Mordell's Equation

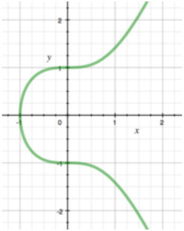
Keith Conrad
University of Connecticut

August 8, 2008

The Equation

$$y^2 = x^3 + k, \quad k \in \mathbf{Z} - \{0\}$$

Called Mordell's equation because of Mordell's (1888-1972) lifelong interest in it. Earlier named after Bachet (1581–1638).



$$y^2 = x^3 + 1$$

Outline

- Examples without integral solutions.
- Examples with integral solutions.
- Connection to the *abc*-conjecture.

No Integral Solutions

We will use congruences to show $y^2 = x^3 + k$ has no integral solutions for some k. Recall for odd primes p that

$$\begin{aligned} -1 \equiv \Box \bmod p \quad &\iff \quad p \equiv 1 \bmod 4, \\ 2 \equiv \Box \bmod p \quad &\iff \quad p \equiv 1, 7 \bmod 8, \\ -2 \equiv \Box \bmod p \quad &\iff \quad p \equiv 1, 3 \bmod 8. \end{aligned}$$

No Integral Solutions

$$y^2 = x^3 + 7$$

Parity Check: If x is even then $y^2 \equiv 7 \equiv 3 \bmod 4$: NO. So x is odd.

Proof # 1: Write

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4).$$

Note $x^2 - 2x + 4 = (x-1)^2 + 3 > 0$, and since x is odd, $(x-1)^2 + 3 \equiv 3 \bmod 4$. So there is a prime $p \equiv 3 \bmod 4$ dividing $x^2 - 2x + 4$.

$$p | (x^2 - 2x + 4) \implies p | (y^2 + 1) \implies -1 \equiv \square \bmod p,$$

so $p \equiv 1 \bmod 4$, a contradiction.

No Integral Solutions

$$y^2 = x^3 + 7$$

Parity Check: If x is even then $y^2 \equiv 7 \equiv 3 \bmod 4$: NO. So x is odd and y is even.
Proof # 2: Write

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4).$$

Since y even, $x^3 \equiv -7 \equiv 1 \bmod 4$. Since x odd, $x \equiv 1 \bmod 4$. Then $x + 2 \equiv 3 \bmod 4$. Have $x + 2 > 0$: otherwise $x \leq -2$, so $x^3 + 7 \leq -1$: NO. Some prime $p \equiv 3 \bmod 4$ divides $x + 2$.

$$p|(x+2) \Longrightarrow p|(y^2+1) \Longrightarrow -1 \equiv \square \bmod p,$$

so $p \equiv 1 \bmod 4$, a contradiction.

No Integral Solutions

$$y^2 = x^3 - 5$$

Parity Check: If x is even then $y^2 \equiv -5 \equiv 3 \bmod 4$: NO. So x is odd and y is even.

Proof: Write

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2+x+1).$$

Have $x^2 + x + 1 = (x + 1/2)^2 + 3/4 > 0$. Since x odd and y even, $0 \equiv x - 1 \bmod 4$, so $x \equiv 1 \bmod 4$. Then $x^2 + x + 1 \equiv 3 \bmod 4$. So a prime $p \equiv 3 \bmod 4$ divides $x^2 + x + 1$.

$p|(x^2{+}x{+}1) \Longrightarrow p|(y^2{+}4) \Longrightarrow -4 \equiv \square \bmod p \Rightarrow -1 \equiv \square \bmod p$,

so $p \equiv 1 \bmod 4$, a contradiction.

No Integral Solutions

$$y^2 = x^3 - 6$$

Parity Check: If x is even then $y^2 \equiv -6 \equiv 2 \bmod 4$: NO. So x is odd and y is odd. Then $1 \equiv x - 6 \bmod 8$, so $x \equiv 7 \bmod 8$.
Proof # 1: Write

$$y^2 - 2 = x^3 - 8 = (x - 2)(x^2 + 2x + 4).$$

Have $x^2 + 2x + 4 > 0$, $x^2 + 2x + 4 \equiv 7^2 + 2 \cdot 7 + 4 \equiv 3 \bmod 8$. So a prime $p \equiv \pm 3 \bmod 8$ divides $x^2 + 2x + 4$.

$$p|(x^2 + 2x + 4) \Longrightarrow p|(y^2 - 2) \Longrightarrow 2 \equiv \square \bmod p,$$

so $p \equiv \pm 1 \bmod 8$, a contradiction.

