Solution of the Cattle Problem of Archimedes

By H. C. Williams, R. A. German and C. R. Zarnke

1. Introduction. In 1773 G. E. Lessing published a Greek epigram [1], attributed in substance, to Archimedes, which states a problem now commonly referred to as the "cattle problem". The verse, when reduced to mathematical notation, asks us to find the numbers W, X, Y and Z, of white, black (or blue), piebald (or spotted), and yellow (or red) bulls, and the numbers w, x, y and z of correspondingly coloured cows, when

(1) $W = (1/2 + 1/3)X + Z$, (2) $X = (1/4 + 1/5)Y + Z$,

(3) $Y = (1/6 + 1/7)W + Z$, (4) $w = (1/3 + 1/4)(X + x)$,

(5) $x = (1/4 + 1/5)(Y + y)$, (6) $y = (1/5 + 1/6)(Z + z)$,

(7) $z = (1/6 + 1/7)(W + w)$, (8) $W + X = \square$,

(9) $Y + Z = \triangle$, (10) $T = W + X + Y + Z + w + x + y + z$,

the symbols in (8) and (9) representing a square and triangular number respectively.

We describe here a machine computation of (the smallest value of) T, the total number of cattle, together with a couple of high-precision computing techniques that were used in this calculation, and which may be of more general interest.

Chr. Leiste found integral solutions [2, pp. 342–343] for conditions (1) to (7) obtaining

$$W = 10366482k, \quad w = 7206360k,$$
$$X = 7460514k, \quad x = 4843246k,$$
$$Y = 7358060k, \quad y = 3515820k,$$
$$Z = 4149387k, \quad z = 5439213k,$$

where k is an integer. Then

$$X + W = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657k,$$

whence

$$k = 3 \cdot 11 \cdot 29 \cdot 4657n^2, \text{ from condition (8).}$$

Now

$$Y + Z = \frac{t^2 + t}{2}, \qquad \text{by (9), for some integral value of } t,$$

which gives

$$(2t + 1)^2 = 8(Y + Z) + 1 \tag{11}$$
$$= an^2 + 1,$$

Received March 8, 1965.

where $a = 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (4657)^2$. Since a is non-square, the resulting "Pell" equation (11) may be solved for n [3, pp. 36–41].

In 1880 A. Amthor put (11) in the form [2, p. 344]:

$$(12) \qquad (2t + 1)^2 = D(2 \cdot 4657 \cdot n)^2 + 1,$$

where $D = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 = 4729494$. It is then necessary to find the least solution (P, Q) to $P^2 - DQ^2 = 1$, for which $2 \cdot 4657$ will divide Q.

By recognizing that

$$(P_m + \sqrt{DQ_m}) = (P + \sqrt{DQ})^m,$$

where (P, Q) is the first solution to (12), he showed that for $m = 2329$, (P_m, Q_m) is the required solution.

The total number of cattle is, therefore, given by the formula

$$T = c(Q_{2329}/2 \cdot 4657)^2,$$

where $c = 2 \cdot 3 \cdot 11 \cdot 29 \cdot 41 \cdot 107 \cdot 4657 \cdot 5743 = 224571490814418$.

2. Computation of T. The calculation may be best illustrated as a sequence of steps. Steps A to C were accomplished on an IBM7040, with a 32K memory, and the computation completed on an IBM1620 (II).

A. The first solution to (12) [2, p. 344] was entered into memory (6 words of storage for each of P and Q) and Q_{2329} generated by following the sequence of subscripts for P and Q below:

1, 2, 4, 8, 9, 18, 36, 72, 144, 145, 290, 291, 582, 1164, 2328, 2329 (Q_{2329} only).

These numbers were formed according to the recursion formulae [2, p. 392, p. 397],

$$P_{2n} = 2P_n^2 - 1, \qquad Q_{2n} = 2P_nQ_n,$$

$$P_{n+1} = PP_n + (DQ)Q_n, \qquad Q_{n+1} = PQ_n + QP_n.$$

Q_{2329} was then divided by $2 \cdot 4657$ and the remainder found to be zero. The time required for the completion of step A was 2 hours and 25 minutes.

B. The result of step A was squared.

As the result of squaring Q_{2329} would occupy approximately 20,000 words of core storage and Q_{2329} itself occupied 10,000 words, we felt it necessary to develop a squaring routine that would require only that space in memory that would be taken up by the product. The method of squaring used is exemplified in the following table.

A	B	C	D	E					
					EA	EB	EC	ED	$\frac{1}{2}EE$
				AD	BD	CD	$\frac{1}{2}DD$		
			AC	BC	$\frac{1}{2}CC$				
		AB	$\frac{1}{2}BB$						
	$\frac{1}{2}AA$								

Here the number to be squared is $ABCDE$ (in this case, the number base is 2^{35}). The product obtained by this means is one half of the square of $ABCDE$. It is

computed by accumulating the numbers in the columns and performing the carry-overs when necessary.

