

## Re: JSH: Hammer falls, Pell's Equation used to solve factoring problem

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2009-02/msg02584.html>

---

- *From:* Rotwang <[sg552@xxxxxxxxxxxxxxx](mailto:sg552@xxxxxxxxxxxxxxx)>
  - *Date:* Thu, 19 Feb 2009 20:40:08 +0000
- 

rdecker@xxxxxxxxxxxxx wrote:

[...]

This talk about minima is a red herring. If you simplify James' algorithm, as I did in an earlier post, you find that  $|r + t|$ ,  $|r - t|$  are  $2(m - (D - 1))^2$  and  $2Dm^2$ , for suitable rational  $m$ . It is impossible to make these simultaneously less than  $D$ , and even restricting the first to be less than  $D$  provides you with no additional information.

I think it's worth pointing out that there are two possible ways that James' thinking is wrong about this. One is the way you give: if you rewrite the formulae for  $x$  and  $y$  given at the start of this thread as rational functions of  $v$  with a common denominator and use the result to define polynomials  $r$ ,  $s$  and  $t$  then you can use calculus to find their minima, but I would /guess/ just by looking at them (I haven't checked your work) that the condition that  $|r + t|$  and  $|r - t|$  are both less than  $D$  is never met. On the other hand, for each rational  $v$  you could divide out any shared factor of  $r(v)$ ,  $s(v)$  and  $t(v)$  so they end up coprime – I assume that in this case you can find values of  $v$  for which  $|r + t|$  and  $|r - t|$  are both less than  $D$ . But of course you can't use calculus to find any minima those functions may have, since they won't be differentiable (more precisely, there won't exist a differentiable function  $r: \mathbb{R} \rightarrow \mathbb{R}$  which restricts to your choice of  $r(v)$  when  $v$  is rational, and similarly for the other two). So it looks a lot like finding a  $v$  which gives rise to a factorisation of  $D$  will turn out to be no easier than finding a factor of  $D$  by trial division.

James: in case the above was too abstract, I mean too much of a lie, consider the following method: given an integer  $D$  to be factored, let  $f(v) = v$  and  $g(v) = D/v$ .  $f$  and  $g$  are rational functions of  $v \neq 0$ , so define integer-valued functions  $r$ ,  $s$  and  $t$  such that  $f(v) = r(v)/t(v)$  and  $g(v) = s(v)/t(v)$ .  $|t(v)|$  is  $\geq 1$ , and if you can find  $v$  such that  $|t(v)| = 1$  then  $f(v)$  and  $g(v)$  give an integer factorisation of  $D$ . So you can find all integer factorisations of  $D$  by minimising  $t(v)$  using calculus, rendering the factoring problem trivial. Can you spot the flaw in this argument?

.