No Integral Solutions

$$y^2 = x^3 - 6$$

Parity Check: If x is even then $y^2 \equiv -6 \equiv 2 \bmod 4$: NO. So x is odd and y is odd. Then $1 \equiv x - 6 \bmod 8$, so $x \equiv 7 \bmod 8$.

Proof # 2: Write

$$y^2 - 2 = x^3 - 8 = (x-2)(x^2 + 2x + 4).$$

Have $x - 2 > 0$: otherwise $x \leq 2$, so $x \leq -1$ since $x \equiv 7 \bmod 8$, so $x^3 - 6 < 0$: NO. A prime $p \equiv \pm 3 \bmod 8$ divides $x - 2$.

$$p|(x-2) \Longrightarrow p|(y^2 - 2) \Longrightarrow 2 \equiv \Box \bmod p,$$

so $p \equiv \pm 1 \bmod 8$, a contradiction.

No Integral Solutions

$$y^2 = x^3 + 46$$

Parity Check: If x is even then $y^2 \equiv 6 \bmod 8$: NO. So x is odd and y is odd. Then $1 \equiv x + 6 \bmod 8$, so $x \equiv 3 \bmod 8$.
Proof: Write

$$y^2 + 18 = x^3 + 64 = (x+4)(x^2 - 4x + 16).$$

Have $x^2 - 4x + 16 > 0$ and $x^2 - 4x + 16 \equiv 5 \bmod 8$. A prime $p \not\equiv 1, 3 \bmod 8$ divides $x^2 - 4x + 16$, and $p \neq 2$.

$$p|(x^2 - 4x + 16) \Longrightarrow -18 \equiv \Box \bmod p \Rightarrow -2 \equiv \Box \bmod p,$$

so $p \equiv 1, 3 \bmod 8$, a contradiction.

Challenge Problem

In 1657, Fermat challenged the British mathematicians to find all integral solutions to

$$y^2 = x^3 - 2$$

and

$$y^2 = x^3 - 4.$$

The solutions to the first are $(3, \pm 5)$ and to the second are $(2, \pm 2)$, $(5, \pm 11)$. We will look at other "challenges."

Applying Unique Factorization in Z

$$y^2 = x^3 + 16$$

Obvious solutions: $(0, \pm 4)$.

Parity Check: $x^3 = (y+4)(y-4)$. If y odd then $y \pm 4$ odd, so $(y+4, y-4) = 1$. Therefore (!) $y+4$ and $y-4$ are cubes in $\mathbf{Z}$. But no odd cubes differ by 8. So y is even and x is even.

Proof: Since $y^2 \equiv 0 \bmod 8$, $4|y$: $y = 4y'$. Then $x^3 \equiv 0 \bmod 16$, so $4|x$: $x = 4x'$.

$$(4y')^2 = (4x')^3 + 16 \Longrightarrow y'^2 = 4x'^3 + 1,$$

so y' odd: $y' = 2m + 1$. Then

$$4m^2 + 4m + 1 = 4x'^3 + 1 \Longrightarrow m(m+1) = x'^3.$$

Thus $m = -1$ or 0, so $x' = 0$: $x = 0$ and $y = \pm 4$.

