Глобальная нормализация и Великая теорема Ферма (объяснение для математика без программирования)

Аннотация

Текст даёт *непрограммистское* объяснение подхода *глобальной нормализации* к Великой теореме Ферма (ВТФ): мы вводим единый параметр $o > 1$ и говорим, что *любой* гипотетический контрпример уравнения $x^n + y^n = z^n$ при $n > 2$ *влечёт* равенство

$$o^n = 2\,n,$$

после чего из *принципа максимального покрытия* следует, что *единственно возможный* выбор — $o = 2$, а равенство $2^n = 2n$ возможно лишь при $n \in \{1, 2\}$. Значит, для $n > 2$ наступает противоречие, что согласуется с ВТФ. Важно: **нормализационное утверждение** (что каждый контрпример действительно тянет $o^n = 2n$ для одного и того же o) принимается как *гипотеза*; всё остальное вытекает элементарно. Формальные аналоги определений и лемм приведены и машинно проверены в Coq (без необходимости знать языки программирования, мы дадим интерпретацию всех шагов на обычном математическом языке).[1]

[1]Формальные определение `covers_with`, "мостовая" лемма и теорема о максимальном покрытии — в модуле *GlobalNormalization*; см. файл с Coq-кодом. Также см. пояснительный препринт с историческим комментарием и поэтапной реконструкцией.

Содержание

1 Короткая дорожная карта

1. **Идея нормализации.** Фиксируем число $o > 1$. Говорим, что "*o покрывает* показатель n", если выполнено $o^n = 2\,n$. Эту мысль удобно упаковать так: *всякий* контрпример при $n > 2$ *влечёт* покрытие n тем же o.

2. **Максимальное покрытие.** Рассмотрим $S(o) = \{n \in \mathbb{N} : o^n = 2\,n\}$. Покажем, что для $o = 2$ множество $S(o)$ состоит ровно из $\{1, 2\}$, а при $o \neq 2$ оно меньше по мощности. Отсюда *единственный* выбор, совместимый с принципом "максимального охвата", — это $o = 2$.

3. **Элементарная причина противоречия.** При $o = 2$ имеем $2^n = 2n$ лишь для $n \in \{1, 2\}$, ибо при $n \geq 3$ $2^n > 2n$. Следовательно, гипотетический контрпример при $n > 2$ не может существовать.

4. **Что осталось гипотезой.** Мы *не* доказываем, что для любого контрпримера неизбежно $o^n = 2n$ с *одним и тем же* $o > 1$. Это и есть *нормализационная предпосылка*. Всё остальное — строгая (и даже формально проверенная) математика.

2 Интуиция, понятная без программирования

Цель — *условно* (при принятии нормализующей предпосылки) свести ВТФ к простой оценке роста. Идея нормализации возникла естественно из классического преобразования

$$(z, x) = (m^n + p^n,\ m^n - p^n),$$

которое удобно для анализа парности и биномиальных разложений: при нечётном n разность $(m^n{+}p^n)^n - (m^n{-}p^n)^n$ содержит только нечётные биномиальные индексы и кратна n.[2]

Здесь важны *две* вещи:

- **Комбинаторика бинома Ньютона.** При вычитании $(A{+}B)^n - (A{-}B)^n$ остаются только слагаемые с нечётными степенями B и общий множитель n — это позволяет *нормализовать* разность к виду $2 \cdot n \cdot$ (что-то).

- **Рост экспоненты против линейной функции.** Равенство $o^n = 2n$ не может держаться при больших n, если $o \geq 2$; а если $1 < o < 2$, то оно может выполниться *в лучшем случае один раз* из-за монотонности $(2n)^{1/n}$ по n. Это ведёт к идее выбрать *тот* o, где охват максимален, — и оказывается, что это ровно $o = 2$, причём покрываются только $n = 1$ и $n = 2$.

[2] В Coq это отражено через элементарные факты о чётности/нечётности сумм/разностей, см. леммы о паритете и делимости биномиальных разностей.

