicitly asked, whereas in the second part of the problem the task is to 'find out all these things and gather them together in one's mind'. The latter can be interpreted to mean finding an algorithm rather than a numerical answer. Although it is not shown in this work, one should notice that the present method can be used as a basis for proving that Pell's equation always has a solution. One should also notice that the transformation in the present algorithm is similar to the Euclidean formula for calculating continued fractions. Archimedes could hardly have been unaware of the Euclidean algorithm, and applying it to the cattle problem might have been a small step for him.

The cattle problem has been considered to be difficult because of the large numbers it contains. These large numbers, however, make no obstruction for finding the method of solution. The problem was perhaps created to contain large numbers only in order to ensure that the solution cannot be found by means of guesswork or trial and error.

My personal opinion is that Archimedes did know the solution of the cattle problem and the above method of solving the Diophantine equations.

Appendix A

The English translation of Archimedes' cattle problem, according to Thomas [5], is as follows:

If thou art diligent and wise, O stranger, compute the number of cattle of the Sun, who once upon a time grazed on the fields of the Thrinacian isle of Sicily, divided into four herds of different colours, one milk white, another glossy black, the third yellow, and the last dappled. In each herd were bulls, mighty in number according to these proportions:

Understand, stranger, that the white bulls were equal to a half and a third of the black together with the whole of the yellow, while the black were equal to the fourth part of the dappled and a fifth, together with, once more, the whole of the yellow. Observe further that the remaining bulls, the dappled, were equal to a sixth part of the white and a seventh, together with all the yellow.

These were the proportions of the cows: The white were precisely equal to the third part and a fourth of the whole herd of the black, while the black were equal to the fourth part once more of the dappled and with it a fifth part, when all, including the bulls, went to pasture together. Now the dappled were equal in number to a fifth part and a sixth of the yellow herd. Finally, the yellow were in number equal to a sixth part and a seventh of the white herd.

If thou canst accurately tell, O stranger, the number of cattle of the Sun, giving separately the number of well-fed bulls and again the number of females according to each colour, thou wouldst not be called unskilled or ignorant in numbers, but not yet shalt thou be numbered among the wise. But come, understand all these conditions regarding the cows of the Sun.

When the white bulls mingled their number with the black, they stood firm, equal in depth and breadth, and the plains of Thrinacia, stretching far in all ways, were filled with their multitude. Again, when the yellow and the dappled bulls were gathered into one herd they stood in such a manner that their number, beginning from one, grew slowly greater till it completed a triangular figure, there being no bulls of other colours in their midst nor none of them lacking.

If thou art able, O stranger, to find all these things and gather them together in your mind, giving all the relations, thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom.

Appendix B

The effect of prime number 353 on the solvability of eqs. (14)–(17) is investigated in this appendix. Because 353 is a factor of p in these equations, only the numbers q must be studied.

It follows from the Fermat little theorem that, for each natural number a which is not divisible by 353, there is the smallest natural number k that $a^k \equiv 1(353)$. This number k must be a factor of 352. It is easy to show by calculation that, when $a = 5$, $k = 352$. Therefore, for each natural number a' which is smaller than 353, there is such a natural number k_1 that $5^{k_1} \equiv a'(353)$.

Eq. (14): In this case $q = 3 \cdot 7 \cdot 29 = 609$. Take a k_1 for which $5^{k_1} \equiv 609(353)$. Because $609^{11} \equiv 1(353)$, it follows that $5^{11k_1} \equiv 1(353) \Rightarrow 11k_1 = 352k'$, where k' is a certain unknown natural number. Thus $k_1 = 32k'$.

Take now $v = 5^{k''}$. Can we choose k'' in such a way that $609v^2 \equiv 1(353)$? Now $609v^2 \equiv 5^{32k'} \cdot 5^{2k''} = 5^{32k'+2k''} \equiv 1(353)$. The latter congruence is valid when $32k' + 2k'' = 352k' \Rightarrow k'' = 160k'$. Hence it has been possible to find a v such that $609v^2 - 1$ is divisible by 353. Therefore eq. (14) will not be rejected.

Eq. (15): In this case $q = 2 \cdot 3 \cdot 7 = 42$. With the same reasoning as above: $5^{k_1} \equiv 42(353)$. $42^4 \equiv 1(353) \Rightarrow 5^{4k_1} \equiv 1(353) \Rightarrow 4k_1 = 352k' \Rightarrow k_1 = 88k'$. $v = 5^{k''} \Rightarrow 42v^2 \equiv 5^{88k'+2k''}(353) \Rightarrow 42v^2 \equiv 1(353)$, when $88k' + 2k'' = 352k' \Rightarrow k'' = 132k'$. Hence equation (15) will not be rejected.

Eq. (16): In this case, $q = 2 \cdot 29 = 58$. $5^{k_1} \equiv 58(353)$. $58^{11} \equiv 1(353) \Rightarrow 5^{11k_1} \equiv 1(353) \Rightarrow 11k_1 = 352k' \Rightarrow k_1 = 32k'$. $v = 5^{k''} \Rightarrow 58v^2 \equiv 5^{32k'+2k''}(353)$. $5^{32k'+2k''} \equiv 1(353)$ when $32k' + 2k'' = 352k' \Rightarrow k'' = 160k'$. Hence, equation (16) will not be rejected.

Eq. (17): In this case, $q = 1$. Obviously, the smallest solution of the equation is $u = 0$, $v = 1$. Hence, equation (17) cannot be rejected.

References

1. A. Amthor, Das Problema bovinum des Archimedes, *Zeitschrift für Math. u. Physik (Hist. litt. Abtheilung)* **25** (1880), 153–171.
2. H.C. Williams, R.A. German, and C.R. Zarnke, Solution of the Cattle Problem of Archimedes, *Math. Comp.* **19** (1965) 671–674.
3. H.L. Nelson, A solution to Archimedes' Cattle Problem, *J. Recreational Math.* **13** (1981), 162–176.
4. I. Vardi, Archimedes' Cattle Problem, *Am. Math. Monthly*, **105**, 305–319, 1998.
5. Greek Mathematical Works (translated by I. Thomas), *The Loeb Classical Library, Harvard University Press,* Cambridge, MA (1941), Vol. II, pp. 203–205.