Applying Unique Factorization in $\mathbf{Z}[i]$

$$y^2 = x^3 - 1$$

Obvious solution: $(1, 0)$.
Parity Check: If x even then $y^2 \equiv -1 \bmod 4$: NO. Thus x is odd and y is even.
Proof: Write
$$x^3 = y^2 + 1 = (y + i)(y - i).$$

If $\delta|(y + i)$ and $\delta|(y - i)$ then $\mathrm{N}(\delta)|(y^2 + 1)$, so $\mathrm{N}(\delta)$ is odd. Also $\delta|2i$, so $\mathrm{N}(\delta)|4$. Thus $\mathrm{N}(\delta) = 1$, so $\delta = \pm 1$ or $\pm i$.
Since $y + i$ and $y - i$ are relatively prime and all units in $\mathbf{Z}[i]$ are cubes,

$$y + i = (m + ni)^3 \Longrightarrow y = m^3 - 3mn^2, \quad 1 = 3m^2 n - n^3.$$

Thus $n|1$, so $n = \pm 1$. If $n = 1$ then $1 = 3m^2 - 1$: NO. If $n = -1$ then $1 = -3m^2 + 1$, so $m = 0$: $y = 0$. So $x = 1$.

Applying Unique Factorization in $\mathbf{Z}[\sqrt{-5}]$

$$y^2 = x^3 - 5$$

We know this has no integral solutions, by congruences.
Parity Check: If x is even then $y^2 \equiv -5 \equiv 3 \bmod 4$: NO. So x is odd and y is even.
Proof: Write

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

If $\delta|(y + \sqrt{-5})$ and $\delta|(y - \sqrt{-5})$ then $\mathrm{N}(\delta)|(y^2 + 5)$, so $\mathrm{N}(\delta)$ odd. Also $\delta|2\sqrt{-5}$, so $\mathrm{N}(\delta)|20$. Thus $\mathrm{N}(\delta)|5$. If $\mathrm{N}(\delta) = 5$ then $5|(y^2 + 5)$, so $5|y$. Then $x^3 \equiv 5 \bmod 25$: NO. So $\mathrm{N}(\delta) = 1$.
Since $y + \sqrt{-5}$ and $y - \sqrt{-5}$ are relatively prime and the units in $\mathbf{Z}[\sqrt{-5}]$ are ± 1, both cubes,

$$y + \sqrt{-5} = (m + n\sqrt{-5})^3 \Rightarrow y = m^3 - 15mn^2, \quad 1 = 3m^2 n - 5n^3.$$

Thus $n|1$, so $n = \pm 1$. If $n = 1$ then $1 = 3m^2 - 5$: NO. If $n = -1$ then $1 = -3m^2 + 5$: NO.

Applying Unique Factorization in $\mathbf{Z}[\sqrt{-5}]$

That proof has a mistake: there is not unique factorization in $\mathbf{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

So our proof reached the correct conclusion by an incorrect method.

It is true in $\mathbf{Z}[\sqrt{-5}]$ that if $\alpha\beta$ is a cube and α and β are relatively prime then α and β are both cubes, but not using unique factorization (need a class number computation).

Applying Unique Factorization in $\mathbf{Z}[\sqrt{-26}]$

$$y^2 = x^3 - 26$$

Obvious solutions: $(3, \pm 1)$.

Parity Check: If x even then $y^2 \equiv 2 \bmod 4$: NO. Thus x is odd and y is odd.

Proof: Write

$$x^3 = y^2 + 26 = (y + \sqrt{-26})(y - \sqrt{-26}).$$

If $\delta | (y + \sqrt{-26})$ and $\delta | (y - \sqrt{-26})$ then $\mathrm{N}(\delta) | (y^2 + 26)$, so $\mathrm{N}(\delta)$ is odd. Also $\delta | 2\sqrt{-26}$, so $\mathrm{N}(\delta) | 4 \cdot 26$. Thus $\mathrm{N}(\delta) | 13$. No solution to $a^2 + 26b^2 = 13$, so $\mathrm{N}(\delta) = 1$: $\delta = \pm 1$.

Since $y + \sqrt{-26}$ and $y - \sqrt{-26}$ are relatively prime and units in $\mathbf{Z}[\sqrt{-26}]$ are ± 1, both cubes,

$$y + \sqrt{-26} = (m + n\sqrt{-26})^3 \Rightarrow y = m^3 - 78mn^2, \;\; 1 = 3m^2n - 26n^3.$$

Thus $n | 1$, so $n = \pm 1$. If $n = 1$ then $1 = 3m^2 - 26$: $m = \pm 3$, so $y = \pm 207$ and $x = 35$. If $n = -1$ then $1 = -3m^2 + 26$: NO.

