A solution to the cannonball problem using elliptic curves

Daniel Fretwell

The cannonball problem is a very old but interesting problem. It asks when a square-pyramidal stack of cannonballs can be arranged into a square. The claim is the following:

Theorem 1. *The only solutions occur when you have* $0, 1$ *or* $4900 = 70^2$ *cannonballs.*

Many people have solved this problem using different theories. Some in elementary ways, using simultaneous Pell equations and similar constructions. Others have used lattices. I propose a solution using the beautiful theory of elliptic curves.

First we note that since:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

we find that (valid) solutions to the cannonball problem correspond to (positive) integral points on the "elliptic curve":

$$E_1 : y^2 = \frac{x(x+1)(2x+1)}{6},$$

defined over the number field $\mathbb{Q}$. This is not in Weierstrass form so the first task is to find a morphism from this curve into one that is in Weierstrass form. However we would like more. We would like such a morphism that preserves integer points (only in one direction though) and is such that the resulting curve is an integer model, so that we may use more theory.

Lemma 2. *Let* E_2 *be the elliptic curve defined by* $y^2 = x^3 - 36x$. *The morphism defined by* $\phi(X, Y) = (12x+6, 72y)$ *gives a bijection* $\phi : E_2(\mathbb{Q}) \longrightarrow E_1(\mathbb{Q})$ *(although not an isogeny so not a group homomorphism). Further the inverse takes integer points of* E_1 *into integer points of* E_2.

Proof. This is trivial to see. □

Now we are able to solve the cannonball problem since we have computational tools for calculating the integer points of (integral) elliptic curves. We are wanting to obtain integer solutions to the cannonball problem, and by the above these must correspond to some subset of the integral points on E_2. We know that this set of points is finite by Siegel's Theorem.

The plan is now obvious, compute the (finitely many) integral points on E_2 and then invert them using ϕ to give (possibly rational) points on E_1. The remaining (positive) integral points then give the only solutions of the cannonball problem.

If I do this using certain S-integer algorithms in SAGE/PARI/MAGMA then I find the following:

Theorem 3. *The only integer points on* E_2 *are:*

$$\{(-6, 0), (-3, \pm 9), (-2, \pm 8), (0, 0), (6, 0), (12, \pm 36), (18, \pm 72), (294, \pm 5040)\}.$$

Inverting ϕ gives the following points on E_1:

$$\{(-1, 0), (-\frac{3}{4}, \pm\frac{1}{8}), (-\frac{2}{3}, \pm\frac{1}{9}), (-\frac{1}{2}, 0), (0, 0), (\frac{1}{2}, \pm\frac{1}{2}), (1, \pm 1), (24, \pm 70)\},$$

from which we see immediately that the only solutions to the cannonball problem are when you have $0, 1$ or $70^2 = 4900$ cannonballs.