3 Формулировка на математическом языке

3.1 Определение и принцип

Определение 3.1 (Покрытие)**.** Для $o > 1$ и $n \in \mathbb{N}$ скажем, что *o покрывает n*, если выполнено

$$o^n = 2\,n.$$

Обозначим множество покрываемых показателей через $S(o) = \{n \in \mathbb{N} : \ o^n = 2\,n\}$.

Определение 3.2 (Глобальная нормализация, принцип максимального покрытия)**.** Говорят, что *имеет место глобальная нормализация*, если существует $o > 1$ такое, что **любой** гипотетический контрпример $x^n + y^n = z^n$ при $n > 2$ *влечёт* покрытие n тем же o, то есть $o^n = 2\,n$ (одно и то же o для всех n). Принцип *максимального покрытия* предписывает выбрать $o > 1$, для которого мощность $|S(o)|$ максимальна среди всех допустимых o.

3.2 Структура множества $S(o)$

Рассмотрим функцию $f(n) = (2n)^{1/n}$ для $n \geq 1$. Тогда $o^n = 2n$ равносильно $o = f(n)$.

Лемма 3.3 (Монотонность f)**.** *Для $n \geq 2$ функция $f(n)$ строго убывает, $f(1) = 2$, $f(2) = 2$, а при $n > 2$ имеем $f(n) < 2$ и $\lim_{n\to\infty} f(n) = 1$.*

Доказательство (эскиз). Рассмотрим $\ln f(n) = \frac{\ln(2n)}{n}$ и производную по n в непрерывной релаксации: $\frac{d}{dn}\big(\ln f(n)\big) = \frac{1-\ln(2n)}{n^2} < 0$ для $n \geq 2$. Вычисления $f(1) = f(2) = 2$ тривиальны, предел к 1 стандартен (используйте $\lim_{n\to\infty} \frac{\ln n}{n} = 0$). □

Предложение 3.4 (Описание $S(o)$)**.** *Для фиксированного $o > 1$:*

1) *если $o \geq 3$, то $S(o) = \varnothing$ (ибо $o^n \geq 3^n > 2n$);*

2) *если $1 < o < 2$, то $|S(o)| \leq 1$ (по лемме 3.3 уровень o пересекается не более одного раза при $n \geq 2$, а $f(1) = 2 > o$);*

3) *если $o = 2$, то $S(2) = \{1, 2\}$, поскольку $f(1) = f(2) = 2$, а при $n > 2$ $f(n) < 2$.*

Следовательно, максимум мощности $|S(o)|$ достигается единственно *при $o = 2$ и равен 2.*

Следствие 3.5 (Выбор нормализации)**.** *Из принципа максимального покрытия следует $o = 2$ и $S(o) = \{1, 2\}$.*

3.3 Элементарная оценка роста экспоненты

Лемма 3.6. *Для всякого $n \geq 3$ верно $2^n > 2n$.*

Доказательство. Индукция по n, или сравнение с биномиальными коэффициентами: $2^n = \sum_{k=0}^{n} \binom{n}{k} \geq \binom{n}{0} + \binom{n}{1} + \binom{n}{n-1} + \binom{n}{n} = 2 + 2n > 2n$ при $n \geq 3$. □

Следствие 3.7. *Равенство $2^n = 2n$ возможно только при $n \in \{1, 2\}$.*

4 Главная условная теорема (логика вывода ВТФ)

Теорема 4.1 (ВТФ из глобальной нормализации)**.** *Пусть существует $o > 1$ такой, что для **любой** гипотетической натуральной тройки x, y, z при $n > 2$, удовлетворяющей $x^n + y^n = z^n$, выполняется покрытие $o^n = 2\,n$ (*одно и то же *o для всех n). Тогда уравнение $x^n + y^n = z^n$ не имеет решений в $\mathbb{N}$ при $n > 2$.*

Доказательство. По принципу максимального покрытия и утв. 3.4 имеем $o = 2$ и $S(o) = \{1, 2\}$. Тогда любое требуемое покрытие при $n > 2$ невозможно, поскольку по следствию 3.7 равенство $2^n = 2n$ не выполняется. Противоречие. □

