Finding arbitrarily many integer solutions to the equation $k^2 - 5 = t^2 - 5u^2$

Jonny Griffiths, mail@jonny-griffiths.net
Department of Mathematics
Paston College, Norfolk, UK

April 11, 2013

Abstract

As we vary k, is there an upper limit on the number of solutions (t, u) for the equation $k^2 - 5 = t^2 - 5u^2$? This article asserts that there is not, and employs an unusual argument to support this claim, one that could be of wider significance to those working on problems in number theory.

Not long ago, I was trying to prove

Conjecture 0.1. *Define a Hikorski Triple (or HT)[1] as* (a, b, c) *where* a, b *and* $c = \frac{ab+1}{a+b}$ *are all natural numbers. Show that the number of HTs whose three elements add to* k *is unbounded as* $k \to \infty$.

This reduced to

Conjecture 0.2. *Show that as we vary* k*, the equation* $k^2 - 5 = t^2 - 5u^2$ *can have arbitrarily many integer solutions for* t *and* u.

Or to put this another way, show that, given any n in $\mathbb{N}$, we can find a k in $\mathbb{N}$ so that $k^2 - 5 = t^2 - 5u^2$ has more than n integer solutions (t, u).

A 'proof' of Conjecture 0.2 did emerge, but not one that would pass any strict tests of rigour. It did, however, utilise a neat trick that I hope might be of interest to *Mathematical Spectrum* readers.

Preliminary computer searches suggest that 3230 will prove to be a fruitful choice for k, one where many (t, u) solutions are possible. In this case, $k^2 - 5 = 10432895 = 5.11.29.31.211$. Now

$$5.11.29.31.211 = (5^2 - 5 \times 2^2)(4^2 - 5 \times 1^2)(7^2 - 5 \times 2^2)(6^2 - 5 \times 1^2)(16^2 - 5 \times 3^2).$$

This suggests that if p is a prime dividing $k^2 - 5$, then p can always be written as $x^2 - 5y^2$. Are there primes that can't be expressed as $x^2 - 5y^2$ for some integers x and y? The prime 2 cannot be so expressed, since $2 = x^2 - 5y^2 \Rightarrow 2 \equiv x^2 \mod 5 \Rightarrow 2$ is a quadratic residue mod 5, which is untrue. Noting that $5 = 5^2 - 5 \times 2^2$, take now an odd prime p that is not equal to 5. If $p = x^2 - 5y^2$ then $p \equiv x^2 \mod 5$, which means $\left(\begin{array}{c} p \\ - \\ 5 \end{array}\right) = 1$, where $\left(\begin{array}{c} a \\ - \\ b \end{array}\right)$ is the Legendre symbol. Now p is congruent to 1, 2, 3 or 4 mod 5, and 1 and 4 are squares, so 1 and 4 are quadratic residues mod 5, while 2 and 3 are not. This gives us $p = 5(2m) + 1$ or $5(2m + 1) + 4$, since p is odd, and so p must be of the form $10m + 1$ or $10m + 9$.

In fact, the implication can be reversed, although not straightforwardly; we can quote

Theorem 0.3. *For an odd prime $p \neq 5, p$ can be expressed as $x^2 - 5y^2$ if and only if $p = 10m + 1$ or $p = 10m + 9$.*

This is a special case of a much larger result concerning the representation of primes by quadratic forms [2].

We now return to

Theorem 0.4. *If $p \neq 2$ is a prime dividing $k^2 - 5$, then p can be written as $x^2 - 5y^2$.*

Proof. We know 5 can be so expressed, so suppose $p \neq 5$. Then $k^2 \equiv 5$ mod p, so $\left(\begin{matrix}5\\-\\p\end{matrix}\right) = 1$. Now by the Theorem of Quadratic Reciprocity, $\left(\begin{matrix}5\\-\\p\end{matrix}\right)$ $= \left(\begin{matrix}p\\-\\5\end{matrix}\right)$, so p is congruent to 1 or 4 mod 5, so p is congruent to 1 or 9 mod 10 (since p is odd). Hence by Theorem (0.3), p can be expressed as $x^2 - 5y^2$. □

So writing $k^2 - 5$ for k even as a product of primes, all of which are of the form $x^2 - 5y^2$, we can see that they each factorise into $(x + y\sqrt{5})(x - y\sqrt{5})$. We can now write out the full factorisation of $k^2 - 5$ as

$$\prod_i (x_i + y_i\sqrt{5}) \prod_i (x_i - y_i\sqrt{5}).$$

The first product simplifies to $\alpha + \beta\sqrt{5}$, while the second product becomes $\alpha - \beta\sqrt{5}$. Thus, for example,

$3230^2 - 5 = 5.11.29.31.211$

$= (5^2 - 5 \times 2^2)(4^2 - 5 \times 1^2)(7^2 - 5 \times 2^2)(6^2 - 5 \times 1^2)(16^2 - 5 \times 3^2)$

