The proof and application of Fermat's last theorem

Xiong Yibing [China]

Abstract: Three variables X,Y,Z **are expressed in terms of undetermined coefficients —— variables, binary, and then put into Fermat's last theorem equations. In the equations composed of undetermined coefficients, the number of independent equations is no less than the number of variables, and the solution is no less than zero, so Fermat's last theorem is established**

Keywords: Fermat, indefinite equation，Diophantine

MR(2020) Subject classification： 11D41

1.1 Proof of Fermat's last theorem

Definition.1.1.1:

A1, The number of variables of a homogeneous (indefinite) system is not more than the number of independent homogeneous (indefinite) equations, and the homogeneous (indefinite) system has at most one solution;

A2, The number of variables in a homogeneous (indefinite) system is greater than the number of independent homogeneous (indefinite) equations, and if the homogeneous (indefinite) system is found to have at least two solutions, then there are infinitely many solutions;

The above method of judging the solution of homogeneous (indefinite) equations is called the judgment rule of the solution of homogeneous (indefinite) equations;

The above conclusions can be proved by elimination method. On the contrary, in homogeneous (indefinite) equations, where the elimination method can be used to eliminate or reduce variables, its solution can use the above judgment rule.

Elimination method: In the independent (indefinite) equations, a variable of any one independent (indefinite) equation is placed on the left side of the independent (indefinite) equation, and the remaining quantity is placed on the right side of the independent (indefinite) equation, and the variable is substituted into the remaining independent (indefinite) equation to eliminate the variable; That is, for every independent (indeterminate) equation used, 1 variable can be eliminated

Baidu Encyclopedia

百度百科

https://baike.baidu.com/item/%E8%B4%B9%E9%A9%AC%E5%A4%A7%E5

%AE%9A%E7%90%86/80363?fr=ge_ala

Around 1637, the French scholar Fermat, while reading the Latin translation of Diophatus' Arithmetics, wrote next to proposition 8 of Book 11: ″It is impossible to divide a cubic number into the sum of two cubic numbers, or a fourth power into the sum of two fourth powers, or in general to divide a power higher than the second into the sum of two powers of the same power. I am sure I have found a wonderful proof of this, but the blank space here is too small to write″ This statement of Fermat may be called Fermat's conjecture or Fermat's last theorem

Theorem 1.2 : Fermat's Last Theorem: When n ≥ 3, the following indefinite equations have no integer solutions that are not equal to zero

$$X^n + Y^n = Z^n \qquad (X < Y < Z) \qquad (1.1.1)$$

Proof : X, Y, Z and their respective NTH power, use the binary , undetermined coefficients —— variables, expressed as follows

$$X^n = \left(\sum_{i=0}^{r_1} a_i 2^i\right)^n = \sum_{m=0}^{R_3}\left[A_m\left(a_i\right) \bmod 2\right]2^m \qquad \left(r_1 \le r_3 - 1\right) \qquad (1.1.2)$$

$$Y^n = \left(\sum_{j=0}^{r_2} b_j 2^j\right)^n = \sum_{m=0}^{R_3}\left[B_m\left(b_j\right) \bmod 2\right]2^m \qquad \left(r_2 \le r_3\right) \qquad (1.1.3)$$

$$Z^n = \left(\sum_{k=0}^{r_3} c_k 2^k \right)^n = \sum_{m=0}^{R_3} \left[C_m \left(c_k \right) \bmod 2 \right] 2^m \qquad \begin{pmatrix} c_{r_3} = 1 \\ n r_3 \le R_3 \end{pmatrix} \qquad (1.1.4)$$

$$\sum_{m=0}^{R_3} \left\{ \left[A_m \left(a_i \right) + B_m \left(b_j \right) \right] \bmod 2 \right\} 2^m = \sum_{m=0}^{R_3} \left[C_m \left(c_k \right) \bmod 2 \right] 2^m \qquad (1.1.5)$$

$$\left[A_m \left(a_i \right) + B_m \left(b_j \right) \right] \bmod 2 = C_m \left(c_k \right) \bmod 2 \qquad \left(0 \le m \le R_3 \right) \qquad (1.1.6)$$

When the coefficients of 2^m on the left and right sides of formula (1.1.5) are equal， $R_3 + 1$ equations of undetermined coefficients are obtained to form equations of undetermined coefficients formula (1.1.6). Since there is no multiplicative term $a_i b_j$ of a_i and b_j on the left side of the equation set， and, the sum of the exponents of the undetermined coefficients for each term is equal to n;So,the equation set has no common factor a_i or b_j , and is independent of each other, construct a homogeneous independent undetermined coefficient equation system

In the formula (1.1.6) of indefinite system of equations ， the undetermined coefficients a_i， b_j ， c_k ， or any of their powers, or the product of any undetermined coefficients of any of their powers, are 0 or 1; In every indefinite equation, the value of each term is either 0 or 1; The sum of the coefficients of X,Y,Z —— the remainder of the set of undetermined coefficients $A_m\left(a_i\right)$， $B_m\left(b_j\right)$， $C_m\left(c_k\right)$， modulo 2, is either 0 or 1;

In the formula (1.1.6) of indefinite system of equations , elimination method can be used: Use an independent indeterminate equation to eliminate an undetermined coefficient; Any power of the undetermined coefficient is still equal to the first power of the undetermined coefficient, that is, in the set of undetermined coefficients, any power of all undetermined coefficients is equivalent to the first power of the undetermined coefficient; First, the undetermined coefficient set is divided into two groups according to whether it contains the undetermined coefficient, which is expressed as follows:

