Что такое *ABC*-гипотеза?

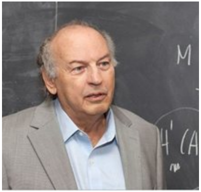
К. Конрад

21 июля 2013 г.

Введение

ABC-гипотеза была сформулирована Массером (Masser) и Остерле (Oesterlé) в 1985 г. под влиянием работы Шпиро (Szpiro).





В сентябре 2012 г. Мочидзуки (Mochizuki) анонсировал доказательство *ABC*-гипотезы в 4 статьях в интернете.

План

- Диофантовы уравнения
- ABC-гипотеза
- Связь ABC-гипотезы с другими проблемами в теории чисел.

ABC-гипотеза [...] *всегда лежит на границе между известным и неизвестным.* Д. Голдфельд

Диофантовы уравнения

Диофантовым уравнением называется многочленное уравнение с целыми (или рациональными) коэффициентами.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

Диофантовы уравнения

Диофантовым уравнением называется многочленное уравнение с целыми (или рациональными) коэффициентами.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

- Сколько решений: конечное число или бесконечное число?
- Если конечное число, можно ли описать их или оценить количество?

Диофантовы уравнения

Диофантовым уравнением называется многочленное уравнение с целыми (или рациональными) коэффициентами.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

- Сколько решений: конечное число или бесконечное число?
- Если конечное число, можно ли описать их или оценить количество?

Пример. $x^2 - 7y^2 = 1$ имеет **бесконечное число** решений в $\mathbf{Z}$: $(1, 0), (8, 3), (127, 48), (2024, 765), \dots$

Диофантовы уравнения

Диофантовым уравнением называется многочленное уравнение с целыми (или рациональными) коэффициентами.

$$7x + 5y = 1, \quad x^2 + y^2 = z^2, \quad y^2 = x^3 - 2, \quad x^3 - x^2y - y^3 = 11$$

- Сколько решений: конечное число или бесконечное число?
- Если конечное число, можно ли описать их или оценить количество?

Пример. $x^2 - 7y^2 = 1$ имеет **бесконечное число** решений в $\mathbf{Z}$: $(1,0),(8,3),(127,48),(2024,765),\dots$

Пример. $x^3 - 7y^3 = 1$ имеет **два** целых решения: $(1,0),(2,1)$. Есть **бесконечное число** рациональных решений: $(1/2,-1/2)$, $(-4/5,-3/5)$, $(-5/4,-3/4)$, $(73/17,38/17),\dots$

Уравнение Морделла

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

Морделла (1888-1972) всегда интересовало это уравнение.

Теорема (Морделл, 1920)

Для каждого $k \in \mathbf{Z} - \{0\}$, $y^2 = x^3 + k$ имеет конечное число решений в $\mathbf{Z}$, т.е. разность квадрата и куба равна k конечно часто.

Его доказательство **неэффективно** (т.е. нет явной, даже непрактичной, оценки количества решений).

Уравнение Морделла

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

Морделла (1888-1972) всегда интересовало это уравнение.

Теорема (Морделл, 1920)

Для каждого $k \in \mathbf{Z} - \{0\}$, $y^2 = x^3 + k$ *имеет конечное число решений в* $\mathbf{Z}$, *т.е. разность квадрата и куба равна* k *конечно часто.*

Его доказательство **неэффективно** (т.е. нет явной, даже непрактичной, оценки количества решений).
Иногда решения очень большие относительно k.

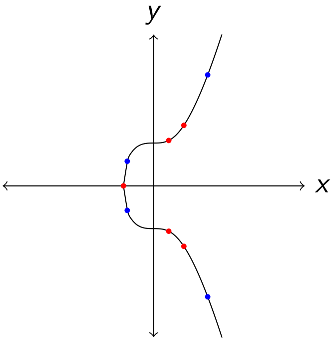
Пример

Целыми решениями уравнениями $y^2 = x^3 + 24$ являются $(-2, \pm 4), (1, \pm 5), (10, \pm 32)$, и $(8158, \pm 736844)$.

График уравнения Морделла

Уравнение $y^2 = x^3 + 8$ имеет бесконечное число решений в $\mathbf{Q}$:

$$(-2, 0), (1, \pm 3), (2, \pm 4), \left(-\frac{7}{4}, \pm\frac{13}{8}\right), \left(\frac{433}{121}, \pm\frac{9765}{1331}\right), \ldots$$

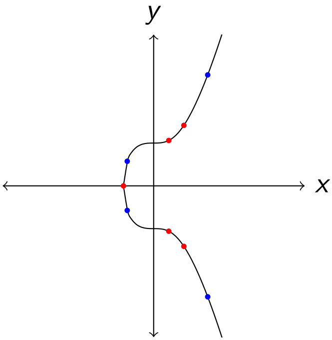


Целые решения $(-2, 0)$, $(1, \pm 3)$, $(2, \pm 4)$, $(46, \pm 312)$.

График уравнения Морделла

Уравнение $y^2 = x^3 + 8$ имеет бесконечное число решений в $\mathbf{Q}$:

$$(-2,0), (1,\pm 3), (2,\pm 4), \left(-\frac{7}{4}, \pm\frac{13}{8}\right), \left(\frac{433}{121}, \pm\frac{9765}{1331}\right), \ldots$$



Целые решения $(-2,0)$, $(1,\pm 3)$, $(2,\pm 4)$, $(46,\pm 312)$.
Если $y^2 = x^3 + k$ в $\mathbf{Z}$ и $k \neq 0$, можно ли оценить $|x|$ через $|k|$?

Гипотеза Холла

Гипотеза (Холл, 1971)

Существует константа $C > 0$, т.ч. если $y^2 = x^3 + k$ в $\mathbf{Z}$ и $k \neq 0$, то $|x| \leq C|k|^2$.

Гипотеза была бы неверна для $|k|^{2(1-\varepsilon)}$ (Данилов, 1982).

Гипотеза Холла

Гипотеза (Холл, 1971)

Существует константа $C > 0$, *т.ч. если* $y^2 = x^3 + k$ *в* $\mathbf{Z}$ *и* $k \neq 0$, *то* $|x| \leq C|k|^2$.

