The abc Conjecture: An Introduction

Robert L. Benedetto
Amherst College

September 20, 2023
2400 + 1 = 2401
Fermat’s Last Theorem. (Wiles, 1995)

Theorem

Given $n \geq 3$ integer, there are no integer solutions to

$$x^n + y^n = z^n$$

for which none of $x, y, z$ is equal to zero.

Proof:

A little too long to fit into this talk.

“QED”
Using **Polynomials** instead of **Integers**

**Recall:** A polynomial $f(t)$ with complex coefficients is a function of the form:

$$f(t) = a_d t^d + a_{d-1} t^{d-1} + \cdots + a_1 t + a_0,$$

where every $a_i \in \mathbb{C}$.

e.g.:  

$$5 - \pi t + t^2$$

$$(14 + 2i) + 17t^{11} - (5 - 3i)t^{38}$$

$$7 + \sqrt{2} i$$

$$0$$

**Notation:**

$$\mathbb{C}[t] = \{\text{polynomials with coefficients in } \mathbb{C}\}.$$
Fermat for Polynomials

Theorem
Let $n \geq 3$ be an integer. There are no polynomials $f, g, h \in \mathbb{C}[t]$ such that

$$(f(t))^n + (g(t))^n = (h(t))^n$$

except for the cases that:

- at least one of $f, g, h$ is the zero polynomial,
- or
- $f, g, h$ are all constant,
- or
- $f$ is a constant times $g$.

Note: $n = 2$ has many solutions. E.g., for any polynomial $f(t)$,

$$(f^2 - 1)^2 + (2f)^2 = (f^2 + 1)^2.$$
Review of Polynomials and Degrees

To say $f = g$ means: for every $t_0 \in \mathbb{C}$, $f(t_0) = g(t_0)$. Equivalently, $f$ and $g$ have exactly the same coefficients.

Writing $f(t) = a_d t^d + \cdots + a_0$ with $a_d \neq 0$, the integer

$$d = d_f = \deg(f)$$

is the degree of $f$.

Note:

- If $f = a_0$ is a nonzero constant, then $\deg(f) = 0$.
- If $f = 0$ is the zero polynomial, either we don’t talk about its degree, or we say that $\deg(f) = -\infty$.
- $\deg(f \cdot g) = \deg(f) + \deg(g)$.
- If $f$ is not a constant, then $\deg(f') = \deg(f) - 1$. 
Roots of Polynomials

Any nonzero polynomial

\[ f = a_d t^d + \cdots + a_0 \]

(with \( a_d \neq 0 \)) has exactly \( d \) roots

\[ \alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{C}, \]

and in particular,

\[ f(t) = a_d \cdot (t - \alpha_1) \cdot (t - \alpha_2) \cdots \cdots (t - \alpha_d). \]

Furthermore, the above factorization of \( f \) is unique.
Examples of Roots of Polynomials

Examples.

\[ f(t) = t^3 - 3t^2 + 2t = t(t - 1)(t - 2) \]

\[ g(t) = t^2 + 4 = (t - 2i)(t + 2i) \]

\[ h(t) = 2t^3 - 3t^2 + 1 = 2\left(t + \frac{1}{2}\right)(t - 1)(t - 1) \]

\[ = 2\left(t + \frac{1}{2}\right)(t - 1)^2 \]
Counting Roots

Example: Are there numbers $a, b \in \mathbb{C}$ so that

$$(t + 1)^5(t + 2)^4(t^3 + at - 3) = (t - 2)^3(t - 1)^2(t^7 + bt + 6)$$

Answer: NO!
We could multiply it out, but here's an easier way:

If the above polynomials were equal, then they would be a single polynomial of degree 12.

This polynomial has as roots at least the following:

- $-1$, appearing 5 times,
- $-2$, appearing 4 times,
- $2$, appearing 3 times
- $1$, appearing 2 times

That’s already at least $5 + 4 + 3 + 2 = 14$ roots for a degree 12 polynomial, which is impossible.
Suppose $f \in \mathbb{C}[t]$ and $\alpha$ is a root of $f$, appearing with multiplicity $r \geq 1$; that is,

$$f(t) = (t - \alpha)^r g(t)$$

for some polynomial $g(t)$. Then

$$f'(t) = r(t - \alpha)^{r-1} g(t) + (t - \alpha)^r g'(t)$$

$$= (t - \alpha)^{r-1} \left[ rg(t) + (t - \alpha)g'(t) \right].$$

That means the polynomial $f'$ has $\alpha$ as a root with multiplicity (at least) $r - 1$. 
The Radical of a Polynomial

