OF CATTLE AND CRYPTANALYSIS

I. THE COWS OF THE MOON

Much has been written about the “Cattle of the Sun”, a counting problem due to Archimedes which ends up with about $7 \times 10^{206,545}$ cows grazing on a field in Sicily. Far less known is the herd that, once upon a time, devoured all the fields on the moon.

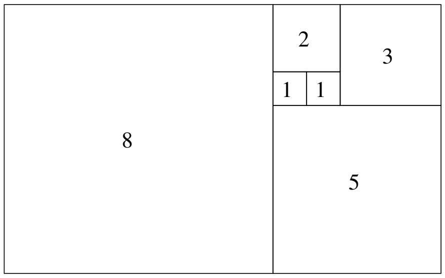
The man in the moon had a curious method of procuring cattle. He was in possession of 11 magical square carpets which would expand to accomodate any *square* number of cows, and waft them up to the moon on a space elevator. (In order that the load balance, the carpets were required to bear the *same number* of cattle each.) Once there, they had to fit inside a square fence with his dog, which is to say that the total number of creatures had also to be square.

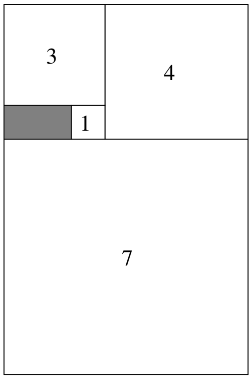
Problem 1. What is the smallest number of cattle the man in the moon could have purchased?

Problem 2. Unfortunately, that small number can’t explain the present day moonscape, created when the cows jumped over the fence to escape the vicious moondog and gobbled up all the grass. It is believed that their number was in the millions. Can you deduce the exact number of cattle now? (Don’t spend *too* much time on this until you’ve seen page 3.)

II. CATTLE OF THE RED PLANET

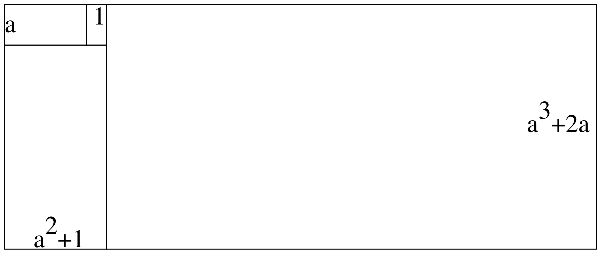
The ranchers on Mars, meanwhile, had their own problems: their herd kept growing, and the Martian grass didn't grow back once it was eaten. So they kept having to add more and more pens, using those already built to form one side of the next enclosure. Some were square, like those built by the ranchers Fibonacci and Lucas:

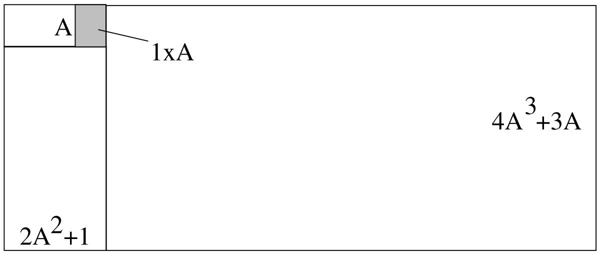




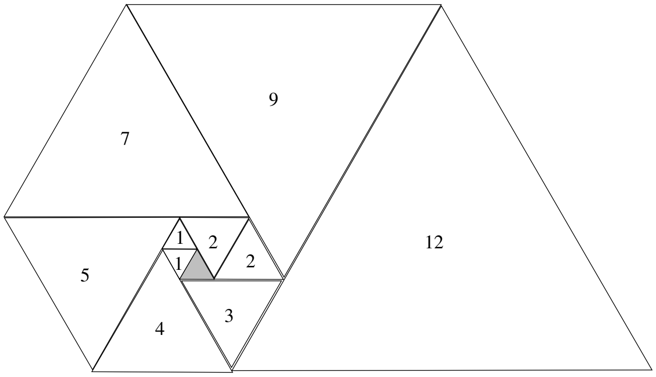
(squares labeled by side–length)

