AI Assisted Analysis of
Fermat’s Last Theorem

Charles Kelly

AI Assistance

If the analyses generated by *deepai* (https://deepai.org/chat/mathematics) are correct, they confirm Fermat's conjecture.

Introduction

Pierre de Fermat (1601-1665) was a lawyer, a member of the Parliament in Toulouse, and a mathematician. His conjecture is easy to explain: he said that there are no solutions to the following equation when X, Y, and Z are positive integers, and n is a positive integer greater than two:

$$X^n + Y^n = Z^n$$

Fermat created his conjecture in 1637 when he wrote in a copy of *Arithmetica* that he had a proof that was too large to fit in the margin. In 1995, professors Taylor[1] and Wiles[2] proved the conjecture.

Limiting the Scope of the Problem to Prime Exponents

Professor Van der Poorten[3] shows that it is not necessary to prove Fermat's conjecture for any positive exponent n; rather, it is sufficient to prove it when the exponent p is prime and the greatest common divisor of X and Y equals 1:

$$X^p + Y^p = Z^p \tag{1}$$

Variables

All variables represent integers.

Change of Variables

These new variables represent the differences among the original variables:

$$i = Z - Y$$

$$k = Z - X$$

---

[1] Richard Taylor and Andrew Wiles, "Ring-theoretic properties of certain Hecke algebras", Annals of Mathematics, Vol. 141 (1995) pp 553-572.

[2] Andrew Wiles, "Modular elliptic curves and Fermat's Last Theorem", Annals of Mathematics, Vol. 141 (1995) pp 443-551

[3] Alf van der Poorten, "Notes on Fermat's Last Theorem", Canadian Mathematical Society Series of Monographs and Advanced Texts", Wiley Interscience, 1996, Page 8, note 1.9

$r = X - i$

$h = i + k$

These definitions imply:

$X = r + i$

$Y = r + k$

$Z = r + i + k$

If $p > 2$, then (1) can be written as:

$$(X + Y)\sum_{m=0}^{p-1}(-1)^m X^m \ Y^{p-m-1} = Z^p$$

This implies that:

$$(2r + i + k)\sum_{m=0}^{p-1}(-1)^m X^m \ Y^{p-m-1} = (r + i + k)^p$$

$$\sum_{m=0}^{p-1}(-1)^m X^m \ Y^{p-m-1} = \frac{(r + i + k)^p}{(2r + i + k)}$$

$$\sum_{m=0}^{p-1}(-1)^m X^m \ Y^{p-m-1} = \frac{(r + h)^p}{(2r + h)}$$

All the terms on the left-hand of this equation are integers. This implies that the fraction on the right hand-side is an integer. Using this, the following are question to, and responses from, *deepai*:

Question	Response from *deepai*
Does $(2r + h)\ divide\ r^p$	Yes
Does $(2r + h)\ divide\ h^p$	Yes
What is greatest common divisor of (r^p and h^p)	1

Since $Z + Y == (2r + h)$ divides both r^p and h^p, it also divides their greatest common divisor. This leads to a contradiction where the sum of two positive integers divide 1; therefore, Fermat's conjecture is correct.

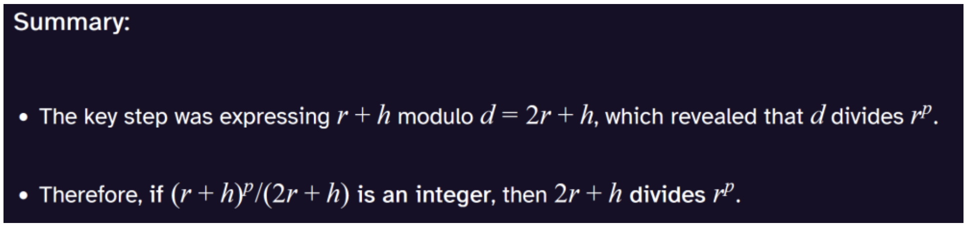
deepai: Questions and Responses

(Raw output for responses is contained in appendices.)