Гипотеза была бы неверна для $|k|^{2(1-\varepsilon)}$ (Данилов, 1982). Примеры в $|x| \leq C|k|^2$ дают нам оценки снизу на C, и по имевшимся у него данным Холл предположил, что $C = 25$ может быть достаточно.

$$736844^2 = 8158^3 + 24 \Longrightarrow C \geq 14{,}1$$
$$223063347^2 = 367806^3 - 207 \Longrightarrow C \geq 8{,}5$$
$$149651610621^2 = 28187351^3 + 1090 \Longrightarrow C \geq 23{,}7$$

Гипотеза Холла

Гипотеза (Холл, 1971)

Существует константа $C > 0$, т.ч. если $y^2 = x^3 + k$ в $\mathbf{Z}$ и $k \neq 0$, то $|x| \leq C|k|^2$.

Гипотеза была бы неверна для $|k|^{2(1-\varepsilon)}$ (Данилов, 1982). Примеры в $|x| \leq C|k|^2$ дают нам оценки снизу на C, и по имевшимся у него данным Холл предположил, что $C = 25$ может быть достаточно.

$$
\begin{aligned}
&736844^2 = 8158^3 + 24 \Longrightarrow C \geq 14{,}1\\
&223063347^2 = 367806^3 - 207 \Longrightarrow C \geq 8{,}5\\
&149651610621^2 = 28187351^3 + 1090 \Longrightarrow C \geq 23{,}7\\
&447884928428402042307918^2 = 5853886516781223^3 - 1641843\\
&\qquad \Longrightarrow C \geq 2171{,}6
\end{aligned}
$$

Холл знал первые три примера, но не четвёртый (Элкис, 1998).

Гипотеза Холла с ε

Старк и Троттер предположили ($\approx$ 1980 г.), что гипотеза Холла была бы верна, если бы степень в $|k|^2$ был бы умножен на $1+\varepsilon$.

Гипотеза

Для каждого $\varepsilon > 0$ существует константа $C_\varepsilon > 0$, т.ч. для каждого $k \in \mathbf{Z} - \{0\}$, если $y^2 = x^3 + k$ в $\mathbf{Z}$, то $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Гипотеза Холла с ε

Старк и Троттер предположили ($\approx$ 1980 г.), что гипотеза Холла была бы верна, если бы степень в $|k|^2$ был бы умножен на $1+\varepsilon$.

Гипотеза

Для каждого $\varepsilon > 0$ существует константа $C_\varepsilon > 0$, т.ч. для каждого $k \in \mathbf{Z} - \{0\}$, если $y^2 = x^3 + k$ в $\mathbf{Z}$, то $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Пусть $\varepsilon = 0{,}1 : |x| \leq C_{0,1}|k|^{2,2}$.

$$736844^2 = 8158^3 + 24 \Longrightarrow C_{0,1} \geq 7{,}5,$$
$$223063347^2 = 367806^3 - 207 \Longrightarrow C_{0,1} \geq 2{,}95,$$
$$149651610621^2 = 28187351^3 + 1090 \Longrightarrow C_{0,1} \geq 5{,}8,$$
$$447884928428402042307918^2 = 58538865167812233^3 - 1641843 \Longrightarrow C_{0,1} \geq 124{,}0.$$

Гипотеза Холла с ε

Старк и Троттер предположили ($\approx$ 1980 г.), что гипотеза Холла была бы верна, если бы степень в $|k|^2$ был бы умножен на $1+\varepsilon$.

Гипотеза

Для каждого $\varepsilon > 0$ существует константа $C_\varepsilon > 0$, т.ч. для каждого $k \in \mathbf{Z} - \{0\}$, если $y^2 = x^3 + k$ в $\mathbf{Z}$, то $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Пусть $\varepsilon = 0{,}1 : |x| \leq C_{0,1}|k|^{2,2}$.

$$
\begin{aligned}
&736844^2 = 8158^3 + 24 \implies C_{0,1} \geq 7{,}5,\\
&223063347^2 = 367806^3 - 207 \implies C_{0,1} \geq 2{,}95,\\
&149651610621^2 = 28187351^3 + 1090 \implies C_{0,1} \geq 5{,}8,\\
&447884928428402042307918^2 = 58538865167812233^3 - 1641843\\
&\qquad\qquad\qquad\implies C_{0,1} \geq 124{,}0.
\end{aligned}
$$

Никто не смог опровергнуть оригинальную гипотезу Холла, но «гипотезой Холла» теперь называется вариант с ε в ней.

Экспоненциальные диофантовы уравнения

Экспоненциальное диофантово уравнение имеет неизвестные степени.

Пример (Великая Теорема Ферма (1630-е))

Для каждого $n \geq 3$ уравнение $x^n + y^n = z^n$ не имеет решения x, y, z в положительных целых. Доказана Уайлсом в 1994 г.

Пример (Гипотеза Каталана (1844))

Единственные последовательные степени в $\mathbf{Z}^+$ — 8 и 9. То есть единственным решением $x^m - y^n = 1$ в $\mathbf{Z}^+$, где $m, n \geq 2$, является $3^2 - 2^3 = 1$. Доказана Михалеску в 2002 г.

Аналитическими методами до Михалеску решения $x^m - y^n = 1$ были оценены явно, но перебирать всю область непрактично.

Экспоненциальные диофантовы уравнения

Экспоненциальное диофантово уравнение имеет неизвестные степени.

Пример (Великая Теорема Ферма (1630-е))

Для каждого $n \geq 3$ уравнение $x^n + y^n = z^n$ не имеет решения x, y, z в положительных целых. Доказана Уайлсом в 1994 г.

Пример (Гипотеза Каталана (1844))

Единственные последовательные степени в $\mathbf{Z}^+$ — 8 и 9. То есть единственным решением $x^m - y^n = 1$ в $\mathbf{Z}^+$, где $m, n \geq 2$, является $3^2 - 2^3 = 1$. Доказана Михалеску в 2002 г.

Аналитическими методами до Михалеску решения $x^m - y^n = 1$ были оценены явно, но перебирать всю область непрактично.

> *Было бы очень интересно [...] оценить неизвестные степени в диофантовых уравнениях в контексте алгебраической геометрии.* С. Ленг, 1978

ABC-Гипотеза

Радикал числа

ABC-гипотеза даёт нам новую точку зрения на экспоненциальные диофантовы уравнения. В гипотезе используется следующее понятие.