Applying Unique Factorization in $\mathbf{Z}[\sqrt{-26}]$

We found unexpected solutions $(35, \pm 207)$ to $y^2 = x^3 - 26$. But we missed the obvious solutions $(3, \pm 1)$!

There is not unique factorization in $\mathbf{Z}[\sqrt{-26}]$:

$$27 = 3 \cdot 3 \cdot 3 = (1 + \sqrt{-26})(1 - \sqrt{-26}).$$

It is not true in $\mathbf{Z}[\sqrt{-26}]$ that if $\alpha\beta$ is a cube and α and β are relatively prime then α and β are cubes: see above equation for a counterexample.

Integral vs. Rational Solutions

k	Integral Solutions	Rational Solutions
-1	$(1, 0)$	$(1, 0)$
-5	None	None
-6	None	None
7	None	None
16	$(0, \pm 4)$	$(0, \pm 4)$
-26	$(3, \pm 1), (35, \pm 207)$	Infinitely Many
46	None	Infinitely Many

$$y^2 = x^3 - 26 : (705/4, 18719/8), (881/256, 15735/4096), \ldots$$

$$y^2 = x^3 + 46 : (-7/4, 51/8), (18585/4624, 3311677/314432), \ldots$$

Rational Solutions

If $k = d^6 k'$ and $y^2 = x^3 + k$, then $(y/d^3)^2 = (x/d^2)^3 + k'$.

Theorem (Fueter (1930), Mordell (1966))

If k is not divisible by a sixth power, $y^2 = x^3 + k$ has infinitely many rational solutions if it has a rational solution where $x \neq 0$ and $y \neq 0$, except when $k = 1$ or -432.

All rational solutions of $y^2 = x^3 + 1$ are $(-1, 0), (0, \pm 1), (2, \pm 3)$.
If $y^2 = x^3 - 432$ with rational x and y then

$$\left(\frac{36 + y}{6x}\right)^3 + \left(\frac{36 - y}{6x}\right)^3 = \frac{216(y^2 + 432)}{216x^3} = 1,$$

so $y = \pm 36$ (and $x = 12$) by Fermat's last theorem for exponent 3.

An Ineffective Finiteness Theorem

Theorem (Mordell, 1922)

For each $k \in \mathbf{Z} - \{0\}$, the equation $y^2 = x^3 + k$ has finitely many integral solutions.

This was later subsumed under a more general finiteness theorem of Siegel (1929).

In terms of k, when can you stop looking?

Example

The integral solutions to $y^2 = x^3 + 24$ are

$$(-2, \pm 4), \quad (1, \pm 5), \quad (10, \pm 32), \text{ and } (8158, \pm 736844).$$

Effective Finiteness Theorems

Theorem (Baker, 1967)

For each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then

$$\max(|x|, |y|) \leq e^{10^{10}|k|^{10000}} = \left(e^{10^{10}}\right)^{|k|^{10000}}.$$

Theorem (Stark, 1973)

Pick $\varepsilon > 0$. There is a constant $C_\varepsilon > 0$ such that for each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then

$$\max(|x|, |y|) \leq C_\varepsilon^{|k|^{1+\varepsilon}}.$$

Effective does not mean practical!

Conjectures on Integral Solutions

Conjecture (M. Hall, 1969)

There is a constant $C > 0$ such that if $y^2 = x^3 + k$ in $\mathbf{Z}$ with $k \neq 0$ then $|x| \leq C|k|^2$ and $|y| \leq C|k|^3$.

$$\begin{aligned}
&736844^2 = 8158^3 + 24 \Longrightarrow C \geq 53.3,\\
&378661^2 = 5234^3 + 17 \Longrightarrow C \geq 77.0,\\
&149651610621^2 = 28187351^3 + 1090 \Longrightarrow C \geq 115.5,\\
&447884928428402042307918^2 = 5853886516781223^3 - 1641843\\
&\qquad\qquad \Longrightarrow C \geq 101197.9.
\end{aligned}$$

Hall knew first three examples, not the last (Elkies, 1998).