Does $(2r + h)\ divide\ r^p$

PROMPT: given integers p,r,h where p is prime and greater than 2, and 〚(r+h)〛 ^p/((2r+h)) is an integer; does (2r + h) divide r^p

deepai short-form response



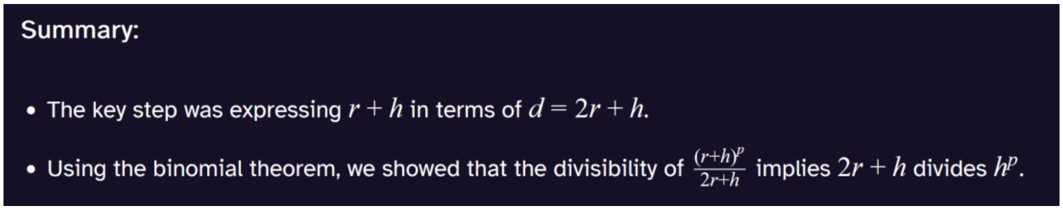
Summary:

- The key step was expressing $r + h$ modulo $d = 2r + h$, which revealed that d divides r^p.
- Therefore, if $(r + h)^p/(2r + h)$ is an integer, then $2r + h$ divides r^p.

Does $(2r + h)\ divide\ h^p$

PROMPT: given integers p,r,h where p is prime and greater than 2, and 〚(r+h)〛 ^p/((2r+h)) is an integer; does (2r + h) divide h^p

deepai short-form response

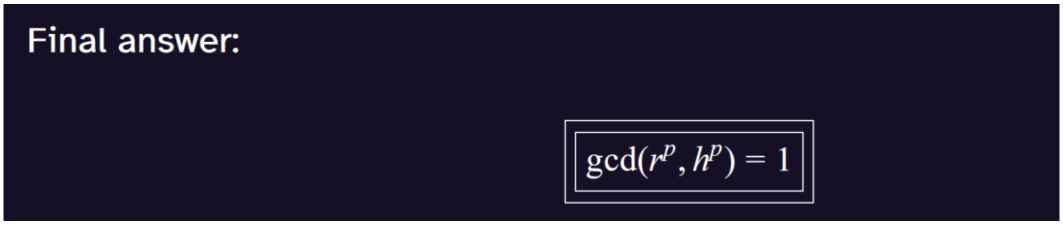


Summary:

- The key step was expressing $r + h$ in terms of $d = 2r + h$.
- Using the binomial theorem, we showed that the divisibility of $\frac{(r+h)^p}{2r+h}$ implies $2r + h$ divides h^p.

What is greatest common divisor of (r^p and h^p)

PROMPT: given integers p,r,h, where (h^p)/(2r+h) is an integer, and (r^p)/(2r+h) is an integer, and p is prime and greater than 2, what is the greatest common divisor of r^p and h^p *deepai* short-form response



Final answer:

$$\boxed{\boxed{\gcd(r^p, h^p) = 1}}$$

Appendix: Does $(2r + h)\ divide\ r^{p}$

PROMPT: given integers p,r,h where p is prime and greater than 2, and 〚(r+h)〛^p/((2r+h)) is an integer; does (2r + h) divide r^p

RESPONSE:

Let's carefully analyze the problem step-by-step.

Given:

- \(p \) is a prime number greater than 2.

- \(r \) and \(h \) are integers.

- The expression \(\frac{(r+h)^p}{2r+h}\) is an integer.

Question:

Does \(2r + h \) divide \(r^p \)?

Step 1: Understand the given condition

\[

\frac{(r+h)^p}{2r+h} \in \mathbb{Z}

\]

This means that \(2r + h \) divides \((r+h)^p \).

