The ABC-conjecture

Frits Beukers

ABC-day, Leiden 9 september 2005
ABC-hits

The product of the distinct primes in a number is called the \textit{radical} of that number. Notation: $\text{rad}()$. For example,

\[ \text{rad}(2^2 \times 3^4) = 2 \times 3 = 6, \quad \text{rad}(2 \times 3 \times 5^2) = 2 \times 3 \times 5 = 30. \]
ABC-hits

- The product of the distinct primes in a number is called the radical of that number. Notation: $\text{rad}()$. For example,

$$\text{rad}(2^2 \times 3^4) = 2 \times 3 = 6, \quad \text{rad}(2 \times 3 \times 5^2) = 2 \times 3 \times 5 = 30.$$  

- Three positive integers $A, B, C$ are called $ABC$-triple if they are coprime, $A < B$ and

$$A + B = C$$
ABC-hits

▶ The product of the distinct primes in a number is called the \textit{radical} of that number. Notation: $\text{rad}()$. For example,

\[
\text{rad}(2^2 \times 3^4) = 2 \times 3 = 6, \quad \text{rad}(2 \times 3 \times 5^2) = 2 \times 3 \times 5 = 30.
\]

▶ Three positive integers $A, B, C$ are called $ABC$-triple if they are coprime, $A < B$ and

\[
A + B = C
\]

▶ Compute $\text{rad}(ABC)$ and check whether $\text{rad}(ABC) < C$. If this inequality is true we say that we have an $ABC$-hit!
ABC-hits

- The product of the distinct primes in a number is called the *radical* of that number. Notation: \( \text{rad}(\cdot) \). For example,

\[
\text{rad}(2^2 \times 3^4) = 2 \times 3 = 6, \quad \text{rad}(2 \times 3 \times 5^2) = 2 \times 3 \times 5 = 30.
\]

- Three positive integers \( A, B, C \) are called ABC-triple if they are coprime, \( A < B \) and

\[
A + B = C
\]

- Compute \( \text{rad}(ABC) \) and check whether \( \text{rad}(ABC) < C \). If this inequality is true we say that we have an ABC-hit!

- Among all \( 15 \times 10^6 \) ABC-triples with \( C < 10000 \) we have 120 ABC-hits.
ABC-hits

- The product of the distinct primes in a number is called the \textit{radical} of that number. Notation: \( \text{rad}(\cdot) \). For example,
\[
\text{rad}(2^2 \times 3^4) = 2 \times 3 = 6, \quad \text{rad}(2 \times 3 \times 5^2) = 2 \times 3 \times 5 = 30.
\]

- Three positive integers \( A, B, C \) are called \( ABC \)-triple if they are coprime, \( A < B \) and

\[
A + B = C
\]

- Compute \( \text{rad}(ABC) \) and check whether \( \text{rad}(ABC) < C \). If this inequality is true we say that we have an \( ABC \)-hit!

- Among all \( 15 \times 10^6 \) \( ABC \)-triples with \( C < 10000 \) we have 120 \( ABC \)-hits.

- Among all \( 380 \times 10^6 \) \( ABC \)-triples with \( C < 50000 \) we have 276 hits.
More hits

- Theorem: There are infinitely many ABC-hits.
More hits

- **Theorem:** There are infinitely many ABC-hits.
- **Proof:** Let us take $A = 1$ and $C = 3, 3^2, 3^4, 3^8, \ldots, 3^{2^k}, \ldots$.
  We determine how many factors 2 occur in $B = 3^{2^k} - 1$. 

Notice $3^{64} - 1 = (3^{32} + 1)(3^{32} - 1) = (3^{32} + 1)(3^{16} + 1)(3^{16} - 1) \cdots = (3^{32} + 1)(3^{16} + 1)(3^8 + 1) \cdots (3 + 1)(3 - 1)$.

So $3^{64} - 1$ is divisible by $2 \cdot 2^8$. 

