Archimedes' Cattle Problem

Ilan Vardi

A Problem

which Archimedes devised in epigrams, and which he communicated to students of such matters at Alexandria in a letter to Eratosthenes of Cyrene.

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 in four parts 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 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 of numbers, but not yet shalt thou be numbered among the wise.

But come, understand also 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 one of them lacking.

If thou art able, O stranger, to find out 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.

This problem, in the form of 22 elegiac couplets, was discovered in modern times by the German critic and dramatist G.E. Lessing who found it in the library of Wolfenbüttel, Northern Germany, where he was librarian. In 1773 he published the problem along with a scholium containing an incorrect solution [27, p. 100]; see [4, Vol. 3, p. 171] for the scholium and its French translation. The translation used here is from [33, Vol. 2, p. 202], where, following D.H. Fowler [13], the word "devised" has been used instead of "solved."

The problem is surprisingly difficult and it was not solved until a hundred years ago by Amthor [1], who showed that the complete solution consists of eight numbers each having about $206,545$ digits. The simple nature of the question and the difficulty of its solution makes this a perfect example of a challenge problem and shows once more that Archimedes is one of the greatest mathematicians of all time.

Naturally, Amthor did not write out the solution; he gave only the first four significant digits. Many accounts of the solution are based on Amthor's paper, e.g., [3], where reduction to a Pell equation is described. Several subsequent papers give detailed derivations of the solution [17].

The aim of this paper is to take the Cattle Problem out of the realm of the "astronomical" and put it into manageable form. This is achieved in formulas (12) and (13), which give explicit forms for the solution. For example, the smallest possible value for the total number of cattle satisfying the conditions of the problem is

$$\left\lceil \tfrac{25194541}{184119152} \left(109931986732829734979866232821433543901088049+50549485234315033074477819735540408986340\sqrt{4729494}\right)^{4658} \right\rceil ,$$

where $\lceil x \rceil$ is the smallest integer $\geq x$. This formula is an analog of the formula expressing the nth Fibonacci number as the closest integer to $\left((1+\sqrt{5})/2\right)^n/\sqrt{5}$. The actual digits of the above number written out take up 47 pages in [29]. Regarding the computation of the digits of a solution to the Cattle Problem, D.H. Fowler [13] comments: "I don't know what anybody would do with a solution, once found, except use it as a piece of mathematical wall–paper!"

I also show how the Cattle Problem leads to a relatively small solution by using classical formulas of analytic number theory. These results allow one to compare the size of solutions to different Pell equations, and I give an example of another Pell equation with smaller coefficients, but whose smallest solution has over 30 million digits (150 times more than the cattle problem).

Apart from this last result, the methods used depend only on some basic results of number theory and the elementary theory of finite fields. The analysis is simplified by good notation and the use of computer algebra systems (*Mathematica* and Pari) that permit some cumbersome computations to be reduced to a single computer command. The method presented here is easily amenable to computer computation (see [37] for details) and the reader can use Section 2.6 to generate a computer solution in a few hours.

1. The solution, part I

1.1. An algebraic formulation. To solve the Cattle Problem, one considers it algebraically by writing W, w for the white bulls and cows, respectively, and similarly, X, x, Y, y, Z, z for the number of black, yellow, and dappled bulls and cows. The first set of relations is

$$\begin{aligned}
&W=\left(\frac{1}{2}+\frac{1}{3}\right)X+Y\,, \quad X=\left(\frac{1}{4}+\frac{1}{5}\right)Z+Y\,, \quad Z=\left(\frac{1}{6}+\frac{1}{7}\right)W+Y\,,\\
&w=\left(\frac{1}{3}+\frac{1}{4}\right)(X+x)\,, \quad x=\left(\frac{1}{4}+\frac{1}{5}\right)(Z+z)\,, \quad y=\left(\frac{1}{6}+\frac{1}{7}\right)(W+w)\,, \quad z=\left(\frac{1}{5}+\frac{1}{6}\right)(Y+y)\,.
\end{aligned} \tag{1}$$

The additional relations are

$$W+X= \text{ a square,} \tag{2}$$

and

$$Y+Z= \text{ a triangular number,} \tag{3}$$

where a triangular number has the form $1 + 2 + 3 + \cdots + n = n(n+1)/2$.

The first part of the problem is quite easy—its solution is essentially what appears in the scholium, so it is the second part which makes the problem a difficult one. As a preliminary exercise, the reader can try solving a simple analog of the second part

Problem: In the game of pool one is given balls arranged in a square tray, but when one ball is used as the cue ball, the others can be racked in a triangle. How many balls are there?

1.2 Solving the linear system. The linear system of equations (1) is easily solved (e.g., with *Mathematica*'s `Solve` command). Letting $\mathbf{S} = (W, X, Y, Z, w, x, y, z)$ denote a solution, one gets a one–dimensional space of solutions parametrized by W

$$\mathbf{S} = \left(1, \frac{267}{371}, \frac{297}{742}, \frac{790}{1113}, \frac{171580}{246821}, \frac{815541}{1727747}, \frac{1813071}{3455494}, \frac{83710}{246821}\right) W\,.$$

Since you can't have fractional cattle, the solution has to be in integers, which you get by multiplying by the least common multiple of the denominators on the right (once again a single *Mathematica* command `LCM` does the trick). This number turns out to be 10366482 and multiplying through gives the general integer solution to the seven equations

$$\text{(4)} \quad \mathbf{S} = (10366482, 7460514, 4149387, 7358060, 7206360, 4893246, 5439213, 3515820)\, n\,, \quad \text{for } n = 1, 2, \ldots.$$

The solution given in the scholium corresponds to $n = 80$.

