

On a Generalized Fermat-Wiles Equation

STEVEN FINCH

September 5, 2002

Fermat's Last Theorem was no more than a conjecture for over 350 years. Let n be an integer greater than 2. Fermat claimed that any integers x , y and z , not necessarily positive, for which

$$x^n + y^n = z^n$$

must consequently satisfy $xyz = 0$. Andrew Wiles' spectacular achievement, building on the work of Kenneth Ribet and others, was to prove beyond any doubt that Fermat's conjecture is true.

To some people, the passage of this conjecture to theoremhood is marked by sadness. They may mistakenly believe that no other interesting Diophantine equations are left to be solved. This essay is aimed at such individuals: there is a much larger class of equations, of which Fermat-Wiles is only a special case, that is well worth everyone's attention!

The equation we'll examine is

$$x^n + y^n = cz^n$$

where c is a positive integer. We wish to learn what conditions on n and c force the existence of a **non-trivial** solution (x, y, z) , that is, $xyz \neq 0$. In other words, when is the equation $x^n + y^n = cz^n$ **solvable** (in nonzero integers)? The case $n = 1$ is easy: taking $x = y = c$ and $z = 2$, we conclude that non-trivial solutions always exist. The case $n = 2$ is somewhat more difficult. Let c' denote the square-free part of c , that is, the divisor of c which is the outcome after all factors of the form d^2 have been eliminated. The equation

$$x^2 + y^2 = cz^2$$

is solvable if and only if all odd prime factors of c' are equal to 1 modulo 4. (See Hardy & Wright's discussion [1] of Waring's problem for a proof.) Here are the first several values of c for which this condition holds:

1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, ...

(see Appendix I for more terms). The infinite sequence of all such integers c can be shown to be highly sparse relative to the sequence of positive integers. By the

⁰Copyright © 2002 by Steven R. Finch. All rights reserved.

density $\delta(N)$ of the c -sequence **in the interval** $[1, N]$, we mean the cardinality of c -values not exceeding N , divided by N . It can be proved that

$$\lim_{N \rightarrow \infty} \delta(N) = 0$$

and, more precisely,

$$\lim_{N \rightarrow \infty} \sqrt{\ln(N)} \delta(N) = K$$

where $K = 0.7642236535\dots$ is known as the Landau-Ramanujan constant [2].

The case $n = 3$ is where things start becoming quite difficult. Observe that earlier we were able to reduce the problem to examining a certain equivalent congruence condition. For $n \geq 3$, I don't know about the existence of equivalent congruence conditions. Sylvester and Pepin discovered a complicated set of conditions sufficient for triviality, which Selmer [3] and others extended. Here is the sequence of c -values for which the equation $x^3 + y^3 = cz^3$ is solvable, obtained by a variety of methods [3]:

2, 6, 7, 9, 12, 13, 15, 16, 17, 19, 20, 22, 26, 28, 30, 31, 33, 34, 35, 37, 42, 43, 48, 49, 50, ...

(see Appendix II for more terms). The fact that 1 is not in this sequence was first proved by Euler [4]. Since our understanding of the sequence is so limited, a precise estimate of its asymptotic density is not possible. For certain values of c , stronger conclusions can be drawn. If $c = 2$, for example, it necessarily follows [5, 6] that $x = y$ or $x = -y$. One must be careful when reviewing the literature: the phrases "trivial solutions" and "solvability" might sometimes be used differently than we have here.

More can be said of the case $n = 4$ since any solution of $x^4 + y^4 = cz^4$ must satisfy $(x^2)^2 + (y^2)^2 = c(z^2)^2$. Thus the c -sequence here is included as a proper subsequence of the c -sequence corresponding to $n = 2$ (so it too has zero asymptotic density). Fermat [4] was the first to prove that this sequence begins with 2 (the only special case he examined of his famous conjecture, as far as we know). Bremner & Morton [7] obtained that the sequence is:

2, 17, 32, 82, 97, 162, 257, 272, 337, 512, 626, 641, 706, 881, 1250,
1297, 1312, 1377, 1552, 1921, 2402, 2417, 2482, 2592, 2657, 3026,
3697, 4097, 4112, 4177, 4352, 4721, 4802, 5392, 5906, ...

and that $5906 = (149/17)^4 + (25/17)^4$ is the least integer expressible as the sum of two rational fourth powers but not as the sum of two integer fourth powers. The case $n = 6$ is likewise highly sparse since it is contained as a proper subsequence of both c -sequences corresponding to $n = 2$ and $n = 3$.