在方程组(1.1.6)式中，可用消元法：使用某个独立不定方程，消除某待定系数；该待定系数的任何次幂，仍等于该待定系数的 1 次幂，即，在待定系数集合中，所有的待定系数的任何次幂，都等价于该待定系数的 1 次幂；首先，将该待定系数集合，按照是否含有该待定系数，分为两组，表达如下：

$$A_m\left(a_i\right) = A1_m\left(a_{j\neq i}\right)a_i + A2_m\left(a_{j\neq i}\right)$$

By substituting the above equation into equations (1.1.6) of the system of indefinite equations, obtain

$$\left[A1_m\left(a_{d\neq i}\right)a_i + A2_m\left(a_{d\neq i}\right) + B_m\left(b_j\right)\right] \bmod 2 = C_m\left(c_k\right) \bmod 2$$

$$\left[A1_m\left(a_{d\neq i}\right)a_i + AB_m\left(a_{d\neq i}, b_j\right)\right] \bmod 2 = C_m\left(c_k\right) \bmod 2$$

$$a_i = \frac{\varepsilon 1 + \left[A1_m\left(a_{d\neq i}\right)a_i + AB_m\left(a_{d\neq i}, b_j\right)\right] \bmod 2}{\varepsilon 2 + A1_m\left(a_{d\neq i}\right) \bmod 2} \quad \left(0< \varepsilon \leq \frac{\varepsilon 1}{\varepsilon 2} \leq 1\right) \quad (7.1.7)$$

The value of the above formula, by introducing three small enough quantities of ε, ε1, ε2, can both overcome the difficulty of 0÷0, and satisfy the need to take any 0 or 1 at this time;

The above formula shows that any undetermined coefficient can be eliminated by an independent indeterminate equation, and the solution of equation of indeterminate equations (1.1.6) is applicable to the judgment method of the solution of homogeneous (indeterminate) equations defined in this paper.

In formula (1.1.6), the number TT of equations of the equations with undetermined coefficients is equal to $R_3 + 1$, then

$$TT = R_3 + 1 \geq nr_3 + 1 \qquad (1.1.8)$$

Because $c_{r3} = 1$, and the size relationship of X, Y, Z, the number tt of undetermined coefficients a_i, b_j, c_k can be determined, get

$$tt = r_1 + 1 + r_2 + 1 + r_3 \leq r_3 - 1 + 1 + r_3 + 1 + r_3 \leq 3r_3 + 1 \qquad (1.1.9)$$

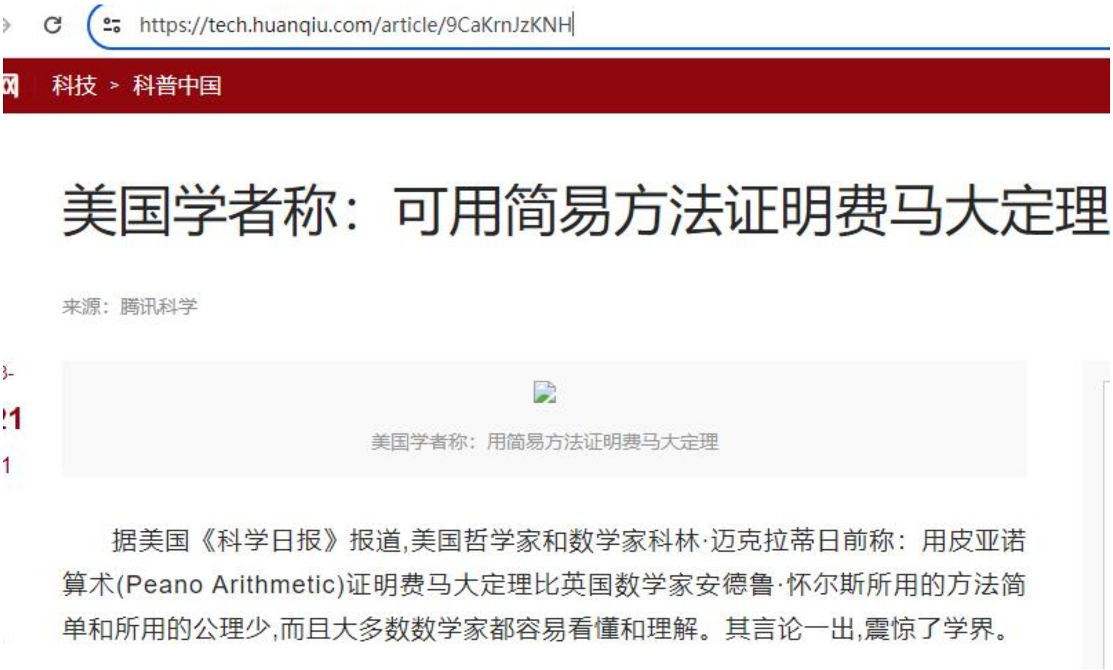
When n≥3, by the number of equations TT of equation (1.1.8) and the number of undetermined coefficients tt of equation (1.1.9), we can get:

$$TT = R_3 + 1 \geq nr_3 + 1 \geq tt \leq 3r_3 + 1 \quad (n \geq 3) \qquad (1.1.10)$$