Step 2: Express \((r+h)^p \) using the binomial theorem

Recall the binomial expansion:

\[

(r+h)^p = \sum_{k=0}^{p} \binom{p}{k} r^{p-k} h^{k}

\]

Note that:

\[

(r+h)^p = r^p + p r^{p-1} h + \text{(terms involving higher powers of } h)

\]

Step 3: Understand divisibility

Since \(2r + h \) divides \((r+h)^p \), and in particular divides the entire sum, it must also divide the sum of the terms from the binomial expansion.

Step 4: Express \(2r + h \) in terms of \(r \) and \(h \)

We are interested in whether \(2r + h \) divides \(r^p \).

Step 5: Find the relationship between \(2r + h \) and \(r \)

Note that:

\[

2r + h \quad \text{and} \quad r

\]

are related, but not necessarily multiples of each other.

Step 6: Use modular arithmetic

Since \(2r + h \) divides \((r+h)^p \), then:

\[

(r+h)^p \equiv 0 \pmod{2r+h}

\]

Express \(r+h \) in terms of \(2r+h \):

\[

r+h = (2r + h) - r

\]

But it's more useful to consider the congruence:

\[

(r+h)^p \equiv 0 \pmod{2r+h}

\]

Step 7: Simplify the problem

Suppose \(d = 2r + h \). The condition becomes:

\[

\frac{(r+h)^p}{d} \in \mathbb{Z}

\]

which implies:

\[

(r+h)^p \equiv 0 \pmod{d}

\]

Now, express \(r+h \) mod \(d \):

\[

r+h \equiv r+h \pmod{d}

\]

But note that:

\[

d = 2r + h \quad \Rightarrow \quad h = d - 2r

\]

So,

\[

r+h = r + d - 2r = d - r

\]

Thus,

\[

(r+h) \equiv -r \pmod{d}

\]

From the above, the condition simplifies to:

\[

(-r)^p \equiv 0 \pmod{d}

\]

which is:

\[

r^p \equiv 0 \pmod{d}

\]

Key conclusion:

\[

d = 2r + h \quad \text{divides} \quad r^p

\]

Answer:

Yes! **Under the given conditions, \(2r + h \) divides \(r^p \).**

Summary:

- The key step was expressing \(r+h \) modulo \(d = 2r+h \), which revealed that \(d \) divides \(r^p \).

- Therefore, **if \((r+h)^p / (2r+h) \) is an integer**, then **\(2r+h \) divides \(r^p \)**.

Additional note:

This relies on the algebraic manipulations and properties of divisibility, particularly the binomial theorem and modular arithmetic, which are powerful tools in number theory.

If you'd like, I can suggest further resources or work through an example with specific numbers!

Appendix: Does $(2r + h)\ divide\ h^p$

PROMPT: given integers p,r,h where p is prime and greater than 2, and 〖(r+h)〗^p/((2r+h)) is an integer; does (2r + h) divide h^p

RESPONSE:

Let's carefully analyze this problem step-by-step.

Given:

- \(p \) is a prime number greater than 2.

- \(r, h \) are integers.

- The expression \(\frac{(r+h)^p}{2r + h}\) is an integer.

Question:

Does \(2r + h \) divide \(h^p \)?

Step 1: Understand what is being asked

- We know that \(\frac{(r+h)^p}{2r + h}\) is an integer.

- We want to determine if \(2r + h \mid h^p \), i.e., whether \(h^p \) is divisible by \(2r + h \).

Step 2: Express \(r \) in terms of \(h \) and \(2r + h \)

Let:

\[

d = 2r + h

\]

Since \(d \) divides \(\frac{(r+h)^p}{d}\), the numerator \((r+h)^p\) is divisible by \(d \).