5 Откуда берётся нормализационная предпосылка

Содержательно предпосылка исходит из *биномиального анализа* разности

$$(m^n + p^n)^n - (m^n - p^n)^n,$$

где при нечётном n выживают только нечётные индексы бинома, а вся сумма кратна n; более того, в конструкциях вида

$$\left(\tfrac{z+x}{2}\right)^{1/n}, \quad \left(\tfrac{z-x}{2}\right)^{1/n}$$

при различной природе n (чётное/нечётное) появляется общий множитель n и, грубо говоря, "универсальный" радикал, способный сворачиваться в одинаковую для всех n норму o.[3]

Важно понимать: **этот переход оставлен как гипотеза**. В препринте сказано впрямую: нормализация *постулируется* и используется как *явная гипотеза*, а не выводится из арифметики самим автором в законченном виде.[4]

6 Мост от вещественных равенств к натуральным степеням

Ключевой "мостовой" факт: если для одного и того же o покрываются два показателя n и m,

$$o^n = 2n, \qquad o^m = 2m,$$

то, возводя в степени и исключая o, получаем равенство целых степеней

$$(2n)^m = (2m)^n.$$

Это удобно, когда надо перенести рассуждение из $\mathbb{R}$ обратно к $\mathbb{N}$ и применить арифметику степеней.

Замечание 6.1 (Зачем это нужно)**.** Мостовая лемма помогает варьировать точки обзора: нормализация живёт в $\mathbb{R}$, а сами $x^n + y^n = z^n$ — в $\mathbb{N}$. Равенство $(2n)^m = (2m)^n$ — это чистая целочисленная симметрия, совместимая с идеей, что набор покрываемых показателей крайне ограничен.

[3] В пояснительном тексте это оформлено как шаги 2–6 с выделением общего множителя n и переходом к равенству вида (некоторое выражение)$^n = 2\,n$; см. раздел *Possible Proof*.

[4] Цитата по смыслу: "The normalization premise is kept as an explicit hypothesis over $\mathbb{N}$; bridge lemmas connect the real equation $o^n = 2 \cdot n$ with the integer comparison."

7 Элементы классики: параметризация, паритет, биномиальная симметрия

7.1 Параметризация $(z, x) = (m^n+p^n,\ m^n-p^n)$

Сама по себе эта запись не обещает целочисленности m, p; однако она даёт сильные *необходимые* условия на чётности $z \pm x$ и на вид выражений $\frac{z\pm x}{2}$. В частности,

$$z + x = 2\,m^n, \qquad z - x = 2\,p^n,$$

так что $z \pm x$ чётны, и если *дополнительно* требовать $m, p \in \mathbb{Z}$, то обе половины должны быть идеальными n-ми степенями. И наоборот: если эти условия выполнены, то m, p реконструируются (с оговорками о знаках при чётных n).

7.2 Нечётные/чётные биномиальные суммы

Суммы чётных и нечётных биномиальных коэффициентов равны и дают 2^{n-1}:

$$\sum_j \binom{n}{2j} = \sum_i \binom{n}{2i+1} = 2^{n-1},$$

что удобно в проверках для $n = 1, 2$ и при разложениях $(A+B)^n \pm (A-B)^n$.

8 Что именно формально проверено, а что — нет

- **Формально в Coq:** определение покрытия $o^n = 2n$; теорема о максимальном покрытии (из $o^1 = 2$ следует $o = 2$ и покрываются лишь $n \in \{1, 2\}$); *мостовая* лемма; элементарные леммы о росте 2^n относительно $2n$; *sanity-цели* вроде «из $o = 2$ не следует покрытие $n = 3$».[5]
- **Оставлено как предпосылка:** *глобальная нормализация* («любой контрпример $\Rightarrow$ покрытие тем же o»). Это сформулировано и подчеркнуто в препринте как явная гипотеза; она мотивируется биномиальными вычислениями и «универсальным» видом, но *не* выводится до конца в рамках классической элементарной теории чисел.

9 Почему выбор $o = 2$ уникален и "естественен"

Уникальность — следствие строгой убывания $f(n) = (2n)^{1/n}$ при $n \geq 2$: только уровень $o = 2$ проходит через две точки $n = 1, 2$; любой иной o даёт не более одной точки пересечения (или вовсе ни одной). Это и есть содержание утв. 3.4. В терминах *метода*: принцип максимального покрытия подсказывает «естественную норму», совпадающую с базой двоичной экспоненты.