Определение. Для каждого положительного целого n **радикалом** (анг. radical) называется $\mathrm{rad}(n) = p_1 p_2 \cdots p_r$, когда $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

Радикал числа

ABC-гипотеза даёт нам новую точку зрению на экспоненциальные диофантовы уравнения. В гипотезе используется следующее понятие.

Определение. Для каждого положительного целого n **радикалом** (анг. radical) называется $\mathrm{rad}(n) = p_1 p_2 \cdots p_r$, когда $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

Примеры.

1) $\mathrm{rad}(1) = 1$
2) $\mathrm{rad}(252) = \mathrm{rad}(2^2 \cdot 3^2 \cdot 7) = 2 \cdot 3 \cdot 7 = 42$
3) $\mathrm{rad}(10000) = 10$
4) $\mathrm{rad}(a^m) = \mathrm{rad}(a)$

Радикал числа

ABC-гипотеза даёт нам новую точку зрению на экспоненциальные диофантовы уравнения. В гипотезе используется следующее понятие.

Определение. Для каждого положительного целого n **радикалом** (анг. radical) называется $\operatorname{rad}(n) = p_1 p_2 \cdots p_r$, когда $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

Примеры.

1) $\operatorname{rad}(1) = 1$
2) $\operatorname{rad}(252) = \operatorname{rad}(2^2 \cdot 3^2 \cdot 7) = 2 \cdot 3 \cdot 7 = 42$
3) $\operatorname{rad}(10000) = 10$
4) $\operatorname{rad}(a^m) = \operatorname{rad}(a)$

Замечание. Неизвестно, как вычислить $\operatorname{rad}(n)$ без разложения n. Сравните с тем, что алгоритмом Евклида НОД(m, n) можно вычислить быстро **без** разложения.

Радикалы чисел a, b, и $a+b$ в $\mathbf{Z}^+$

Очевидно, $a+b \geq \mathrm{rad}(a+b)$. Рассмотрим неравенство $a+b \geq \mathrm{rad}(ab(a+b))$, когда НОД$(a,b) = 1$.

Пример. Среди всех 3044 пар (a,b), т.ч. $1 \leq a \leq b \leq 100$ и НОД$(a,b) = 1$, неравенство $a+b \geq \mathrm{rad}(ab(a+b))$ имеет место 7 раз: $(1,1)$, $(1,8)$, $(1,48)$, $(1,63)$, $(1,80)$, $(5,27)$ и $(32,49)$.

Радикалы чисел a, b, и $a+b$ в $\mathbf{Z}^+$

Очевидно, $a+b \geq \mathrm{rad}(a+b)$. Рассмотрим неравенство $a+b \geq \mathrm{rad}(ab(a+b))$, когда НОД$(a,b) = 1$.

Пример. Среди всех 3044 пар (a,b), т.ч. $1 \leq a \leq b \leq 100$ и НОД$(a,b) = 1$, неравенство $a+b \geq \mathrm{rad}(ab(a+b))$ имеет место 7 раз: $(1,1)$, $(1,8)$, $(1,48)$, $(1,63)$, $(1,80)$, $(5,27)$ и $(32,49)$.

Возникает много примеров неравенства $a+b \geq \mathrm{rad}(ab(a+b))$.

Пример. Пусть $a = 1$ и $b = 3^{2^{10}} - 1$. Тогда b делится на 2^{12}, так что

$$\mathrm{rad}(ab(a+b)) = \mathrm{rad}(b \cdot 3) \leq \frac{b}{2^{11}} \cdot 3 < \frac{3}{2^{11}}(a+b).$$

Поэтому $a+b > \dfrac{2^{11}}{3}\mathrm{rad}(ab(a+b)) \gg \mathrm{rad}(ab(a+b))$.

Радикалы чисел a, b, и $a+b$ в $\mathbf{Z}^+$

Очевидно, $a+b \geq \operatorname{rad}(a+b)$. Рассмотрим неравенство $a+b \geq \operatorname{rad}(ab(a+b))$, когда НОД$(a,b) = 1$.

Пример. Среди всех 3044 пар (a,b), т.ч. $1 \leq a \leq b \leq 100$ и НОД$(a,b) = 1$, неравенство $a+b \geq \operatorname{rad}(ab(a+b))$ имеет место 7 раз: $(1,1)$, $(1,8)$, $(1,48)$, $(1,63)$, $(1,80)$, $(5,27)$ и $(32,49)$.

Возникает много примеров неравенства $a+b \geq \operatorname{rad}(ab(a+b))$.

Пример. Пусть $a = 1$ и $b = 3^{2^{10}} - 1$. Тогда b делится на 2^{12}, так что

$$\operatorname{rad}(ab(a+b)) = \operatorname{rad}(b \cdot 3) \leq \frac{b}{2^{11}} \cdot 3 < \frac{3}{2^{11}}(a+b).$$

Поэтому $a+b > \dfrac{2^{11}}{3} \operatorname{rad}(ab(a+b)) \gg \operatorname{rad}(ab(a+b))$.
Для $b = 3^{2^n} - 1$, $(a+b)/\operatorname{rad}(ab(a+b))$ сколь угодно большое.

ABC-Гипотеза

Определение. *ABC-тройкой* называется тройка полож. целых (a, b, c), т.ч. $a + b = c$ и $\text{НОД}(a, b, c) = 1$ ($\Leftrightarrow \text{НОД}(a, b) = 1$).

Из предыдущего слайда: $c > \text{rad}(abc)$ бесконечно часто.
Насколько больше?

ABC-Гипотеза

Определение. ABC-тройкой называется тройка полож. целых (a, b, c), т.ч. $a + b = c$ и НОД$(a, b, c) = 1$ ($\Leftrightarrow$ НОД$(a, b) = 1$).

Из предыдущего слайда: $c > \mathrm{rad}(abc)$ бесконечно часто.
Насколько больше? Среди всех известных ABC-троек, т.ч. $c > \mathrm{rad}(abc)$, все удовлетворяют $c < \mathrm{rad}(abc)^2$, все, кроме 3, удовлетворяют $c < \mathrm{rad}(abc)^{1,6}$, и все, кроме 13, удовлетворяют $c < \mathrm{rad}(abc)^{1,5}$.

ABC-Гипотеза

Определение. ABC-тройкой называется тройка полож. целых (a, b, c), т.ч. $a + b = c$ и $\text{НОД}(a, b, c) = 1$ ($\Leftrightarrow \text{НОД}(a, b) = 1$).