The ABC-conjecture
More hits

- Theorem: There are infinitely many ABC-hits.
- Proof: Let us take $A = 1$ and $C = 3, 3^2, 3^4, 3^8, \ldots, 3^{2^k}, \ldots$. We determine how many factors 2 occur in $B = 3^{2^k} - 1$.
- Notice

\[
3^{64} - 1 = (3^{32} + 1)(3^{32} - 1) \\
= (3^{32} + 1)(3^{16} + 1)(3^{16} - 1) \\
\ldots \\
= (3^{32} + 1)(3^{16} + 1)(3^8 + 1) \cdots (3 + 1)(3 - 1)
\]

So $3^{64} - 1$ is divisible by $2 \cdot 2^8$. 
More hits

- Theorem: *There are infinitely many ABC-hits.*
- Proof: Let us take $A = 1$ and $C = 3, 3^2, 3^4, 3^8, \ldots, 3^{2^k}, \ldots$. We determine how many factors 2 occur in $B = 3^{2^k} - 1$.
- In general $3^{2^k} - 1$ is divisible by $2^{k+2}$. So

$$\text{rad}(B) = \text{rad}(3^{2^k} - 1) \leq (3^{2^k} - 1)/2^k < C/2^{k+1}$$

We conclude

$$\text{rad}(ABC) = 3 \cdot \text{rad}(B) < 3C/2^{k+1}.$$
More hits

- **Theorem:** _There are infinitely many ABC-hits._
- **Proof:** Let us take $A = 1$ and $C = 3, 3^2, 3^4, 3^8, \ldots, 3^{2^k}, \ldots$.

  We determine how many factors 2 occur in $B = 3^{2^k} - 1$.

  - In general, $3^{2^k} - 1$ is divisible by $2^{k+2}$. So

    \[
    \text{rad}(B) = \text{rad}(3^{2^k} - 1) \leq (3^{2^k} - 1)/2^k < C/2^{k+1}
    \]

    We conclude

    \[
    \text{rad}(ABC) = 3 \cdot \text{rad}(B) < 3C/2^{k+1}.
    \]

  - In other words, $C > \text{rad}(ABC) \cdot 2^{k+1}/3$. So when $k \geq 1$ we have an ABC-hit.
More hits

- **Theorem:** *There are infinitely many ABC-hits.*
- **Proof:** Let us take $A = 1$ and $C = 3, 3^2, 3^4, 3^8, \ldots, 3^{2^k}, \ldots$. We determine how many factors 2 occur in $B = 3^{2^k} - 1$.
- In general $3^{2^k} - 1$ is divisible by $2^{k+2}$. So
  \[
  \text{rad}(B) = \text{rad}(3^{2^k} - 1) \leq (3^{2^k} - 1)/2^k < C/2^{k+1}
  \]
  We conclude
  \[
  \text{rad}(ABC) = 3 \cdot \text{rad}(B) < 3C/2^{k+1}.
  \]
- In other words, $C > \text{rad}(ABC) \cdot 2^{k+1}/3$. So when $k \geq 1$ we have an ABC-hit.
- But we have shown more. For any number $M > 1$ there exist infinitely many ABC-triples such that $C > M \cdot \text{rad}(ABC)$. 

The ABC-conjecture
Super hits

▶ Instead of something linear in $\text{rad}(ABC)$ let us take something quadratic.

Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^2$ ?
Super hits

- Instead of something linear in $\text{rad}(ABC)$ let us take something quadratic.
  Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^2$?
- Answer: Unknown
Super hits

- Instead of something linear in $\text{rad}(ABC)$ let us take something quadratic.
  Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^2$?
- Answer: Unknown
- Working hypothesis: For every $ABC$-triple: $C < \text{rad}(ABC)^2$. 
Super hits

- Instead of something linear in \( \text{rad}(ABC) \) let us take something quadratic.
  Question: Are there \( ABC \)-triples such that \( C > \text{rad}(ABC)^2 \) ?
- Answer: Unknown
- Working hypothesis: For every \( ABC \)-triple: \( C < \text{rad}(ABC)^2 \).
- Consequence: Let \( x, y, z, n \) be positive integers such that \( \gcd(x, y, z) = 1 \) and \( x^n + y^n = z^n \). Then the hypothesis implies \( n < 6 \).
Super hits