In the above equation, when n≥3, the number of equations with undetermined coefficients TT is not less than the number of undetermined coefficients tt; According to the judgment rule for the solution of equations defined 1. 1,know : equations (1.1.6) and equations (1.1.1) have at most one zero solution, that is, no more than zero solution, Fermat's last theorem is established and the proof is complete

1.2 Application of Fermat's last theorem

The short (simple) proof of Fermat's Last theorem involved in this article is still highly valued, refer to the following websites, etc: https://tech.huanqiu.com/article/9CaKrnJzKNH



https://tech.huanqiu.com/article/9CaKrnJzKNH

科技 > 科普中国

美国学者称：可用简易方法证明费马大定理

来源：腾讯科学

美国学者称：用简易方法证明费马大定理

据美国《科学日报》报道,美国哲学家和数学家科林·迈克拉蒂日前称：用皮亚诺算术(Peano Arithmetic)证明费马大定理比英国数学家安德鲁·怀尔斯所用的方法简单和所用的公理少,而且大多数数学家都容易看懂和理解。其言论一出,震惊了学界。

Based on Fermat's description of the proof of this problem: potential brevity —— "not written here"; Latent elementary methods —— "beautiful proofs"

Based on the brief, elementary method proved in this paper, the following conjecture is proposed

Conjecture 1.2.1： The method of proving Fermat's last theorem in this paper is the method of proving Fermat's last theorem

Inference 1.2.2: The following equations, called S-element n-degree homogeneous indefinite equations, the number of their solutions, the qualitative judgment rule

$$\sum_{i=1}^{S-1} X_i^n = X_S^n \qquad (1.2.1)$$

Rule 1: When S≤n-1, this condition is no more than zero solution;

Rule 2: When S=n=3, this condition is no more than zero solution;

Rule 3: When S=n= 4,5,6,8, no less than 2 solutions are found, so there are infinite solutions for each of these conditionss;

Rule 4: When S≥N, and if there are at least 2 solutions, then there are infinite solutions to this condition;

Proof: Rule 1, With the help of the judgment rule of the solution of homogeneous (indefinite) equations, the conditional conclusion is valid;

Rule 2, By means of the proof of Fermat's last theorem, under the condition S=n=3, the conclusion of this condition is valid;

Rule 3: By virtue of the judgment rule of the solution of homogeneous (indefinite) equations, the conditional conclusion is valid;

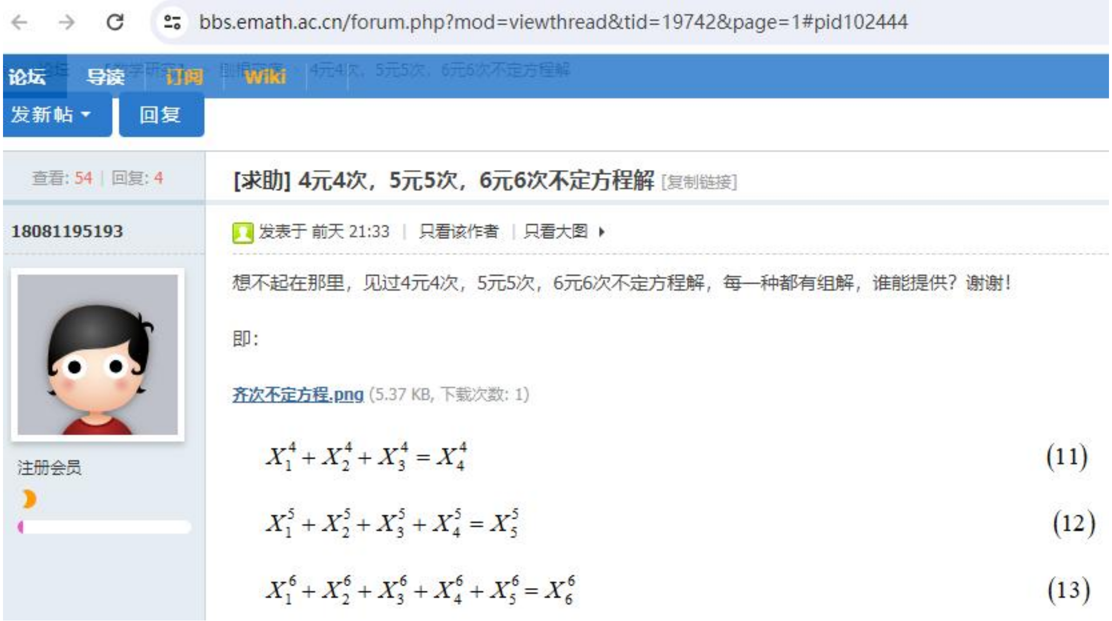
Rule 4: With the help of the judgment rule of the solution of homogeneous (indefinite) equations, the conditional conclusion is established and the proof is completed;

Question 1.2.3: formula (1.2.1), also those indefinite equations of n value, have infinitely many solutions?

$$\sum_{i=1}^{S-1} A_i X_i^n = A_S X_S^n \tag{1.2.2}$$

Thanks to mathematics research and development forum users: northwolves in the following website, to provide S=n= 4, 5, 6, 8, multiple solutions of these four equations and other data!

https://bbs.emath.ac.cn/forum.php?mod=viewthread&tid=19742&page=1#pid102444



bbs.emath.ac.cn/forum.php?mod=viewthread&tid=19742&page=1#pid102444
论坛
导读
订阅
Wiki
发新帖
回复
查看: 54 | 回复: 4
18081195193
注册会员
发表于 前天 21:33 | 只看该作者 | 只看大图

