Open Access Library Journal
2024, Volume 11, e12171
ISSN Online: 2333-9721
ISSN Print: 2333-9705

A Proof of a Conjecture and Twenty-Five Conjectures in Number Theory

Zhongqi Zhou

Hubei Coal Geology Bureau, Wuhan, China
Email: zhouzongqi1058@163.com

How to cite this paper: Zhou, Z.Q. (2024) A Proof of a Conjecture and Twenty-Five Conjectures in Number Theory. *Open Access Library Journal*, **11**: e12171.
https://doi.org/10.4236/oalib.1112171

Received: August 26, 2024
Accepted: September 24, 2024
Published: September 27, 2024

Abstract

1) Fermat has proved that $x^4+y^4=z^2$ has no positive integer solution, and in 2011, J. Cullen [1] reported that $x,y\in\{0,1,\cdots,10^7\}$, x^4+y^4+1 is not a square greater than 1, and conjecture: $x^4+y^4+1\neq z^2$, $z\in\{2,3,\cdots\}$, $x,y\in\{0,1,\cdots\}$. On May 15, 2021, Sun Zhiwei [2] proposed that neither $x^4+y^4+1(x,y\in N)$ is a perfect power based on Cullen's conjecture (the form is $z^m,(z,m\in\{2,3,\cdots\})$ called perfect power). This paper generalizes and proves J. Cullen's conjecture. 2) A lot of data calculation and verification are carried out, and 25 conjectures in number theory are put forward for number theory lovers to study.

Subject Areas

Integer Equation, Number Theory

Keywords

New Conjecture in Number Theory, A Generalization of Cullen's Conjecture, Proof of the Conjecture, Computational Verification Methods

1. Introduction

An important factor in the never-ending progress of mathematics is the constant supply of new problems to stimulate its development. The mathematician W. Sierpinski said: "The accumulation of our knowledge of number theory depends not only on theorems that have been proved, but also on conjectures that are unknown".

In this paper, based on the generalization and proof of J. Cullen's conjecture, we present 25 conjectures in number theory, most of which are related to unsolved problems in a certain class of number theory. We know that none of the following problems in number theory have been completely solved:

1) There are infinitely many twin prime numbers (related to conjecture 1).

2) Any even number greater than 4 can be expressed as the sum of two primes (related to conjecture 3).

3) There are infinitely many prime primes of the shape x^2+1 (related to conjecture 5).

4) There are infinitely many prime primes of the shape x^2+m^2. m is a given positive integer (related to conjecture 4).

5) There are infinitely many or only finite number of Fermat prime (related to conjecture 7.16).

6) The Guiga conjecture holds (related to conjecture 10).

7) There are infinitely many Mersenne primes (related to conjecture 25).

8) There are infinitely many Fibonacci primes (related to conjecture 23).

9) There are infinitely many Lucas primes (related to conjecture 24).

10) −2 perfect numbers only have the form $\frac{F_n(F_n-1)}{2}$. $F_n=2^{2^n}+1$ is a prime. (related to conjecture 2).

There are also conjectures which raise some new number theory questions.

The formulation of these conjectures also suggested possible ways to prove the above problems. These conjectures are programmed with Maple, after a lot of calculation and verification.

2. A Proof of a Conjecture

In 2011, J. Cullen reported in [1] that: $x,y\in\{0,1,2,\cdots,10^7\}$, x^4+y^4+1 is not a square greater that 1, and guesses: $x,y\in\{0,1,2,\cdots\}$, $z\in\{2,3,\cdots\}$, there are all:

$$x^4+y^4+1\neq z^2.$$

This paper generalizes and proves J. Cullen's conjecture.