Из предыдущего слайда: $c > \operatorname{rad}(abc)$ бесконечно часто. Насколько больше? Среди всех известных ABC-троек, т.ч. $c > \operatorname{rad}(abc)$, все удовлетворяют $c < \operatorname{rad}(abc)^2$, все, кроме 3, удовлетворяют $c < \operatorname{rad}(abc)^{1,6}$, и все, кроме 13, удовлетворяют $c < \operatorname{rad}(abc)^{1,5}$.

Гипотеза (Массер, Остерле, 1985)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $c < \operatorname{rad}(abc)^{1+\varepsilon}$.

ABC-Гипотеза

Определение. *ABC-тройкой* называется тройка полож. целых (a, b, c), т.ч. $a + b = c$ и $\text{НОД}(a, b, c) = 1$ ($\Leftrightarrow \text{НОД}(a, b) = 1$).

Из предыдущего слайда: $c > \text{rad}(abc)$ бесконечно часто.
Насколько больше? Среди всех известных ABC-троек, т.ч. $c > \text{rad}(abc)$, все удовлетворяют $c < \text{rad}(abc)^2$, все, кроме 3, удовлетворяют $c < \text{rad}(abc)^{1{,}6}$, и все, кроме 13, удовлетворяют $c < \text{rad}(abc)^{1{,}5}$.

Гипотеза (Массер, Остерле, 1985)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $c < \text{rad}(abc)^{1+\varepsilon}$.

Идея: посмотрим на кратность простых множителей. Трудно найти

$$\underbrace{a}_{\text{высок. кратн.}} + \underbrace{b}_{\text{высок. кратн.}} = \underbrace{c}_{\text{высок. кратн.}}, \quad \text{НОД}(a, b) = 1.$$

Пр: $2^6 + 3^4 = 5^1 \cdot 29^1$, $2^4 \cdot 3^5 + 31^1 \cdot 7^6 \cdot 11^3 = 173^1 \cdot 2459^1 \cdot 11411^1$.

Переформулирование ABC-гипотезы

В опр. ABC-тройки, где $a+b=c$ и $\text{НОД}(a,b,c)=1$, заменяем «$a,b,c>0$» на «$a,b,c\neq 0$». Для $n<0$, пусть $\operatorname{rad}(n)=\operatorname{rad}(|n|)$.

Гипотеза (Допуская ненулевые a,b,c)

Для каждого $\varepsilon>0$ все ABC-тройки (a,b,c), кроме конечного числа, удовлетворяют $\max(|a|,|b|,|c|)<\operatorname{rad}(abc)^{1+\varepsilon}$.

Гипотеза (Нет конечного числа исключений)

Для каждого $\varepsilon>0$ существует константа $\kappa_\varepsilon>0$, т.ч. для всех ABC-троек (a,b,c), $\max(|a|,|b|,|c|)<\kappa_\varepsilon\operatorname{rad}(abc)^{1+\varepsilon}$.

Переформулирование *ABC*-гипотезы

В опр. *ABC*-тройки, где $a + b = c$ и $\text{НОД}(a, b, c) = 1$, заменяем «$a, b, c > 0$» на «$a, b, c \neq 0$». Для $n < 0$, пусть $\mathrm{rad}(n) = \mathrm{rad}(|n|)$.

Гипотеза (Допуская ненулевые a, b, c)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Гипотеза (Нет конечного числа исключений)

Для каждого $\varepsilon > 0$ существует константа $\kappa_\varepsilon > 0$, т.ч. для всех ABC-троек (a, b, c), $\max(|a|, |b|, |c|) < \kappa_\varepsilon \, \mathrm{rad}(abc)^{1+\varepsilon}$.

<u>PROBLEM OF D.W. MASSER</u> (After Oesterlé)

Disprove (or prove) that for every $\varepsilon > 0$ there exists $C(\varepsilon)$ such that

$$\max(|a|, |b|, |c|) \leq C(\varepsilon) \left(\prod_{p \mid abc} p \right)^{1+\varepsilon}$$

for all coprime integers a,b,c with $a + b + c = 0$.

Аналог *ABC*-гипотезы для многочленов

Когда $f(t)$ многочлен (с коэффициентами в $\mathbf{C}$, скажем), пусть $\mathrm{rad}(f)$ — произведение унитарных неприводимых множителей.

Пр. Если $f(t) = t(1-t)^3(1+t)^2$, то $\mathrm{rad}(f) = t(t-1)(t+1)$.

Аналог *ABC*-гипотезы для многочленов

Когда $f(t)$ многочлен (с коэффициентами в $\mathbf{C}$, скажем), пусть $\mathrm{rad}(f)$ — произведение унитарных неприводимых множителей.

Пр. Если $f(t) = t(1-t)^3(1+t)^2$, то $\mathrm{rad}(f) = t(t-1)(t+1)$.

Теорема (Мейсон (1983), Стотерс (1981))

Если $f(t)+g(t)=h(t)$, где f, g, h ненулевые, взаимно просты, не все константы, то $\max(\deg f, \deg g, \deg h) \leq \deg(\mathrm{rad}(fgh))-1$.

Сравните с логарифмической формой *ABC*-гип. ($\ln|n| \leftrightarrow \deg f$): для всех *ABC*-троек, кроме конечного числа,

$$\begin{aligned} \max(|a|,|b|,|c|) &< \mathrm{rad}(abc)^{1+\varepsilon} \\ \iff \ln(\max(|a|,|b|,|c|)) &< (1+\varepsilon)\ln(\mathrm{rad}(abc)) \\ \iff \max(\ln|a|,\ln|b|,\ln|c|) &< (1+\varepsilon)\ln(\mathrm{rad}(abc)). \end{aligned}$$

Для многочленов $\varepsilon = 0$ и в правой части есть -1.

Следствия ABC-гипотезы

Применения *ABC*-гипотезы

Гипотеза

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

В применениях используется «для каждого ε» по-разному:

- один выбор ε (без условий),
- один выбор ε меньше некоторой оценки (например, $\varepsilon < 1/5$),
- все малые ε.

Применения ABC-гипотезы

Гипотеза

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

В применениях используется «для каждого ε» по-разному:

- один выбор ε (без условий),
- один выбор ε меньше некоторой оценки (например, $\varepsilon < 1/5$),
- все малые ε.