Conjecture (Weak Hall Conjecture)

Pick $\varepsilon > 0$. There is $C_\varepsilon > 0$ such that for each $k \in \mathbf{Z} - \{0\}$, if $y^2 = x^3 + k$ in $\mathbf{Z}$ then $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$, $|y| \leq C_\varepsilon |k|^{3(1+\varepsilon)}$.

The *abc*-conjecture

Definition

The radical of n is product of its prime factors: $\mathrm{Rad}(n) = \displaystyle\prod_{p|n} p$.

$$\mathrm{Rad}(10) = 10, \quad \mathrm{Rad}(72) = 6, \quad \mathrm{Rad}(150) = 30, \quad \mathrm{Rad}(-1024) = 2.$$

Conjecture (Masser, Oesterlé, 1985)

For each $\varepsilon > 0$ there is a constant $\lambda_\varepsilon > 0$ such that whenever a, b, and c are nonzero integers with $a + b = c$ and $(a, b) = 1$,

$$\max(|a|, |b|, |c|) \le \lambda_\varepsilon \,\mathrm{Rad}(abc)^{1+\varepsilon}.$$

Why can't we take $\varepsilon = 0$? Analogy: for $x \ge 1$, $\log x \le B_\varepsilon x^\varepsilon$ for all $\varepsilon > 0$, but $\log x \not\le B$.

Fermat's Last Theorem

Maybe $\lambda_1 = 1$:

$$a + b = c, (a, b) = 1 \overset{?}{\Rightarrow} \max(|a|, |b|, |c|) \leq \mathrm{Rad}(abc)^2.$$

No counterexamples to this are yet known.
Suppose $x^n + y^n = z^n$ with $n \geq 3$ and $x, y, z \in \mathbf{Z}^+$. We may take $(x, y) = 1$. Suppose $\lambda_1 = 1$. Then

$$\begin{aligned} z^n &\leq \mathrm{Rad}(x^n y^n z^n)^2 \\ &= \mathrm{Rad}(xyz)^2 \\ &\leq (xyz)^2 \\ &\leq z^6, \end{aligned}$$

so $n \leq 6$. Thus we have Fermat's Last Theorem for $n \geq 7$. For the rest see Euler ($n = 3$), Fermat ($n = 4$), and Legendre ($n = 5$).

Fermat's Last Theorem

$$a + b = c, (a, b) = 1 \Rightarrow \max(|a|, |b|, |c|) \leq \lambda_\varepsilon \operatorname{Rad}(abc)^{1+\varepsilon}.$$

Suppose $x^n + y^n = z^n$ with $n \geq 3$ and $x, y, z \in \mathbf{Z}^+$. We may take $(x, y) = 1$. Suppose the *abc*-conjecture is proved for some ε. Then

$$\begin{aligned} z^n &\leq \lambda_\varepsilon \operatorname{Rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \lambda_\varepsilon \operatorname{Rad}(xyz)^{1+\varepsilon} \\ &\leq \lambda_\varepsilon (xyz)^{1+\varepsilon} \\ &\leq \lambda_\varepsilon z^{3(1+\varepsilon)}. \end{aligned}$$

For $n > 3(1 + \varepsilon)$,

$$z \leq \lambda_\varepsilon^{1/(n-3(1+\varepsilon))} < 2 \text{ for large } n,$$

so n is bounded above. If *abc*-conjecture holds for some $\varepsilon < 1/3$, then for any $n \geq 4 > 3(1 + \varepsilon)$ we have $z \leq \lambda_\varepsilon^{1/(n-3(1+\varepsilon))}$, so FLT is a finite calculation for remaining exponents.