Others were rectangular (rancher Pell), with longer edges $a = 2A$ times the shorter:





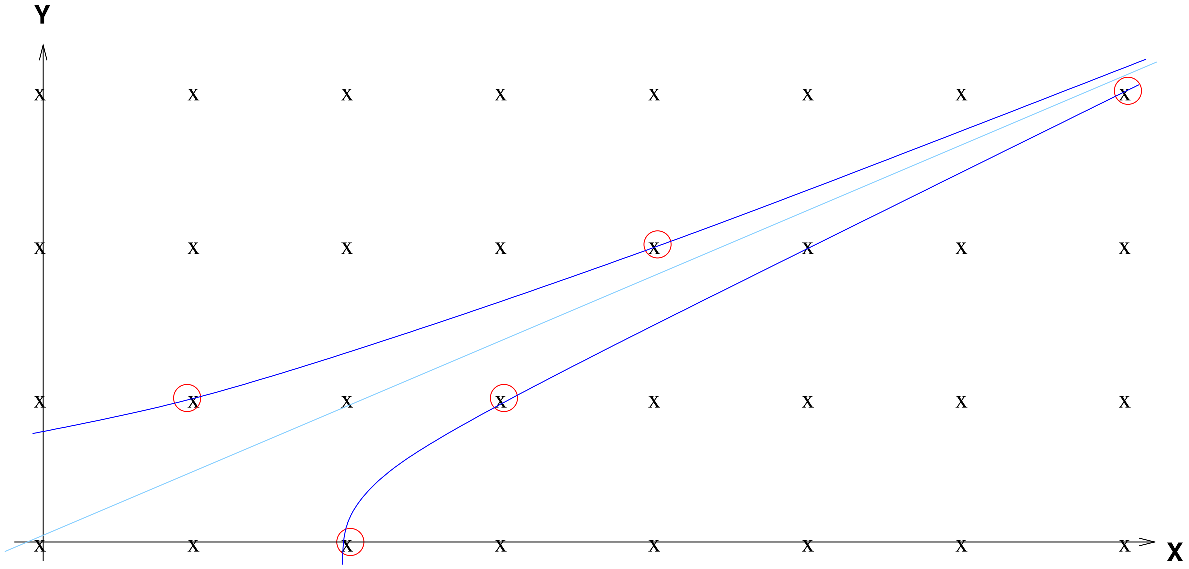
or even triangular (rancher Padovan):



Problem 3. In each case, to what number r did the ratio $\frac{\ell_{k+1}}{\ell_k}$ of side-lengths tend? (For rectangles, only use the shorter side-lengths; for triangles, just find an equation for r.)

III. Falling through the cracks

According to recent news, ranchers in California have been trying to account for cattle who disappeared into gigantic smoking crevices following the latest earthquake. The cows had been arranged evenly in a grid pattern with positive-integer coordinates (x, y); and the ground opened up lear L.A. along the hyperbolas $x^2 - 5y^2 = \pm 4$:



Problem 4. There's a secret relationship between the vanishing cows and the first two squares of fence-lengths on Mars. Can you see the link? Use it to help the not-so-jolly ranchers find coordinates of a few more missing cattle.

Problem 5. What if we change the equation to $x^2 - dy^2 = \pm 1$, with $d = A^2 + 1$? (Try $A = 3$, and use the rectangular fences.) If (x_1, y_1) and (x_2, y_2) pinpoint two missing cows, what happens when you multiply $x_1 + y_1\sqrt{d}$ and $x_2 + y_2\sqrt{d}$? (Try it first with both coordinates equal to $(A, 1)$.)

Problem 6. Near Sacramento, the chasm in the field is described by the equation $x^2 - 11y^2 = 1$. One cow has clearly been swallowed up at $(x, y) = (10, 3)$. Can you use this to determine the number of cattle on the moon (Problem 2)?

IV. Ring around the bovines

The points in the (x, y)-plane with integer coordinates make up what is called the *square lattice*.