Dirichlet and Legendre [4] were the first to prove that the c -sequence for $n = 5$ starts with 2; the same for $n = 7$ was first proved by Lamé and Kummer [4]. For

both $n = 5$ and $n = 7$, Dénes [8] confirmed that if $c = 2$ then $x = y$ or $x = -y$ must follow (resolving two conjectures in [9] – see the Addendum below for an update on larger n). David Wilson has suggested that the c -sequence for $n = 5$ is:

2, 31, 33, 64, 211, 242, 244, 275, 486, 781, 992, 1023, 1025, 1056,
 1267, 2048, 2101, 2882, 3093, 3124, 3126, 3157, 3368, 4149, 4651,
 6250, 6752, 7533, 7744, 7775, 7777, 7808, 8019, 8800, 9031, 10901,
 13682, 15552, 15783, 15961, 16564, 16775, 16806, 16808, 16839,
 17050, 17831, 19932, 24583, 24992, 26281, 29643, 31744, 32525,
 32736, 32767, 32769, 32800, 33011, 33614, 33792, 35893, 40544,
 40951, 42242, 49575, 51273, 55924, 58025, 58806, 59017, 59048,
 59050, 59081, 59292, 60073, 61051, 62174, 65536, 66825, 67232,
 68101, ...

and that $68101 = (15/2)^5 + (17/2)^5$ is the least integer expressible as the sum of two rational fifth powers but not as the sum of two integer fifth powers. As far as I know, this remains unproved. Wilson has found that $1124326946 = (73/5)^6 + (161/5)^6$ seems not to be the sum of two integer sixth powers and $69071941639 = (63/2)^7 + (65/2)^7$ seems not to be the sum of two integer seventh powers. He also wonders if the expression

$$\left(\frac{2^{n-1} + 1}{2}\right)^n + \left(\frac{2^{n-1} - 1}{2}\right)^n$$

is never the sum of two integer n^{th} powers for any odd $n \geq 5$. Clearly $(p/r)^n + ((qr^n - p)/r)^n$ is an integer for any such n .

Wiles' achievement was to show that the first term of the c -sequence for *every* $n \geq 3$ is necessarily 2 (not 1). Very few other statements of such generality have been proved. We conjecture, for example, that the next nineteen terms of the c -sequence for every even $n \geq 4$ are:

$$\begin{array}{ccccc} 1 + 2^n, & 2^{n+1}, & 1 + 3^n, & 2^n + 3^n, & 2 \cdot 3^n \\ 1 + 4^n, & 2^n + 4^n, & 3^n + 4^n, & 2 \cdot 4^n, & 1 + 5^n, \\ 2^n + 5^n, & 3^n + 5^n, & 4^n + 5^n, & 2 \cdot 5^n, & 1 + 6^n, \\ 2^n + 6^n, & 3^n + 6^n, & 4^n + 6^n, & 5^n + 6^n & \end{array}$$

and that the next twenty-three terms of the c -sequence for every odd $n \geq 5$ are:

$$\begin{array}{ccccc} -1 + 2^n, & 1 + 2^n, & 2^{n+1}, & -2^n + 3^n, & -1 + 3^n, \\ 1 + 3^n, & 2^n + 3^n, & 2 \cdot 3^n, & -3^n + 4^n, & -2^n + 4^n, \\ -1 + 4^n, & 1 + 4^n, & 2^n + 4^n, & 3^n + 4^n, & 2 \cdot 4^n, \\ -4^n + 5^n, & -3^n + 5^n, & -2^n + 5^n, & -1 + 5^n, & 1 + 5^n, \\ 2^n + 5^n, & 3^n + 5^n, & 4^n + 5^n. & & \end{array}$$

A verification would perhaps begin with the following proposition of Serre [10], the truth of which is rooted in Wiles' proof of the semi-stable Taniyama-Shimura-Weil theorem. If $p \geq 11$ is a prime number, c is a power of one of the primes belonging to the set $\{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$ but c is not a power of p , then the equation $x^p + y^p = cz^p$ is insolvable. I gather that most number theorists believe the restriction $p \geq 11$ can be relaxed to $p \geq 5$, but a proof of this belief is not known.

0.1. Appendix I: c -sequence for $n = 2$. For the sake of economy, let us list only the square-free members of the c -sequence C corresponding to $n = 2$. The c -sequence is homogeneous in the sense that c is in C if and only if all square-multiples of c are in C .