It is easily seen that the storage word E, for example, could be occupied by $AD + BC$ (and the appropriate carry-over from the adjacent column) without altering the product, since E has been completely utilized by the time of this replacement. By this means of replacing the multiplier by the product, no more than twice the number of words occupied by the multiplier were required at any time during the course of the squaring operation.

This algorithm, since it requires only one half of the number of multiplications, is twice as fast as the usual means of determining the square. The time required for the completion of Step B was 1 hour and 18 minutes.

C. We converted the result of step B from binary to decimal notation. In doing this, we increased the speed of conversion over that of the usual routing (successive divisions by 10^{10}) by a factor of 9/4. This was effected by the following procedure.

The number N to be converted was divided by 5^{15} seven times and the resulting seven remainders $(r_0, r_1, \cdots, r_6)$ stored.

Then

$$R_1 = r_0 + r_1 5^{15} + \cdots + r_6 5^{90}$$

is the remainder on dividing N by 5^{105}.

The three lowest order words containing N form the remainder on division by 2^{105}; call it R_2. Then

$$N = R_1 + K5^{105},$$

and

$$N = R_2 + M2^{105},$$

where M and K are integers. Taking congruences (Mod 5^{105}),

$$R_1 \equiv R_2 + M2^{105} \pmod{5^{105}}, \tag{13}$$

$$\text{or } M2^{105} \equiv (R_1 - R_2) \pmod{5^{105}}. \tag{14}$$

If M' is the solution of the congruence

$$M'2^{105} \equiv 1 \pmod{5^{105}}, \text{ where } M' < 0, \tag{15}$$

then the solution to (14) is

$$M \equiv (R_1 - R_2)M' \pmod{5^{105}}.$$

Thus, we have

$$M = (R_1 - R_2)M' + L5^{105},$$

where L is an integer. Putting this result into (13), we obtain

$$\begin{aligned} N &= R_1 + [(R_1 - R_2)M' + L5^{105}]2^{105} \\ &\equiv R_2 + (R_1 - R_2)M'2^{105} \pmod{10^{105}} \\ &\equiv R_2 + 2^{105}(5^{105} + M')R_1 + (-M')R_2 \pmod{10^{105}}, \end{aligned}$$

where $5^{105} + M', -M' > 0$ (this precludes the possibility of a negative remainder).

The solution to the congruence (15) was obtained by Euclid's algorithm [3, pp. 2–3] and the numbers $5^{105} + M'$, and $-M'$ were entered in the program as constants. The remainder on division by 10^{105}, found by this means, was then converted to decimal notation in the usual way.

This number (n^2) was then punched on cards. The time required to complete step C was 3 hours and 48 minutes.

The calculation was completed by multiplying n^2 by 224571490814418; this required 18 minutes including input and output operations.

The length of the number T, its first 30 digits, and its last 12 digits verify the calculations [4] performed by A. H. Bell in 1889.

The total computing time required was 7 hours and 49 minutes.

3. Analysis of the number T. The number T comprises 206545 decimal digits. A copy of T, printed on 42 computer sheets, has been deposited in the Unpublished Mathematical Tables file of this journal. The first 50 and the last 50 digits are:

$$77602714064868182695302328332138866642323224059233\cdots$$

$$\cdots 05994630144292500354883118973723406626719455081800.$$

In lieu of the actual number T, we give here instead a statistical analysis of its digits. This helps to identify the number and shows, as expected, that the digits are essentially random.

Length of run	No. of runs for each digit										Total no. of runs	Expected no. of runs
	0	1	2	3	4	5	6	7	8	9		
1	16638	16726	16858	16761	16477	16967	16974	16641	16620	16760	167422	167301.46
2	1623	1707	1707	1704	1622	1666	1662	1704	1619	1683	16697	16730.15
3	149	153	169	184	148	163	179	144	157	178	1624	1673.01
4	21	13	21	18	19	20	8	19	23	23	185	167.30
5	4	1	3	0	3	0	1	2	4	3	21	16.73
6	1	0	0	0	0	0	0	0	1	0	2	1.67
Totals for single digits	20441	20656	20878	20793	20256	20868	20872	20567	20447	20767		

The longest run of repeated digits in T is that of six eights beginning at digit number 37307 and six zeros beginning at digit number 191148; these being reckoned from the beginning of the number.

4. Acknowledgments. The authors are indebted to Dr. R. G. Stanton, and to the referee, for their suggestions, and to Professor J. W. Graham for the use of the University's Computing facilities.

University of Waterloo,
Waterloo, Ontario, Canada

1. *Selections Illustrating the History of Greek Mathematics*. Vol. II. *From Aristarchus to Pappus*, with an English translation by Ivor Thomas, Harvard Univ. Press, Cambridge, Mass. and Heinemann, London, 1951, pp. 202–205. MR **13**, 419.
2. L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea, New York, 1952.
3. H. N. Wright, *First Course in Theory of Numbers*, Wiley, New York, 1959.
4. A. H. Beiler, *Recreations in the Theory of Numbers*, Dover, New York, 1964, p. 251.