1.3. Wurm's problem. Actually, the language of the Cattle Problem leaves some ambiguity as to whether equation (2) refers to a square *number* of bulls or whether they form a square figure, since bulls are longer than they are wide. The latter problem requires that $W + X$ be a "rectangular" number, i.e., a nonprime. Since this amounts to ignoring condition (2), its solution is much simpler and was solved by J.F. Wurm [43], so it is called *Wurm's problem* while the former is called the *complete problem.*

To solve Wurm's problem, one needs to find a value of n for which (3) is satisfied, i.e., $Y + Z = q(q+1)/2$, and for which $W + X$ can be written as a product of two numbers whose ratio is roughly that of a bull. Using (4) $Y + Z = (4149387 + 7358060)n = 11507447n$, so this can be rewritten as $11507447n = q(q+1)/2$, or $q^2 + q - 2 \cdot 11507447n = 0$. Since q must be an integer, one is looking for n such that this quadratic has an integer solution, i.e., $\sqrt{1 + 4(2 \cdot 11507447n)}$ is an integer. Thus, a solution exists exactly when $1 + 92059576n$ is a perfect square. This can be written as $x^2 = 1 + 92059576n$ for some n. Another way to state this is to find x for which

$$\text{(5)} \qquad x^2 \equiv 1 \pmod{92059576}\,.$$

To solve this equation, one uses the Chinese Remainder Theorem, which says that a solution of (5) exists for each combination of solutions of

$$\text{(6)} \qquad x^2 \equiv 1 \pmod{d}$$

where d is a prime power factor of $92059576 = 2^3 \cdot 7 \cdot 353 \cdot 4657$.

The solutions to (6) are given by $x = 1, 3, 5, 7 \bmod 8$ and $x = \pm 1 \bmod d$ for $d = 7$, 353, and 4657. The solutions mod 92059576 are built up from these. This can be done using *Mathematica*'s implementation of the Chinese Remainder Theorem algorithm. The complete list of solutions that are greater than 1 is

$$
\begin{aligned}
&3287843, 4303069, 7590911, 15423983, 18711825, 19727051, 23014893, 23014895,\\
&26302737, 27317963, 30605805, 38438877, 41726719, 42741945, 46029787, 46029789,\\
&49317631, 50332857, 53620699, 61453771, 64741613, 65756839, 69044681, 69044683,\\
&72332525, 73347751, 76635593, 84468665, 87756507, 88771733, 92059575\,.
\end{aligned}
$$

Each of these generates a family of solutions; the smallest being 3287843. The corresponding value of n is

$$(3287843^2 - 1)/92059576 = 117423\,.$$

Letting $n = 117423$ in (4) yields the solution

$$
\begin{aligned}
&(1217263415886, 876035935422, 487233469701, 864005479380,\\
&\quad 846192410280, 574579625058, 638688708099, 412838131860)\,,
\end{aligned}
$$

and the total number of cattle is 5916837175686.

To check conditions (2) and (3) note that

$$W + X = 2093299351308 = 2^2 \cdot 3^4 \cdot 11 \cdot 29 \cdot 4349 \cdot 4657\,,$$

is not prime; the closest representation to a square is $W + X = 1409076 \cdot 1485583$. Moreover, $Y + Z = 487233469701 + 86400547938 = 573634017639$, and the equation $q^2 + q - 2 \cdot 573634017639 = 0$ has the positive solution $q = 1643921$, so

$$Y + Z = \frac{1643921(1643921 + 1)}{2}\,,$$

as required.

2. The solution, part II

2.1. Reduction to the Pell equation. The solution to the complete problem requires satisfying the extra condition that $W + X$ is a square. From (4), one has

$$W + X = (10366482 + 7460514)n = 17826996n\,.$$

One can get information about n by looking at the factorization $17826996 = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657$, which shows that $2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657\, n$ is a square and thus

$$n = 3 \cdot 11 \cdot 29 \cdot 4657\, m^2 = 4456749 m^2\,,$$

for some integer m. Inserting this in (4) gives

$$
\begin{aligned}
\mathbf{S} = (&46200808287018, 33249638308986, 18492776362863, 32793026546940,\\
&32116937723640, 21807969217254, 24241207098537, 15669127269180)\, m^2\,.
\end{aligned}
\tag{7}
$$

As before, $Y+Z$ must be a triangular number, i.e.,

$$Y+Z=(18492776362863+32793026546940)m^2=51285802909803m^2=\frac{q(q+1)}{2}\,,$$

so one solves $q^2+q-2\cdot 51285802909803m^2=0$, which has an integer solution exactly when $1+4\cdot 2\cdot 51285802909803m^2$ is a square, i.e., it has solution $(k-1)/2$ if

$$1+410286423278424m^2=k^2\,, \tag{8}$$

for some k. Equation (8) is the well–known *Pell's equation* from number theory [31].

If we factor

$$410286423278424=2^3\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353\cdot 4657^2\,,$$

(8) can be written as $1+2\cdot3\cdot7\cdot11\cdot29\cdot353(2\cdot4657m)^2=k^2$, which, upon noting that $4729494=2\cdot3\cdot7\cdot11\cdot29\cdot353$, is equivalent to

$$k^2-4729494\ell^2=1\,, \tag{9}$$

where ℓ is divisible by 2 and by 4657.

Remarks: According to the analysis of Section 3.9, one should actually look at the equation $x^2-4\cdot 4729494\,y^2=4$. This equation is equivalent to (9) since x must be an even number, so dividing by 4 gives $(x/2)^2-4729494\,y^2=1$, which is the same as (9).

The reader should have similarly reduced the Pool Problem to the equation $x^2-2y^2=-7$, which is solved by finding its minimal solutions and combining them with solutions to the Pell equation $u^2-2v^2=1$.