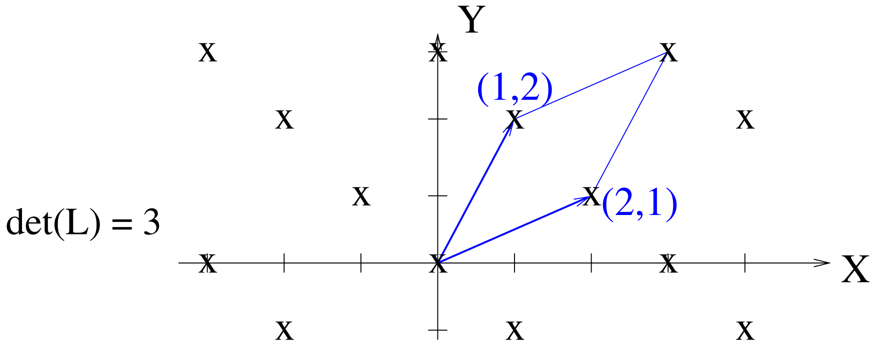
Problem 7. How many lattice points / cows are enclosed by a circle / fence of radius r, centered at the origin? Try it using a compass and graph paper for small r (= 1, 2, 3, etc.): record $A(r) =$ area of circle, $L(r) =$ lattice points (in, not on, the circle), and $E(r) =$ the "error" $|A(r) - L(r)|$. Then try to guess an upper bound on the error (or look up the "Gauss circle problem"!).

r	
A(r)	
L(r)	
E(r)	

Now the square lattice is a bit boring. We can make all kinds of lattices as follows: let $\mathbf{w_1} = (a, b)$ and $\mathbf{w_2} = (c, d)$ be two points, and simply take *all* points of the form

$$n_1\mathbf{w_1} + n_2\mathbf{w_2} = (n_1a + n_2c, n_1b + n_2d).$$

The quantity $\det(L) := ad - bc$ is called the *determinant* of the lattice L generated by $\mathbf{w_1}$ and $\mathbf{w_2}$. It gives the area of the parallelogram in the picture:



For large radius r, the circle encloses approximately $\pi r^2/\det(L)$ lattice points.

V. Minkowski's bound

A *lattice polygon* is one whose vertices are points of our lattice L. It is *convex* if the segment connecting any two points in the polygon is itself contained in the polygon.

Problem 8. How many convex lattice polygons can you draw in the square lattice (on graph paper) that only enclose *one* point? (There are a lot!) What if we insist that they be *symmetric* about this point? Which one has the largest area?

Problem 9. For any lattice L: if S is a convex set, symmetric about the origin $(0, 0)$, and containing no other lattice points (don't count ones on the boundary), what do you think is the maximum possible area of S?

Deduce that any lattice L contains a point within $\sqrt{2\det(L)}$ units of the origin. [**Hint**: use the square with points (t_1, t_2) with $-\sqrt{\det(L)} \leq t_i \leq \sqrt{\det(L)}$.]

Problem 10. Let L be the lattice generated by $\mathbf{w_1} = (50, -34)$ and $\mathbf{w_2} = (268, -182)$. These are obviously both pretty far from $(0, 0)$. Does L have (nonzero) points closer to $(0, 0)$? How close? Can you find some?

VI. Gauss's algorithm

The $\mathbf{w_1}$ and $\mathbf{w_2}$ in Problem 10 are a *bad* generating set. Why? Suppose someone at $(x, y) = (1, 0)$ asks you the way to the nearest lattice point. We can write their location as

$$(1, 0) = -\frac{91}{6}\mathbf{w_1} + \frac{17}{6}\mathbf{w_2}$$

and round the coefficients to their nearest integers: $-\frac{91}{6} \approx -15$, $\frac{17}{6} \approx 3$. This suggests the closest lattice point would be

$$-15\mathbf{w_1} + 3\mathbf{w_2} = (54, -36).$$

Trouble is, the actual nearest lattice point is $(0, 0)$.