[求助] 4元4次，5元5次，6元6次不定方程解 [复制链接]

想不起在那里，见过4元4次，5元5次，6元6次不定方程解，每一种都有组解，谁能提供？谢谢！

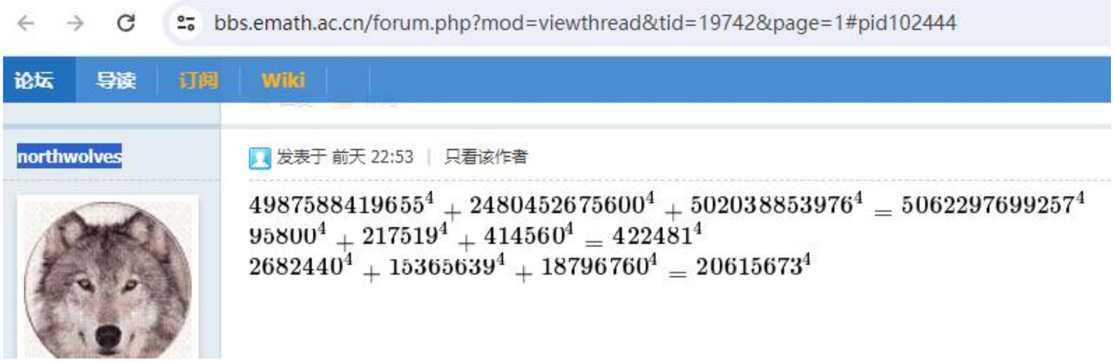
即：

齐次不定方程.png (5.37 KB, 下载次数: 1)

$$X_1^4 + X_2^4 + X_3^4 = X_4^4 \tag{11}$$

$$X_1^5 + X_2^5 + X_3^5 + X_4^5 = X_5^5 \tag{12}$$

$$X_1^6 + X_2^6 + X_3^6 + X_4^6 + X_5^6 = X_6^6 \tag{13}$$

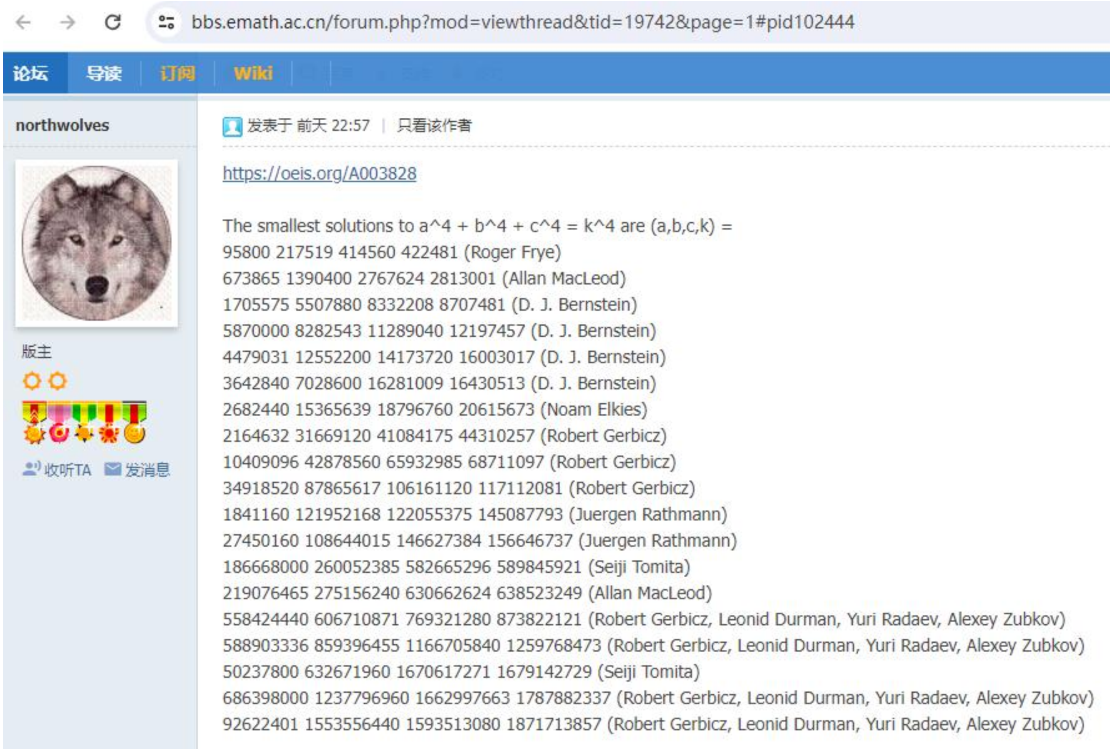


bbs.emath.ac.cn/forum.php?mod=viewthread&tid=19742&page=1#pid102444

northwolves

发表于 前天 22:53

$$4987588419655^4+2480452675600^4+5020388539764^4=5062297699257^4$$
$$95800^4+217519^4+414560^4=422481^4$$
$$2682440^4+15365639^4+18796760^4=20615673^4$$