Definition
Given a polynomial

\[ f(t) = A(t - \alpha_1)^{r_1}(t - \alpha_2)^{r_2} \cdots (t - \alpha_k)^{r_k}, \]

with \( \alpha_1, \ldots, \alpha_k \) distinct, the radical of \( f \) is the polynomial

\[ \text{rad}(f) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_k). \]

Note:
1. If \( f \) is not constant, then \( 1 \leq \deg(\text{rad}(f)) \leq \deg(f) \).
2. The number of distinct roots of \( f \) is \( k = \deg(\text{rad}(f)) \).
3. \( r_1 + r_2 + \cdots + r_k = \deg(f) \).
Theorem (Stothers, Mason, early 1980s)

Let \( a(t), b(t), c(t) \) be nonzero polynomials, not all constant, such that

1. \( a + b = c \), and
2. \( a \) and \( b \) have no common roots.

Then

\[
\max\{\deg(a), \deg(b), \deg(c)\} \leq -1 + \deg(\text{rad}(abc)).
\]

That is:

The largest degree of \( a, b, \) and \( c \) is strictly less than the total number of distinct roots of \( a, b, \) and \( c \).
Example 1

\[
\begin{align*}
t^3(5t + 2) + (3t + 1)^3(t + 1) &= (2t + 1)^3(4t + 1) \\
\underbrace{t^3(5t + 2)}_{a(t)} + \underbrace{(3t + 1)^3(t + 1)}_{b(t)} &= \underbrace{(2t + 1)^3(4t + 1)}_{c(t)}
\end{align*}
\]

\[
\max\{\deg a, \deg b, \deg c\} = 4
\]

\[
\rad(abc) = t(t + 1)\left(t + \frac{1}{2}\right)\left(t + \frac{1}{3}\right)\left(t + \frac{1}{4}\right)\left(t + \frac{2}{5}\right),
\]

so \(\deg(\rad(abc)) = 6\), and \(4 \leq (-1) + 6\).
Example 2

\[
\frac{t^{1821}}{a(t)} - 1 + \frac{1}{b(t)} = \frac{t^{1821}}{c(t)}
\]

\[ \max\{\deg a, \deg b, \deg c\} = \deg a = \deg c = 1821 \]

\[ \rad(abc) = t(t^{1821} - 1), \]

so \[ \deg(\rad(abc)) = 1822, \text{ and } 1821 \leq (-1) + 1822. \]
Example 3

\[
\underbrace{\left(t^{1821} + 1\right)}_{a(t)} + \underbrace{\left(-t^{1821} + 1\right)}_{b(t)} = \underbrace{2}_{c(t)}
\]

\[
\max\{\deg a, \deg b, \deg c\} = \deg a = \deg b = 1821
\]

\[\text{rad}(abc) = t^{3642} - 1,\]

so \(\deg(\text{rad}(abc)) = 3642\), and \(1821 \leq (-1) + 3642\).
Proving $abc$ for Polynomials: Setup

**Without loss:** The largest degree is $\deg(a) = \deg(b) = d \geq 1$.
Let $d_c = \deg(c)$. Then $0 \leq d_c \leq d$.

Factor the polynomials as:

\[
\begin{align*}
    a(t) &= A(t - \alpha_1)^{q_1}(t - \alpha_2)^{q_2} \cdots (t - \alpha_k)^{q_k} \\
    b(t) &= B(t - \beta_1)^{r_1}(t - \beta_2)^{r_2} \cdots (t - \beta_\ell)^{r_\ell} \\
    c(t) &= C(t - \gamma_1)^{s_1}(t - \gamma_2)^{s_2} \cdots (t - \gamma_m)^{s_m}
\end{align*}
\]

By hypothesis, note that:
- $q_1 + \cdots + q_k = r_1 + \cdots + r_\ell = d$,
- $s_1 + \cdots + s_m = d_c \leq d$,
- $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_\ell, \gamma_1, \ldots, \gamma_m$ are all distinct.

Let $N = k + \ell + m = \deg(\text{rad}(abc))$.

Our goal is to show: $d \leq N - 1$. 
Proof of Fermat for Polynomials

Suppose $n \geq 3$ and $f^n + g^n = h^n$, where

- $f$, $g$, $h$ are nonzero, and
- $f$ is not a constant multiple of $g$.

