О p-адической аппроксимации сумм биномиальных коэффициентов

Р. Р. АЙДАГУЛОВ
Московский государственный университет им. М. В. Ломоносова

М. А. АЛЕКСЕЕВ
Университет Джорджа Вашингтона, США
e-mail: maxal@gwu.edu

УДК 511.172

Ключевые слова: биномиальный коэффициент, p-адическая аппроксимация, делимость.

Аннотация

Найдены обобщения соотношений Якобсталя для p-адической аппроксимации биномиальных коэффициентов на высокие порядки аппроксимации. Из найденных соотношений следуют явные формулы для линейных комбинаций биномиальных коэффициентов вида $\binom{ip}{p}$ (для $i = 1, 2, \ldots$), делящихся на сколь угодно большие степени простых чисел p.

Abstract

R. R. Aidagulov, M. A. Alekseyev, On p-adic approximation of sums of binomial coefficients, Fundamentalnaya i prikladnaya matematika, vol. 21 (2016), no. 1, pp. 37—48.

We propose higher-order generalizations of Jacobsthal's p-adic approximation for binomial coefficients. Our results imply explicit formulas for linear combinations of binomial coefficients $\binom{ip}{p}$ $(i = 1, 2, \ldots)$ that are divisible by arbitrarily large powers of prime p.

1. Введение

Определение степени простого числа p, делящей заданное число, можно интерпретировать как установление его p-адической малости. При этом степень p, на которую делится заданное число, указывает, насколько оно мало в p-адической метрике, так как делимость $p^r \mid n$ влечёт оценку $n = O(p^r)$.

Задачу об установлении p-адической близости биномиальных коэффициентов $\binom{ap}{bp}$ и $\binom{a}{b}$ приписывают Э. Люка [2]. А именно, в 1878 году Э. Люка доказал [4,5], что

$$\binom{a}{b} = \prod_{i=0}^{d} \binom{a_i}{b_i} + O(p),$$

Фундаментальная и прикладная математика, 2016, том 21, № 1, с. 37—48.
© 2016 *Национальный Открытый Университет «ИНТУИТ»*

где $a = a_0 + a_1 p + \ldots + a_d p^d$ и $b = b_0 + b_1 p + \ldots + b_d p^d$ — это представления чисел a, b в p-ичной системе счисления. Ещё раньше, в 1869 году, Х. Антон получил более сильный результат:

$$\frac{(-1)^\ell}{p^\ell}\binom{a}{b} = \prod_{i=0}^{d} \frac{a_i!}{b_i!\, c_i!} + O(p),$$

где c_i — это p-ичные цифры разности $c = a - b = c_0 + c_1 p + \ldots + c_d p^d$, а $\ell = \nu_p\big(\binom{a}{b}\big)$. Здесь $\nu_p(x)$ обозначает максимальную степень простого числа p, на которую делится число x. Ранее, в 1852 году, Э. Куммер показал, что ℓ равно числу переносов при сложении чисел $a - b$ и b в p-ичной системе счисления.

Нетрудно убедиться, что из результата Х. Антона следует оценка

$$\binom{ap}{bp} \Big/ \binom{a}{b} = 1 + O(p), \tag{1}$$

которая была известна ещё Э. Куммеру. Для удобства определим модифицированные (p-адические) факториалы и биномиальные коэффициенты следующим образом:

$$a!_p = \prod_{\substack{k=1\\ p\nmid k}}^{a} k, \qquad \binom{a}{b}_p = \frac{a!_p}{b!_p\,(a-b)!_p}.$$

Заметим, что модифицированные биномиальные коэффициенты также являются целыми. Теоремы, уточняющие оценку (1) на более высокие степени p вида

$$\binom{ap}{bp} \Big/ \binom{a}{b} = \binom{ap}{bp}_p = 1 + O(p^r), \quad r > 1, \tag{2}$$

в [4, 5] относят к соотношениям типа Вольстенхольма. Первая теорема такого рода была доказана ещё в 1819 году Ч. Бэббиджем. А именно, он доказал, что

$$\binom{2p}{p}_p = \frac{1}{2}\binom{2p}{p} = \binom{2p-1}{p-1} = 1 + O(p^r) \tag{3}$$

для $r = 2$ и всех простых $p > 2$. Эта оценка соответствует (2) при $a = 2$ и $b = 1$. Дж. Вольстенхольм уточнил оценку Ч. Бэббиджа, доказав справедливость (3) для $r = 3$ и простого $p > 3$, а также рассмотрел вопрос нахождения простых p, для которых она верна при $r = 4$. Теперь такие простые называются *простыми Вольстенхольма* (их известно только два: 16 843 и 2 124 679). Для произвольных $a > b > 0$, $r = 3$ и $p > 3$ оценка (2) была доказана В. Льюнггреном в 1949 году [4], а в 1952 году Э. Якобсталь усилил этот результат:

$$\binom{ap}{bp}_p = 1 + O(p^r), \quad r = 3 + \nu_p\big(ab(a-b)\big), \quad p > 3, \tag{4}$$

причём r может быть увеличено ещё на 1 при условии делимости числа Бернулли B_{p-3} на p. Сейчас частные случаи этих результатов часто встречаются в виде задач на математических олимпиадах и в журналах для школьников [1, 3].