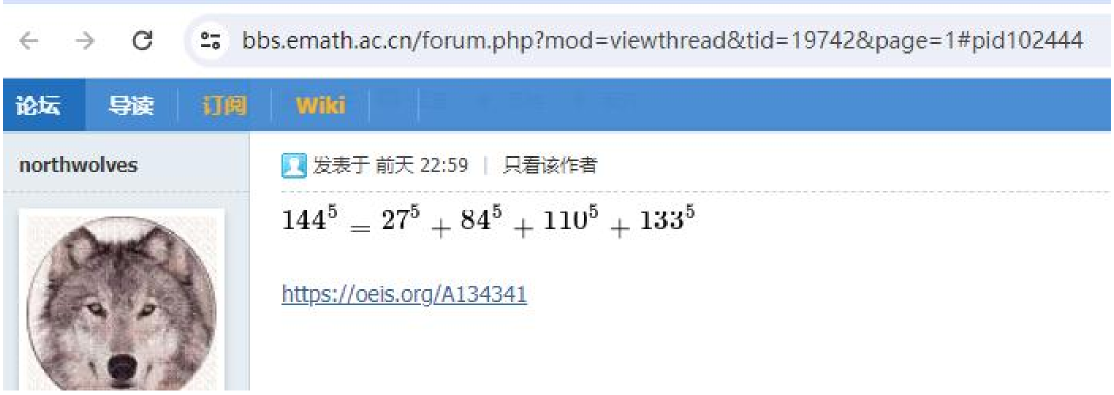
bbs.emath.ac.cn/forum.php?mod=viewthread&tid=19742&page=1#pid102444

northwolves

发表于 前天 22:57

https://oeis.org/A003828

The smallest solutions to a^4 + b^4 + c^4 = k^4 are (a,b,c,k) =
95800 217519 414560 422481 (Roger Frye)
673865 1390400 2767624 2813001 (Allan MacLeod)
1705575 5507880 8332208 8707481 (D. J. Bernstein)
5870000 8282543 11289040 12197457 (D. J. Bernstein)
4479031 12552200 14173720 16003017 (D. J. Bernstein)
3642840 7028600 16281009 16430513 (D. J. Bernstein)
2682440 15365639 18796760 20615673 (Noam Elkies)
2164632 31669120 41084175 44310257 (Robert Gerbicz)
10409096 42878560 65932985 68711097 (Robert Gerbicz)
34918520 87865617 106161120 117112081 (Robert Gerbicz)
1841160 121952168 122055375 145087793 (Juergen Rathmann)
27450160 108644015 146627384 156646737 (Juergen Rathmann)
186668000 260052385 582665296 589845921 (Seiji Tomita)
219076465 275156240 630662624 638523249 (Allan MacLeod)
558424440 606710871 769321280 873822121 (Robert Gerbicz, Leonid Durman, Yuri Radaev, Alexey Zubkov)
588903336 859396455 1166705840 1259768473 (Robert Gerbicz, Leonid Durman, Yuri Radaev, Alexey Zubkov)
50237800 632671960 1670617271 1679142729 (Seiji Tomita)
686398000 1237796960 1662997663 1787882337 (Robert Gerbicz, Leonid Durman, Yuri Radaev, Alexey Zubkov)
92622401 1553556440 1593513080 1871713857 (Robert Gerbicz, Leonid Durman, Yuri Radaev, Alexey Zubkov)



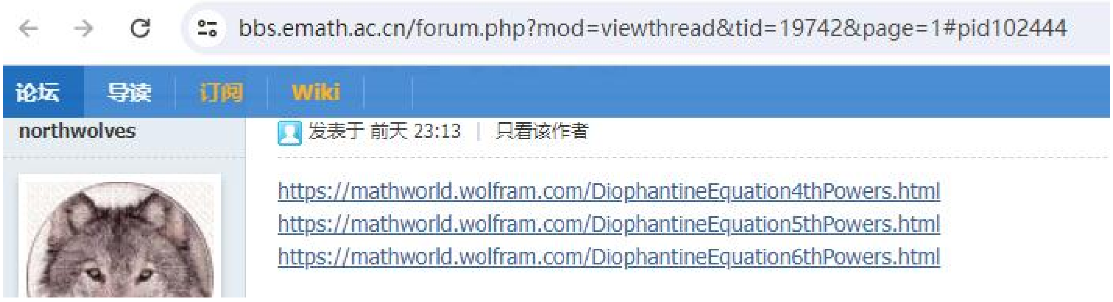
bbs.emath.ac.cn/forum.php?mod=viewthread&tid=19742&page=1#pid102444

