FERMAT'S FOUR SQUARES THEOREM

ALF VAN DER POORTEN

Abstract. Fermat proved that there is no arithmetic progression of more than three squares (of rationals). In other words, the pair of *diophantine equations*

$$a^2 + c^2 = 2b^2 \quad \text{and} \quad b^2 + d^2 = 2c^2$$

has no solution in rationals a, b, c and d. Curiously, the readily accessible literature seems not to contain a straightforward proof.

Several years ago, after explaining why three rational squares in arithmetic progression correspond to pythagorean triangles with integer area, I found it natural to tell my graduate student audience that "Fermat proved that there is no arithmetic progression of more than three squares (of rationals). In other words, the pair of *diophantine equations* $a^2 + c^2 = 2b^2$ and $b^2 + d^2 = 2c^2$ has no solution in rationals a, b, c and d." But my suggestion that they be Fermat and write me an essay on the proof fell on stony ground and, worse, the best *I* could provide as a solution was to say: "Too hard for me? I looked this up in [3] and found at p54 the unhelpful footnote "Fermat could show by descent that one cannot have four squares in AP ... . Gerry Myerson has pointed me to a reference but the argument there seems utterly soulless and I remain searching for a decent descent argument warranting report to you."

I decided recently that such a proof was most readily found on a (previously) blank page of my notebook.

Fermat's four squares theorem. *There are no four distinct rational squares in arithmetic progression.*

Proof. It is rather more convenient to work with integer squares. First, this is a not altogether trivial exercise, note that the four integer squares $x - 3n$, $x - n$, $x + n$, $x + 3n$ may be presumed to be pairwise relatively prime, and all odd. By the way, if two squares differ by an even integer $2n$ they must differ by an integer divisible by 4; so n must be even and x is odd.

Thus, second, we have integers x, y, and n satisfying

$$y^2 = (x^2 - n^2)(x^2 - 9n^2) = x^4 - 10n^2x^2 + 9n^4 = (x^2 - 5n^2)^2 - 16n^4,$$

whence there are relatively prime integers u and v so that both

$$4n^2 = 4uv \quad \text{and} \quad x^2 - 5n^2 = 4u^2 + v^2\,.$$

It follows that both u and v are squares and that we may replace $u \leftarrow A^2$ and $v \leftarrow D^2$, so obtaining

$$x^2 = (A^2 + D^2)(4A^2 + D^2)\,.$$

Hence, third, noting that $A^2 + D^2$ and $4A^2 + D^2$ are relatively prime, it must be that both $A^2 + D^2$ and $4A^2 + D^2$ are squares, and that necessarily A is even

Typeset April 2, 2007 [11:58].

and D is odd. Moreover, conversely, given those two squares one may define x as a square root of their product, and $n =: AD$. It then readily follows that $(x-3n)(x-n)(x+n)(x+3n)$ is a square, yielding an arithmetic progression of four squares of integers with common difference $2n$.

We therefore suppose that A and D are relatively prime and that each of A^2+D^2 and $4A^2+D^2$ is a square and we recall that then, necessarily, A is even and D is odd.

Then we see that there are four pairwise relatively prime positive integers a, b, c, d of which a is even and so that $2A = 2\cdot 2ab\cdot cd = 4ac\cdot bd$ and $c^2d^2 - a^2b^2 = b^2d^2 - 4a^2c^2$. Here we have used that $2\cdot A = 2A$ and that $D = D$.

Thus, $c^2(4a^2+d^2) = b^2(a^2+d^2)$ and it follows that both a^2+d^2 and $4a^2+d^2$ are squares. Equivalently, there is an arithmetic progression of four pairwise relatively prime squares of integers with common difference $2ad$.

However, because $A = 2abcd$, it is plain that ad is a proper divisor of A and thus is noticeably less than AD.

Hence the set of common differences of four term arithmetic progressions of integer squares has no smallest element and is therefore empty; in other words, there is no nontrivial four term arithmetic progressions of integer squares. ∎

Degeneracy. Because of the hypothesis *distinct* squares, my remarks above neglect the degenerate case $n = 2AD = 0$ where, since we have noted that without loss of generality the four squares are pairwise relatively prime, $x^2 = D^4 = 1$, so $A = 0$ (and $D^2 = 1$). In this case the descent on the common difference $2n$ fails and the argument correctly affirms that $1,\ 1,\ 1,\ 1$ is indeed a (trivial) arithmetic progression of four integer squares.

Summary. The argument points out that the existence of a four term arithmetic progression of distinct integer squares with common difference $2n$ is equivalent to n having a factorisation $n = AD$ so that both A^2+D^2 and $4A^2+D^2$ are squares. However it then readily follows that A has a factorisation $abcd$ so that also both a^2+d^2 and $4a^2+d^2$ are squares. Because ad is a proper divisor of AD unless $n = 0$, it follows that $n = 0$, contradicting the nontriviality of the arithmetic progression.