2.2. Solution of Pell's equation using continued fractions. It is known [13, Chapter 9] [24, Section 4.5.3] that every real number can be expanded as a continued fraction. For example

$$\begin{aligned}
\pi &= 3.141592653\ldots = 3 + .141592653\ldots \\
&= 3 + \frac{1}{7.062513305\ldots} = 3 + \frac{1}{7 + .062513305\ldots} \\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15.99659440\ldots}} = 3 + \cfrac{1}{7 + \cfrac{1}{15 + .99659440\ldots}} \\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1.003417231\ldots}}} = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + .003417231\ldots}}} \\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292.63459088\ldots}}}} = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 \quad + \ddots}}}}
\end{aligned}$$

which is conventionally written, for typographical convenience, as $\pi = [3, 7, 15, 1, 292, \ldots]$. A representation of this type terminates only if the number is rational. Good approximations occur when one truncates the expansion, especially just before a large coefficient. For example, $\pi \approx [3, 7] = 3 + 1/7 = 22/7$, and a much better approximation is given by $[3, 7, 15, 1] = 355/113$. In fact, it can be shown that such truncations give *optimal* approximations in the following sense: if p/q is an approximation from truncation then p'/q' is a poorer approximation for any $1 \leq q' < q$.

The point is that solutions to the Pell equation (9) give very good approximations to $\sqrt{4729494}$ in the sense that k/ℓ is very close to $\sqrt{4729494}$. To see this, divide by ℓ in (9) and factor as a difference of squares to get

$$\left| \frac{k}{\ell} - \sqrt{4729494} \right| = \frac{1}{\ell\,(k + \ell\sqrt{4729494})}\,,$$

where the right hand side is $< 1/(2\ell^2)$, which implies that k/ℓ comes from truncating the continued fraction expansion of $\sqrt{4729494}$ [31, p. 339]

The continued fraction expansion of the square root of an integer is periodic [31] and the optimal approximation property implies that cutting off the expansion at multiples of the length of the period yields rational numbers whose numerator and denominator are solutions to the Pell equation (9). An algorithm for solving (9) is then: (a) expand $\sqrt{4729494}$ as a continued fraction (analogous to the expansion of π above), (b) write out each partial result as a rational fraction and test the numerator and denominator [8, Section 5.7]. This algorithm does not come as a standard package in *Mathematica* but implementing this special case takes only a few lines [37]; Stan Wagon has written a general program [39]. In fact, this computation can be done by hand without too much difficulty and [1] gives an explicit description of the intermediate steps. This method yields

$$\begin{aligned}\sqrt{4729494} = [&2174,1,2,1,5,2,25,3,1,1,1,1,1,1,15,1,2,16,1,2,1,1,\\ &8,6,1,21,1,1,3,1,1,1,2,2,6,1,1,5,1,17,1,1,47,3,1,1,\\ &6,1,1,3,47,1,1,17,1,5,1,1,6,2,2,1,1,1,3,1,1,21,1,6,\\ &8,1,1,2,1,16,2,1,15,1,1,1,1,1,1,3,25,2,5,1,2,1,4348,\ldots],\end{aligned}$$

where truncating the expansion just before 4348 (the last number in the period) gives the rational number

$$\frac{109931986732829734979866232821433543901088049}{50549485234315033074477819735540408986340},$$

which in turn yields the minimal solution to (9):

$$k = 109931986732829734979866232821433543901088049,$$

$$\ell = 50549485234315033074477819735540408986340.$$

Computing these numbers took less than one second. It is a basic result of number theory [31] that this minimal solution gives a "fundamental solution"

$$\begin{aligned}\varepsilon = &\ 109931986732829734979866232821433543901088049\\ &+ 50549485234315033074477819735540408986340\sqrt{4729494}\end{aligned}$$

in the sense that all other solutions to the Pell equation (9) are of the form k_d and ℓ_d where $\varepsilon^d = k_d + \ell_d\sqrt{4729494}$.

We must find a d for which ℓ_d is divisible by 2 and by 4657. Since 4729494 is even, in any solution to $k^2 - 4729494\ell^2 = 1$, k must be odd, so $k^2 \equiv 1 \pmod 8$. Since 4729494 is not divisible by 4, ℓ must be even. Thus, it suffices to find a solution of this equation for which ℓ is divisible by 4657, i.e., a power ε^n for which ℓ is divisible by 4657.

Remark: The methods of this section show that the Pool Problem has solution any number $(b/2)^2$, where $a + b\sqrt{2} = (1 \pm 2\sqrt{2})(1+\sqrt{2})^{2n}\,,\quad n = 1, 2, \ldots.$

2.3. Using modular arithmetic to speed up the search. The search is greatly simplified by using congruences modulo 4657. One can generalize arithmetic modulo 4657 to include terms of the form $a + b\sqrt{4729494}$; in fact, one can replace $\sqrt{4729494}$ with $\sqrt{4729494 \bmod 4657} = \sqrt{2639}$ in the sense that in all addition and multiplication operations, the coefficients are the same modulo 4657, and so $\varepsilon \equiv 4406 + 3051\sqrt{2639} \pmod{4657}$. This type of arithmetic yields a *finite field,* i.e., all arithmetic operations including division are allowed [19, Section 7.1]. Moreover, since 2639 is not a perfect square modulo 4657 (*Mathematica*'s `JacobiSymbol` function verifies this) this field is a *quadratic extension* of $\mathbf{Z}/4657\mathbf{Z}$.