northwolves

发表于 前天 22:59

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

https://oeis.org/A134341



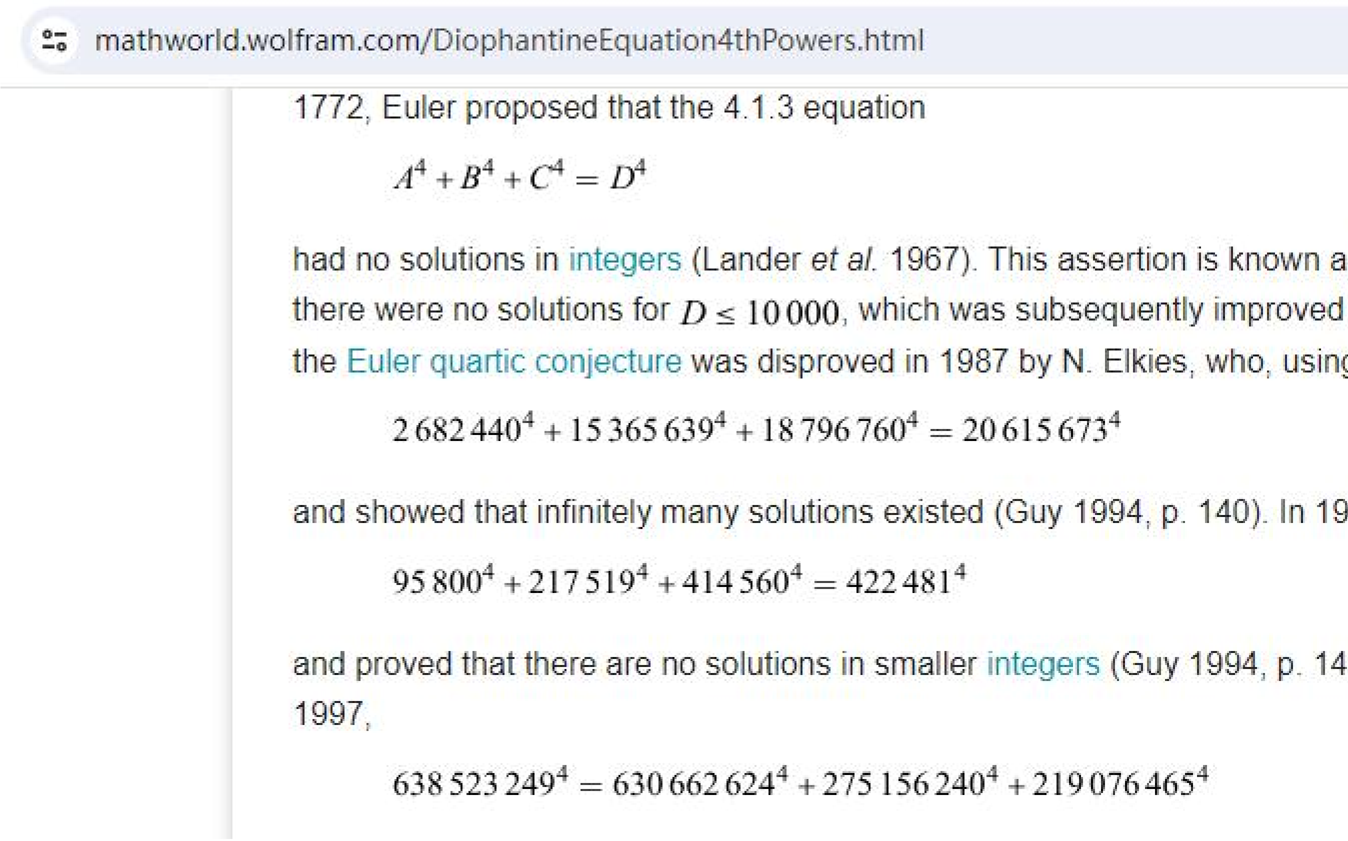
bbs.emath.ac.cn/forum.php?mod=viewthread&tid=19742&page=1#pid102444

northwolves

发表于 前天 23:13

https://mathworld.wolfram.com/DiophantineEquation4thPowers.html
https://mathworld.wolfram.com/DiophantineEquation5thPowers.html
https://mathworld.wolfram.com/DiophantineEquation6thPowers.html

https://mathworld.wolfram.com/DiophantineEquation4thPowers.html
https://mathworld.wolfram.com/DiophantineEquation5thPowers.html
https://mathworld.wolfram.com/DiophantineEquation6thPowers.html
https://mathworld.wolfram.com/DiophantineEquation7thPowers.html
https://mathworld.wolfram.com/DiophantineEquation8thPowers.html
https://mathworld.wolfram.com/DiophantineEquation9thPowers.html
https://mathworld.wolfram.com/DiophantineEquation10thPowers.html



1772, Euler proposed that the 4.1.3 equation

$$A^4 + B^4 + C^4 = D^4$$

had no solutions in integers (Lander *et al.* 1967). This assertion is known a
there were no solutions for $D \leq 10\,000$, which was subsequently improved
the Euler quartic conjecture was disproved in 1987 by N. Elkies, who, usin

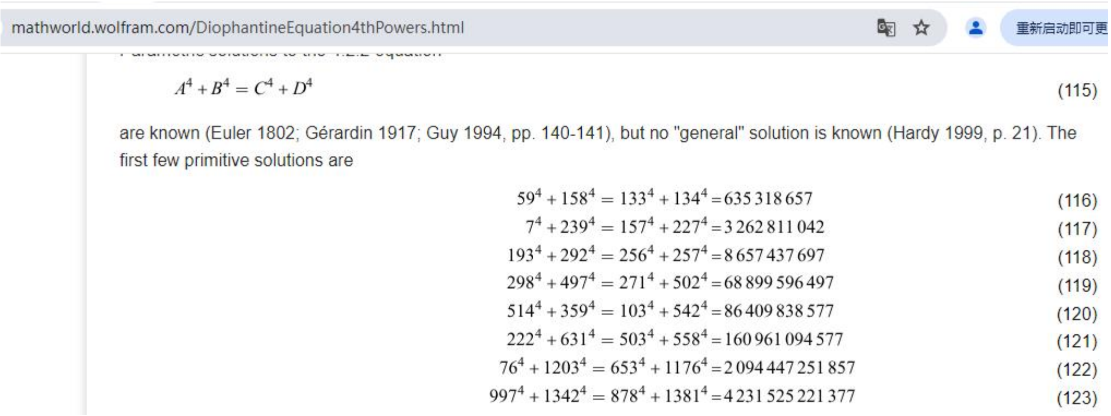
$$2\,682\,440^4 + 15\,365\,639^4 + 18\,796\,760^4 = 20\,615\,673^4$$