The ingredients building the proof are the following basic facts.

(i) If an integer has factorisations AB and CD with both $\gcd(A,B) = 1$ and $\gcd(C,D) = 1$ then there are pairwise relatively prime integers a, b, c, and d so that $A = ab$, $B = cd$, $C = ac$, and $D = bd$.

(ii) If A and B are nonnegative relatively prime integers and AB is a k-th power then both A and B are k-th powers.

(iii) An integer square is $\equiv 0$ or $4 \bmod 8$ if even and is $\equiv 1 \bmod 8$ if odd.

(iv) The parametrisation $x = x(t) = 2t/(1+t^2)$, $y = y(t) = (1-t^2)/(1+t^2)$ is equivalent to the equation $x^2+y^2 = 1$. The familiar t-formulas, $\cos\theta = 2t/(1+t^2)$, $\sin\theta = (1-t^2)/(1+t^2)$, with $t = \tan\frac{1}{2}\theta$, manifest this fact. Specifically, if x, y, and z are relatively prime integers then, by taking $t = v/u$, it follows that $x^2+y^2 = z^2$ is equivalent to $x = 2uv$, $y = u^2-v^2$, and $z = u^2+v^2$; here u and v are relatively prime integers not both odd.

(v) A non-empty set of nonnegative integers contains a least element.

Ingredient (i) is, in my view, the least likely to come to mind though it is no more than a restatement of unique factorisation. In the present context, ingredient (iv)

seems more likely to be recalled; and is in any case easily derived by first principles. One notes that without loss of generality $x = 2x'$ is even and both y and z are odd so, by (ii), $x'^2 = \frac{1}{2}(z-y)\cdot\frac{1}{2}(z+y)$ entails $\frac{1}{2}(z-y) = v^2$, $\frac{1}{2}(z+y) = u^2$ with one of u or v even. 'One notes without loss of generality' by applying (iii). Although the first principles argument is fairly simple, it seems to me much more contrived than recalling that the circular functions $\cos\theta$ and $\sin\theta$ parametrise the unit circle. Incidentally, (ii) is more subtle than (i) in that it fails if one omits the adjective 'nonnegative'; specifically, its analogue in a unique factorisation domain with nontrivial units requires a more complicated proclamation.

The fact that the putative four squares in arithmetic progression may be assumed odd and pairwise relatively prime is primarily a consequence of ingredient (iii).

Finally, the Well Ordering Principle (v) is equivalent to the Principle of Induction (and showing that in detail is a useful exercise). I use it here disguised as Fermat's Method of Descent, wherein the absence of a least instance proves that the set of instances is empty.

What's going on here? It seems helpful to rewrite the opening assumption as alleging that the curve $\mathcal{C} : Y^2-(X^2-5)Y-4 = 0$ contains a rational point (X, Y); specifically, so that X has denominator n and Y has denominator n^2.

Indeed, $\mathcal{C}$ is a quartic model for an elliptic curve $\mathcal{E} : y^2 = x(x+1)(x+4)$ obtained by taking $x = Y$ and $y = XY$; thus, for the presumed rational point on $\mathcal{E}$, the denominator of x is n^2 and that of y is n^3. $\mathcal{E}$ is curve 24A1 of Cremona's tables [1]. The argument confirms that the only rational points on $\mathcal{E}$ are the 2-torsion points $(0,0)$, $(-1,0)$, and $(-4,0)$; these points do not correspond to a nontrivial arithmetic progression.

History. Dickson [2] reports at II, XiV, p. 440 that Fermat proposed the problem to Frenicle in 1640 and stated that it is impossible; and *inter alia* gives a summary of an uncompelling 1813 proof. Dickson, at II, XXII, p. 635 mentions an argument of Euler which leads one to see that x^2+y^2 and x^2+4y^2 are not both squares for x odd, $y \neq 0$ even; with the four squares theorem a corollary. I imagine that this effectively coincides with my argument. Reassuringly, back at p. 440 Dickson cites (what I presume to be) an 1898 *Amer. Math. Monthly* problem asking for a proof of the theorem, and remarks: "Several writers failed to find a solution."

References

[1] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992. vi+343 pp.

[2] Leonard Eugene Dickson, *History of the theory of numbers*, Vol. I: Divisibility and primality; Vol. II: Diophantine analysis; Vol. III: Quadratic and higher forms. Chelsea Publishing Co., New York 1966.

[3] Alf van der Poorten, *Notes on Fermat's Last Theorem*, (New York, N. Y.: Wiley-Interscience, 1996), xvi + 222pp.

Centre for Number Theory Research, 1 Bimbil Place, Killara, Sydney, NSW 2071, Australia

E-mail address: alf@maths.usyd.edu.au (Alf van der Poorten)