If $f$ and $g$ have a common root $a \in \mathbb{C}$, then so does $h$; so divide both sides by $(t - a)^n$. Repeat until $f$ and $g$ have no common roots.

Rearrange so that $\deg f = d \geq \deg(g), \deg(h)$. By abc Theorem,

$$\underbrace{\deg(f^n)}_{nd} \leq -1 + \underbrace{(\#\text{distinct roots of } f^n g^n h^n)}_{\leq \deg(fgh)} \leq 3d$$

So $nd \leq 3d - 1$, i.e., $(n - 3)d \leq -1$. Contradiction! QED
Given a positive integer \( n \geq 1 \), what’s the analogue of the “degree” of \( n \)?

**Idea:**

\[
2548 = 2 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 8
\]

vs.

\[
2 \cdot t^3 + 5 \cdot t^2 + 4 \cdot t + 8
\]

So “degree” is roughly analogous to “number of digits”, which means (roughly) \( \log |n| \).

Another parallel:

\[
\text{deg}(fg) = \text{deg}(f) + \text{deg}(g)
\]

\[
\log |mn| = \log |m| + \log |n|
\]
What about the **radical** of an integer?

Polynomials have factorizations

\[ f(t) = A(t - \alpha_1)^{r_1}(t - \alpha_2)^{r_2} \cdots (t - \alpha_k)^{r_k}, \]

and the radical of \( f \) is

\[ \text{rad}(f) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_k). \]

Similarly, integers have **prime** factorizations

\[ n = \pm p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \]

so

**Definition**

Let \( n \in \mathbb{Z} \) be a nonzero integer \( n = \pm p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \).

The **radical** of \( n \) is \( \text{rad}(n) = p_1 p_2 \cdots p_k \).
An Analogous Conjecture for Integers

Conjecture

There is a constant $C \in \mathbb{R}$ with the following property: For all positive integers $a, b, c \in \mathbb{N}$ satisfying:

1. $a + b = c$, and
2. $a$ and $b$ have no common prime factors,

we have

$$\max\{\log a, \log b, \log c\} \leq C + \log (\text{rad}(abc)).$$

[Recall: If $abc = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, then $\text{rad}(abc) = p_1 p_2 \cdots p_k$.]

But: this conjecture is **FALSE!!!!**
Lemma
For any integer \( j \geq 1 \), \( 3^{(2^j)} - 1 \) is divisible by \( 2^{j+2} \).

Proof of Lemma: By induction on \( j \):

For \( j = 1 \), \( 3^2 - 1 = 8 \) is divisible by \( 2^{1+2} = 8 \).

If the statement is true for some \( j \geq 1 \), then

\[
3^{2^{j+1}} - 1 = \underbrace{\left(3^{2^j} - 1\right)}_{\text{divisible by } 2^{j+2}} \cdot \underbrace{\left(3^{2^j} + 1\right)}_{\text{divisible by } 2}.
\]

Thus, \( 3^{2^{j+1}} \) is divisible by \( 2^{j+3} \).

QED Lemma
A Counterexample to the Conjecture

For each \( j \geq 1 \), write \( \underbrace{2^{j+2} n_j + 1}_{a_j} = \underbrace{3^{2j}}_{b_j} \), for some \( n_j \in \mathbb{N} \).

Note (for later) that \( n_j < \frac{3^{2j}}{2^{j+2}} \). We compute:

\[
\log \max\{a_j, b_j, c_j\} = \log (3^{2j}) = 2^j \log 3,
\]
and

\[
\log \text{rad}(a_j b_j c_j) \leq \log(2 \cdot 3 \cdot n_j) = \log 6 + \log(n_j)
\]

\[
< \log 6 + \log (3^{2j}) - \log(2^{j+2})
\]

\[
= \log 6 + 2^j \log 3 - (j + 2) \log 2.
\]

So if the conjecture were true, we would have

\[
2^j \log 3 \leq C + \log 6 + 2^j \log 3 - (j + 2) \log 2,
\]
i.e., \((j + 2) \log 2 \leq C + \log 6\) for all \( j \geq 1 \), which is impossible.
The *abc* Conjecture

Conjecture (David Masser and Joseph Oesterlé, 1985.)