До работы Мочидзуки никто не объявил доказательство для одной величины ε.

Великая теорема Ферма для больших степеней

Предположим, что ABC-гипотеза доказана для одного ε: $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ для всех ABC-троек, кроме конечночо числа. Если $x^n + y^n = z^n$, где $n \geq 3$ и $x, y, z \in \mathbf{Z}^+$, то хотим показать, что n ограничен. Не теряя общности, НОД$(x, y) = 1$, поэтому (x^n, y^n, z^n) — ABC-тройка.

Великая теорема Ферма для больших степеней

Предположим, что ABC-гипотеза доказана для одного ε: $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ для всех ABC-троек, кроме конечночо числа. Если $x^n + y^n = z^n$, где $n \geq 3$ и $x, y, z \in \mathbf{Z}^+$, то хотим показать, что n ограничен. Не теряя общности, НОД$(x, y) = 1$, поэтому (x^n, y^n, z^n) — ABC-тройка.
Тогда для всех таких троек (x^n, y^n, z^n), кроме конечного числа,

$$\begin{aligned} z^n &< \mathrm{rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \mathrm{rad}(xyz)^{1+\varepsilon} \\ &\leq (xyz)^{1+\varepsilon} \end{aligned}$$

Великая теорема Ферма для больших степеней

Предположим, что ABC-гипотеза доказана для одного ε: $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ для всех ABC-троек, кроме конечночо числа. Если $x^n + y^n = z^n$, где $n \geq 3$ и $x, y, z \in \mathbf{Z}^+$, то хотим показать, что n ограничен. Не теряя общности, НОД$(x, y) = 1$, поэтому (x^n, y^n, z^n) — ABC-тройка.
Тогда для всех таких троек (x^n, y^n, z^n), кроме конечного числа,

$$\begin{aligned} z^n &< \mathrm{rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \mathrm{rad}(xyz)^{1+\varepsilon} \\ &\leq (xyz)^{1+\varepsilon} \\ &< z^{3(1+\varepsilon)} \\ \Rightarrow n &< 3(1+\varepsilon). \end{aligned}$$

Великая теорема Ферма для больших степеней

Предположим, что ABC-гипотеза доказана для одного ε: $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ для всех ABC-троек, кроме конечноcо числа. Если $x^n + y^n = z^n$, где $n \geq 3$ и $x, y, z \in \mathbf{Z}^+$, то хотим показать, что n ограничен. Не теряя общности, НОД$(x, y) = 1$, поэтому (x^n, y^n, z^n) — ABC-тройка.
Тогда для всех таких троек (x^n, y^n, z^n), кроме конечного числа,

$$\begin{aligned} z^n &< \mathrm{rad}(x^n y^n z^n)^{1+\varepsilon} \\ &= \mathrm{rad}(xyz)^{1+\varepsilon} \\ &\leq (xyz)^{1+\varepsilon} \\ &< z^{3(1+\varepsilon)} \\ \Rightarrow n &< 3(1+\varepsilon). \end{aligned}$$

В исключениях z^n в конечной списке и $z > 1 \Rightarrow n$ ограничен: если исключения $\max(|a|,|b|,|c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ известны для одного ε, то ВТФ верна для больших n, причём эффективно.

Великая теорема Ферма для многочленов

Предположим, что $f(t)^n + g(t)^n = h(t)^n$, где f, g, h ненулевые и **все не константы**. Хотим проверить, что $n < 3$. Не теряя общности, f, g, и h взаимно просты.

Великая теорема Ферма для многочленов

Предположим, что $f(t)^n + g(t)^n = h(t)^n$, где f, g, h ненулевые и **все не константы**. Хотим проверить, что $n < 3$. Не теряя общности, f, g, и h взаимно просты. По теореме MC,

$$\deg f^n, \deg g^n, \deg h^n \leq \deg(\operatorname{rad}(f^n g^n h^n)) - 1 = \deg(\operatorname{rad}(fgh)) - 1.$$

Великая теорема Ферма для многочленов

Предположим, что $f(t)^n + g(t)^n = h(t)^n$, где f, g, h ненулевые и **все не константы**. Хотим проверить, что $n < 3$. Не теряя общности, f, g, и h взаимно просты. По теореме MC,

$$\deg f^n, \deg g^n, \deg h^n \leq \deg(\operatorname{rad}(f^n g^n h^n)) - 1 = \deg(\operatorname{rad}(fgh)) - 1.$$

Так как $\deg(\operatorname{rad}(fgh)) \leq \deg(fgh)$,

$$n \deg f, n \deg g, n \deg h \leq \deg(fgh) - 1.$$

Великая теорема Ферма для многочленов

Предположим, что $f(t)^n + g(t)^n = h(t)^n$, где f, g, h ненулевые и **все не константы**. Хотим проверить, что $n < 3$. Не теряя общности, f, g, и h взаимно просты. По теореме MC,

$$\deg f^n, \deg g^n, \deg h^n \leq \deg(\mathrm{rad}(f^n g^n h^n)) - 1 = \deg(\mathrm{rad}(fgh)) - 1.$$

Так как $\deg(\mathrm{rad}(fgh)) \leq \deg(fgh)$,

$$n \deg f, n \deg g, n \deg h \leq \deg(fgh) - 1.$$

Сложите:

$$n \deg(fgh) \leq 3(\deg(fgh) - 1) < 3 \deg(fgh).$$

Следовательно, действительно $n < 3$.

Замечание. Первое доказательство ВТФ для многочленов было дано в XIX веке. Оно гораздо сложнее вышеприведенного доказательства.

Гипотеза Каталана и ABC-гипотезы

Из ABC-гипотезы для некоторого $\varepsilon < 1/5$ следует, что $x^m - y^n = 1$ имеет конечное число решений в $\mathbf{Z}^+$, когда $m, n \geq 2$. Подробности утомительны.

Гипотеза Каталана и *ABC*-гипотезы

Из *ABC*-гипотезы для некоторого $\varepsilon < 1/5$ следует, что $x^m - y^n = 1$ имеет конечное число решений в $\mathbf{Z}^+$, когда $m, n \geq 2$. Подробности утомительны.
Аналог для многочленов: *Если $f(t)^m - g(t)^n = 1$ где $m, n \geq 2$, то f и g константы.*

Гипотеза Каталана и ABC-гипотезы

Из ABC-гипотезы для некоторого $\varepsilon < 1/5$ следует, что $x^m - y^n = 1$ имеет конечное число решений в $\mathbf{Z}^+$, когда $m, n \geq 2$. Подробности утомительны.