Lemma 1. If p is a prime number, $n\mid p-1$, $(p,a)=1$, then

$$x^n\equiv a\left(\bmod p^\alpha\right) \tag{1}$$

the necessary and sufficient condition for a solution is

$$a^{\frac{\varphi(p^\alpha)}{n}}\equiv 1\left(\bmod p^\alpha\right)$$

Proof: Necessity: If congruence (1) has a solution x_0, then $(p,x_0)=1$, according to Fermat's little theorem:

$$a^{\frac{\varphi(p^\alpha)}{n}}\equiv\left(x_0^n\right)^{\frac{\varphi(p^\alpha)}{n}}\equiv x_0^{\varphi(p^\alpha)}\equiv 1\left(\bmod p^\alpha\right).$$

Adequacy: If $a^{\frac{\varphi(p^\alpha)}{n}}\equiv 1\left(\bmod p^\alpha\right)$ is true, then

$$x\left(x^{\varphi(p^\alpha)}-1\right)=x\left(\left(x^n\right)^{\frac{\varphi(p^\alpha)}{n}}-a^{\frac{\varphi(p^\alpha)}{n}}+a^{\frac{\varphi(p^\alpha)}{n}}-1\right)=\left(x^n-a\right)P(x)+x\left(a^{\frac{\varphi(p^\alpha)}{n}}-1\right).$$

Where $P(x)$ is the polynomial with integral coefficients about *x*.

Lemma 2. Let $t\geq 2$, if $x^{2^t}\equiv -1\pmod{l}$ has a solution, then

$$l=2^\beta\times p_1^{\beta_1}\cdots p_r^{\beta_r}.$$

p_i is a different prime number, $p_i\equiv 1\left(\bmod 2^{t+1}\right)$, $i=1,2,\cdots,r$, $\beta=0,1$.

Proof: According to lemma 1, the necessary and sufficient conditions for $x^{2^t}\equiv -1\left(\bmod p_i^\alpha\right)$ to have a solution are:

$$(-1)^{\frac{\phi(p_i^\alpha)}{2^t}}=(-1)^{\frac{p_i^{\alpha-1}(p_i-1)}{2^t}}\equiv 1\left(\bmod p_i^\alpha\right).$$

i.e.

$$p_i\equiv 1\left(\bmod 2^{t+1}\right).$$

Also, $1^{2^t}\equiv -1\pmod{2}$, so 1 is the solution to $x^{2^t}\equiv -1\pmod{2}$.

Based on the above proof, the following conclusions can be drawn:

1) If $x^{2^t}\equiv -1\pmod{l}$ has a solution, then $l=2^\beta\times p_1^{\beta_1}\cdots p_r^{\beta_r}$. $p_i\equiv 1\left(\bmod 2^{t+1}\right)$,

$$i=1,2,\cdots,r.\quad \beta=0,1.$$

2) If there are non-2 non- $2^{t+1}h+1\,(h\in N)$ factors in *l*, then $x^{2^t}\equiv -1\pmod{l}$ has no positive integer solution.

Lemma 3. Let $z\in\{2,3,\cdots\}$, $m\geq 2$, and *m* be even, then: z^m-1 must have a factor that is neither 2 nor $2^{t+1}h+1\,(h\in N)$.

Proof: When $z=2u$ and *m* is even, $(2u)^m-1\not\equiv 1\left(\bmod 2^{t+1}\right)$,

i.e.

$$(2u)^m-1\neq 2^{t+1}k+1.$$

When $z=2u+1$ and *m* is even, $4\mid(2u+1)^m-1$.

So z^m-1 must have a factor that is neither 2 nor $2^{t+1}k+1$.

Lemma 4. Let $t,z\in\{2,3,\cdots\}$, $m\geq 2$, $m\equiv 0\pmod{2}$, then $s^{2^t}\equiv -1\left(\bmod z^m-1\right)$ has no positive integer solution.

Proof. According to lemma 2: if $s^{2^t}\equiv -1\left(\bmod z^m-1\right)$ has a positive integer solution, then $z^m-1=2^\beta\times p_1^{\beta_1}\cdots p_r^{\beta_r}$. $p_i\equiv 1\left(\bmod 2^{t+1}\right)$, $i=1,\cdots,r$. $\beta=0,1$. According to lemma 3, z^m-1 must have a factor that is neither 2 nor $2^{t+1}h+1$, $h\in N$. The combination of the two lemma gives: $s^{2^t}\equiv -1\left(\bmod z^m-1\right)$ has no positive integer solution.

