Math-Net.Ru

Общероссийский математический портал

Хенг Хуат Чан, Линг Лонг, В. В. Зудилин, О супер-сравнении, мотивированном лежандровым семейством эллиптических кривых, *Матем. заметки*, 2010, том 88, выпуск 4, 620–624

DOI: <https://doi.org/10.4213/mzm8851>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.27.143

26 апреля 2023 г., 17:52:29

О суперсравнении, мотивированном лежандровым семейством эллиптических кривых

Хенг Хуат Чан, Линг Лонг, В. В. Зудилин

В работе доказываются новое суперсравнение, связанное с гауссовым гипергеометрическим рядом, и одно из сравнений Мортенсона. Также приводятся лежандровы преобразования некоторых последовательностей.

Библиография: 8 названий.

Светлой памяти Анатолия Алексеевича Карацубы

1. Введение. Лежандрово семейство эллиптических кривых

$$E_a: y^2 = x(x-1)(x-a)$$

хорошо известно в литературе. Для произвольного фиксированного комплексного числа a кривая E_a отвечает двойному накрытию комплексной прямой с четырьмя точками ветвления: $0, 1, a$ и ∞ . В случае, когда a отлична от $0, 1, \infty$, соответствующая накрывающая кривая является эллиптической кривой, т.е. топологически изоморфна тору. Эллиптические кривые – хорошо изученный объект с многочисленными приложениями, например, в криптографии.

Пусть p – произвольное нечетное простое и a является p -целочисленным, $a \neq 0, 1$. Обозначим через $\#(E_a/\mathbf{F}_p)$ количество решений уравнения E_a над конечным полем $\mathbf{F}_p$. Согласно вычислениям инварианта Хассе эллиптической кривой E_a [1; гл. V, раздел 4] выполнено

$$\#(E_a/\mathbf{F}_p) \equiv - \sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} a^k \pmod{p}. \quad (1)$$

Отметим, что суммирование в правой части обычно берется в пределах до $p-1$, однако мы можем заменить $p-1$ на $(p-1)/2$: при $k \geq (p+1)/2$ имеем

$$\binom{2k}{k} \equiv 0 \pmod{p}.$$

С другой стороны, согласно [2; разделы 2.8–2.11] мы знаем, что

$$\#(E_a/\mathbf{F}_p) \equiv - \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 a^k \pmod{p}. \quad (2)$$

Работа первого автора выполнена при финансовой поддержке NUS Academic Research (грант R-146-000-103-112); работа второго автора выполнена при финансовой поддержке NSA (грант H98230-08-1-0076).

Объединяя (1) и (2), приходим к выводу, что

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} a^k \equiv \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 a^k \pmod{p}. \quad (3)$$

На самом деле, сравнение (3) может быть получено непосредственно, используя

$$\binom{(p-1)/2}{k}^2 \equiv \binom{2k}{k}^2 2^{-4k} \pmod{p}. \quad (4)$$

В случае $a = 2$ эллиптическая кривая обладает так называемым комплексным умножением. На простом языке это означает, что на кривой E_2 имеются дополнительные симметрии; например, если пара (x, y) – решение E_2 , то $(-x + 2, \sqrt{-1} \cdot y)$ также является решением. Известно, что кривая E_2 суперсингулярна над $\mathbf{F}_p$ в случае $p \equiv 3 \pmod{4}$ (см. соответствующее определение в [1; § V.4]). Поэтому из доказательства теоремы 4.1 в [1; § V.4] следует, что для $p \equiv 3 \pmod{4}$ выполнено

$$\#(E_a/\mathbf{F}_p) \equiv 0 \pmod{p}. \quad (5)$$

Иными словами, имеет место следующая “модифицированная” версия сравнения (3):

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-3k} \equiv (-1)^{(p-1)/2} \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 2^k \pmod{p} \quad (6)$$

с дополнительным множителем $(-1)^{(p-1)/2}$ в правой части.

