Глобальная нормализация по основанию 2 (GN(2)) ⇒ ВТФ: Условный подход, верифицированный в Coq

Григорий Деденко

Аннотация Мы представляем формулировку идеи Деденко с явным основанием, в которой единственной гипотезой является глобальная нормализация по основанию 2 (GN(2)): для любого предполагаемого натурального решения уравнения Ферма $x^n + y^n = z^n$ при $n > 2$ должно выполняться равенство $2^n = 2 \cdot n$. В совокупности с элементарным фактом о росте $2^n > 2 \cdot n$ для всех $n \geq 3$ это немедленно приводит к противоречию и, следовательно, к Великой теореме Ферма (ВТФ). Результат формулируется как условная импликация Арифметика+GN(2) ⇒ ВТФ и полностью формализован в Coq. Ядро формального доказательства построено исключительно над натуральными числами; удобный вещественный предикат «покрытия» $\mathrm{pow}\, 2\, n = 2 \cdot \mathrm{INR}\, n$ связан с $2^n = 2 \cdot n$ через лемму-мост. Стандартная параметризация $(z, x) = (m^n + p^n,\ m^n - p^n)$ и тождества четности включены только для мотивации/проверки согласованности и не играют роли в финальном шаге. Данное представление с GN(2) заменяет более раннюю формулировку с глобальным нормализатором $o > 1$.

Keywords: Великая теорема Ферма · GN(2) · нормализация · Coq · формальная верификация

1 Введение

Рассмотрим уравнение Ферма

$$x^n + y^n = z^n, \qquad x, y, z \in \mathbb{N},\ n \in \mathbb{N}. \tag{1}$$

В настоящей трактовке анализ сводится к одной-единственной гипотезе с явным основанием:

Definition 1 (Глобальная нормализация по основанию 2 (GN(2))). *Для любого $n > 2$ и всех $x, y, z \in \mathbb{N}$,*

$$x^n + y^n = z^n \implies 2^n = 2 \cdot n.$$

Комбинирование GN(2) с элементарным неравенством о росте $2^n > 2 \cdot n$ для $n \geq 3$ немедленно даёт ВТФ.

2 Мотивация: алгебраическая постановка и четность (не используется в ядре доказательства)

Следуя стандартному приему, положим $z := m^n + p^n$ и $x := m^n - p^n$ (изначально над $\mathbb{R}$, чтобы кольцевые равенства были прямолинейными). Тогда

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

представляет собой сумму нечетных членов биномиального разложения. Переходя к $\mathbb{Z}$, мы получаем, что $z \pm x$ четны; в Coq это отражено в леммах `sum_diff_from_parameters_R`, `sum_diff_from_parameters_Z`, и `parity_condition_Z`. Эти факты о четности логически не зависят от финального шага и включены только для полноты изложения.

3 Формализация в Coq: ядро для натуральных чисел и вещественная обертка

В разработке доказываются элементарные сравнения роста $2^n > 2n$ для $n \geq 3$ (и $3^n > 2n$ для $n \geq 1$) и они упаковываются в лемму о том, что $2^n = 2 \cdot n$ влечет $n \in \{1, 2\}$ (`pow_eq_linear_positive`).

Гипотеза GN(2) кодируется непосредственно над $\mathbb{N}$:

GN(2) (Coq).

```
Definition GN2 : Prop :=
  forall (n x y z : nat),
    2 < n ->
    Nat.pow x n + Nat.pow y n = Nat.pow z n ->
    2 ^ n = 2 * n.
```

Из GN(2) немедленно следует противоречие для $n > 2$:

ВТФ из GN(2) (Coq).

```
Lemma FLT_from_GN2 :
  GN2 ->
  forall n x y z,
    2 < n ->
    Nat.pow x n + Nat.pow y n = Nat.pow z n -> False.
```

Для удобства также используется вещественный предикат «покрытия»:

$$\mathrm{pow}\,2\,n \;=\; 2 \cdot \mathrm{INR}\,n,$$

который связывается обратно с $2^n = 2 \cdot n$ через леммы-мосты `covers_two_nat`, `INR_two_mul_nat` и импликацию `GN2_R_implies_GN2`. Это дает следствие `fermat_last_theorem_from_GN2_R`.

4 Что *не* предполагается

Данная трактовка *не* опирается на какие-либо безусловные сравнения, такие как $(m^n + p^n)^n - (m^n - p^n)^n \equiv 0 \pmod{2n}$ (которое в общем случае неверно). Единственным дополнительным предположением является GN(2); алгебраическая параметризация и четность служат для мотивации/проверки согласованности и не используются в финальном шаге.

5 Соответствие между статьей и кодом Coq

Статья (пункт)	**Формализация в Coq (лемма/теорема)**
Алгебраическая параметризация над $\mathbb{R}$; факты о четности целых чисел	`sum_diff_from_parameters_R`, `sum_diff_from_parameters_Z`, `parity_condition_Z`.
Гипотеза GN(2) над $\mathbb{N}$	`GN2` (определение Prop).
Сравнение роста с линейной функцией; $2^n = 2 \cdot n \Rightarrow n \in \{1, 2\}$	`pow2_gt_linear`, `pow3_gt_linear`, `pow_eq_linear_positive`.
Вещественная обертка и мост обратно к $\mathbb{N}$	`covers_two_nat`, `INR_two_mul_nat`, `GN2_R`, `GN2_R_implies_GN2`.
ВТФ из GN(2) (напрямую) / через вещественную обертку	`FLT_from_GN2` / `fermat_last_theorem_from_GN2_R`.

Таблица 1. Соответствие между шагами статьи и разработкой на Coq.

6 Заключение

При единственном предположении GN(2), примененном к любому гипотетическому контрпримеру, файл Coq выводит ВТФ для всех $n > 2$, используя только элементарные леммы о росте. Ограничения по четности из параметризации проверяются отдельно. Данное представление с GN(2) заменяет более ранний подход с глобальным нормализатором ($o > 1$).

Приложение: избранные объявления Coq (имена)

`sum_diff_from_parameters_R`, `sum_diff_from_parameters_Z`, `parity_condition_Z`, `pow2_gt_linear`, `pow3_gt_linear`, `pow_eq_linear_positive`, `GN2`, `GN2_R`, `covers_two_nat`, `INR_two_mul_nat`, `GN2_R_implies_GN2`, `FLT_from_GN2`, `fermat_last_theorem_from_GN2_R`.

Список литературы

1. A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics* 141 (1995), 443–551. (Рус. пер.: Уайлс Э. Модулярные эллиптические кривые и Великая теорема Ферма)
2. G. L. Dedenko. The "Difficulties" in Fermat's Original Discourse on the Indecomposability of Powers Greater Than a Square: A Retrospect. Preprint, 2025. DOI: 10.13140/RG.2.2.24342.32321. (Рус. пер.: Деденко Г. Л. «Острые углы» в рассуждении Пьера Ферма о неразложимости степени выше квадрата (обзор) DOI: 10.13140/RG.2.2.24531.39207/12)
3. The Coq Development Team. The Coq Proof Assistant. `https://coq.inria.fr`. (Рус. пер.: Команда разработчиков Coq. Система доказательства теорем Coq)