$= (5 + 2\sqrt{5})(4 + 1\sqrt{5})(7 + 2\sqrt{5})(6 + 1\sqrt{5})(16 + 3\sqrt{5}) \times (5 - 2\sqrt{5})(4 - 1\sqrt{5})(7 - 2\sqrt{5})(6 - 1\sqrt{5})(16 - 3\sqrt{5})$

$= 63410^2 - 5 \times 28321^2.$

Now here is the neat trick: if we exchange a set of plus signs in the first product for the corresponding set of minus signs in the second, the pair of products becomes $(\alpha'\sqrt{5}+\beta')(\alpha'\sqrt{5}-\beta') = k^2 - 5$. Thus, for example,

$3230^2 - 5 = 5.11.29.31.211$

$= (5 + 2\sqrt{5})(4 + 1\sqrt{5})(7 + 2\sqrt{5})(6 + 1\sqrt{5})(16 - 3\sqrt{5})\times (5-2\sqrt{5})(4-1\sqrt{5})(7-2\sqrt{5})(6-1\sqrt{5})(16+3\sqrt{5})$

$= 26030^2 - 5 \times 11551^2$

$= (5 + 2\sqrt{5})(4 + 1\sqrt{5})(7 + 2\sqrt{5})(6 - 1\sqrt{5})(16 - 3\sqrt{5})\times (5-2\sqrt{5})(4-1\sqrt{5})(7-2\sqrt{5})(6+1\sqrt{5})(16+3\sqrt{5})$

$= 12070^2 - 5 \times 5201^2$.

The full set of resulting values for t and u are given in Table 1.

t	63410	26030	29050	14150	18070	4270	3610	4130
u	28321	11551	12911	6161	7951	1249	721	1151
t	3230	3250	4610	8510	7690	6790	6170	12070
u	1	161	1471	3521	3121	2671	2351	5201

Table 1: Possible values for (t,u) when $k = 3230$

A computer search tells us that these are not the only possibilities. It seems that predicting the number of solutions for (t,u) from the starting k is not an exact science, but we can certainly say that the more prime factors we have, the more (t,u) pairs we are likely to find.

So one thing remains: can we always find a value for k such that k^2-5 has arbitrarily many prime factors? There is a helpful identity here: two integers of the form x^2-5y^2 always multiply to an integer of the same shape, since

$$(x_1^2 - 5y_1^2)(x_2^2 - 5y_2^2) = (x_1 + y_1\sqrt{5})(x_2 + y_2\sqrt{5})(x_1 - y_1\sqrt{5})(x_2 - y_2\sqrt{5})$$

$$\equiv (x_1x_2 + 5y_1y_2)^2 - 5(x_1y_2 + x_2y_1)^2.$$

Given this, we can multiply together arbitrarily many distinct odd prime factors, say $p_1, p_2, \ldots, p_m$, each of the form $x^2 - 5y^2$ (primes ending in 1 or 9) to give a number of the form $X^2 - 5Y^2$. So we have $X^2 - 5Y^2 \equiv 0$ mod $p_1 p_2 \ldots p_m$, and so $X^2 \equiv 5Y^2$ mod $p_1 p_2 \ldots p_m$, and so $(XY^{-1})^2 \equiv 5$ mod $p_1 p_2 \ldots p_m$, and $p_1 p_2 \ldots p_m | ((XY^{-1})^2 - 5)$. (We know that Y^{-1} exists, since $\gcd(Y, p_1 p_2 \ldots p_m)$ is 1, because if $p_i | Y$, then $p_i | X$, and $p_i^2 | X^2 - 5Y^2$, which contradicts the fact that the p_i are distinct.) Thus we have a number of the form $k^2 - 5$ that has arbitrarily many prime factors of the desired form, which lends support to (but does not prove) Conjecture 0.2.

I hope this method deserves wider attention.

Acknowledgements

With warm thanks to Professor Shaun Stevens at the University of East Anglia, and to the editor for his kind help.

Bibliography

[1] J. Griffiths. *Lyness Cycles, Elliptic Curves, and Hikorski Triples* MSc Thesis, University of East Anglia, 2012, **http://www.s253053503.websitehome.co.uk/jg-msc-uea/index.html** (accessed Mar 2013).

[2] Wolfram Mathworld *Prime Representation* **http://mathworld.wolfram.com/PrimeRepresentation.html** (accessed Mar 2013).

About the author

Jonny Griffiths teaches mathematics at Paston Sixth Form College in Norfolk, where he has been for the last twenty years. He has studied mathematics and education at a combination of Cambridge University, the Open University, and the University of East Anglia. Possible claims to fame include being a member of *Harvey and the Wallbangers*, a popular band in the Eighties, and playing the character Stringfellow on the childrens' television programme *Playdays.*