- Instead of something linear in $\text{rad}(ABC)$ let us take something quadratic.
  Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^2$?
- Answer: Unknown
- Working hypothesis: For every $ABC$-triple: $C < \text{rad}(ABC)^2$.
- Consequence: Let $x, y, z, n$ be positive integers such that $\gcd(x, y, z) = 1$ and $x^n + y^n = z^n$. Then the hypothesis implies $n < 6$.
- Proof: Apply the hypothesis to the triple $A = x^n, B = y^n, C = z^n$. Notice that $\text{rad}(x^ny^nz^n) \leq xyz < z^3$. So, $z^n < (z^3)^2 = z^6$. Hence $n < 6$. Fermat’s Last Theorem for $n \geq 6$ follows!
Formulation

▶ Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^{1.5}$?
The riddle

Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^{1.5}$?

or $C > \text{rad}(ABC)^{1.05}$?

The conjecture

Formulation

We expect at most finitely many instances.

The ABC-conjecture (Masser-Oesterl´e, 1985): Let $\kappa > 1$. Then, with finitely many exceptions we have $C < \text{rad}(ABC)^{\kappa}$. 

Consequences

Evidence
Formulation

- Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^{1.5}$?
- or $C > \text{rad}(ABC)^{1.05}$?
- or $C > \text{rad}(ABC)^{1.005}$?
Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^{1.5}$?

- or $C > \text{rad}(ABC)^{1.05}$?
- or $C > \text{rad}(ABC)^{1.005}$?

- We expect at most finitely many instances.
Formulation

- Question: Are there $ABC$-triples such that $C > \text{rad}(ABC)^{1.5}$?
- or $C > \text{rad}(ABC)^{1.05}$?
- or $C > \text{rad}(ABC)^{1.005}$?
- We expect at most finitely many instances.
- $ABC$-Conjecture (Masser-Oesterlé, 1985): Let $\kappa > 1$. Then, with finitely many exceptions we have $C < \text{rad}(ABC)^{\kappa}$. 

The ABC-conjecture
Fermat-Catalan

The Fermat-Catalan equation $x^p + y^q = z^r$ in $x, y, z$ coprime positive integers. Of course we assume $p, q, r > 1$. We distinguish three cases.
Fermat-Catalan

The Fermat-Catalan equation \( x^p + y^q = z^r \) in \( x, y, z \) coprime positive integers. Of course we assume \( p, q, r > 1 \). We distinguish three cases.

- **1)** \( \frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1 \). It is an exercise to show that \((p, q, r)\) is a permutation of one of \((2, 2, k), (2, 3, 3), (2, 3, 4), (2, 3, 5)\). In any such case the number of solutions is infinite.
Fermat-Catalan

The Fermat-Catalan equation \( x^p + y^q = z^r \) in \( x, y, z \) coprime positive integers. Of course we assume \( p, q, r > 1 \). We distinguish three cases.

1. \( \frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1 \). It is an exercise to show that \( (p, q, r) \) is a permutation of one of \( (2, 2, k), (2, 3, 3), (2, 3, 4), (2, 3, 5) \). In any such case the number of solutions is infinite.

2. \( \frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1 \). Again it is an exercise to show that \( (p, q, r) \) is a permutation of one of \( (2, 4, 4), (2, 3, 6), (3, 3, 3) \). There are finitely many solutions.
The Fermat-Catalan equation $x^p + y^q = z^r$ in $x, y, z$ coprime positive integers. Of course we assume $p, q, r > 1$. We distinguish three cases.

▸ 1) $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$. It is an exercise to show that $(p, q, r)$ is a permutation of one of $(2, 2, k), (2, 3, 3), (2, 3, 4), (2, 3, 5)$. In any such case the number of solutions is infinite.

▸ 2) $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$. Again it is an exercise to show that $(p, q, r)$ is a permutation of one of $(2, 4, 4), (2, 3, 6), (3, 3, 3)$. There are finitely many solutions.