Let $p = 4657$ and $D = 4729494$. Since $1/\varepsilon^d = k_d - \ell_d\sqrt{D}$, one has to check that $\varepsilon^d - 1/\varepsilon^d \equiv 0 \pmod p$, so one is solving

$$\varepsilon^{2d} \equiv 1 \pmod p\,. \tag{10}$$

It is a fundamental result [19, Section 7.1] that $x^{p^2-1} \equiv 1 \pmod p$ for any x in this field, so any d satisfying (10) must be a divisor of $(p^2-1)/2$. Thus, one needs to check only the divisors d of $(p^2-1)/2$ by taking modular powers $\varepsilon^{2d} \bmod p$.

Amthor [1] further showed that only the divisors of $p+1$ need to be checked, but H.W. Lenstra [26] brought to my attention that a further reduction to just the divisors of $(p+1)/2$ is possible, i.e., that $\varepsilon^{p+1} \equiv 1 \pmod p$. To prove this last reduction, note that in our finite field x^p equals the *conjugate* of x, i.e., if $x = a + b\sqrt{D}$ then $x^p \equiv a - b\sqrt{D} \pmod p$ as follows from the computation

$$x^p = \sum_{k=0}^{p} a^k (b\sqrt{D})^{p-k} \binom{p}{k} \equiv a^p + D^{(p-1)/2}\, b^p \sqrt{D} \equiv a - b\sqrt{D} \pmod p\,,$$

where the following elementary number theory facts have been used [31]: (a) $\binom{p}{k}$ is divisible by p for $k = 1, \ldots, p-1$, (b) $n^p \equiv n \pmod p$ for any integer n, (c) $D^{(p-1)/2} \equiv -1 \pmod p$ when D is not a perfect square $\bmod\, p$. One therefore concludes that

$$\varepsilon^{p+1} \equiv (k + \ell\sqrt{D})(k - \ell\sqrt{D}) \pmod p = 1\,,$$

where the last equality follows from (9).

One can now proceed with the divisibility test. First, let $\gamma = \varepsilon^2 \bmod 4657$ so that $\gamma = 262 + 551\sqrt{2639}$. Exponentiation can be done efficiently by repeated squaring and by reducing $\bmod\, 4657$ at each step [36, Chapter 1]; Amthor [1] used this method. Each exponentiation $\gamma^d \pmod{4657}$ takes about $\log d$ modular operations. Since $4658/2 = 17 \cdot 137$, there are only two cases to check and one quickly finds $d = 2329$. It follows from basic algebra that any solution of (10) is of the form $d = 2329n$, where $n = 1, 2, 3, \ldots$.

2.4. Explicit formulas. We now know that all solutions to (9) are given by $k = \alpha_n$, $\ell = \beta_n$, where

$$\varepsilon^{2329n} = \alpha_n + \beta_n\sqrt{4729494}\,, \quad n = 1, 2, \ldots.$$

Recalling that the value of m in (8) was derived from the value of ℓ in (9) by $m = \ell/(2 \cdot 4657)$, it follows that $m = \beta_n/(2 \cdot 4657)$. Using

$$\frac{1}{\alpha_n + \beta_n\sqrt{4729494}} = \alpha_n - \beta_n\sqrt{4729494}\,,$$

one has

$$\beta_n = \frac{1}{2\sqrt{4729494}} \left(\varepsilon^{2329n} - \frac{1}{\varepsilon^{2329n}}\right)\,,$$

which means that

$$m^2 = \frac{1}{4 \cdot 410286423278424} \left(\varepsilon^{4658n} + \frac{1}{\varepsilon^{4658n}} - 2\right)\,. \tag{11}$$

Using this value in (7) gives

$$\mathbf{S} = \left(\frac{159}{5648}, \frac{801}{39536}, \frac{891}{79072}\frac{395}{19768}, \frac{128685}{6575684}, \frac{2446623}{184119152}, \frac{5439213}{368238304}, \frac{125565}{13151368}\right) \left(\varepsilon^{4658n} + \frac{1}{\varepsilon^{4658n}} - 2\right)\,. \tag{12}$$

Note that

$$-1 < \frac{159}{5648}\left(\frac{1}{\varepsilon^{4658n}} - 2\right) < 0\,,$$

so

$$W = \left\lceil \frac{159}{5648}\,\varepsilon^{4658n} \right\rceil\,.$$

The same holds for the other variables, so for each $n = 1, 2, 3, \ldots$, a complete solution is given by

$$\mathbf{S} = \left\lceil \left(\frac{159}{5648}, \frac{801}{39536}, \frac{891}{79072}\frac{395}{19768}, \frac{128685}{6575684}, \frac{2446623}{184119152}, \frac{5439213}{368238304}, \frac{125565}{13151368} \right) \varepsilon^{4658n} \right\rceil , \tag{13}$$

where $\lceil \mathbf{V} \rceil$ for a vector of real numbers means that $\lceil \cdot \rceil$ is applied to every entry. Similarly, the total number of cattle is

$$\left\lceil \frac{25194541}{184119152} \varepsilon^{4658n} \right\rceil .$$

2.5. Approximate formulas. A nice feature of formula (13) is that it immediately gives approximate formulas. For example, the smallest possible value of W is $\approx \frac{159}{5648} \varepsilon^{4658}$ with error less than one, so approximating ε gives a good approximation to the final answer. If asked to approximate ε to 60 digits, *Mathematica* responds with

$$\varepsilon \approx 219863973465659469959732465642867087802176098.$$

Note that only 45 digits are given even though 60 digits of an irrational number were asked for. Actually *Mathematica* is doing the right thing, and what is going on is that $\varepsilon + 1/\varepsilon$ is an integer and $1/\varepsilon$ is very small. In fact, to 100 digits,

$$\varepsilon = 219863973465659469959732465642867087802176097.9999999999999999999999999999999999999999999954517332501\ldots$$