The Idea Behind the *abc*-Conjecture

It is hard to make a sum or difference of two integers with high prime power factors another such number.

$$\begin{aligned}
2^5 + 7^2 &= 3^4 \\
3^5 + 11^4 &= 122^2 \\
33^8 + 1549034^2 &= 15613^3 \\
109 \cdot 3^{10} + 2 &= 23^5 \\
3^{11} \cdot 5^4 + 7 \cdot 11^6 \cdot 43 &= 2^{17} \cdot 17^3
\end{aligned}$$

Notice there is a prime to at most the second power in all of these examples.

The *abc*-conjecture with $\varepsilon = 0$

$$a+b=c, (a,b)=1 \Rightarrow \max(|a|,|b|,|c|) \leq \lambda_\varepsilon \operatorname{Rad}(abc)^{1+\varepsilon}.$$

If $a+b=c$ with $(a,b)=1$, could $\max(|a|,|b|,|c|) \leq \lambda \operatorname{Rad}(abc)$? Let p be prime and take $a = 2^{p(p-1)} - 1,\ b = 1,\ c = 2^{p(p-1)}$. Then

$$2^{p-1} \equiv 1 \bmod p \Longrightarrow 2^{p(p-1)} \equiv 1 \bmod p^2,$$

so $p^2 | a$. Thus

$$\operatorname{Rad}(abc) = \operatorname{Rad}(a \cdot 2) \leq \frac{2a}{p}.$$

so the *abc*-conjecture with $\varepsilon = 0$ would say

$$a \leq \lambda \cdot \frac{2a}{p} \Longrightarrow p \leq 2\lambda.$$

This is false for large primes p!

Catalan's Conjecture (Mihailescu's Theorem)

Conjecture (Catalan, 1844)

The only consecutive perfect powers in $\mathbf{Z}^+$ *are* $8 = 2^3$ *and* $9 = 3^2$.

Reduced to finite but impractical number of cases by Tijdeman (1974), proved by Mihailescu (2002). What does *abc*-conj. say? Suppose $x^m - y^n = 1$ in $\mathbf{Z}^+$ where $m, n \geq 2$. Of course $m \neq n$, so $1/m + 1/n \leq 1/2 + 1/3 = 5/6$. Since $(x, y) = 1$, by *abc*-conj.

$$y^n < x^m \leq \lambda_\varepsilon \operatorname{Rad}(x^m y^n)^{1+\varepsilon} = \lambda_\varepsilon \operatorname{Rad}(xy)^{1+\varepsilon} \leq \lambda_\varepsilon (xy)^{1+\varepsilon}.$$

Since $y^n < x^m$, $y < x^{m/n}$, so

$$x^m < \lambda_\varepsilon (x^{1+m/n})^{1+\varepsilon} = \lambda_\varepsilon x^{m(1/m+1/n)(1+\varepsilon)} \leq \lambda_\varepsilon x^{m(5/6)(1+\varepsilon)}.$$

Then

$$x^{m(1-5\varepsilon)/6} < \lambda_\varepsilon \Longrightarrow x < \lambda_\varepsilon^{6/m(1-5\varepsilon)} \text{ for } 0 < \varepsilon < 1/5,$$

so

$$y < x^{m/n} < \lambda_\varepsilon^{6/n(1-5\varepsilon)}.$$

Catalan's Conjecture (Mihailescu's Theorem)

We have for $0 < \varepsilon < 1/5$ that

$$x < \lambda_\varepsilon^{6/m(1-5\varepsilon)}, \quad y < \lambda_\varepsilon^{6/n(1-5\varepsilon)}.$$

Fix ε. Large m and n force $x < 2$ and $y < 2$, so $x = 1$ and $y = 1$. So m and n are bounded above, and for each m and n we have upper bounds on x and y: an effectively finite number of cases to check if the *abc*-conjecture is proved for a specific $\varepsilon < 1/5$. This application doesn't follow from *abc*-conjecture for $\varepsilon = 1$.