▸ 3) $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. There are infinitely many possible triples $(p, q, r)$. For any such triple the number of solutions is at most finite (Darmon-Granville, 1995).
Numeric results

\[ 1^k + 2^3 = 3^2 \ (k > 6), \quad 13^2 + 7^3 = 2^9, \quad 2^7 + 17^3 = 71^2 \]
\[ 2^5 + 7^2 = 3^4, \quad 3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2 \]
\[ 1414^3 + 2213459^2 = 65^7, \quad 33^8 + 1549034^2 = 15613^3 \]
\[ 43^8 + 96222^3 = 30042907^2, \quad 9262^3 + 15312283^2 = 113^7. \]
Fermat-Catalan conjecture

Consequence of ABC-conjecture:

The set of triples $x^p, y^q, z^r$ with $x, y, z$ coprime positive integers such that $x^p + y^q = z^r$ and $1/p + 1/q + 1/r < 1$, is finite.
Fermat-Catalan conjecture

Consequence of \(ABC\)-conjecture:

The set of triples \(x^p, y^q, z^r\) with \(x, y, z\) coprime positive integers such that \(x^p + y^q = z^r\) and \(1/p + 1/q + 1/r < 1\), is finite.

- Observation, \(1/p + 1/q + 1/r < 1\) implies \(1/p + 1/q + 1/r \leq 1 - 1/42.\)
Fermat-Catalan conjecture

Consequence of $ABC$-conjecture:

The set of triples $x^p, y^q, z^r$ with $x, y, z$ coprime positive integers such that $x^p + y^q = z^r$ and $1/p + 1/q + 1/r < 1$, is finite.

- Observation, $1/p + 1/q + 1/r < 1$ implies $1/p + 1/q + 1/r \leq 1 - 1/42$.

- Apply $ABC$ with $\kappa = 1.01$ to $A = x^p, B = y^q, C = z^r$. Notice that \( \text{rad}(x^r y^q z^r) \leq xyz < z^{r/p} z^{r/q} z \).
Fermat-Catalan conjecture

Consequence of ABC-conjecture:

The set of triples $x^p, y^q, z^r$ with $x, y, z$ coprime positive integers such that $x^p + y^q = z^r$ and $1/p + 1/q + 1/r < 1$, is finite.

- Observation, $1/p + 1/q + 1/r < 1$ implies $1/p + 1/q + 1/r \leq 1 - 1/42$.

- Apply ABC with $\kappa = 1.01$ to $A = x^p, B = y^q, C = z^r$. Notice that $\operatorname{rad}(x^r y^q z^r) \leq xyz < z^{r/p} z^{r/q} z$.

- Hence, with finitely many exceptions we get

$$z^r < z^{\kappa(r/p+r/q+1)}$$
Fermat-Catalan conjecture

Consequence of ABC-conjecture:

The set of triples $x^p, y^q, z^r$ with $x, y, z$ coprime positive integers such that $x^p + y^q = z^r$ and $1/p + 1/q + 1/r < 1$, is finite.

- Observation, $1/p + 1/q + 1/r < 1$ implies $1/p + 1/q + 1/r \leq 1 - 1/42$.

- Apply ABC with $\kappa = 1.01$ to $A = x^p, B = y^q, C = z^r$. Notice that $\text{rad}(x^r y^q z^r) \leq xyz < z^{r/p} z^{r/q} z$.

- Hence, with finitely many exceptions we get $z^r < z^{\kappa(r/p + r/q + 1)}$.

- This implies $r < \kappa (r/p + r/q + 1)$ and hence $1 < \kappa (1/p + 1/q + 1/r)$. But this is impossible because $\kappa = 1.01$ and $1/p + 1/q + 1/r \leq 1 - 1/42$. 

The ABC-conjecture
Catalan

As a special case we see that $x^p - y^q = 1$ has finitely many solutions. But this was shown in 1974 by Tijdeman and completely solved in 2002 by Michailescu.
Mordell’s conjecture

Consider a diophantine equation $P(x, y) = 0$ in the unknown rational numbers $x, y$.
For example
$x^5 + 3x^2y - y^3 + 1 = 0$, $x^4 + y^4 + 3xy + x^3 - y^3 = 0$, etc.
Mordell’s conjecture

Consider a diophantine equation $P(x, y) = 0$ in the unknown rational numbers $x, y$.