Аналог для многочленов: *Если $f(t)^m - g(t)^n = 1$ где $m, n \geq 2$, то f и g константы.*

Д-во: Предположим, что f или g **не константы**. Так как f, g взаимно просты, по теореме MC для тройки $(f(t)^m, -g(t)^n, 1)$,

$$\deg f^m, \deg g^n \leq \deg(\mathrm{rad}(f^m g^n)) - 1 = \deg(\mathrm{rad}(fg)) - 1,$$

поэтому $m \deg f,\ n \deg g < \deg(fg) = \deg f + \deg g$.

Гипотеза Каталана и ABC-гипотезы

Из ABC-гипотезы для некоторого $\varepsilon < 1/5$ следует, что $x^m - y^n = 1$ имеет конечное число решений в $\mathbf{Z}^+$, когда $m, n \geq 2$. Подробности утомительны.

Аналог для многочленов: *Если $f(t)^m - g(t)^n = 1$ где $m, n \geq 2$, то f и g константы.*

Д-во: Предположим, что f или g **не константы**. Так как f, g взаимно просты, по теореме МС для тройки $(f(t)^m, -g(t)^n, 1)$,

$$\deg f^m, \deg g^n \leq \deg(\operatorname{rad}(f^m g^n)) - 1 = \deg(\operatorname{rad}(fg)) - 1,$$

поэтому $m \deg f,\ n \deg g < \deg(fg) = \deg f + \deg g$. Отсюда

$$\deg f < \frac{\deg g}{m-1}, \quad \deg g < \frac{\deg f}{n-1},$$

Гипотеза Каталана и ABC-гипотезы

Из ABC-гипотезы для некоторого $\varepsilon < 1/5$ следует, что $x^m - y^n = 1$ имеет конечное число решений в $\mathbf{Z}^+$, когда $m, n \geq 2$. Подробности утомительны.

Аналог для многочленов: *Если $f(t)^m - g(t)^n = 1$ где $m, n \geq 2$, то f и g константы.*

Д-во: Предположим, что f или g **не константы**. Так как f, g взаимно просты, по теореме MC для тройки $(f(t)^m, -g(t)^n, 1)$,

$$\deg f^m, \deg g^n \leq \deg(\mathrm{rad}(f^m g^n)) - 1 = \deg(\mathrm{rad}(fg)) - 1,$$

поэтому $m \deg f, \; n \deg g < \deg(fg) = \deg f + \deg g$. Отсюда

$$\deg f < \frac{\deg g}{m-1}, \quad \deg g < \frac{\deg f}{n-1},$$

поэтому $\deg f < \dfrac{\deg f}{(m-1)(n-1)} \leq \deg f \implies \deg f < \deg f$.

Это противоречие, поэтому f и g константы.

Аналог гипотезы Холла для многочленов

Теорема (Дэвенпорт, 1965)

Если $g(t)^2 = f(t)^3 + k(t)$, *где* $k(t)$ *не константа, и* $f(t)$ *и* $g(t)$ *ненулевые, то* $\deg f(t) \leq 2(\deg k(t) - 1)$.

Сравните с Холлом: $y^2 = x^3 + k, k \neq 0$ в $\mathbf{Z} \Rightarrow |x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Аналог гипотезы Холла для многочленов

Теорема (Дэвенпорт, 1965)

Если $g(t)^2 = f(t)^3 + k(t)$, *где* $k(t)$ *не константа, и* $f(t)$ *и* $g(t)$ *ненулевые, то* $\deg f(t) \leq 2(\deg k(t) - 1)$.

Сравните с Холлом: $y^2 = x^3 + k, k \neq 0$ в $\mathbf{Z} \Rightarrow |x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Д-во. *Для простоты в доказательстве*, предположим, что $f(t)$ и $g(t)$ взаимно просты. Тогда уравнение $g(t)^2 = f(t)^3 + k(t)$ удовлетворяет условиям теоремы Мейсона-Стотерса

Аналог гипотезы Холла для многочленов

Теорема (Дэвенпорт, 1965)

Если $g(t)^2 = f(t)^3 + k(t)$, *где* $k(t)$ *не константа, и* $f(t)$ *и* $g(t)$ *ненулевые, то* $\deg f(t) \le 2(\deg k(t) - 1)$.

Сравните с Холлом: $y^2 = x^3 + k, k \ne 0$ в $\mathbf{Z} \Rightarrow |x| \le C_\varepsilon |k|^{2(1+\varepsilon)}$.

Д-во. *Для простоты в доказательстве*, предположим, что $f(t)$ и $g(t)$ взаимно просты. Тогда уравнение $g(t)^2 = f(t)^3 + k(t)$ удовлетворяет условиям теоремы Мейсона-Стотерса, так

$$\begin{aligned}\deg f(t)^3,\ \deg g(t)^2 &\le \deg \operatorname{rad}(f(t)^3 g(t)^2 k(t)) - 1 \\ &\le \deg(f(t)g(t)k(t)) - 1.\end{aligned}$$

Аналог гипотезы Холла для многочленов

Теорема (Дэвенпорт, 1965)

Если $g(t)^2 = f(t)^3 + k(t)$, где $k(t)$ не константа, и $f(t)$ и $g(t)$ ненулевые, то $\deg f(t) \leq 2(\deg k(t) - 1)$.

Сравните с Холлом: $y^2 = x^3 + k, k \neq 0$ в $\mathbf{Z} \Rightarrow |x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Д-во. *Для простоты в доказательстве*, предположим, что $f(t)$ и $g(t)$ взаимно просты. Тогда уравнение $g(t)^2 = f(t)^3 + k(t)$ удовлетворяет условиям теоремы Мейсона-Стотерса, так

$$\begin{aligned} \deg f(t)^3,\ \deg g(t)^2 &\leq \deg \operatorname{rad}(f(t)^3 g(t)^2 k(t)) - 1 \\ &\leq \deg(f(t)g(t)k(t)) - 1. \end{aligned}$$

Поэтому $3\deg f, 2\deg g \leq \deg f + \deg g + \deg k - 1$, отсюда

$$2\deg f \leq \deg g + (\deg k - 1), \quad \deg g \leq \deg f + (\deg k - 1).$$

Аналог гипотезы Холла для многочленов

Теорема (Дэвенпорт, 1965)

Если $g(t)^2 = f(t)^3 + k(t)$, *где* $k(t)$ *не константа, и* $f(t)$ *и* $g(t)$ *ненулевые, то* $\deg f(t) \le 2(\deg k(t) - 1)$.