One then has

$$\varepsilon^{4658} \approx 5.671127688542531014809969777238244773907823652628606272641 19 \cdot 10^{206545} .$$

Using this in (13) with $n = 1$ gives an approximation to the smallest complete solution

$$\begin{aligned}
(&1.596510804671144531435526194371248086139065086345517700690 42,\\
&1.148971387728289999712359821825130024256416113353782280550788,\\
&.639034648230902865008559676183639732592051658550699133564764,\\
&1.133192754438638077119555879203311759254143232895740326635608,\\
&1.109829892373319039723960215825309623653339008897800134852635,\\
&.753594142054542639814429119589686473435022187613875093482301,\\
&.837676882418524438692221984108458338745267934241979330049041,\\
&.541460894571456678023619942107102626157017184023982103325062) \cdot 10^{206544},
\end{aligned}$$

so the total number of cattle is approximately

$$7.760271406486818269530232833213886664232322405923376103150 62 \cdot 10^{206544} .$$

Similarly, one can find the next solution by letting $n = 2$ in (13) and approximating. For example, the total number of cattle is approximately

$$4.400949004393228581671923516934836986419423493402088107901 42 \cdot 10^{413090} .$$

2.6. Generating exact solutions. Of course, one could have done the same computations with more than 60-digit accuracy, but it is interesting to see whether computer algebra systems can handle the *exact* answer. To do this, one uses the same method but with the explicit formula (12). This can be done by noting that the term

$$\frac{1}{2}\left(\varepsilon^{4658n}+\frac{1}{\varepsilon^{4658n}}-2\right)$$

is equal to $a_n - 1$, where $\varepsilon^{4658n} = a_n + b_n\sqrt{4729494}$. This has the computational advantage that a_n is easily extracted from the expression $a_n + b_n\sqrt{4729494}$. The exact solution is then given by

$$\mathbf{S} = \left(\frac{159}{2824}, \frac{801}{19768}, \frac{891}{39536}, \frac{395}{9884}, \frac{128685}{3287842}, \frac{2446623}{92059576}, \frac{5439213}{184119152}, \frac{125565}{6575684}\right)(a_n - 1)\,, \tag{14}$$

while the total number of cattle is

$$\frac{25194541}{92059576}\,(a_n-1)\,.$$

Formula (14) was used to generate the complete solution for $n = 1$ (the smallest possible solution). The main step was computing ε^{4658} exactly. This was done by repeated squaring, in other words, writing

$$x^{4658} = ((((x^{2^3}\cdot x)^{2^4}\cdot x)^2\cdot x)^{2^3}\cdot x)^2$$

so that computing ε^{4658} took 16 multiplications instead of 4657. The computation was done on a Sun (!) workstation using *Mathematica* and took one and a half hours, of which a half hour was spent computing ε^{4658} (the final multiplication step was simplified); one hour was required for the 8 multiplications in (14). The result was saved to a file of size 1,788,196 bytes. A similar computation for $n = 2$ took three hours.

2.7. Least significant digits. One can easily compute the least significant digits of a solution. This is important, as it is a good check that a complete answer is correct. For example, to compute the 13 least significant digits of the smallest solution, one considers

$$\varepsilon_{13} = \varepsilon \bmod (16\cdot 10^{13}) = 153543901088049 + 55540408986340\sqrt{4729494}\,;$$

I use $16\cdot 10^{13}$ instead of 10^{13} because a division by 16 follows. One then uses repeated squaring modulo $16\cdot 10^{13}$ to obtain

$$\varepsilon_{13}^{4658} \equiv 40903550724801 + 147391701494280\sqrt{4729494}\ (\bmod\, 16\cdot 10^{13})\,.$$

The answer is then obtained by substituting 40903550724801 for a_n in (14) and computing the result modulo 10^{13}

$$\begin{aligned}
&\left(\frac{159}{2824}, \frac{801}{19768}, \frac{891}{39536}, \frac{395}{9884}, \frac{128685}{3287842}, \frac{2446623}{92059576}, \frac{5439213}{184119152}, \frac{125565}{6575684}\right) 40903550724800\\
&= \left(\frac{812958070655400}{353}, \frac{4095468016320600}{2471}, \frac{2277816480987300}{2471}, \frac{4039225634074000}{2471},\right.\\
&\qquad \left.\frac{2631836712510444000}{1643921}, \frac{12509445998120293800}{11507447}, \frac{13905195303030723900}{11507447}, \frac{1284013586689878000}{1643921}\right)\\
&\equiv (9385150341800, 2899825178600, 8635296026300, 3921175894000,\\
&\qquad 5914059564000, 7238562645400, 2116422113700, 6608963318000)\ (\bmod\, 10^{13})\,.
\end{aligned}$$

The 13 least significant digits of the total number of cattle are 6719455081800.

A similar computation can be done for larger values of n. For example, for $n = 2$, the last 13 digits of the total number of cattle are 9744397607200.

Remark: I used *Mathematica*'s `PowerMod` function to find the modular inverses

$$\left(\frac{1}{353}, \frac{1}{2471}, \frac{1}{1643921}, \frac{1}{11507447}, \frac{1}{1643921}\right)$$

$$\equiv (8328611898017, 5475515985431, 2967216794481, 6138173827783, 2967216794481) \pmod{10^{13}}.$$

3. The relative size of the solution

One way to estimate the relative size of the solution to the Cattle Problem is to study the sizes of fundamental solutions to different Pell equations. After looking at many numerical cases, one would guess that the number of digits of a fundamental solution of $x^2 - d\,y^2 = 1$ is very roughly about $\sqrt{d}$. This is true, and the exact behavior is given by an important formula of analytic number theory, *Dirichlet's class number formula,* proved by him in 1839 in order to show that there are infinitely many primes in arithmetic progressions [9, Chapter 4]. It states that for d a squarefree number

$$\log \varepsilon_D = \frac{L(1,\chi_D)\sqrt{D}}{2h_D}\,, \tag{15}$$

where $D = d$ if d is of the form $4k+1$, and $D = 4d$ otherwise, $\varepsilon_D = (x + y\sqrt{D})/2$, where x, y give the smallest solution of $x^2 - Dy^2 = \pm 4$, and h_D is a positive integer called the *class number,* while $L(1,\chi_D)$ is the infinite series $\sum_{n=1}^{\infty} (D/n)/n$, where $(D/\cdot)$ is Kronecker's extension of the Legendre symbol.