For example

$x^5 + 3x^2y - y^3 + 1 = 0, \quad x^4 + y^4 + 3xy + x^3 - y^3 = 0, \text{ etc.}$

Noam Elkies (1991) observed:

The $ABC$-conjecture implies: If $\text{genus}(P) > 1$ then the number of rational solutions to $P(x, y) = 0$ is at most finite.
Mordell’s conjecture

Consider a diophantine equation $P(x, y) = 0$ in the unknown rational numbers $x, y$.
For example
$x^5 + 3x^2y - y^3 + 1 = 0$, $x^4 + y^4 + 3xy + x^3 - y^3 = 0$, etc.

Noam Elkies (1991) observed:

The $ABC$-conjecture implies: If $\text{genus}(P) > 1$ then the number of rational solutions to $P(x, y) = 0$ is at most finite.

Previously known as Mordell’s conjecture (1923) and Faltings’ theorem (1983).
Schinzel-Tijdeman theorem

- An integer $n$ is called a *perfect power* if it is either a square, a cube, a fourth power, etc of another integer.
Schinzel-Tijdeman theorem

- An integer $n$ is called a *perfect power* if it is either a square, a cube, a fourth power, etc of another integer.
- Let $P(x)$ be a polynomial with integer coefficients and at least three simple zeros.
Schinzel-Tijdeman theorem

- An integer $n$ is called a *perfect power* if it is either a square, a cube, a fourth power, etc of another integer.
- Let $P(x)$ be a polynomial with integer coefficients and at least three simple zeros.
- Theorem (Schinzel-Tijdeman, 1976) Among the numbers $P(1), P(2), P(3), \ldots$ there are at most finitely many perfect powers.

Example: $P(x) = x^3 + 17$. We have $2^3 + 17 = 5^2$, $4^3 + 17 = 9^2$, $8^3 + 17 = 23^2$, $43^3 + 17 = 282^2$, $52^3 + 17 = 375^2$, $5234^3 + 17 = 378661^2$. 

The ABC-conjecture
The riddle

The conjecture

Consequences

Evidence

Schinzel-Tijdeman theorem

- An integer $n$ is called a **perfect power** if it is either a square, a cube, a fourth power, etc of another integer.
- Let $P(x)$ be a polynomial with integer coefficients and at least three simple zeros.
- Theorem (Schinzel-Tijdeman, 1976) Among the numbers $P(1), P(2), P(3), \ldots$ there are at most finitely many perfect powers.
- Example: $P(x) = x^3 + 17$. We have $2^3 + 17 = 5^2$, $4^3 + 17 = 9^2$, $8^3 + 17 = 23^2$, $43^3 + 17 = 282^2$, $52^3 + 17 = 375^2$, $5234^3 + 17 = 378661^2$. 

The ABC-conjecture
Schinzel-Tijdeman conjecture

- An integer \( n \) is called *powerfull* if all of its prime divisors occur with exponent 2 or higher in the prime factorisation.
Schinzel-Tijdeman conjecture

- An integer $n$ is called *powerfull* if all of its prime divisors occur with exponent 2 or higher in the prime factorisation.
- Gary Walsh (1998) observed that the ABC-conjecture implies the Schinzel-Tijdeman conjecture: *among the numbers $P(1), P(2), P(3), \ldots$ there are at most finitely many powerful numbers.*
Schinzel-Tijdeman conjecture

An integer \( n \) is called *powerfull* if all of its prime divisors occur with exponent 2 or higher in the prime factorisation.

Gary Walsh (1998) observed that the \( ABC \)-conjecture implies the Schinzel-Tijdeman conjecture: among the numbers \( P(1), P(2), P(3), \ldots \) there are at most finitely many powerful numbers.

Example: \( P(x) = x^3 + 17 \). We have
\[
2^3 + 17 = 5^2, \quad 4^3 + 17 = 9^2, \quad 8^3 + 17 = 23^2, \quad 43^3 + 17 = 28^2 \\
52^3 + 17 = 375^2, \quad 5234^3 + 17 = 378661^2.
\]
State of knowledge

What do we know about $ABC$?
State of knowledge

What do we know about $ABC$?