Мы доказываем далее, что на самом деле справедливо более сильное сравнение (суперсравнение).

ТЕОРЕМА 1. Пусть p – нечетное простое и $n = (p-1)/2$. Тогда

$$\sum_{k=0}^n \binom{2k}{k}^2 2^{-3k} \equiv (-1)^n \sum_{k=0}^n \binom{n}{k}^2 2^k \pmod{p^2}. \quad (7)$$

Цель этой заметки – доказательство (7). Удивительно то, что оно использует только элементарные тождества для биномиальных коэффициентов, в то время как большинство доказательств других “суперсравнений” привлекает такие методы, как алгоритм Уилфа–Цайлбергера (см. [3], [4]), гауссовы гипергеометрические ряды (например, [5], [3]), формулы суммирования гипергеометрических рядов (к примеру, [6]).

2. Доказательство теоремы 1. Доказательство теоремы 1 вытекает из двух простых лемм.

ЛЕММА 1. Пусть p – нечетное простое и $n = (p-1)/2$; тогда

$$\sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} \equiv \sum_{k=0}^n \binom{2k}{k}^2 2^{-3k} \pmod{p^2}. \quad (8)$$

ДОКАЗАТЕЛЬСТВО. Заметим, что

$$\begin{aligned} \frac{(1/2 + \varepsilon)_k}{k!} &= \frac{(1/2 + \varepsilon)(1/2 + \varepsilon + 1) \cdots (1/2 + \varepsilon + k - 1)}{k!} \\ &= \frac{(1/2)_k}{k!} \left(1 + 2\varepsilon \sum_{j=1}^k \frac{1}{2j-1} + O(\varepsilon^2) \right). \end{aligned} \quad (9)$$

Подставляя $\varepsilon = p/2$ и $\varepsilon = -p/2$ в (9), находим

$$\begin{aligned} \binom{n+k}{k} &= \frac{(1/2)_k}{k!} \left(1 + p \sum_{j=1}^k \frac{1}{2j-1} + O(p^2) \right), \\ (-1)^k \binom{n}{k} &= \frac{(1/2)_k}{k!} \left(1 - p \sum_{j=1}^k \frac{1}{2j-1} + O(p^2) \right) \end{aligned}$$

соответственно. Таким образом,

$$(-1)^k \binom{n}{k} \binom{n+k}{k} = \left(\frac{(1/2)_k}{k!} \right)^2 (1 + O(p^2)). \quad (10)$$

Домножая обе части на 2^k и суммируя по k , приходим к требуемому сравнению (8).

Напомним, что *лежандрово преобразование* последовательности $\{c_k\}_{k=0}^{\infty}$ есть последовательность $\{a_n\}_{n=0}^{\infty}$, определяемая в соответствии с соотношением

$$a_n = \sum_{k=0}^n \binom{n+k}{k} \binom{n}{k} c_k, \quad n = 0, 1, 2, \dots$$

Для завершения доказательства теоремы 1 укажем лежандрово преобразование последовательности $(-2)^k$.

ЛЕММА 2. Для любого целого неотрицательного n справедливо тождество

$$\sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} = (-1)^n \sum_{k=0}^n \binom{n}{k}^2 2^k. \quad (11)$$

ДОКАЗАТЕЛЬСТВО. Запишем

$$\binom{n+k}{k} = \sum_{j=0}^k \binom{n}{j} \binom{k}{k-j}.$$

Тогда

$$\begin{aligned} \sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} &= \sum_{k=0}^n (-2)^k \binom{n}{k} \sum_{j=0}^k \binom{n}{j} \binom{k}{k-j} \\ &= \sum_{j=0}^n \binom{n}{j} \sum_{k=j}^n (-2)^k \binom{n}{k} \binom{k}{k-j} \\ &= \sum_{j=0}^n \binom{n}{j}^2 \sum_{k=j}^n (-2)^k \binom{n-j}{k-j}, \end{aligned}$$