Consequences of the *abc*-conjecture

- Fermat's Last Theorem for all large exponents (Wiles for all exponents, 1995)
- Catalan's Conjecture for any large parameters (Mihailescu for all, 2002)
- Roth's theorem (Roth, 1955) in a stronger form
- The Mordell Conjecture (Faltings, 1983) in a stronger form

> *It would be of tremendous interest* [. . .] *to bound degrees of integral diophantine equations in contexts of algebraic geometry.* S. Lang, 1978

> [*The abc-conjecture*] *always seems to lie on the boundary of what is known and what is unknown.* D. Goldfeld

abc-Conjecture implies Weak Hall Conjecture

Theorem

If the abc-conjecture is true then for all $\varepsilon > 0$ there is $C_\varepsilon > 0$ such that whenever $y^2 = x^3 + k$ in $\mathbf{Z}$ with $k \neq 0$,

$$|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}, \quad |y| \leq C_\varepsilon |k|^{3(1+\varepsilon)}.$$

May suppose $x, y \neq 0$. Let $d = (x^3, y^2)$.

$$\frac{y^2}{d} = \frac{x^3}{d} + \frac{k}{d}.$$

Set $a = x^3/d$, $b = k/d$, $c = y^2/d$, $R = \mathrm{Rad}(abc)$. By *abc*-conj.,

$$\frac{|x|^3}{d} \leq \lambda_\varepsilon R^{1+\varepsilon}, \quad \frac{|y|^2}{d} \leq \lambda_\varepsilon R^{1+\varepsilon}.$$

$$\text{Upper Bound} : R \leq \prod_{p|ac} p \cdot \prod_{p|b} p \leq |x||y| \,\mathrm{Rad}(b) \leq |x||y| \frac{|k|}{d}.$$

abc-Conjecture implies Weak Hall Conjecture

From $R = \text{Rad}(abc) \leq |x||y||k|/d$,

$$|x|^3, |y|^2 \leq d\lambda_\varepsilon R^{1+\varepsilon} \leq d\lambda_\varepsilon \left(\frac{|x||y||k|}{d}\right)^{1+\varepsilon} < \lambda_\varepsilon(|x||y|)^{1+\varepsilon}|k|^{1+\varepsilon}.$$

Now we take cases: $|y|^2 \leq |x|^3$ or $|x|^3 \leq |y|^2$.
If $|y|^2 \leq |x|^3$ then $|y| \leq |x|^{3/2}$, so

$$|x|^3 < \lambda_\varepsilon |x|^{(5/2)(1+\varepsilon)}|k|^{1+\varepsilon} \implies |x|^{(1-5\varepsilon)/2} < \lambda_\varepsilon |k|^{1+\varepsilon},$$

so for $0 < \varepsilon < 1/5$,

$$|x| < \lambda_\varepsilon^{2/(1-5\varepsilon)}|k|^{2(1+\varepsilon)/(1-5\varepsilon)},$$

and

$$|y| \leq |x|^{3/2} < \lambda_\varepsilon^{3/(1-5\varepsilon)}|k|^{3(1+\varepsilon)/(1-5\varepsilon)}.$$

abc-Conjecture implies Weak Hall Conjecture

If instead $|x|^3 \leq |y|^2$ then $|x| \leq |y|^{2/3}$, so

$$|y|^2 < \lambda_\varepsilon |y|^{(5/3)(1+\varepsilon)}|k|^{1+\varepsilon} \Longrightarrow |y|^{(1-5\varepsilon)/3} < \lambda_\varepsilon |k|^{1+\varepsilon},$$

so for $0 < \varepsilon < 1/5$,

$$|y| < \lambda_\varepsilon^{3/(1-5\varepsilon)}|k|^{3(1+\varepsilon)/(1-5\varepsilon)},$$

and

$$|x| \leq |y|^{2/3} < \lambda_\varepsilon^{2/(1-5\varepsilon)}|k|^{2(1+\varepsilon)/(1-5\varepsilon)}.$$

We have the same x-bound and y-bound in both cases:

$$|x| < \lambda_\varepsilon^{2/(1-5\varepsilon)}|k|^{2(1+\varepsilon)/(1-5\varepsilon)}, \quad |y| < \lambda_\varepsilon^{3/(1-5\varepsilon)}|k|^{3(1+\varepsilon)/(1-5\varepsilon)}.$$

Set $(1+\varepsilon)/(1-5\varepsilon) = 1+\varepsilon'$, so $0 < \varepsilon' < \infty$ for $0 < \varepsilon < 1/5$ and ε' small iff ε small. Let $C_{\varepsilon'} = \max(\lambda_\varepsilon^{2/(1-5\varepsilon)}, \lambda_\varepsilon^{3/(1-5\varepsilon)})$.