Stewart, Kunrui Yu (1996): For any $\epsilon > 0$:

$$C < \exp \left( \gamma \text{rad}(ABC)^{1/3+\epsilon} \right)$$

where $\gamma$ depends on the choice of $\epsilon$. 
An analogy

Why do we believe in $ABC$?
An analogy

Why do we believe in $ABC$?

There is an analogy with polynomials with rational numbers as coefficients: $\mathbb{Q}[x]$. 

The ABC-conjecture
An analogy

Why do we believe in $ABC$?

There is an analogy with polynomials with rational numbers as coefficients: $\mathbb{Q}[x]$.

A polynomial $F(x)$ with rational coefficients and leading coefficient 1 is called *prime* if it cannot be factored into polynomials with rational coefficients and lower degree.
An analogy

Why do we believe in $ABC$?

There is an analogy with polynomials with rational numbers as coefficients: $\mathbb{Q}[x]$.

A polynomial $F(x)$ with rational coefficients and leading coefficient 1 is called prime if it cannot be factored into polynomials with rational coefficients and lower degree.

Theorem: Any polynomial with rational numbers as coefficient can be written in a unique way as a constant times a product of prime polynomials.
Factors of polynomials

For example: \( x^2 + 1 \), whereas \( x^2 - 1 \) is reducible. Example of a factorisation:

\[
x^{21} - 1 = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \times (x - 1)(x^2 + x + 1) \times (x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1).
\]

Degree of a polynomial \( F \): \( \deg(F) \).

The *radical* of a polynomial \( F(x) \) is the product of the prime polynomials dividing \( F(x) \). Notation \( \text{rad}(F) \).
PQR-Theorem

\textit{PQR-Theorem} (Hurwitz, Stothers, Mason): Let $P, Q, R$ be coprime polynomials, not all constant, such that $P + Q = R$. Suppose that $\deg(R) \geq \deg(P), \deg(Q)$. Then

$$\deg(R) < \deg(\text{rad}(PQR)).$$
PQR-Theorem

PQR-Theorem (Hurwitz, Stothers, Mason): Let $P, Q, R$ be coprime polynomials, not all constant, such that $P + Q = R$. Suppose that $\deg(R) \geq \deg(P), \deg(Q)$. Then

$$\deg(R) < \deg(\text{rad}(PQR)).$$

Translation to $ABC$: Replace $P, Q, R$ by $A, B, C$ and $\deg$ by $\log$. Note the analogy: $\deg(PQ) = \deg(P) + \deg(Q)$ for polynomials and $\log(ab) = \log(a) + \log(b)$ for numbers. We get:

$$\log(C) < \log(\text{rad}(ABC)).$$
Proof of PQR, I

Observe that for any polynomial $F$,

$$\text{rad}(F) = \frac{F}{\gcd(F, F')}$$
Proof of PQR, I

Observe that for any polynomial $F$,

$$\text{rad}(F) = \frac{F}{\gcd(F, F')}$$

Example, $F = x^3(x - 1)^5$. Then $F' = (8x - 5)x^2(x - 1)^4$. Hence $\gcd(F, F') = x^2(x - 1)^4$ and $F/\gcd(F, F') = x(x - 1)$. 
Proof of PQR, I

Observe that for any polynomial $F$,

$$\text{rad}(F) = F / \gcd(F, F')$$

Example, $F = x^3(x - 1)^5$. Then $F' = (8x - 5)x^2(x - 1)^4$. Hence $\gcd(F, F') = x^2(x - 1)^4$ and $F / \gcd(F, F') = x(x - 1)$.

Start with

$$P + Q = R$$

and differentiate:

$$P' + Q' = R'$$
Proof of PQR, I

Observe that for any polynomial $F$,

$$\text{rad}(F) = \frac{F}{\gcd(F, F')}$$

Example, $F = x^3(x - 1)^5$. Then $F' = (8x - 5)x^2(x - 1)^4$. Hence $\gcd(F, F') = x^2(x - 1)^4$ and $F/\gcd(F, F') = x(x - 1)$.