and showed that infinitely many solutions existed (Guy 1994, p. 140). In 19

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4$$

and proved that there are no solutions in smaller integers (Guy 1994, p. 14
1997,

$$638\,523\,249^4 = 630\,662\,624^4 + 275\,156\,240^4 + 219\,076\,465^4$$



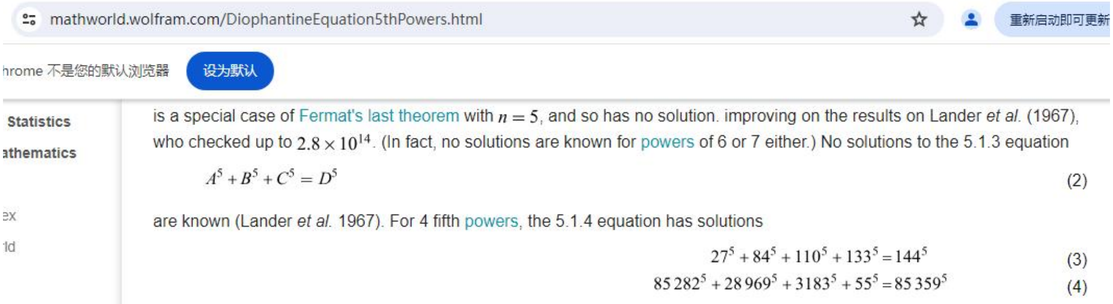
mathworld.wolfram.com/DiophantineEquation4thPowers.html

Parametric solutions to the 4.2.2 equation

$$A^4+B^4=C^4+D^4 \qquad (115)$$

are known (Euler 1802; Gérardin 1917; Guy 1994, pp. 140-141), but no "general" solution is known (Hardy 1999, p. 21). The first few primitive solutions are

$$59^4+158^4=133^4+134^4=635\,318\,657 \qquad (116)$$
$$7^4+239^4=157^4+227^4=3\,262\,811\,042 \qquad (117)$$
$$193^4+292^4=256^4+257^4=8\,657\,437\,697 \qquad (118)$$
$$298^4+497^4=271^4+502^4=68\,899\,596\,497 \qquad (119)$$
$$514^4+359^4=103^4+542^4=86\,409\,838\,577 \qquad (120)$$
$$222^4+631^4=503^4+558^4=160\,961\,094\,577 \qquad (121)$$
$$76^4+1203^4=653^4+1176^4=2\,094\,447\,251\,857 \qquad (122)$$
$$997^4+1342^4=878^4+1381^4=4\,231\,525\,221\,377 \qquad (123)$$



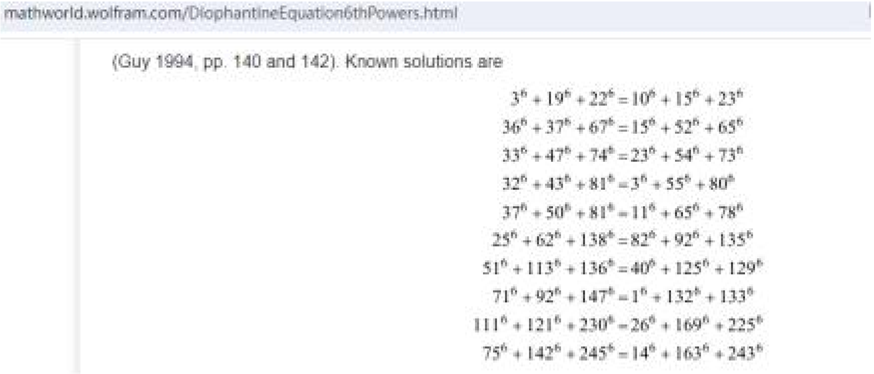
mathworld.wolfram.com/DiophantineEquation5thPowers.html

is a special case of Fermat's last theorem with $n=5$, and so has no solution. improving on the results on Lander *et al.* (1967), who checked up to 2.8×10^{14}. (In fact, no solutions are known for powers of 6 or 7 either.) No solutions to the 5.1.3 equation

$$A^5+B^5+C^5=D^5 \qquad (2)$$

are known (Lander *et al.* 1967). For 4 fifth powers, the 5.1.4 equation has solutions

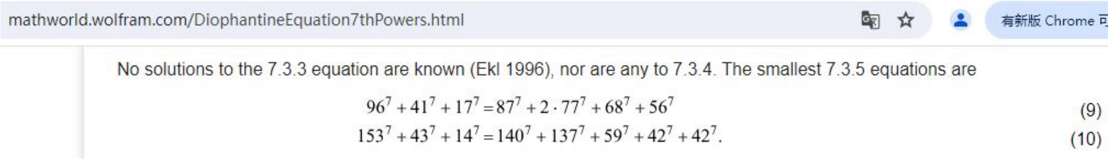
$$27^5+84^5+110^5+133^5=144^5 \qquad (3)$$
$$85\,282^5+28\,969^5+3183^5+55^5=85\,359^5 \qquad (4)$$