*For any* $\varepsilon > 0$, *there is a constant* $C_\varepsilon \in \mathbb{R}$ *with the following property.*

*For all positive integers* $a, b, c \in \mathbb{N}$ *satisfying*

1. $a + b = c$, and
2. *a and b have no common prime factors,*

we have

$$\log c \leq C_\varepsilon + (1 + \varepsilon) \log(\text{rad}(abc)).$$
Given $a, b, c$ as in the conjecture, let

$$R(a, b, c) = \frac{\log c}{\log \text{rad}(abc)},$$

called the “$abc$ ratio” or the “quality” of the triple $(a, b, c)$.

**Idea:** Intuitively, the $abc$ conjecture says $R(a, b, c)$ cannot be much bigger than 1.

More precisely, it says that for any $\varepsilon > 0$, there are only finitely many triples $(a, b, c)$ for which $R(a, b, c) > 1 + \varepsilon$. 
Examples of $abc$ ratios

“Most” of the time, $R(a, b, c)$ is a lot smaller than 1:

- $18384 + 73295 = 91679$ is $2^4 \cdot 3 \cdot 383 + 5 \cdot 107 \cdot 137 = 7^2 \cdot 1871$, so

$$R = \frac{\log(91679)}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 107 \cdot 137 \cdot 383 \cdot 1871)} = 0.40201\ldots$$

- $5^{12} + 3^{16} = 287187346 = 2 \cdot 137 \cdot 1048129$ has

$$R = \frac{\log(287187346)}{\log(2 \cdot 3 \cdot 5 \cdot 137 \cdot 1048129)} = 0.877926\ldots$$

- But $1 + 2400 = 2401$ is $1 + 2^5 \cdot 3 \cdot 5^2 = 7^4$, so

$$R = \frac{\log(2401)}{\log(2 \cdot 3 \cdot 5 \cdot 7)} = 1.455673\ldots,$$

which is number 37 on the all-time worst (best?) list of known $(a, b, c)$-triples.
Top ten worst known \((a, b, c)\)-triples:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(3^{10} \cdot 109)</td>
<td>(23^5)</td>
<td>1.62991…</td>
</tr>
<tr>
<td>(11^2)</td>
<td>(3^2 \cdot 5^6 \cdot 7^3)</td>
<td>(2^{21} \cdot 23)</td>
<td>1.62599…</td>
</tr>
<tr>
<td>(19 \cdot 1307)</td>
<td>(7 \cdot 29^2 \cdot 31^8)</td>
<td>(2^8 \cdot 3^{22} \cdot 5^4)</td>
<td>1.62349…</td>
</tr>
<tr>
<td>283</td>
<td>(5^{11} \cdot 13^2)</td>
<td>(2^8 \cdot 3^8 \cdot 17^3)</td>
<td>1.58075…</td>
</tr>
<tr>
<td>1</td>
<td>(2 \cdot 3^7)</td>
<td>(5^4 \cdot 7)</td>
<td>1.56788…</td>
</tr>
<tr>
<td>(7^3)</td>
<td>(3^{10})</td>
<td>(2^{11} \cdot 29)</td>
<td>1.54707…</td>
</tr>
<tr>
<td>(7^2 \cdot 41^2 \cdot 31^3)</td>
<td>(11^{16} \cdot 13^2 \cdot 79)</td>
<td>(2 \cdot 3^3 \cdot 5^{23} \cdot 953)</td>
<td>1.54443…</td>
</tr>
<tr>
<td>(5^3)</td>
<td>(2^9 \cdot 3^{17} \cdot 13^2)</td>
<td>(11^{5} \cdot 17 \cdot 31^3 \cdot 137)</td>
<td>1.53671…</td>
</tr>
<tr>
<td>(13 \cdot 19^6)</td>
<td>(2^{30} \cdot 5)</td>
<td>(3^{13} \cdot 11^2 \cdot 31)</td>
<td>1.52699…</td>
</tr>
<tr>
<td>(3^{18} \cdot 23 \cdot 2269)</td>
<td>(17^3 \cdot 29 \cdot 31^8)</td>
<td>(2^{10} \cdot 5^2 \cdot 7^{15})</td>
<td>1.52216…</td>
</tr>
</tbody>
</table>
For more information

For a list of all 240 known \((a, b, c)\) triples with \(R > 1.4\), see Bart de Smit’s list at


(or search for desmit abc)

For more on the \(abc\) conjecture, see Abderrahmane Nitaj’s page at:

http://www.math.unicaen.fr/~nitaj/abc.html

(or search for nitaj abc)