Следующее обобщение соотношения Вольстенхольма на сколь угодно высокие степени простых было предложено вторым автором.

Теорема 1. *Для любых целых чисел $n, m \geqslant 1$ и простого числа $p > 2n+1$ линейная комбинация модифицированных биномиальных коэффициентов*

$$\sum_{j=0}^{n}(-1)^j\binom{2n+1}{j}\frac{2(n-j)+1}{2n+1}\cdot\binom{(n+1-j)m}{m}_p \tag{5}$$

делится на $p^{(2n+1)\nu_p(m)}$.

Заметим, что коэффициенты при p-адических биномиальных коэффициентах в выражении (5) являются целыми ввиду равенства

$$\binom{2n+1}{j}\frac{2(n-j)+1}{2n+1}=\binom{2n-1}{j}-\binom{2n-1}{j-2}=\binom{2n}{j}-\binom{2n}{j-1}.$$

Из теоремы 1 следует аналогичное утверждение для обычных биномиальных коэффициентов.

Следствие 2. *Для любого целого числа $n \geqslant 1$ и любого простого числа $p > 2n+1$ линейная комбинация биномиальных коэффициентов*

$$\sum_{i=1}^{n+1} c_i\binom{ip}{p},$$

где коэффициенты

$$c_i=(-1)^{i-1}\frac{\text{НОК}(1,2,\ldots,2n)\binom{2n+1}{n+1-i}(2i-1)}{\binom{2n+1}{n}i}$$

являются целыми и взаимно простыми в совокупности, делится на p^{2n+1}.

Например, для $n = 1, 2, 3$ следствие 2 даёт такие делимости на степени простых:

$$p^3 \mid 2-\binom{2p}{p}, \qquad p>3;$$

$$p^5 \mid 12-9\binom{2p}{p}+2\binom{3p}{p}, \qquad p>5;$$

$$p^7 \mid 60-54\binom{2p}{p}+20\binom{3p}{p}-3\binom{4p}{p}, \qquad p>7.$$

Здесь делимость для $n = 1$ в точности эквивалентна оценке Вольстенхольма (3) для $r = 3$. Коэффициенты c_i представлены в онлайн-энциклопедии целочисленных последовательностей [6] последовательностью `A268512`, а соответствующие частные для $n = 1, 2, 3$ — последовательностями `A087754`, `A268589` и `A268590`.

Основным результатом данной работы является следующая теорема, из которой теорема 1 следует как частный случай, соответствующий арифметической прогрессии верхних индексов $a_i = ib$ и $m = bq$.

Теорема 3. *Пусть q — степень простого числа p, $b > 0$ — целое число и $a = a_{n+1}, a_1, \ldots, a_n$ — различные целые числа, не меньшие b. Тогда существует единственный набор рациональных чисел*

$$y_i = \prod_{\substack{k=1\\k\neq i}}^{n} \frac{(a-a_k)(a+a_k-b)}{(a_i-a_k)(a_i+a_k-b)},$$

наилучшим образом аппроксимирующий модифицированный биномиальный коэффициент $\binom{aq}{bq}_p$ как аддитивно,

$$\binom{aq}{bq}_p = \sum_{i=1}^{n} y_i \binom{a_i q}{bq}_p + O(p^r),$$

так и мультипликативно[1],

$$\binom{aq}{bq}_p = \prod_{i=1}^{n} \left(\binom{a_i q}{bq}_p\right)^{y_i} \bigl(1 + O(p^r)\bigr).$$

При этом для всех простых $p > \max\{2n+1,\, a_i + a_k - b\colon 1 \leqslant i < k \leqslant n\}$ степень аппроксимации не ниже[2]

$$r = (2n+1)\nu_p(q) + \nu_p\bigl(g_0(a)\bigr) + \nu_p(b) + \varepsilon,$$

где

$$g_0(x) = \prod_{k=1}^{n} (x-a_k)(x+a_k-b),$$

$$\varepsilon = \min\{t,\, \nu_p(B_{M-2n})\}, \quad t = \nu_p(bq), \quad M = p^{t-1}(p-1).$$

Теорема 3 также обобщает соотношения Якобсталя, получаемые здесь при $n = 1$, $a_1 = b$ и $q = p$.