Сравните с Холлом: $y^2 = x^3 + k, k \neq 0$ в $\mathbf{Z} \Rightarrow |x| \le C_\varepsilon |k|^{2(1+\varepsilon)}$.

Д-во. *Для простоты в доказательстве*, предположим, что $f(t)$ и $g(t)$ взаимно просты. Тогда уравнение $g(t)^2 = f(t)^3 + k(t)$ удовлетворяет условиям теоремы Мейсона-Стотерса, так

$$\begin{aligned} \deg f(t)^3,\ \deg g(t)^2 &\le \deg \operatorname{rad}(f(t)^3 g(t)^2 k(t)) - 1 \\ &\le \deg(f(t)g(t)k(t)) - 1. \end{aligned}$$

Поэтому $3\deg f, 2\deg g \le \deg f + \deg g + \deg k - 1$, отсюда

$$2\deg f \le \deg g + (\deg k - 1), \quad \deg g \le \deg f + (\deg k - 1).$$

Подставим второе неравенство в первое:
$2\deg f \le \deg f + 2(\deg k - 1)$, поэтому $\deg f \le 2(\deg k - 1)$.

Сравнение гипотезы Холла и *ABC*-гипотезы

Теорема (Из *ABC* следует гипотеза Холла)

Если ABC **верна**, *то для всех* $\varepsilon > 0$ *существует* $C_\varepsilon > 0$, *т.ч. если* $y^2 = x^3 + k$ *в* $\mathbf{Z}$ *и* $k \neq 0$, *то* $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.

Теорема (Из *ABC* следует «радикальная гип. Холла»)

Если ABC **верна**, *то для всех* $\varepsilon > 0$ *существует* $C'_\varepsilon > 0$, *т.ч. если* $y^2 = x^3 + k$ *в* $\mathbf{Z}$, $k \neq 0$, $\text{НОД}(x, y) = 1$, *то* $|x| \leq C'_\varepsilon \operatorname{rad}(k)^{2(1+\varepsilon)}$.

Эта оценка вообще **сильнее**, чем в гипотезе Холла, когда НОД(x, y)=1, так как $\operatorname{rad}(k)$ может быть меньше, чем $|k|$.

Сравнение гипотезы Холла и ABC-гипотезы

Теорема (Из ABC следует гипотеза Холла)

Если ABC **верна**, *то для всех $\varepsilon > 0$ существует $C_\varepsilon > 0$, т.ч. если $y^2 = x^3 + k$ в $\mathbf{Z}$ и $k \neq 0$, то $|x| \leq C_\varepsilon |k|^{2(1+\varepsilon)}$.*

Теорема (Из ABC следует «радикальная гип. Холла»)

Если ABC **верна**, *то для всех $\varepsilon > 0$ существует $C'_\varepsilon > 0$, т.ч. если $y^2 = x^3 + k$ в $\mathbf{Z}$, $k \neq 0$, $\text{НОД}(x, y) = 1$, то $|x| \leq C'_\varepsilon \text{rad}(k)^{2(1+\varepsilon)}$.*

Эта оценка вообще **сильнее**, чем в гипотезе Холла, когда $\text{НОД}(x, y)=1$, так как $\text{rad}(k)$ может быть меньше, чем $|k|$.

Теорема

Из радикальной гип. Холла следует ABC: они эквивалентны.

Таким образом, оценка целых решений уравнения Морделла более центральна, чем может показаться на первый взгляд!

Хорошие рациональные приближения

Для иррационального $\alpha \in \mathbf{R}$, **бесконечно много** $a/b \in \mathbf{Q}$ (приведённых форм) удовлетворяют

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Пример. Пусть $\alpha = \sqrt[5]{2} \approx 1{,}1486$. Тогда

$$\left|\sqrt[5]{2} - \frac{1148}{1000}\right| \gg \frac{1}{1000^2} \qquad (0{,}0006 \gg 0{,}000001),$$

$$\left|\sqrt[5]{2} - \frac{309}{269}\right| < \frac{1}{269^2} \qquad (0{,}0000005 < 0{,}0000138).$$

Хорошие рациональные приближения

Для иррационального $\alpha \in \mathbf{R}$, **бесконечно много** $a/b \in \mathbf{Q}$ (приведённых форм) удовлетворяют

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Пример. Пусть $\alpha = \sqrt[5]{2} \approx 1{,}1486$. Тогда

$$\left|\sqrt[5]{2} - \frac{1148}{1000}\right| \gg \frac{1}{1000^2} \qquad (0{,}0006 \gg 0{,}000001),$$

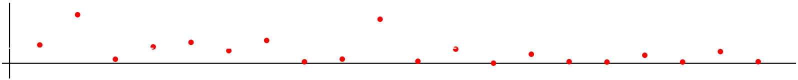
$$\left|\sqrt[5]{2} - \frac{309}{269}\right| < \frac{1}{269^2} \qquad (0{,}0000005 < 0{,}0000138).$$

Приведённые дроби, которые удовлетворяют $\left|\sqrt[5]{2} - \frac{a}{b}\right| < \frac{1}{b^2}$, в порядке возрастания знаменателя $b > 1$:

$$\frac{7}{6}, \frac{8}{7}, \frac{15}{13}, \frac{23}{20}, \frac{31}{27}, \frac{54}{47}, \frac{85}{74}, \frac{139}{121}, \frac{224}{195}, \frac{309}{269}, \ldots.$$

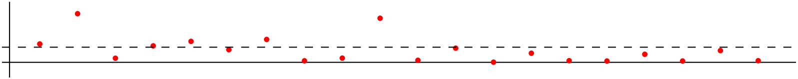
Теорема Рота

Пусть $\frac{a_i}{b_i}$ (приведённые) дроби, т.ч. $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ и $b_1 < b_2 < b_3 < \cdots$. Пусть $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, где $\varepsilon_i > 0$. Вот график всех ε_i для первых 20 таких дробей ($i = 1, 2, \ldots$).