A simple computation shows that the fundamental solution of $x^2 - Dy^2 = 1$ corresponds to ε_D when D is not of the form $4k+1$ (as in the Remark of Section 2.1); otherwise, it corresponds to

(i) ε_D when $x^2 - Dy^2 = -1$ has no solution and $x^2 - Dy^2 = 4$ has no solution with odd x, y,

(ii) ε_D^2 when $x^2 - Dy^2 = -1$ has a solution, and $x^2 - Dy^2 = 4$ has no solution with odd x, y,

(iii) ε_D^3 when $x^2 - Dy^2 = -1$ has no solution and $x^2 - Dy^2 = 4$ has a solution with odd x, y,

(iv) ε_D^6 when $x^2 - Dy^2 = -1$ has a solution and $x^2 - Dy^2 = 4$ has a solution with odd x, y.

The equation $x^2 - D\,y^2 = -1$ is called the *negative Pell equation*; an arithmetic characterization (e.g., congruence conditions) of the D for which it has a solution remains an open problem [7, Chapter 9]. Similarly, there does not seem to be a simple characterization of the D for which $x^2 - Dy^2 = \pm 4$ has a solution with odd x, y.

This implies that for a given class number and size of $L(1,\chi_D)$, the size of the fundamental solution to the Pell equation (15) is smallest when D is not of the form $4k+1$; otherwise it is the same size in case (i), its logarithm is about twice as big in case (ii), 3 times bigger in case (iii), and 6 times bigger in case (iv). Since the Cattle Problem yields a number not of the form $4k+1$, its solution is minimal in this respect.

Another influence on the size of ε_D is $L(1,\chi_D)$, which can be estimated by assuming the Generalized Riemann Hypothesis. Littlewood [28] showed that the GRH implies the asymptotic bounds

$$\frac{\pi^2}{12\,e^{\gamma}\log\log D} < L(1,\chi_D) < 2\,e^{\gamma}\log\log D\,.$$

For $D = 4 \cdot 4729494$ this gives $0.163826 < 1.50236 < 10.0407$, which shows that $L(1, \chi_D)$ is neither very large nor very small.

The most important factor affecting the relative size of ε_D is the class number, since $\log \varepsilon_D$ is inversely proportional to h_D. Genus theory, first developed by Gauss in [15] (see [7] for a modern treatment), shows that the class number is divisible by 2^{t-1}, where t is the number of distinct prime divisors of D. So in this case, $h(4 \cdot 4729494)$ is divisible by 32 and Pari [8] finds this to be the actual number. This is a large value (the class number is conjectured to be 1 infinitely often) so the fundamental solution in this case is relatively small. But since the process leading to the Pell equation (9) results in a highly composite d, general "Cattle Problems" always yield relatively small solutions.

This can be illustrated by comparing with other numbers in the same range. Consider a D that has class number one and for which there is a solution to $x^2 - Dy^2 = -4$ with odd x, y. This is true for $p = 18916669$, a prime slightly smaller than than $4 \cdot 4729494$. The period of the continued fraction of $\sqrt{p}$ is 6831, but in this case *two periods* are required. The fundamental solution to $x^2 - p\,y^2 = 1$ is given by $x \approx 7.6442 \cdot 10^{7061}$, $y \approx 1.7575 \cdot 10^{7058}$. If 18916669 were substituted for $4 \cdot 4729494$, the solution to the Cattle Problem would have over 30 million digits.

In the other direction, one can get smaller solutions by picking highly composite numbers not of the form $4k + 1$. For example, $d = 13123110 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23$, which has corresponding class number $h(4d) = 320$. The continued fraction expansion of $\sqrt{d}$ has period 8, and the fundamental solution to $x^2 - d\,y^2 = 1$ is $x = 43471$, $y = 12$. The Cattle Problem with this d substituted for 4729494 would have only twenty thousand digits.

4. Historical remarks

4.1. The Cattle of the Sun play a pivotal role in the *Odyssey*, where they are mentioned in the *proem* (the prologue) [22, I, line 6]: "Yet even so he did not save his comrades, for all his desire, for through their own blind folly they perished—fools, who devoured the cattle of Helios Hyperion; whereupon he took from them the day of their returning." The fact that this is the only adventure mentioned in the proem has been the subject of much debate [16], [40]. The Odyssey specifies the number of cattle [22, XII, line 127]: "And you will come to the island of Thrinacia. There in great numbers feed the cattle of Helios and his sturdy flocks, seven herds of cattle and as many fine flocks of sheep, and fifty in each. These bear no young, nor do they ever die. . . " G.E. Dimock [11] suggest that 350 alludes to the number of days and nights in a year.

The Cattle Problem identifies Thrinacia with Sicily, where Archimedes lived. Evidence for this has been given by interpreting Thrinacia to mean "three–cornered," which describes Sicily [20, p. 133] while Thucydides [34, Book VI, 2] gives Trinacria as the original name for Sicily.