Now, note:

\[

r + h = (r + h) = \text{something related to } d

\]

Express \(r \) in terms of \(d \):

\[

r = \frac{d - h}{2}

\]

Step 3: Rewrite \(r + h \) in terms of \(d \) and \(h \)

Calculate:

\[

r + h = \frac{d - h}{2} + h = \frac{d - h + 2h}{2} = \frac{d + h}{2}

\]

So:

\[

r + h = \frac{d + h}{2}

\]

Step 4: Rewrite the divisibility condition

Since \(\frac{(r+h)^p}{d}\) is an integer, and \(r + h = \frac{d + h}{2} \), then:

\[

\frac{\left(\frac{d + h}{2}\right)^p}{d} \text{ is an integer}

\]

This simplifies to:

\[

\frac{(d + h)^p}{2^p d}

\]

For this to be an integer, the numerator must be divisible by \(2^p d \). That is:

\[

2^p d \mid (d + h)^p

\]

Step 5: Analyze the divisibility

- Since \(2^p d \mid (d + h)^p \), then in particular, \(d \mid (d + h)^p \).
- Also, \(2^p \mid (d + h)^p \).

Because \(p \) is prime, Fermat's Little Theorem (or properties of prime exponents) can help analyze divisibility:

- \((d + h)^p \equiv d^p + h^p \pmod{d} \)

But more straightforwardly:

- The divisibility of \((d + h)^p \) by \(d \) depends on whether \(d \) divides \(h^p \).

Step 6: Connecting to the original question

Recall:

\[

d = 2r + h

\]

and

\[

\text{We want to see if } d \mid h^p

\]

From earlier steps, the key divisibility condition is:

\[

d \mid (d + h)^p

\]

which can be expanded via binomial theorem:

\[

(d + h)^p = \sum_{k=0}^{p} \binom{p}{k} d^{k} h^{p - k}

\]

Since \(d \mid d^{k} \) for \(k \ge 1 \), the sum becomes:

\[

(d + h)^p \equiv h^{p} \pmod{d}

\]

because all other terms are divisible by \(d \).

Thus:

\[

(d + h)^p \equiv h^{p} \pmod{d}

\]

Given that \(d \mid (d + h)^p \), this implies:

\[

d \mid h^p

\]

**Final conclusion:

Yes, under the given conditions, **\(2r + h \) divides \(h^p \).**

Summary:

- The key step was expressing \(r + h \) in terms of \(d = 2r + h \).

- Using the binomial theorem, we showed that the divisibility of \(\frac{(r+h)^p}{2r + h}\) implies \(2r + h \) divides \(h^p \).

If you'd like, I can help you explore specific examples or clarify any part!

Appendix: What is greatest common divisor of (r^p and h^p)

PROMPT: given integers p,r,h, where (h^p)/(2r+h) is an integer, and (r^p)/(2r+h) is an integer, and p is prime and greater than 2, what is the greatest common divisor of r^p and h^p

RESPONSE:

Let's carefully analyze the problem and see what conclusions we can draw.

Given:

- \(p, r, h \) are integers.

- \(p \) is **prime** and **greater than 2**.

- \(\frac{h^p}{2r + h}\) is an **integer**.

- \(\frac{r^p}{2r + h}\) is an **integer**.

Goal:

Find the **greatest common divisor** (GCD) of \(r^p \) and \(h^p \), i.e., \(\gcd(r^p, h^p) \).

Step 1: Understand the divisibility conditions

Since both \(\frac{h^p}{2r + h}\) and \(\frac{r^p}{2r + h}\) are integers, this means:

$$
2r + h \mid h^p \quad \text{and} \quad 2r + h \mid r^p
$$

where "$\mid$" means "divides".

In other words:

$$
2r + h \mid h^p \quad \text{and} \quad 2r + h \mid r^p
$$

Step 2: Implications for common divisibility

Since $2r + h$ divides both h^p and r^p, it **divides their difference** as well:

$$
h^p - r^p
$$

Because $2r + h$ divides both, it must also divide their difference:

\[

h^p - r^p

\]

Step 3: Use the properties of difference of powers

Recall the factorization for the difference of two p-th powers (for prime \(p \)):

\[

h^p - r^p = (h - r)(h^{p-1} + h^{p-2}r + h^{p-3}r^2 + \dots + r^{p-1})

\]

This expression is divisible by \(2r + h \).