Теорема Рота

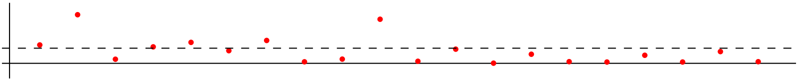
Пусть $\frac{a_i}{b_i}$ (приведённые) дроби, т.ч. $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ и $b_1 < b_2 < b_3 < \cdots$. Пусть $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, где $\varepsilon_i > 0$. Вот график всех ε_i для первых 20 таких дробей ($i = 1, 2, \ldots$).



Чилса ε_i колеблются, но $\varepsilon_i \to 0$. Эквивалентно, $2 + \varepsilon_i \to 2$.

Теорема Рота

Пусть $\frac{a_i}{b_i}$ (приведённые) дроби, т.ч. $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| < \frac{1}{b_i^2}$ и $b_1 < b_2 < b_3 < \cdots$. Пусть $\left|\sqrt[5]{2} - \frac{a_i}{b_i}\right| = \frac{1}{b_i^{2+\varepsilon_i}}$, где $\varepsilon_i > 0$. Вот график всех ε_i для первых 20 таких дробей ($i = 1, 2, \dots$).



Чилса ε_i колеблются, но $\varepsilon_i \to 0$. Эквивалентно, $2 + \varepsilon_i \to 2$.

Теорема (Рот, 1955)

Если α **алгебраическое** *иррациональное, то для всех $\varepsilon > 0$ все $\frac{a}{b}$, кроме конечного числа, удовлетворяют $\left|\alpha - \frac{a}{b}\right| \geq \frac{1}{|b|^{2+\varepsilon}}$.*

Доказательства **неэффективны** в оценке исключений.

ABC-Гипотеза и Теорема Рота

Гипотеза (Первый вариант ABC-гипотезы)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Гипотеза (Эквивалентная оценка снизу $\mathrm{rad}(abc)$)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\mathrm{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$. *(Для $\varepsilon \geq 1$ это очевидно.)*

ABC-Гипотеза и Теорема Рота

Гипотеза (Первый вариант *ABC*-гипотезы)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$.

Гипотеза (Эквивалентная оценка снизу $\mathrm{rad}(abc)$)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\mathrm{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$. *(Для $\varepsilon \geq 1$ это очевидно.)*

Элкис и Ленгевин независимо вывели из 2го варианта ABC, что для всех $\varepsilon > 0$, $\mathrm{rad}(a^5 - 2b^5) > \max(|a|, |b|)^{3-\varepsilon}$ для всех взаимно простых a и b, кроме конечного числа; отсюда следует теорема Рота для $\alpha = \sqrt[5]{2}$.

ABC-Гипотеза и Теорема Рота

Гипотеза (Первый вариант ABC-гипотезы)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\max(|a|, |b|, |c|) < \operatorname{rad}(abc)^{1+\varepsilon}$.

Гипотеза (Эквивалентная оценка снизу $\operatorname{rad}(abc)$)

Для каждого $\varepsilon > 0$ все ABC-тройки (a, b, c), кроме конечного числа, удовлетворяют $\operatorname{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$. (Для $\varepsilon \geq 1$ это очевидно.)

Элкис и Ленгевин независимо вывели из 2го варианта ABC, что для всех $\varepsilon > 0$, $\operatorname{rad}(a^5 - 2b^5) > \max(|a|, |b|)^{3-\varepsilon}$ для всех взаимно простых a и b, кроме конечного числа; отсюда следует теорема Рота для $\alpha = \sqrt[5]{2}$.

Вообще, Элкис и Ленгевин получили, что из ABC-гипотезы следует **полная** теорема Рота, и следовала бы эффективная оценка исключений в Роте из эффективного варианта ABC.

FAQ о работе Мочидзуки над ABC-гипотезой

1. Как он **использует** решение такого простого уравнения $a + b = c$?
2. Для $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ получается ли **явная** оценка исключений (зависящая от ε)?

FAQ о работе Мочидзуки над ABC-гипотезой

1. Как он **использует** решение такого простого уравнения $a + b = c$?
2. Для $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ получается ли **явная** оценка исключений (зависящая от ε)?

1) Исходя из уравнения $a + b = c$ рассматривается **кривая Фрея** $y^2 = x(x - a)(x + b)$. Цель Мочидзуки — **доказать** гипотезу Шпиро об эллиптических кривых, из которой следует ABC-гипотеза, когда гипотеза Шпиро применяется ко кривой Фрея.

FAQ о работе Мочидзуки над ABC-гипотезой

1. Как он **использует** решение такого простого уравнения $a + b = c$?
2. Для $\max(|a|, |b|, |c|) < \mathrm{rad}(abc)^{1+\varepsilon}$ получается ли **явная** оценка исключений (зависящая от ε)?

1) Исходя из уравнения $a + b = c$ рассматривается **кривая Фрея** $y^2 = x(x - a)(x + b)$. Цель Мочидзуки — **доказать** гипотезу Шпиро об эллиптических кривых, из которой следует ABC-гипотеза, когда гипотеза Шпиро применяется ко кривой Фрея.

2) Он так не думает. В работе есть одна явная оценка, прямо применимая к ABC-гипотезе, для «общих» эллиптических кривых (в Теореме 1.10 4ой статьи); «необщему» случаю нужны редукции, использующие **функции Белого**. Он думает, что это не совместимо с явным вариантом ABC-гипотезы.

Вопросы?

Литература

С. Ленг, Математические беседы для студентов, http://www.sci-lib.org/books_1/L/leng.pdf.

E. Bombieri и W. Gubler, *Heights in Diophantine Geometry*.

V. Dimitrov, http://mathoverflow.net/questions/106560/philosophy-behind-mochizukis-work-on-the-abc-conjecture

A. Granville и T. Tucker, "It's as easy as *abc*", Notices AMS, 2002.

S. Lang, "Old and New Conjectured Diophantine Inequalities", *Bull. Amer. Math. Society*, 1990.

A. Nitaj, "La conjecture abc", *Enseign. Math.*, 1996.

A. Nitaj, http://www.math.unicaen.fr/~nitaj/abc.html (веб страница ABC-гипотезы).

M. Waldschmidt, "Perfect Powers: Pillai's works and their developments", http://www.math.jussieu.fr/~miw/articles/pdf/PerfectPowers.pdf.