When Is (xy + 1)(yz + 1)(zx + 1) a Square?

Kiran S. Kedlaya

Mathematics Magazine, Vol. 71, No. 1 (Feb., 1998), 61-63.

Stable URL:
http://links.jstor.org/sici?sici=0025-570X%28199802%2971%3A1%3C61%3AWI%28%2B1%2B%3E2.0.CO%3B2-Q

Mathematics Magazine is currently published by Mathematical Association of America.

When is $(xy+1)(yz+1)(zx+1)$ a Square?

KIRAN S. KEDLAYA
Princeton University
Princeton, NJ 08544

To cut the suspense, let's start with the surprising answer to the title question.

Theorem. *If x, y, z are positive integers, then $(xy+1)(yz+1)(zx+1)$ is a perfect square if and only if $xy+1$, $yz+1$, and $zx+1$ are all perfect squares.*

The purpose of this note is to prove this result using Fermat's method of infinite descent, to provide historical context, and to investigate (and eventually refute) a possible generalization.

For t a positive integer, a *P_t-set* is a set of positive integers, the product of any two distinct elements of which is t less than a perfect square. (The positivity restriction is sometimes relaxed, but we will impose it throughout.) Classical examples of P_t-sets include the P_{256}-set $\{1, 33, 68, 105\}$ found by Diophantos and the P_1-set $\{1, 3, 8, 120\}$ found by Fermat.

A sizable literature exists addressing the existence or nonexistence of P_t-sets of certain forms; some early examples are chronicled in [**3**, Chap. XIX, pp. 513–520]. A little experimentation shows that P_t-sets become nontrivial to construct when they must have four or more elements; Euler found a general construction of four-element P_1-sets which includes Fermat's example. Since this construction is essential for the proof of the theorem, we state it as a lemma (following [**5**]).

Lemma. *If $\{p, q, r\}$ is a P_1-set, then so is $\{p, q, r, s\}$ for*

$$s = p + q + r + 2pqr \pm 2\sqrt{(pq+1)(qr+1)(rp+1)}, \tag{1}$$

as long as $s > 0$. (Note that s is necessarily an integer.)

Proof. The values of s defined in (1) are the roots of the quadratic equation

$$p^2 + q^2 + r^2 + s^2 - 2(pq + pr + qr + ps + qs + rs) - 4pqrs - 4 = 0, \tag{2}$$

which can be rewritten in the following ways:

$$(p + q - r - s)^2 = 4(pq + 1)(rs + 1)$$
$$(p + r - q - s)^2 = 4(pr + 1)(qs + 1)$$
$$(p + s - q - r)^2 = 4(qr + 1)(ps + 1).$$

Since $rs + 1$ is an integer which is the quotient of two perfect squares, it is also a square, as are $ps + 1$ and $qs + 1$ by the same argument. Thus $\{p, q, r, s\}$ is a P_1-set.

Not surprisingly, constructing five-element P_t-sets is substantially harder. Euler gave a general construction, and a number of additional examples are also known; however, it is not known whether there exist infinitely many five-element P_t-sets for any particular values of t, or whether there exist any at all for $t = 1$.

The first significant nonexistence result for P_t-sets is due to Baker and Davenport [**1**]; using Baker's theory of linear forms in logarithms of algebraic numbers, they

showed that Fermat's P_1-set $\{1, 3, 8\}$ can only be extended by adding 120. Their method was later refined by Grinstead [4] and Brown [2] and applied to other P_t-sets. An elementary approach to such questions is given by Kangasabapathy and Ponnudurai [6] and by Mohanty and Ramasamy [8]; a systematic presentation and a more complete bibliography appear in [7].

The above theorem does not directly apply to studying the existence or nonexistence of P_t-sets, but it does give an interesting characterization of three-element P_1-sets; after the proof, we will see that this phenomenon is (almost) unique to the case $t = 1$.

Proof of the Theorem. Suppose there exist triples p, q, r of positive integers (where we might as well assume $p \le q \le r$) such that $(pq + 1)(qr + 1)(rp + 1)$ is a perfect square, but not all of $pq + 1$, $qr + 1$, $rp + 1$ are squares. Choose a triple that minimizes $p + q + r$, and define s as in (1) using the negative square root. We will show that $0 < s < r$ and that $(pq + 1)(qs + 1)(sp + 1)$ is a square, but that not all of $pq + 1$, $qs + 1$, $sp + 1$ are squares, contradicting the minimality of $p + q + r$.

By the equivalent forms of (2), we know that

$$\begin{aligned} &16(pq + 1)^2(pr + 1)(qs + 1)(qr + 1)(ps + 1) \\ &\quad = (pq + 1)^2(p + r - q - s)^2(p + s - q - r)^2 \end{aligned}$$

is a perfect square; since $(pq + 1)(qr + 1)(rp + 1)$ is a square, so then is $(pq + 1)(qs + 1)(sp + 1)$. Moreover, $ps + 1$ is a square if and only if $qr + 1$ is a square, and $pr + 1$ is a square if and only if $qs + 1$ is a square, so not all of $pq + 1$, $qs + 1$, $sp + 1$ are squares.