2. Доказательство теоремы 3

Пусть выполняются условия теоремы 3. Нашей ближайшей целью будет отыскание коэффициентов $y_1, \ldots, y_n$, не зависящих от p, которые наилучшим образом приближают биномиальный коэффициент $\binom{aq}{bq}_p$ в p-адической метрике, т. е. установление оценки

$$\binom{aq}{bq}_p - \sum_{i=1}^{n} y_i \binom{a_i q}{bq}_p = O(p^r) \tag{6}$$

[1] Заметим, что согласно (1) выполняется $\binom{a_i q}{bq}_p = 1 + O(p)$, и поэтому возведение $\binom{a_i q}{bq}_p$ в рациональную степень корректно определено по биномиальному разложению: $(1+t)^y = 1 + \binom{y}{1}t + {} + \binom{y}{2}t^2 + \ldots$.

[2] Слагаемое ε в формуле для r здесь является аналогом условия $p \mid B_{p-3}$, повышающего степень аппроксимации в соотношении Якобсталя (4).

с максимально возможной степенью r. Как мы увидим в дальнейшем, существуют единственные рациональные числа $y_1, \ldots, y_n$, максимизирующую r (т. е. дающие наилучшую аппроксимацию для модифицированных коэффициентов). При этом их единственность обеспечивается тем, что y_i не зависят от простого числа p, т. е. аппроксимация является наилучшей для всех простых начиная с некоторого.

Нам потребуется следующая лемма.

Лемма 4. *Пусть*

$$S = \left\{ \frac{bq}{2} - \ell \colon 0 \leqslant \ell < \frac{bq}{2},\ p \nmid \frac{bq}{2} - \ell \right\}.$$

Обозначим

$$N = |S| = \frac{bq(p-1)}{2p}$$

(когда $p = q = 2$ и b нечётно, мы рассматриваем S как мультимножество, в которое элемент b, соответствующий $\ell = 0$, входит с весом $1/2$). Тогда модифицированные биномиальные коэффициенты $\binom{a_i q}{bq}_p$ выражаются в виде

$$\binom{a_i q}{bq}_p = \frac{f(z_i)}{f\left(\frac{b^2}{4}\right)}, \tag{7}$$

где

$$z_i = \left(a_i - \frac{b}{2}\right)^2$$

и

$$f(x) = \prod_{k \in S} \left(1 - x\frac{q^2}{k^2}\right) = \sum_{i=0}^{N} (-xq^2)^i \sigma_i. \tag{8}$$

Здесь σ_i — элементарные симметрические многочлены от величин $1/k^2$, $k \in S$.

Доказательство. Действительно,

$$\binom{a_i q}{bq}_p = \prod_{k \in S} \frac{\left((a_i - \frac{b}{2})q + k\right)\left((a_i - \frac{b}{2})q - k\right)}{(\frac{bq}{2} + k)(\frac{bq}{2} - k)} = \prod_{k \in S} \frac{1 - x(\frac{q}{k})^2}{1 - (\frac{bq}{2k})^2} = \frac{f(z_i)}{f(\frac{b^2}{4})}. \qquad \square$$

Согласно лемме 4 после умножения левой части соотношения (6) на $f(b^2/4) = \pm 1 + O(q)$ она приобретает вид

$$f(z_0) - \sum_{i=1}^{n} y_i f(z_i). \tag{9}$$

Таким образом, наша задача сводится к нахождению чисел y_i, наилучшим (в p-адической метрике) образом аппроксимирующих значения многочлена $f(z_0)$ по значениям $f(z_i)$. Этого можно добиться, выбирая y_i так, чтобы в разности (9) исчезли все младшие степени p, что ввиду (8) соответствует решению линейной системы уравнений

$$z_0^d = \sum_{i=1}^{n} y_i z_i^d, \quad d = 0, 1, \ldots, n-1. \tag{10}$$

Так как по условию все a_i не меньше b и попарно различны, то различными будут и $z_i \neq z_j$ при всех $i \neq j$. Поэтому определитель системы уравнений, являющийся определителем Вандермонда, не равен нулю. Чтобы найти решение системы (10), заметим, что для любого многочлена $g(z)$ степени, меньшей n, должно выполняться соотношение

$$g(z_0) = \sum_{i=1}^{n} y_i g(z_i).$$

Взяв последовательно многочлены

$$g_i(z) = \prod_{j \neq i} (z - z_j),$$

получаем, что $g_i(z_0) = y_i g_i(z_i)$. Следовательно, значения y_i находятся единственным образом:

$$y_i = \prod_{\substack{k=1 \\ k \neq i}}^{n} \frac{z_0 - z_k}{z_i - z_k} = \prod_{\substack{k=1 \\ k \neq i}}^{n} \frac{(a - a_k)(a + a_k - b)}{(a_i - a_k)(a_i + a_k - b)}. \tag{11}$$

Рациональные числа y_i являются p-адическими целыми согласно условию $p > \max\limits_{1 \leqslant i < k \leqslant n} a_i + a_k - b$.