Start with

$$P + Q = R$$

and differentiate:

$$P' + Q' = R'$$

Multiply first equality by $P'$, second equality by $P$ and subtract,

$$P'Q - pQ' = P'R - PR'$$
Proof of PQR, II

\[ P'Q - pQ' = P'R - PR' \]
Proof of PQR, II

\[ P'Q - pQ' = P'R - PR' \]

So, \( \gcd(R, R') \) divides \( P'Q - PQ' \). A fortiori, \( \gcd(R, R') \) divides

\[
\frac{P'Q - PQ'}{\gcd(P, P') \gcd(Q, Q')}.\]
Proof of PQR, II

\[ P'Q - pQ' = P'R - PR' \]

So, gcd\((R, R')\) divides \(P'Q - PQ'\). A fortiori, gcd\((R, R')\) divides

\[ \frac{P'Q - PQ'}{\gcd(P, P')\gcd(Q, Q')} \]

Consequently, if \(P'Q - pQ' \neq 0\),

\[ \deg(\gcd(R, R')) < \deg(\text{rad}(P)) + \deg(\text{rad}(Q)) = \deg(\text{rad}(PQ)). \]
Proof of PQR, II

\[ P'Q - pQ' = P'R - PR' \]

So, \( \gcd(R, R') \) divides \( P'Q - PQ' \). A fortiori, \( \gcd(R, R') \) divides

\[
\frac{P'Q - PQ'}{\gcd(P, P') \gcd(Q, Q')}. 
\]

Consequently, if \( P'Q - pQ' \neq 0 \),

\[
\deg(\gcd(R, R')) < \deg(\text{rad}(P)) + \deg(\text{rad}(Q)) = \deg(\text{rad}(PQ)).
\]

Add \( \deg(R/ \gcd(R, R')) = \deg(\text{rad}(R)) \) to get

\[
\deg(R) < \deg(\text{rad}(PQR)).
\]
Proof of PQR, II

$$P'Q - pQ' = P'R - PR'$$

So, $\text{gcd}(R, R')$ divides $P'Q - PQ'$. A fortiori, $\text{gcd}(R, R')$ divides

$$\frac{P'Q - PQ'}{\text{gcd}(P, P') \text{gcd}(Q, Q')}.$$ 

Consequently, if $P'Q - pQ' \neq 0$,

$$\deg(\text{gcd}(R, R')) < \deg(\text{rad}(P)) + \deg(\text{rad}(Q)) = \deg(\text{rad}(PQ)).$$

Add $\deg(R/\text{gcd}(R, R')) = \deg(\text{rad}(R))$ to get

$$\deg(R) < \deg(\text{rad}(PQR)).$$

If $P'Q - PQ' = 0$, then $P/Q$ is constant and all of $P, Q, R$ are constant.
The quest

Main questions

If the $ABC$-conjecture is true, there should be a minimal number $\kappa$ such that $C \geq \text{rad}(ABC) \kappa$ for all $ABC$-triples. What is the value of $\kappa$?

How does the number of $ABC$-hits with $C < X$ grow as $X \to \infty$? Are there distribution laws? How are the ratios $\log(C) / \log(\text{rad}(ABC))$ distributed?

Happy hunting, or fishing!
The quest

Main questions

- If the $ABC$-conjecture is true, there should be a minimal number $\kappa$ such that $C \geq \text{rad}(ABC)^\kappa$ for all $ABC$-triples. What is the value of $\kappa$?
The quest

Main questions

- If the $ABC$-conjecture is true, there should be a minimal number $\kappa$ such that $C \geq \text{rad}(ABC)^\kappa$ for all $ABC$-triples. What is the value of $\kappa$?
- How does the number of $ABC$-hits with $C < X$ grow as $X \to \infty$? Are there distribution laws? How are the ratios $\log(C)/\log(\text{rad}(ABC))$ distributed?
The quest

Main questions

- If the ABC-conjecture is true, there should be a minimal number $\kappa$ such that $C \geq \text{rad}(ABC)^{\kappa}$ for all ABC-triples. What is the value of $\kappa$?

- How does the number of ABC-hits with $C < X$ grow as $X \to \infty$? Are there distribution laws? How are the ratios $\log(C) / \log(\text{rad}(ABC))$ distributed?

Happy hunting, or fishing!