1, 2, 5, 10, 13, 17, 26, 29, 34, 37, 41, 53, 58, 61, 65, 73, 74, 82, 85,
 89, 97, 101, 106, 109, 113, 122, 130, 137, 145, 146, 149, 157, 170, 173,
 178, 181, 185, 193, 194, 197, 202, 205, 218, 221, 226, 229, 233, 241, 257,
 265, 269, 274, 277, 281, 290, 293, 298, 305, 313, 314, 317, 337, 346, 349,
 353, 362, 365, 370, 373, 377, 386, 389, 394, 397, 401, 409, 410, 421, 433,
 442, 445, 449, 457, 458, 461, 466, 481, 482, 485, 493, ...

0.2. Appendix II: c -sequence for $n = 3$. For the sake of economy, let us list only the cube-free members of the c -sequence C corresponding to $n = 3$. The c -sequence is homogeneous in the sense that c is in C if and only if all cube-multiples of c are in C .

2, 6, 7, 9, 12, 13, 15, 17, 19, 20, 22, 26, 28, 30, 31, 33, 34, 35, 37,
 42, 43, 49, 50, 51, 53, 58, 61, 62, 63, 65, 67, 68, 69, 70, 71, 75, 78,
 79, 84, 85, 86, 87, 89, 90, 91, 92, 94, 97, 98, 103, 105, 106, 107, 110,
 114, 115, 117, 123, 124, 126, 127, 130, 132, 133, 134, 139, 140, 141, 142,
 143, 151, 153, 156, 157, 159, 161, 163, 164, 166, 169, 170, 171, 172, 177,
 178, 179, 180, 182, 183, 186, 187, 193, 195, 197, 198, 201, 202, 203, 205,
 206, 209, 210, 211, 212, 213, 214, 215, 217, 218, 219, 222, 223, 228, 229,
 231, 233, 236, 238, 241, 244, 246, 247, 249, 251, 254, 258, 259, 265, 267,
 269, 271, 273, 274, 275, 277, 278, 279, 282, 283, 284, 285, 286, 287, 289,
 294, 295, 301, 303, 305, 306, 308, 309, 310, 313, 314, 316, 319, 321, 322,
 323, 325, 330, 331, 333, 335, 337, 339, 341, 342, 345, 346, 348, 349, 355,
 356, 357, 358, 359, 363, 366, 367, 370, 372, 373, 377, 379, 380, 382, 385,
 386, 387, 388, 390, 391, 393, 394, 395, 396, 397, 399, 402, 403, 407, 409,
 411, 413, 414, 418, 420, 421, 422, 425, 427, 428, 429, 430, 431, 433, 435,
 436, 438, 439, 441, 444, 445, 446, 447, 449, 450, 452, 453, 454, 457, 458,
 460, 462, 463, 465, 466, 467, 468, 469, 474, 477, 481, 483, 484, 485, 490,
 493, 494, 495, 497, 498, 499, ...

This is far as Selmer [3] performed his calculations. Surely someone else has gone farther?

Selmer [3] additionally listed sample solutions (x, y, z) for each of the above c -values; we give just a few here:

c	x	y	z
2	1	1	1
6	37	17	21
7	2	-1	1
9	2	1	1
12	89	19	39
13	7	2	3
15	683	397	294
17	18	-1	7
19	3	-2	1
20	19	1	7
22	25469	17299	9954
26	3	-1	1
28	3	1	1

0.3. Addendum. Kenneth Ribet very kindly replied to a sci.math.research question of mine, pointed out Dénes' [8] solution, and then added:

“The problem of resolving $x^n + y^n = cz^n$ becomes more difficult, however, if you take a large prime number n in place of 5 or 7 (and keep $c = 2$).

“In his 1987 Duke Journal paper, Serre shows that the elliptic curve methods which resolved the Fermat problem shed light on such equations. Serre gives a list of prime numbers which can be taken as “ c ” – for those, there are no solutions in non-zero x , y , and z when n is a prime no less than 11 and n is different from c . Serre’s prime numbers “ c ” are all odd, and they lead to semistable elliptic curves. The choice $c = 2$ leads to a non-semistable curve. It’s also different in character because the equation $x^n + y^n = 2z^n$ does have non-zero solutions, namely those with $x = y = z!$

“Several years ago, I received a letter from an amateur mathematician about such equations. I wrote an article which will appear (some day) in Acta Arithmetica [11]. Basically, I prove that $x^n + y^n = 2z^n$ has only the obvious non-zero solutions when n is congruent to 1 mod 4. My methods are pretty much the same as those introduced previously by H. Darmon to deal with some other Diophantine equations.