Заметим, что, максимизируя r в мультипликативной аппроксимации

$$\binom{aq}{bq}_p \cdot \prod_{i=1}^{n} \left(\binom{a_i q}{bq}_p \right)^{-y_i} = 1 + O(p^r), \tag{12}$$

мы приходим к тому же уравнению (10) и его решению (11). (Уравнение (10) при $d = 0$ здесь необходимо для сокращения множителей $f(b^2/4)$ при подстановке выражений (7) в левую часть (12).)

Найдём теперь точность аппроксимации (6), т. е. оценим

$$\sum_{i=0}^{N} (-q^2)^i \sigma_i \Delta_i, \quad \Delta_i = z_0^i - y_1 z_1^i - \ldots - y_n z_n^i.$$

Для $i < n$ выполняется $\Delta_i = 0$. При $i = n$ имеем $z^n = g(z) + r_n(z)$, $\deg\bigl(r_n(z)\bigr) < n$, где $g(z) = (z - z_1)(z - z_2) \cdots (z - z_n)$. Отсюда получаем, что $\Delta_n = g(z_0)$. Из представления

$$z^{n+1} = (z + z_1 + z_2 + \ldots + z_n) g(z) + r_{n+1}(z), \quad \deg\bigl(r_{n+1}(z)\bigr) < n,$$

выводим, что $\Delta_{n+1} = (z_0 + z_1 + \ldots + z_n) g(z_0)$. Аналогично при $i > n$ получаем, что $\Delta_i = f_i(z_0, z_1, \ldots, z_n) g(z_0)$. Можно представить $f(x)$ как $f_1(x) g(x) + r(x)$, где $\deg\bigl(r(x)\bigr) < n$, и сказать, что ошибка находится как $f_1(z_0)g(z_0)$. Однако нам нужно разложение по растущим степеням q, и мы ограничимся формулой для остатка:

$$\sum_{i=n}^{N}(-q^2)^i\sigma_i\Delta_i = g(z_0)(-1)^n q^{2n}\bigl(\sigma_n - q^2\sigma_{n+1}(z_0+z_1+\ldots+z_n) + O(q^4\sigma_{n+2})\bigr).$$

Таким образом, точность аппроксимации для простых чисел $p > n$ определяется формулой

$$r = (2n+1)\nu_p(q) + \nu_p\bigl(g(z_0)\bigr) + \nu_p\left(\frac{\sigma_n}{q}\right). \tag{13}$$

Точность для мультипликативной аппроксимации такая же.

Заметим, что формула (13) для ошибки аппроксимации обобщает соотношение Якобсталя (4). А именно, $(2n+1)\nu_p(q)$ в (13) соответствует слагаемому 3 в (4) (при $n=1$), следующий член $\nu_p\bigl(g(z_0)\bigr)$ соответствует $\nu_p\bigl(a(a-b)\bigr)$, а аналогом члена $\nu_p(b)+\nu_p(B_{p-3})$ является $\nu_p(\sigma_n/q)$. Для доказательства последнего утверждения оценим σ_n, используя формулы Ньютона—Жирара:

$$n\sigma_n = \sum_{i=1}^{n}(-1)^{i-1}\sigma_{n-i}s_i, \tag{14}$$

где s_i обозначают соответствующие степенные суммы

$$s_i = \sum_{k\in S}k^{-2i} \equiv \sum_{k\in S}k^{M-2i} \pmod{p^{2t}},$$

где $t = \nu_p(bq)$ и $M = p^{t-1}(p-1)$. Покажем, что для простых $p > 2n+1$ и всех $i = 1, 2, \ldots, n$ справедливо неравенство

$$\nu_p(s_i) \geqslant \nu_p(bq) + \theta_i, \quad \text{где} \quad \theta_i = \min\{t, \nu_p(B_{M-2i})\}. \tag{15}$$

Пусть

$$S_i = \sum_{\substack{\ell=1\\ p\nmid\ell}}^{bq-1}\ell^{-2i} = \sum_{k\in S}\left(\frac{bq}{2}-k\right)^{-2i} + \left(\frac{bq}{2}+k\right)^{-2i}. \tag{16}$$