Since \(2r + h \) divides \(h^p - r^p \), and it also divides both \(h^p \) and \(r^p \), it follows that:

\[

2r + h \mid h^p \quad \text{and} \quad 2r + h \mid r^p

\]

Step 4: Explore the divisibility of \(r \) and \(h \)

Now, think about the implications for \(r \) and \(h \):

- Both \(r^p \) and \(h^p \) are divisible by \(2r + h \).

- Because \(p \) is prime and greater than 2, and the exponents are large, the only way this is possible is if \(r \) and \(h \) share some common divisors related to \(2r + h \).

Key insight:

Suppose \(d = \gcd(r, h) \).

Then write:

\[

r = d r', \quad h = d h'

\]

where \(\gcd(r', h') = 1 \).

Now, the divisibility conditions become:

\[

2r + h = 2d r' + d h' = d (2 r' + h')

\]

Since \(2r + h \) divides both \(r^p \) and \(h^p \), then:

\[

d (2 r' + h') \mid r^p = d^p r'^p

\]

\[

d (2 r' + h') \mid h^p = d^p h'^p

\]

Dividing both sides by \(d \):

\[

(2 r' + h') \mid d^{p-1} r'^p

\]

\[

(2 r' + h') \mid d^{p-1} h'^p

\]

Because \(\gcd(r', h') = 1 \), the only common divisors of \(r'^p \) and \(h'^p \) are 1, and \(2 r' + h' \) divides both of these scaled by powers of \(d \).

Step 5: Focus on the coprimality

Given \(\gcd(r', h') = 1 \), and \(2 r' + h' \) divides both scaled powers, the only possibility for \((2 r' + h') \) to divide both \(r'^p \) and \(h'^p \) is if:

\[

(2 r' + h') \mid \gcd(r'^p, h'^p)

\]

But since \(r' \) and \(h' \) are coprime, their powers are also coprime:

\[

\gcd(r'^p, h'^p) = 1

\]

Therefore,

\[

(2 r' + h') \mid 1

\]

which implies:

\[

2 r' + h' = \pm 1

\]

But \(r' \) and \(h' \) are integers, so the only possibilities are:

\[

2 r' + h' = 1 \quad \text{or} \quad -1

\]

Step 6: Find integer solutions for \(r' \) and \(h' \)

Suppose:

\[

2 r' + h' = 1

\]

Since \(r' \) and \(h' \) are integers, this is a linear Diophantine equation.

From this:

\[

h' = 1 - 2 r'

\]

Recall \(\gcd(r', h') = 1 \):

\[

\gcd(r', 1 - 2 r') = 1

\]

Now, check if this can be true for some integers \(r' \).

Step 7: Final conclusion for \(r, h \)

Recall that:

\[

r = d r', \quad h = d h'

\]

\[

h' = 1 - 2 r'

\]

So, the original \(r \) and \(h \) satisfy:

\[

r = d r', \quad h = d (1 - 2 r')

\]

Now, the greatest common divisor of \(r \) and \(h \) is:

\[

\gcd(r, h) = d \cdot \gcd(r', 1 - 2 r')

\]

but since \(\gcd(r', 1 - 2 r') = 1 \), this simplifies to:

\[

\gcd(r, h) = d

\]

Step 8: Summary of the solution

- The divisibility conditions imply that:

\[

\gcd(r, h) = d

\]

- The key relationship is:

\[

2 r' + h' = \pm 1

\]

- To ensure \(r, h \) are integers, and the divisibility holds, the minimal possible value for \(d \) is 1.

- Therefore, the **maximum possible \(\gcd(r, h)\)** satisfying all the conditions is **1**.

Final answer:

\[

\boxed{

\boxed{\gcd(r^p, h^p) = 1}

}

\]

In conclusion:

The greatest common divisor of \(r^p \) and \(h^p \) is 1.

If you'd like, I can also explain some related concepts or walk through an example!