Does the Weak Hall Conjecture Imply the *abc*-Conjecture?

Theorem

Assume abc-conj. If $y^2 = x^3 + k$ *in* $\mathbf{Z} - \{0\}$ *and* $(x, y) = 1$, *then*

$$|x| \leq C_\varepsilon \operatorname{Rad}(k)^{2(1+\varepsilon)}, \quad |y| \leq C_\varepsilon \operatorname{Rad}(k)^{3(1+\varepsilon)}. \tag{1}$$

If $3y^2 = x^3 + k$ *in* $\mathbf{Z} - \{0\}$ *and* $(x, 3y) = 1$, *then*

$$|x| \leq B_\varepsilon \operatorname{Rad}(k)^{2(1+\varepsilon)}, \quad |y| \leq B_\varepsilon \operatorname{Rad}(k)^{3(1+\varepsilon)}. \tag{2}$$

These bounds use $\operatorname{Rad}(k)$, not $|k|$, so they're stronger than weak Hall conjecture (but only apply when $(x, y) = 1$ or $(x, 3y) = 1$).

Theorem

Equations (1) *and* (2) *imply the abc-conjecture, and thus are together equivalent to the abc-conjecture.*

This shows Mordell's equation is a far more central equation than it at first may appear to be!

Does the Weak Hall Conjecture Imply the *abc*-Conjecture?

Suppose $a + b = c$ in nonzero integers with $(a, b) = 1$. Set

$$x = a^2 + ab + b^2 \in \mathbf{Z}^+, \quad y = \frac{(a-b)(a+2b)(2a+b)}{2} \in \mathbf{Z} - \{0\}.$$

Then

$$y^2 = x^3 - 27\left(\frac{abc}{2}\right)^2, \quad \max(|a|, |b|, |c|) \leq 2\sqrt{x}, \quad (x, y) = 1 \text{ or } 3.$$

We look here just at the case $(x, y) = 1$. From equation (1),

$$|x| \leq C_\varepsilon \operatorname{Rad}\left(-27\left(\frac{abc}{2}\right)^2\right)^{2(1+\varepsilon)} \leq C_\varepsilon(3 \operatorname{Rad}(abc))^{2(1+\varepsilon)},$$

so

$$\max(|a|, |b|, |c|) \leq 2\sqrt{x} \leq 2C_\varepsilon^{1/2} 3^{1+\varepsilon} \operatorname{Rad}(abc)^{1+\varepsilon}.$$

Mordell's Review of Lang's *Diophantine Geometry*, 1962

The author's style and exposition leave a great deal to be desired. [. . .] Whenever possible all the resources of algebraic geometry are brought into the proofs of the theorems. He seems to use a method of infinite ascent in expounding his proofs, that is, simple ideas are often developed using more complicated ones. [. . .] The would-be reader will require the patience of Job, the courage of Achilles, and the strength of Hercules to understand the proofs of some of the essential theorems.

How much greater thanks would [Lang] have received if the book had been written in such a way that more of it could have been more easily comprehended by a larger class of readers! It is to be hoped that some one will undertake the task of writing such a book.

Lang's Review of Mordell's *Diophantine Equations*, 1969

Even though I find the succession of equations treated somewhat arbitrary, there seems to be one thread which runs through them. [They are] ordered according to degree. Of course, one's first attempt in dealing with diophantine equations is to experiment with equations of low degree and small coefficients. But it soon becomes apparent that the degree is not a good invariant [. . .] and the classification by degree is to a large extent misleading.
It is also possible to connect both results and methods of diophantine analysis with algebraic geometry. [. . .] The intense dislike which Mordell has for this kind of exposition is clearly evidenced by his famous review of [my] book. (If this review is not famous, it should be.)