4.2. History of the computation. Amthor [1] was the first to tackle the complete problem and gave the values $W \approx 1.598 \cdot 10^{206544}$, total cattle $\approx 7.766 \cdot 10^{206544}$, which are both off in the fourth-most significant digit. On the other hand, [6] gives these numbers to 32 significant digits, which are correct up to the 30th digit. Also given are the correct 12 least significant digits. These results were the fruit of 4 years of labour from 1889 to 1893 by A.H. Bell, E. Fish, and G.H. Richard, constituting the Hillsboro, Illinois, Mathematical Club. The length of this computation suggests that they did not use a fast exponentiation algorithm.

With the advent of computers came the first complete solution by H.C. Williams, R.A. German, and

C.R. Zarnke at the University of Waterloo in 1965 [42]. The actual digits of the smallest total number of cattle were published by H.L. Nelson in [29] (also reported in [30]), who used a CRAY–1 computer in 1981 to find the smallest solution in about 10 minutes. This was not considered enough to serve as a "proper" test, so the program went on to compute the next five sets of solutions.

4.3. Could Archimedes have solved this problem? It has been debated whether Archimedes actually posed the problem. The generally accepted view [10] [3] is that of Krumbiegel [25] who claims that though the text of the problem was not written by Archimedes, the problem itself is probably due to Archimedes. For example, Krumbiegel cites the Scholia to Plato's *Charmides* 165E [33, Vol. 1, p. 17], where one finds a reference to a problem "called by Archimedes the Cattle–problem."

F.O. Hultsch [32, II.1, p. 534] [3, p. xxxv] [10, p. 399] hypothesized that Archimedes wrote the problem in response to Apollonius' improvement on his measurement of the circle and Apollonius' treatise on naming large numbers that rivaled the one in the *Sand Reckoner*. Knorr [23, p. 295] speculates that Eratosthenes composed the first part of the problem, and that the second part is Archimedes' response. The former hypothesis was the inspiration for the title of the recent book *Archimedes' Revenge* [21].

It seems very unlikely that Archimedes would have been able to solve the complete problem due to the tremendous size of the answer. A better question is whether Archimedes knew that a solution *exists.* Due to the size of the coefficient in the resulting Pell equation, knowing how to solve this special case amounts to knowing how to solve a general Pell equation, which, according to A. Weil [41, p. 19], would depend, explicitly or not, upon the construction of the continued fraction of $\sqrt{D}$. Continued fractions were known in Archimedes' time, and D.H. Fowler [14] makes a convincing argument that continued fractions were fundamental in the way ratios were understood by Greek mathematics of the time. Pell's equation is mentioned in work of that period, in particular, Theon of Smyrna (circa 130 A.D.), who gave the approximations $3:2$, $7:5$, $17:12$, to $\sqrt{2}:1$, together with a rule for generating them ($7 = 3 + 2 \times 2$, $5 = 3 + 2, \ldots$ etc.); these are the convergents of $\sqrt{2}$ and the rule is equivalent to finding all solutions of the Pell equation $x^2 - 2y^2 = \pm 1$ from the fundamental solution. Furthermore, Archimedes' own paper *The Measurement of the Circle* contains very good approximations to square roots of integers, in particular, the approximation $1351 : 780$ to $\sqrt{3} : 1$, which corresponds to the sixth solution to the Pell equation $x^2 - 3y^2 = 1$, in the sense that $1351 + 780\sqrt{3} = (2 + \sqrt{3})^6$.

One can imagine that, having solved some simple problems leading to Pell's equation (such as the Pool Problem), Archimedes came to believe that all such problems had solutions. In fact Fowler [13] has proposed simple forms of the Cattle Problem that can be solved by hand. However, actually *proving* that Pell's equation always has a solution is a subtle problem, which was also posed as a challenge by Fermat and was finally solved completely by Lagrange [14, p. 335]. To underscore this point, let me note that there are still important open problems regarding the Pell equation, e.g., understanding the negative Pell equation. It therefore seems unlikely that Archimedes could have *known* that a large Pell equation always has a solution.

If Archimedes had solved the problem, then one can speculate, [32] that he might have expressed it using the system developed in the *Sand Reckoner* [3, p. 227], though the evidence [14, p. 225] [38] is that Archimedes only intended his system as a way of expressing large powers of 10. Archimedes' solution for the smallest number of total cattle would have been:

7 units of 2 myriad 5819th numbers, and 7602 myriad 7140 units of 2 myriad 5818th numbers,

and 6486 myriad 8182 units of 2 myriad 5817th numbers,…, and 9737 myriad 2340 units of 3rd numbers, and 6626 myriad 7194 units of 2nd numbers, and 5508 myriad 1800.

5. Acknowledgement.

The comments of C. Davis, D.H. Fowler, and H.W. Lenstra were most valuable. I would also like to thank T. Lengyel, I. Rivin, and S. Wagon, of Occidental College, Caltech, and Macalester College, respectively, where this paper was written.

References

[1] A. Amthor, Das Problema bovinum des Archimedes, *Zeitschrift für Math. u. Physik (Hist. litt. Abtheilung)* **25** (1880), 153–171.

[2] R.C. Archibald, The Cattle Problem of Archimedes, *Amer. Math. Monthly* **25** (1918), 411–414.

[3] Archimedes, *The Works of Archimedes,* edited in modern notation with introductory chapters by T.L. Heath, Dover, New York, 1953. Reprinted (translation only) in *Great Books of the Western World, Vol. 11,* R.M. Hutchins, editor, Encyclopaedia Britannica, Inc., Chicago, 1952.

[4] Archimède, *Oeuvres, 3 vol.,* texte établi et traduit par C. Mugler, Les Belles Lettres, Paris, 1970–71.