We also have

$$rs + 1 \frac{(p + q - r - s)^2}{4(pq + 1)} \ge 0$$

and so $s \ge -1/r$. Note that $r = 1$ implies (by our assumption that $p \le q \le r$) that $p = q = r = 1$, in which case $(pq + 1)(qr + 1)(rp + 1)$ is not a square, a contradiction. Hence $r > 1$ and so $s \ge 0$. Moreover, if $s = 0$, then we have

$$4(pq + 1) = (p + q - r)^2, \quad 4(qr + 1) = (q + r - p)^2, \quad 4(rp + 1) = (r + p - q)^2,$$

contradicting the assumption that not all of $pq + 1$, $qr + 1$, and $rp + 1$ are squares. Therefore s is a positive integer.

If s' is the other root of (2) (which is to say, s' satisfies (1) using the positive square root), then we have

$$\begin{aligned} ss' &= p^2 + q^2 + r^2 - 2pq - 2pr - 2qr - 4 \\ &< r^2 - p(2r - p) - q(2r - q) \\ &< r^2. \end{aligned}$$

Since s is the smaller of the two roots, $s^2 \le ss'$ and so we conclude $s < r$, yielding the desired contradiction. ∎

Does an analogous characterization of P_t-sets exist for $t > 1$? In other words, is $(pq + t)(qr + t)(rp + t)$ a square if and only if $pq + t$, $qr + t$, $rp + t$ are all squares? The proof above does not work in general; the natural analogue of (2) would be

$$t(p^2 + q^2 + r^2 + s^2) - 2t(pq + pr + qr + ps + qs + rs) - 4pqrs - 4t^2 = 0, \quad (3)$$

whose equivalent forms are

$$4(pq+t)(rs+t)=t(p+q-r-s)^2$$

and so on, but two obstructions arise. If t is not a perfect square, then $\{p,q,r\}$ can be a counterexample even if $\{p,q,s\}$ is not. Even if t is a perfect square, though, if $t>4$, we cannot ensure that s is an integer.

Neither obstruction arises for $t=4$, and indeed the reader may check that the natural analogue of the theorem holds in this case with essentially the same proof. However, we will now show that this analogue does not hold for $t\neq 1,4$.

We first construct a counterexample $\{p,q,r\}$ where t is not a perfect square. Put $p=1$, $q=a^2-t$, where q is not a perfect square (which certainly holds if $t<2a+1$); we shall find r such that $r+t=tb^2$, $qr+t=tc^2$, which is equivalent to solving

$$c^2-qb^2=1-q.$$

Indeed, $b=c=1$ is a solution, but it yields $r=0$, which is not a positive integer. Nonetheless it is useful! To produce a nontrivial solution, let (u,v) be a solution in positive integers of the Pell equation

$$u^2-qv^2=1,$$

and put

$$\left(c+b\sqrt{q}\right)=\left(1+\sqrt{q}\right)\left(u+v\sqrt{q}\right).$$

Now $r=t[(u+v)^2-1]$ yields a counterexample. For example, if $t=a=q=2$, the solution $(3,2)$ of the Pell equation gives the set $\{p,q,r\}=\{1,2,48\}$.

On the other hand, if $t=d^2$ for $d>2$, we can write $t=a^2-p^2$ for some positive a,p, and a similar argument starting from the bogus counterexample p,p,r (r arbitrary) yields an actual counterexample.

Acknowledgment. Thanks to George Berzsenyi for providing ideas for my entry in the 1992 Westinghouse Science Talent Search, where the above result first appeared.

REFERENCES

1. A. Baker and H. Davenport, The equations $3x^2-2=y^2$ and $8x^2-7=z^2$, *Quart. J. Math. Oxford* (2) **20** (1969), 129–137.
2. E. Brown, Sets in which $xy+k$ is always a square, *Math. Comp.* **45** (1985), 613–620.
3. L. E. Dickson, *History of the Theory of Numbers, Volume 2*, Carnegie Institute, Washington, DC, 1920.
4. C. M. Grinstead, On a method of solving a class of Diophantine equations, *Math. Comp.* **32** (1978), 936–940.
5. P. Heichelheim, The study of positive integers (a,b) such that $ab+1$ is a square, *Fibon. Quart.* **17** (1979), 269–274.
6. P. Kangasabapathy and T. Ponnudurai, The simultaneous Diophantine equations $y^2-3x^2=-2$ and $z^2-8x^2=-7$, *Quart. J. Math. Oxford* (3) **26** (1975), 275–278.
7. K. S. Kedlaya, Solving constrained Pell equations, *Math. Comp.*, to appear.
8. S. P. Mohanty and A. M. S. Ramasamy, The simultaneous diophantine equations $5y^2-20=x^2$ and $2y^2+1=z^2$, *J. Number Theory* **18** (1984), 356–359.