“In a recent preprint, Darmon and L. Merel deal with the case where n is congruent to 3 mod 4, thereby proving for all odd primes n that the only non-zero solutions to $x^n + y^n = 2z^n$ are the evident ones with $x = y = z$. This theorem resolves a problem which has been of interest at least since the 17th century! [12]”

We also have Darmon & Granville's result [13]: given non-zero integer coefficients a, b, c and positive integer exponents i, j, k satisfying $1/i+1/j+1/k < 1$, the equation $ax^i + by^j = cz^k$ has at most finitely many coprime integer solutions (x, y, z) . This is a byproduct of Falting's theorem (Mordell's conjecture). A special case in which $a = b = c = 1$ was publicized in [14]. See also [15]. More can be said if we assume the truth of the (still unproved) **abc-conjecture**: the equation $ax^n + by^n = cz^n$ cannot have more than two such solutions for $n > M$ (independent of a, b, c) and it has no solutions for $n > N(a, b, c)$. See, for example, [16].

What happens if we increase the number of terms on the left-hand side of Fermat's original equation? People are often surprised to see the classical result

$$3^3 + 4^3 + 5^3 = 6^3$$

as well as Norrie's (1911) result

$$30^4 + 120^4 + 272^4 + 315^4 = 353^4,$$

Lander & Parkin's (1966) result

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

and Elkies & Frye's (1988) result

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

See [17, 18, 19] for more details.

Roland Quême submitted a manuscript [20]; his results extend to the equation $x^n + y^n = cz^n$.

The recent proof of the full Taniyama-Shimura-Weil theorem by Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor holds many benefits for number theory [21].

REFERENCES

- [1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, 1985; MR 81i:10002.
- [2] S. R. Finch, Landau-Ramanujan constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 98–104; MR 2004i:00001.
- [3] E. S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta. Math.* 85 (1951) 203–362 and 92 (1954) 191–197; MR 13,13i and 16,674e.
- [4] H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag 1977; MR 97g:11028.

- [5] L. E. Dickson, *History of the Theory of Numbers*, vol. II, *Diophantine Analysis*, Chelsea 1971; MR 39 #6807b.
- [6] R. D. Carmichael, *Diophantine Analysis*, Wiley, 1915; pp. 67–72; MR 21 #4123.
- [7] A. Bremner and P. Morton, A new characterization of the integer 5906, *Manuscripta Math.* 44 (1983) 187–229; MR 84i:10016.
- [8] P. Dénes, Über die Diophantische Gleichung, *Acta Math.* 88 (1952) 241–251; MR 16,903h.
- [9] J. M. Gandhi, On Fermat’s last theorem, *Amer. Math. Monthly* 71 (1964) 998–1006; MR 30 #1088.
- [10] J. P. Serre, Sur les représentations modulaires de degré 2 de $\text{Gal}(\bar{Q}/Q)$, *Duke Math. J.* 54 (1987) 179–230; MR 88g:11022.
- [11] K. A. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* 79 (1997) 7–16; available online at <http://math.berkeley.edu/~ribet/Articles/>; MR 98e:11035.
- [12] H. Darmon and L. Merel, Winding quotients and some variants of Fermat’s last theorem, *J. Reine Angew. Math.* 490 (1997) 81–100; available online at <http://www.math.mcgill.ca/darmon/pub/pub.html>; MR 98h:11076.
- [13] H. Darmon and A. Granville, On the equations and $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* 27 (1995) 513–543; available online at <http://www.dms.umontreal.ca/~andrew/1995.html>; MR 96e:11042.
- [14] R. D. Mauldin, A generalization of Fermat’s last theorem: the Beal conjecture and prize problem, *Notices Amer. Math. Soc.* 44 (1997) 1436–1437; 45 (1998) 359; MR 98j:11020; <http://www.bealconjecture.com/>.
- [15] H. Cohen, $a^m + b^n = c^p$, USENET newsgroup sci.math.research posting (1998); available online at <http://www.math.u-bordeaux1.fr/~cohen/fermatgen>.
- [16] A. Granville, On the number of solutions to the generalized Fermat equation, *Number Theory*, Proc. 1994 Halifax conf., ed. K. Dilcher, Amer. Math. Soc., 1995; pp. 197–207; available online at <http://www.dms.umontreal.ca/~andrew/1995.html>; MR 96j:11035.
- [17] J.-C. Meyrignac, Computing Minimal Equal Sums Of Like Powers, <http://euler.free.fr/>.
- [18] C. Shuwen, Equal Sums of Like Powers, <http://euler.free.fr/eslp/>.

- [19] T. Womack, Equal Sums of Like Powers, http://tom.womack.net/math/dissert_abstract.htm.
- [20] R. Queme, A classical approach on cyclotomic fields and Fermat-Wiles theorem, arXiv:math/0211467.
- [21] B. Poonen, Some Diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* 86 (1998) 193-205; MR 99h:11034.