Proof of Fermat's last theorem (Part I of III)

\[ a^n + b^n = c^n \quad (n > 1 \text{ and odd}) \]

Objet: Proof of Fermat's last theorem with conventional means.

Author: Romdhane DHIFAOUI (romdhane.dhifaoui@yahoo.fr).

1) Introduction:
   ✓ I am not a professional of mathematics.
   ✓ My English is poor. I use google translate to write these pages.

2) I prove that \( c < (a + b) \)

\[
(a + b)^n = a^n + b^n + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n-k}
\]

Then \((a + b)^n > (a^n + b^n)\)
Then \((a + b)^n > c^n\) because \(c^n = a^n + b^n\)
Then \((a + b) > c\)
d is a natural number. It is the complement of c to \((a + b)\).
\[
c + d = a + b
\]
\[
c = a + b - d
\]
\[
c - b = a - d
\]
\[
c - a = b - d
\]

3) I prove a parity of d
Whatever the parity of a, b and c, we can easily verify that d is always even.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>even</td>
<td>even</td>
<td>even</td>
<td>even</td>
</tr>
<tr>
<td>even</td>
<td>odd</td>
<td>odd</td>
<td>even</td>
</tr>
<tr>
<td>odd</td>
<td>even</td>
<td>odd</td>
<td>even</td>
</tr>
<tr>
<td>odd</td>
<td>odd</td>
<td>even</td>
<td>even</td>
</tr>
</tbody>
</table>

\[ 2^n \text{ divide } d^n. \]
4) **Conditions (supposition) to prove Fermat's last theorem:**

- a, b, c, d and n are non-zero positive integers
- a, b and c are pairwise coprime
- n > 1 and odd
- $a^n + b^n = c^n$
- $a + b = c + d$
- $a < b$

5) I prove that c is not coprime with d

\[
\begin{align*}
d^n &= d^n \\
c^n - a^n - b^n &= 0 \\
d^n &= d^n + c^n - a^n - b^n \\
d^n &= (d^n + c^n) - (a^n + b^n) \\
(c + d) &\text{ divide } (d^n + c^n) \\
(a + b) &\text{ divide } (a^n + b^n) \\
(c + d) &= (a + b) \\
(c + d) &\text{ divide } d^n
\end{align*}
\]

Any integer which divide $(c + d)$ divide $d^n$

Any prime number which divide $(c + d)$ divide $d^n$

Any prime number which divide $(c + d)$ divide $d$

Any prime number which divide $[(c + d) \text{ and } d]$ divide $c$

**c is not coprime with d**

$(c + d) = (a + b)$

**a+b divide d**

Any integer which divide $(a + b)$ divide $d$

6) I prove that a is not coprime with d

\[
\begin{align*}
d^n &= d^n \\
c^n - a^n - b^n &= 0 \\
d^n &= d^n + c^n - a^n - b^n \\
d^n &= (c^n - b^n) - (a^n - d^n) \\
(c - b) &\text{ divide } (c^n - b^n) \\
(a - d) &\text{ divide } (a^n - d^n) \\
(c - b) &= (a - d) \\
(a - d) &\text{ divide } d^n \\
(c - b) &\text{ divide } d^n
\end{align*}
\]
Any integer which divide \((a - d)\) divide \(d^n\)
Any prime number divide \((a - d)\) divide \(d^n\)
Any prime number divide \((a - d)\) divide \(d\)
Any prime number divide \([(a - d)\ and \ d]\) divide \(a\)
a \textit{is not coprime with} \(d\) (Except if \((a - d) = 1\)).
\((c - b) = (a - d)\)
\((c - b)\ divide \(d^n\)
Any prime number which divide \((c - b)\) divide \(d\).

7) \textbf{I prove that} \(b\ \textit{is not coprime with} \(d\)
\(d^n = d^n\)
\(c^n - a^n - b^n = 0\)
\(d^n = d^n + c^n - a^n - b^n\)
\(d^n = (c^n - a^n) - (b^n - d^n)\)
\((c - a)\ divide \(c^n - a^n\)\)
\((b - d)\ divide \(b^n - d^n\)\)
\((c - a) = (b - d)\)
\((b - d)\ divide \(d^n\)\)
\((c - a)\ divide \(d^n\)\)
Any integer which divide \((b - d)\) divide \(d^n\)
Any prime number divide \((b - d)\) divide \(d^n\)
Any prime number divide \((b - d)\) divide \(d\)
Any prime number divide \([(b - d)\ and \ d]\) divide \(b\)
b \textit{is not coprime with} \(d\)
\((c - a) = (b - d)\)
\((c - a)\ divide \(d^n\)\)
Any prime number which divide \((c - a)\) divide \(d\)
8) Contraductions

I proved that:
1. Any prime number which divide \((a + b)\) divide \(d\).
2. Any prime number which divide \((c + d)\) divide \(d\).
3. Any prime number which divide \((a - d)\) divide \(d\).
4. Any prime number which divide \((c - b)\) divide \(d\).
5. Any prime number which divide \((b - d)\) divide \(d\).
6. Any prime number which divide \((c - a)\) divide \(d\).

Proof 1 and proof 3
Any prime number that divide \((d\) and \(a)\) must necessarily divide \(b\); but \(a\) and \(b\) are hypothetically pairwise coprime.

Proof 2 and proof 6
Any prime number that divide \((c\) and \(d)\) must necessarily divide \(a\); but \(c\) and \(a\) are hypothetically pairwise coprime.

Proof 2 and proof 4
Any prime number that divide \((c\) and \(d)\) must necessarily divide \(b\); but \(c\) and \(b\) are hypothetically pairwise coprime.

...