[5] Sanity-checks в конце файла служат регрессионными тестами: при o=2 неверно покрытие $n \geq 3$, и т. п.

10 Мини-FAQ для читателя

- **Слабое место?** Единственное — *нормализационная предпосылка*. Все остальные шаги элементарны и/или формально проверены.
- **Не противоречит ли Уайлсу?** Нет. Это *не* новое независимое доказательство ВТФ, а *редукция* ВТФ к конкретному нормализационному утверждению. Доказательство Уайлса остаётся единственным безусловным на сегодня.
- **Зачем Coq?** Чтобы минимальные алгебраические детали (рост, мостовая лемма, "только $n = 1, 2$ при $o = 2$") были проверены машиной, исключая человеческую невнимательность.
- **Есть ли p-адический взгляд?** В коде есть набросок «двухадической скобки» для универсального параметра и факт, что $v_p(o)$ исчезает для нечётных p; это иллюстративно и не используется в основном антагонизме роста.

11 Детальные приложения (элементарные доказательства)

11.1 Почему $2^n > 2n$ при $n \geq 3$

См. лемму 3.6. Доказательство можно сделать и по индукции: при переходе $n \to n{+}1$ из $2^n > 2n$ следует $2^{n+1} = 2 \cdot 2^n > 4n \geq 2(n{+}1)$ для $n \geq 2$.

11.2 Строгая убывчивость $(2n)^{1/n}$

См. лемму 3.3. Ещё одна опция — воспользоваться неравенством AM–GM:

$$(2n)^{1/n} \leq \frac{2 + \underbrace{1 + \cdots + 1}_{n-1 \text{ раз}}}{n} \xrightarrow[n\to\infty]{} 1.$$

А для строгой убывчивости для $n \geq 3$ можно сравнить $f(n)$ и $f(n{+}1)$ напрямую.

11.3 Нечётные биномиальные индексы в разности

Разность $(A{+}B)^n - (A{-}B)^n$ уничтожает все чётные индексы, оставляя

$$2 \sum_j \binom{n}{2j{+}1} A^{n-(2j+1)} B^{2j+1},$$

что и даёт общий множитель $2 \cdot B$ и, в соответствующих подстановках, множитель n (через $\binom{n}{1} = n$ и дальнейшие кратности).

11.4 Параметризация и паритет

Если $z = m^n{+}p^n$, $x = m^n{-}p^n$, то $z{\pm}x = 2 \cdot$ (идеальная степень), следовательно, $z \pm x$ чётны. Из этого вытекают удобные *негативные* критерии: если $z{\pm}x$ странной чётности, соответствующей параметризации целыми m, p нет.

12 Как читать формальные имена (мини-глоссарий без программирования)

- `covers_with` $o\ n$ означает $o^n = 2 \cdot n$.
- `covers_with_two_characterisation` — из $2^n = 2n$ следует $n \in \{1, 2\}$.
- `maximum_coverage_as_theorem` — формализация принципа максимального покрытия: из покрытия $n = 1$ выводится $o = 2$ и ограничение $n \in \{1, 2\}$.
- `two_real_normalizations_imply_nat_power_eq` — мост: из $o^n = 2n$ и $o^m = 2m$ следует $(2n)^m = (2m)^n$.
- `sanity goals` — небольшие автоматические проверки вида «при o=2 нет покрытия для $n \geq 3$».

Заключение (в духе Ферма)

Если поверить, что всякая гипотетическая тройка при $n > 2$ принуждает *одно и то же* число o удовлетворять $o^n = 2n$, то из принципа максимального охвата немедленно получаем $o = 2$ и тем самым исключаем все $n > 2$, поскольку $2^n > 2n$. Лаконичность результата резонирует с идеей «короткой маргиналии». Но именно *нормализация* — предмет основного вопроса и дальнейших исследований.

Что делать дальше? Уточнять и обосновывать нормализационную предпосылку (например, через диофантовы оценки, p-адические аргументы или сравнение с программами типа ABC/десцента), сохраняя при этом элементарную эстетическую линию рассуждений.