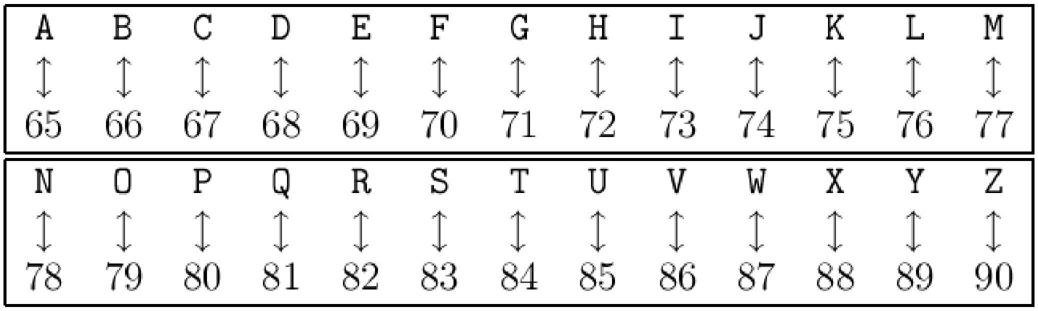
Fortunately, Gauss wrote an algorithm for finding a *good* generating set for our lattice L: begin by setting $\mathbf{v_1} := \mathbf{w_1}$, $\mathbf{v_2} := \mathbf{w_2}$; and write $(a, b) \cdot (c, d) := ac + bd$. Now

- if $\mathbf{v_2} \cdot \mathbf{v_2} < \mathbf{v_1} \cdot \mathbf{v_1}$, swap $\mathbf{v_1}$ with $\mathbf{v_2}$;
- compute $M =$ nearest integer to $\frac{\mathbf{v_1} \cdot \mathbf{v_2}}{\mathbf{v_1} \cdot \mathbf{v_1}}$;
- if $M = 0$, stop: $\mathbf{v_1}, \mathbf{v_2}$ is the good set;
- otherwise, replace $\mathbf{v_2}$ with $\mathbf{v_2} - M\mathbf{v_1}$;
- return to first step.

Problem 11. Apply Gauss's algorithm to produce a good generating set $\mathbf{v_1}, \mathbf{v_2}$ for our lattice L. What happens when you write $(1, 0) = \alpha\mathbf{v_1} + \beta\mathbf{v_2}$ and round the coefficients?

VII. BREAKING A LATTICE-BASED CRYPTOSYSTEM

In a simple case of the GGH (= Goldreich, Goldwasser, and Halevi) cryptosystem, Alice has a good generating set $\mathbf{v_1}, \mathbf{v_2}$ for a lattice L, but broadcasts a bad generating set $\mathbf{w_1}, \mathbf{w_2}$. Now Bob encodes a message as follows: first, turn each pair of letters into a pair of numbers m_1, m_2 by using Table 1:



A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
65	66	67	68	69	70	71	72	73	74	75	76	77

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
78	79	80	81	82	83	84	85	86	87	88	89	90

Table 1: ASCII encodings of English capital letters.

Then send the coordinate

$$m_1\mathbf{w_1} + m_2\mathbf{w_2} + (r_1, r_2)$$

to Alice, where r_1 and r_2 are small random numbers (like $(1, 0)$ on the last page). If the coordinate is intercepted, and written as $\mu_1\mathbf{w_1} + \mu_2\mathbf{w_2}$, then rounding μ_1 and μ_2 off will give garbage, because $\mathbf{w_1}$ and $\mathbf{w_2}$ are bad generators for the lattice.

In theory, only Alice knows the good generators, so only she can decode the message. She does this by writing the transmitted coordinate as $\eta_1\mathbf{v_1} + \eta_2\mathbf{v_2}$, rounding η_1, η_2 to n_1, n_2, and finally rewriting $n_1\mathbf{v_1} + n_2\mathbf{v_2}$ as a sum $m_1\mathbf{w_1} + m_2\mathbf{w_2}$ to recover the message m_1, m_2. Unfortunately, the "theory" has not accounted for the fact that you have a lattice-reduction algorithm, thanks to Gauss!

Here is the encrypted message Bob sent Alice:

$$(25977, -17644),\ (24286, -16497),\ (25425, -17270),\ (21339, 14494).$$

It is the solution to a Cowculus question: what is the first derivative of a heifer?

Problem 12. Decrypt Bob's message!