Lemma 5 [3]. Let $n\geq 2$ and $m>3$ be the given positive integers, and if $s^n\equiv -1\pmod{m}$ has no positive integer solution, then

$$m=x^n+y^n$$

Has no positive integer solution. Where $(x,y)=1$.

Theorem. Let $z,t\in\{2,3,\cdots\}$, $k\in\{1,2,\cdots\}$, $x,y\in\{0,1,\cdots\}$, then

$$x^{2^t}+y^{2^t}+1\neq z^{2k}.$$

Proof: According to lemma 4: $s^{2^t}\equiv -1\left(\bmod z^{2k}-1\right)$ has no positive integer solution, and according to lemma 5, it can be obtained:

$$x^{2^t}+y^{2^t}\neq z^{2k}-1,$$

namely

$$x^{2^t}+y^{2^t}+1\neq z^{2k}.$$

Corollary 1.

$z^{2k}-x^{2^t}=1$ no positive integer solution.

Where $z,t\in\{2,3,\cdots\}$, $k\in\{1,2,\cdots\}$, $x\in\{0,1,\cdots\}$.

Corollary 2.

Let $t,z,m\in\{2,3,\cdots\}$, if $z\not\equiv 3\left(\bmod 2^{t+2}\right)$, then $x^{2^t}+y^{2^t}+1\neq z^m$.

Where $z,m,t\in\{2,3,\cdots\}$, $x,y\in\{0,1,\cdots\}$.

Proof. When z,m are both odd, $z^m-1=(z-1)\left(z^{m-1}+z^{m-2}+\cdots+z+1\right)$, since $z\not\equiv 3\left(\bmod 2^{t+2}\right)$, so $\frac{z-1}{2}\not\equiv 1\left(\bmod 2^{t+1}\right)$. Therefore, there must be a factor that is neither 2 nor $2^{t+1}l+1$ in $z-1$, and then there is also a factor that is neither 2 nor $2^{t+1}l+1$ in z^m-1, according to lemma 3 and lemma 4, then $s^{2^t}\equiv -1\left(\bmod z^m-1\right)$ has no positive integer solution, according to the theorem and lemma 5, $x^{2^t}+y^{2^t}\neq z^m-1$, and thus

$$x^{2^t}+y^{2^t}+1\neq z^m.$$

3. Twenty-Five Conjectures in Number Theory

Conjecture 1

Let $a\geq 2$, there must be a b between a and $2a$ such that $b(b+1)\pm 1$ are both prime.

Verify until $a\leq 10^8$.

Since $b(b+1)\pm 1$ is a pair of twin prime, it follows that there are infinitely many twin prime.

Conjecture 2

Definition of z perfect number:

Let m be a positive integer, $\sigma(m)$ be the sum of all positive factors of m, and z be any integer, if

$$\sigma(m)-2m=z$$

Then m called z perfect number.

If $z=0$, then m is perfect number.

From the above definition, if $F_n=2^{2^n}+1$ (Fermat number) is a prime, then $\frac{F_n(F_n-1)}{2}$ is −2 perfect number.

Proof: Since $m=\frac{F_n(F_n-1)}{2}=2^{2^n-1}\left(2^{2^n}+1\right)$, $2^{2^n}+1$ is a prime number, then

$\sigma(m)=\left(2^{2^n}-1\right)\left(2^{2^n}+2\right)=2\left(2^{2^n-1}\left(2^{2^n}+1\right)-1\right)=2m-2$.

Which is to say:

$$2^{2^0-1}\left(2^{2^0}+1\right)=3$$

$$2^{2^1-1}\left(2^{2^1}+1\right)=10$$

$$2^{2^2-1}\left(2^{2^2}+1\right)=136$$

$$2^{2^3-1}\left(2^{2^3}+1\right)=32896$$

$$2^{2^4-1}\left(2^{2^4}+1\right)=2147516416$$

Both are −2 perfect numbers.