[5] A.H. Beiler, *Recreations in the Theory of Numbers,* Dover, New York, 1964.

[6] A.H. Bell, "Cattle Problem," by Archimedes 251 B.C., *Amer. Math. Monthly* **2** (1895), 140.

[7] D.A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations,* Springer–Verlag, New York, 1989.

[8] H. Cohen, *A Course in Computational Algebraic Number Theory,* Springer Verlag, New York, 1993.

[9] H. Davenport, *Multiplicative Number Theory,* Second Edition, Springer Verlag, New York, 1980.

[10] E.J. Dijksterhuis, *Archimedes,* Princeton University Press, Princeton, 1987.

[11] G.E. Dimock, *The Unity of the Odyssey,* University of Massachusetts Press, Amherst, MA, 1989.

[12] H. Dörrie. *100 Great Problems of Elementary Mathematics*, Dover, New York, 1965.

[13] D.H. Fowler, *Archimedes' "Cattle Problem" and the pocket calculating machine,* University of Warwick, Math. Inst. Preprint 1980, supplemented 1981.

[14] D.H. Fowler, *The Mathematics of Plato's Academy: A New Reconstruction,* Clarendon Press, Oxford, 1987.

[15] C.F. Gauss, *Disquisitiones Arithmeticae,* translated by A.A. Clarke, revised by W.C. Waterhouse, C.G. Greither, and A.W. Grootendorst, Springer–Verlag, New York 1986.

[16] B.A. Van Groningen, The proems of the Iliad and the Odyssey, *Mededeelingen der Koninklijke Nederlandsche Akad. van Wetenschappen, Afd. Letterkunde N.R.* 9, 8 (1946), 279–94.

[17] C.C. Grosjean and H.E.D. Meyer, A new contribution to the mathematical study of the cattle–problem of Archimedes, in T. M. Rassias (ed.) *Constantin Carathéodory: An International Tribute,* World Scientific, Singapore, 1991, pp. 404–453.

[18] J.G. Hermann, *De archimedis problemate bovino,* Leipzig, 1828.

[19] I.N. Herstein, *Topics in Algebra, Second Edition,* Wiley, New York, 1975.

[20] A. Heubeck and A. Hoekstra, *A Commentary on Homer's Odyssey, Vol. II,* Clarendon Press, Oxford, 1989.

[21] P. Hoffman, *Archimedes' Revenge,* Norton, New York, 1988.

[22] Homer, *The Odyssey,* translated by A.T. Murray, revised by G.E. Dimock, Loeb Classical Library **104, 105**, Harvard University Press, Cambridge, MA 1995.

[23] W. Knorr, *The Ancient Tradition of Geometric Problems,* Birkhäuser, Boston, 1986.

[24] D.E. Knuth, *The Art of Computer Programming, Volume 2, Seminumerical Algorithms,* Second Edition, Addison–Wesley, Reading, MA, 1981.

[25] B. Krumbiegel, Das problema bovinum des Archimedes, *Zeitschrift für Math. u. Physik (Hist. litt. Abtheilung)* **25** (1880), 121–136.

[26] H.W. Lenstra, Jr., Electronic mail, February 24, 1997.

[27] G.E. Lessing, *Sämmtliche Schriften,* herausgegeben von K. Lachmann, besort durch F. Munker, Leipzig, Band 12, 1897.

[28] J.E. Littlewood, On the class number of the corpus $P(\sqrt{-k})$, *Proc. London Math. Soc.* **28** (1928), 358–372.

[29] H.L. Nelson, A solution to Archimedes' Cattle Problem, *J. Recreational Math.* **13** (1981), 162–176.

[30] H.L. Nelson, Oxen of the Sun, *Scientific American* **245** (1981) no. 1, p. 84.

[31] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers,* Fifth Edition, Wiley, New York, 1991.

[32] A.F. Pauly, *Paulys Real–Encyclopädie der classischen Altertumswissenschaft,* Neue Bearbeitung begonnen von G. Wissowa fortgeführt von W. Kroll und K. Mittelhaus. J.B. Metzler, Stuttgart and Munich, 1894–1996.

[33] I. Thomas, *Greek Mathematical Works,* Loeb Classical Library **335**, **362**, Harvard University Press, Cambridge, MA, 1980.

[34] Thucydides, *History of the Peloponnesian War, Books V and VI,* translated by C.F. Smith, Loeb Classical Library **110**, Harvard University Press, Cambridge, MA, 1992.

[35] M. Trott, *The Mathematica Guidebook*, Telos, Springer Verlag, New York, (to appear).

[36] I. Vardi, *Computational Recreations in Mathematica,* Addison–Wesley, Reading, MA, 1991.

[37] I. Vardi, *The Art of Symbolic Computation,* Telos, Springer Verlag, New York, (in preparation).

[38] I. Vardi, *Archimedes, the Sand Reckoner*, preprint 1997.

[39] S. Wagon, *The Mathematica Explorer,* Wolfram Media, Inc., Champaign, IL, 1997.

[40] T.R. Walsh, Odyssey 1.6–9: A little more than kine, *Mnemosyne* **48** (1995), 385–410.

[41] A. Weil, *Number Theory, An approach through history, From Hammurapi to Legendre,* Birkhäuser, Boston, 1984.

[42] H.C. Williams, R.A. German, and C.R. Zarnke, Solution of the Cattle Problem of Archimedes, *Math. Comp.* **19** (1965), 671–674.

[43] J.F. Wurm, *Jahrbücher für Philologie und Pädagogik* **14** (1830), 194.

Mathematics Department
Occidental College, Los Angeles, CA 90041
`ilan@math.stanford.edu, www.oxy.edu/~ilan/`