mathworld.wolfram.com/DiophantineEquation6thPowers.html

(Guy 1994, pp. 140 and 142). Known solutions are

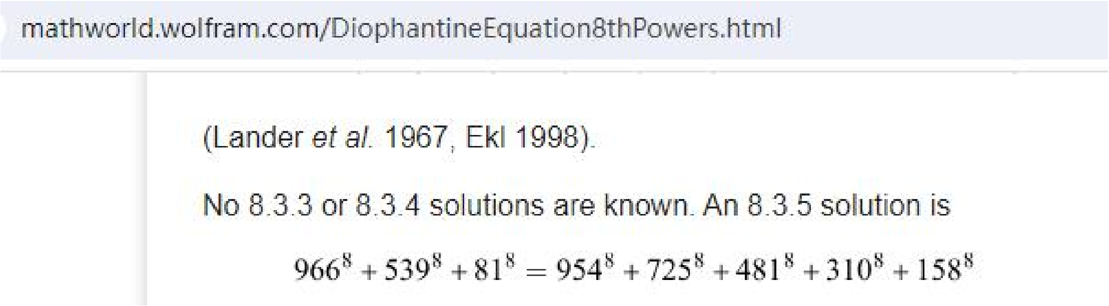
$$3^6+19^6+22^6=10^6+15^6+23^6$$
$$36^6+37^6+67^6=15^6+52^6+65^6$$
$$33^6+47^6+74^6=23^6+54^6+73^6$$
$$32^6+43^6+81^6=3^6+55^6+80^6$$
$$37^6+50^6+81^6=11^6+65^6+78^6$$
$$25^6+62^6+138^6=82^6+92^6+135^6$$
$$51^6+113^6+136^6=40^6+125^6+129^6$$
$$71^6+92^6+147^6=1^6+132^6+133^6$$
$$111^6+121^6+230^6=26^6+169^6+225^6$$
$$75^6+142^6+245^6=14^6+163^6+243^6$$



mathworld.wolfram.com/DiophantineEquation7thPowers.html

No solutions to the 7.3.3 equation are known (Ekl 1996), nor are any to 7.3.4. The smallest 7.3.5 equations are

$$96^7+41^7+17^7=87^7+2\cdot77^7+68^7+56^7 \qquad (9)$$
$$153^7+43^7+14^7=140^7+137^7+59^7+42^7+42^7. \qquad (10)$$

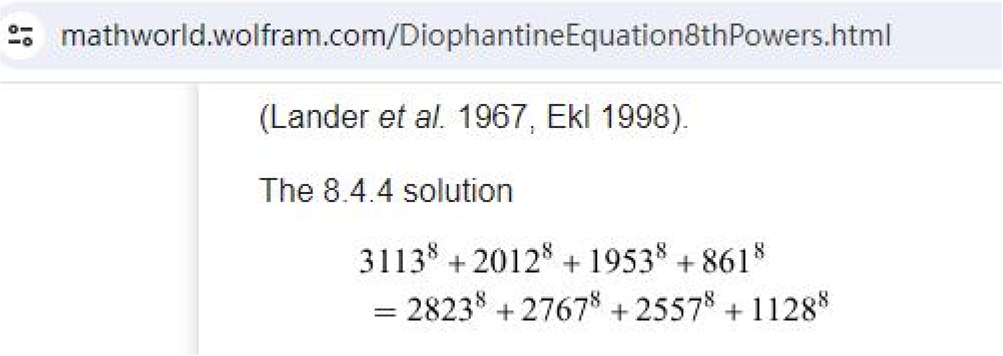


mathworld.wolfram.com/DiophantineEquation8thPowers.html

(Lander *et al.* 1967, Ekl 1998).

No 8.3.3 or 8.3.4 solutions are known. An 8.3.5 solution is

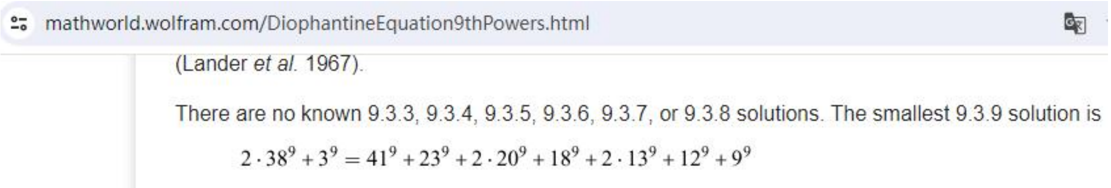
$$966^8+539^8+81^8=954^8+725^8+481^8+310^8+158^8$$



(Lander *et al.* 1967, Ekl 1998).

The 8.4.4 solution

$$\begin{aligned}&3113^8+2012^8+1953^8+861^8\\&=2823^8+2767^8+2557^8+1128^8\end{aligned}$$



(Lander *et al.* 1967).

There are no known 9.3.3, 9.3.4, 9.3.5, 9.3.6, 9.3.7, or 9.3.8 solutions. The smallest 9.3.9 solution is

$$2\cdot 38^9+3^9=41^9+23^9+2\cdot 20^9+18^9+2\cdot 13^9+12^9+9^9$$

The more variables, the higher the index, the larger the search scope, the greater the amount of calculation, and the more difficult it is to find the data, which is not found at present, not necessarily not.

The main idea behind the proof of Fermat's Last Theorem mentioned above was initially completed by the author in early 1983 when he decided to study mathematics, but it failed to be submitted multiple times.