Guess:

All even −2 perfect number can only have the form: $\frac{F_n(F_n-1)}{2}$, *i.e.* the sufficient and necessary condition for *m* to be −2 perfect number is

$$m=\frac{F_n(F_n-1)}{2}.$$

where $F_n=2^{2^n}+1$ is a prime number.

There are no longer odd −2 perfect numbers.

Verify until $m\le 10^9$.

Conjecture 3

Let $\varphi(m)$ be the Euler function, *m* is a positive integer, when $m\ge 4$, there are at least two prime numbers p_1 and p_2 between $m-\varphi(m)$ and $m+\varphi(m)$ such that

$$p_1+p_2=2m.$$

Verify until $m\le 10^8$.

This conjecture is stronger than Gldbach's conjecture, and if this conjecture is true, Gldbach's conjecture must be true.

Conjecture 4

Given a positive integer *m*, if $n>m>3$, there must be an $i=1,2,\cdots,n$ to makes

$$(n+i)^2+m^2$$

is a prime number.

Verify until $m\le 10^6$.

If this conjecture is true, then there are infinitely many prime numbers of the shape x^2+m^2.

Conjecture 5

If $n\ge 2$, then there must be an $i=1,2,\cdots,n$ makes

$$(n+i)^2+1$$

is a prime number.

Verify until $n\le 10^8$.

If this conjecture is true, then there are infinitely many prime number of the shape x^2+1.

Conjecture 6

Let *q* be a odd prime, $W_q=\frac{2^q+1}{3}$ (Wagstaff number), if $7^{\frac{W_q-1}{2}}\equiv -1\left(\bmod W_q\right)$, then W_q is a prime.

Verify until $q\le 10^5$.

Conjecture 7

For a given positive integer *n*, if $n\ge 5$, equation

$$x^2+x+y^2=2^{2^n-2} \tag{2}$$

There are always integer solutions, and if this conjecture is true, then $F_n=2^{2^n}+1$ for $n\ge 5$ is composite. Because: Multiply both sides of (2) by 4 and add 1 to get:

$$(2x+1)^2+(2y)^2=2^{2^n}+1.$$

Since F_n (Fermat number) can be expressed in forms as the sum of two squares, F_n is composite.

If *n* exist such that (2) has no integer solution, then F_n is prime.

Verify until $n\le 32$.

Conjecture 8

Let $Z_{\max}(n)=p$, where *p* is the largest prime factor of *n*. Take $5\times Z_{\max}(m)+1$ for any odd natural number *m*, or divide by 2 for any even number, and so on, to get 1.

Verify until $m\le 5\times 10^3$.

Conjecture 9

Let $Z_{\max}(n)=p$, where *p* is the largest prime factor of *n*. Take $3\times Z_{\max}(m)+1$ for any odd natural number *m*, or divide by 2 for any even number, and so on, to get 1.

Verify until $m\le 5\times 10^3$.

Conjecture 10

Let Carmichael number $m=p_1p_2\cdots p_r$. p_i are different odd prime number, $i=1,\cdots,r$, then

$$\sum_{i=1}^{r}\frac{1}{p_i}<1.$$

Verify until $m\le 10^8$.

If this conjecture is true, so is the Giuga conjecture [4].

Conjecture 11

Let $x,y,z>1$, $x,y,z\in N$, Then

$$x^0+x^1+\cdots+x^z=y^2$$

There are only two sets of positive integer solutions:

$x=3,z=4,y=11$ and $x=7,z=3,y=20$.

Verify until $x \le 10^3, z \le 30$ (different values are high values).

Conjecture 12

Indeterminate equation

$$x^p - y^q = 2$$

Only $x = 3,\ p = 3,\ y = 5,\ q = 2$ a set of positive integer solutions. $p, q > 1$.

Conjecture 13

Indeterminate equation

$$x^p - y^q = 3$$

Only $x = 2,\ p = 7,\ y = 5,\ q = 3$ a set of positive integer solutions. $p, q > 1$.

Conjecture 14

Let $p > 3$ be odd, then p is prime if and only if

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} \equiv 0 \pmod{p}.$$

Verify until $p \le 10^6$.