поскольку

$$\binom{n}{k} \binom{k}{k-j} = \binom{n}{j} \binom{n-j}{k-j}.$$

Следовательно,

$$\begin{aligned} \sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} &= \sum_{j=0}^n \binom{n}{j}^2 \sum_{l=0}^{n-j} (-2)^{l+j} \binom{n-j}{l} \\ &= \sum_{j=0}^n \binom{n}{j}^2 (-2)^j \sum_{l=0}^{n-j} (-2)^l \binom{n-j}{l} \\ &= \sum_{j=0}^n \binom{n}{j}^2 (-2)^j (-1)^{n-j} = (-1)^n \sum_{j=0}^n \binom{n}{j}^2 2^j. \end{aligned}$$

Лемма доказана.

Теорема 1 теперь следует из (8) и (11).

Как следствие теоремы 1, мы видим, что справедливо сравнение (5).

ЗАМЕЧАНИЕ 1. В случае $a = 1$ кубическая кривая $y^2 = x(x-1)^2$ сингулярна, т.е. кривая E_1 изоморфна сфере, а не тору. Этот вырожденный случай соответствует схожему суперсравнению

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} \equiv (-1)^{(p-1)/2} \pmod{p^2}, \quad (12)$$

доказанному Мортенсоном [7; теорема 1] (см. также [8; (1.1)]). Это суперсравнение также можно показать, используя элементарные идеи доказательств лемм 1 и 2.

Действительно, суммируя (10) по k , получаем

$$\sum_{k=0}^{(p-1)/2} \binom{n}{k} \binom{n+k}{k} (-1)^k \equiv \sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} \pmod{p^2}. \quad (13)$$

С другой стороны, несложно видеть, что

$$\sum_{k=0}^n \binom{n}{k} \binom{n+k}{k} (-1)^k = (-1)^n. \quad (14)$$

Объединяя (13) и (14), мы приходим к сравнению (12).

Интересной задачей является получение схожих элементарных доказательств других сравнений Мортенсона [8; (1.2)–(1.4)].

Авторам хотелось бы поблагодарить Роберта Осбурна, обсуждения которого со вторым автором инспирировали наши результаты, а также Эрика Мортенсона за ценные замечания. Первый и второй авторы признательны Национальному Центру теоретических наук в Синьчжу (Тайвань), где данный проект стартовал. Работа первого автора над проектом проходила во время визита в Институт математики им. Макса Планка в Бонне (Германия); он благодарен институту за предоставленные прекрасные исследовательские условия.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math., **106**, Springer-Verlag, New York, 1986.
- [2] C. H. Clemens, *A Scrapbook of Complex Curve Theory*, Univ. Ser. Math., Plenum Press, New York, 1980.
- [3] R. Osburn, C. Schneider, “Gaussian hypergeometric series and supercongruences”, *Math. Comp.*, **78**:265 (2009), 275–292.
- [4] W. Zudilin, “Ramanujan-type supercongruences”, *J. Number Theory*, **129**:8 (2009), 1848–1857.
- [5] S. Ahlgren, K. Ono, “A Gaussian hypergeometric series evaluation and Apéry number congruences”, *J. Reine Angew. Math.*, **518** (2000), 187–212.
- [6] D. McCarthy, R. Osburn, “A p -adic analogue of a formula of Ramanujan”, *Arch. Math. (Basel)*, **91**:6 (2008), 492–504.
- [7] E. Mortenson, “A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function”, *J. Number Theory*, **99**:1 (2003), 139–147.
- [8] E. Mortenson, “Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogs”, *Trans. Amer. Math. Soc.*, **355**:3 (2003), 987–1007.

Хенг Хуат Чан

National University of Singapore, Singapore

E-mail: matchh@nus.edu.sg

Поступило

24.01.2010

Линг Лонг

Iowa State University, USA

E-mail: linglong@iastate.edu

В. В. Зудилин

University of Newcastle, Australia

E-mail: wadim.zudilin@newcastle.edu.au