Conjecture 15

p is prime when $p \equiv 1 \pmod{8}$, then

$$p = x^2 + q.$$

Where x is an integer and q is a odd prime. $q \equiv 1 \pmod{12}$.

Verify until $p \le 10^7$.

Conjecture 16

Definition of number of children:

Let n be even, and if $a + b = n$ and $a \times b = 2^r k\left(2^r k + 1\right)$ or $a \times b = 2^r k\left(2^r k - 1\right)$, then a and b are called pairs of children of n. where $r \ge 1$ and k is odd.

Guess:

When $m \ge 9, n = 2^m$ always has a number of children.

Verify until $m \le 2^{32}$ (can prove it).

If this conjecture is true, then conjecture 7 is also true.

Conjecture 17

Let $m \ge 3$ is odd, then

$$q_m(2) = \frac{2^{\varphi(m)} - 1}{m} \equiv \frac{1}{2} \sum_{\substack{k=1 \\ (k,m)=1}}^{m-1} \frac{(-1)^{k-1}}{k} \pmod{m}$$

Verify until $m \le 10^5$.

Conjecture 18

Let $(a, m) = 1, a \ge 2, m \ge 3$, then

$$q_m(a) = \frac{a^{\varphi(m)} - 1}{m} \equiv \frac{1}{a} \sum_{\substack{k=1 \\ (k,m)=1}}^{m-1} \frac{1}{k}\left[\frac{ka}{m}\right] \pmod{m}$$

Verify until $m \le 10^5$.

Conjecture 19

If $m \equiv -1 \pmod{12}$, then m is not a Carmichael number.

Verify until $m \le 10^8$.

Conjecture 20

Any odd number m greater than 1 can be represented as

$$m^2 = p + 2x^2.$$

p odd prime number.

Verify until $m \le 10^5$.

Conjecture 21

Any odd number m greater than 3, $(m,3)=1$, can be expressed as:

$$m^2 = p + 3x^2.$$

$p \equiv 1 \pmod{12}$, p odd prime.

Verify until $m \le 10^5$.

Conjecture 22

R is odd, if $\varsigma(R) \mid R-2$, then $R = p_1$ or $R = p_1 p_2$ or $R = p_1 p_2 p_3$.

p_i is the different odd prime numbers, $i = 1,2,3$. $\varsigma(R)$ is the sum of all true factors of R.

Verify until $R \le 5 \times 10^9$.

If this conjecture is true, then conjecture 2 is also true.

Conjecture 23

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = bu_n - cu_{n-1},\ n = 0,1,2,\cdots \quad u_n = u_n(b,c).$$

Let $2^{2^{k-1}} < p \le 2^{2^k}$, p is prime, then there are $\ge 2^k$ p's such that $u_p(1,1)$ is prime.

Verify until $p \le 8 \times 10^4$.

Conjecture 24

$$v_0 = 2,\ v_1 = b,\ v_{n+1} = bv_n - cv_{n-1},\ n = 1,2,\cdots \quad v_n = v_n(b,c).$$

Let $2^{2^{k-1}} \le p \le 2^{2^k}$, p is prime, then there are $\ge 2^k$ p's such that $v_p(1,1)$ is prime.

Verify until $p \le 8 \times 10^4$.

Conjecture 25

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = bu_n - cu_{n-1},\ n = 0,1,2,\cdots \quad u_n = u_n(b,c).$$

Let $2^{2^{k-1}} < p < 2^{2^k}$, p is prime, then there are $\ge 2^k - 1$ p's such that $u_p(3,2)$ is prime.

Verify until $p \le 10^6$.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Cullen, J. (2011) Diophantine Equations-Computer Search Results. http://members.bex.net/jtcullen515/Math10.htm

[2] Sun, Z.W. (2021) New Conjectures in Number Theory and Combination. Harbin Institute of Technology Press, 143.

[3] Zhou, Z.Q. (2024) The Solution of the Indefinite Equation by the Method of Euclidean Algorithm. *Open Access Library Journal*, **11**, e12011. https://doi.org/10.4236/oalib.1112011

[4] Liebenbaum, P. (2007) Profound Prime Numbers. Science Press, 19.