Так как нам нужны элементарные симметрические многочлены от обратных величин, во избежание отрицательных степеней в последней формуле мы заменим отрицательные степени $-2i$ на $m = M - 2i$. Это даст оценку

$$S_i = \frac{1}{m+1}\sum_{k=1}^{m+1}B_{m+1-k}(bq)^k + O(p^r) = bqB_m + \frac{m(m-1)}{6}B_{m-2}(bq)^3 + O\bigl((bq)^4\bigr),$$

где мы учли чётность $2i$ и m. Следовательно, $\nu_p(S_i) \geqslant \nu_p(bq) + \theta_i$. С другой стороны, выражая члены S_i в (16) через s_i (раскрыв скобки в степени, предварительно заменив $-2i$ на m), получим, что

$$S_i = 2s_i + O\bigl((bq)^2\bigr) \equiv 2s_i \pmod{p^{2t}}.$$

Отсюда следует требуемая оценка (15) для s_i.

Из формулы (14) получаем выражение для σ_n:

$$\sigma_n = \frac{(-1)^{n-1}}{n}(s_n - \sigma_1 s_{n-1} + \ldots + (-1)^{n-1}\sigma_{n-1}s_1) =$$
$$= \frac{(-1)^{n-1}}{n}\left(s_n - \sum_{j=1}^{n-1}\frac{s_{n-j}}{j}\left(s_j + \sum_{i=1}^{j-1}(-1)^{i-1}s_{j-i}\sigma_i\right)\right) = \ldots$$

Продолжение приводит к формуле

$$\sigma_n = (-1)^n \sum_{k=1}^{n}(-1)^k \sum_{j_1+j_2+\ldots+j_k=n} \frac{s_{j_1}s_{j_2}\cdots s_{j_k}}{j_1(j_1+j_2)\cdots(j_1+j_2+\ldots+j_k)}. \qquad (17)$$

Заметим, что простые числа, бо́льшие n, не делят знаменатели в формуле (17). Для простого $p > 2n+1$ из оценки (15) следует, что сумма членов (17) с фиксированным k оценивается как $O(p^{k\cdot\nu_p(bq)})$. Поэтому из выражения (17) для σ_n следует оценка $\nu_p(\sigma_n) \geqslant \min\{\nu_p(s_n), 2\nu_p(bq)\}$. Из формулы (15) для s_n мы получаем

$$\nu_p(\sigma_n) \geqslant \min\{\nu_p(bq) + \theta_n,\, 2\nu_p(bq)\} = \nu_p(bq) + \theta_n.$$

Поэтому из (13) следует, что для простых

$$p > \max\{2n+1,\, a_i + a_k - b\colon 0 \leqslant i < k \leqslant n\}$$

точность аппроксимации (6) не ниже

$$r = (2n+1)\nu_p(q) + \nu_p\big(g(z_0)\big) + \nu_p(b) + \theta_n.$$

Это завершает доказательство теоремы 3.

3. Доказательство теоремы 1 и следствия 2

Теорема 1 легко получается как следствие теоремы 3 при $a_i = bi$ и $m = bq$. Теорема 1 может быть также доказана напрямую через оператор конечной разности

$$\Delta f(x) = f(x+1) - f(x).$$

Очевидно, что Δ уменьшает степень многочлена на 1 (как и обычное дифференцирование), а константы переводит в 0. Соответственно, m-я степень оператора Δ

$$\Delta^m f(x) = \sum_{i=0}^{m}(-1)^{m-i}\binom{m}{i}f(x+i)$$

уменьшает степень многочлена на m.

Доказательство теоремы 1. По аналогии с леммой 4 модифицированный биномиальный коэффициент $\binom{xm}{m}_p$ при фиксированном m представляется в виде многочлена:

$$\binom{xm}{m}_p = f(x) = \prod_{\substack{k=1\\ p\nmid k}}^{m}\Big(1-\frac{xm}{k}\Big) = f(1-x) = \sum_{i=0}^{N}(-1)^i\sigma_i(xm)^i.$$

Тогда сумму (5) можно записать в виде

$$S=\sum_{j=0}^{n}(-1)^j\binom{2n+1}{j}\frac{2n+1-2j}{2n+1}f(n+1-j)= \\ =\sum_{j=0}^{n}(-1)^j\binom{2n}{j}f(n+1-j)+\sum_{j=0}^{n}(-1)^{j+1}\binom{2n}{j-1}f(n+1-j).$$

Нашей целью будет представление S через оператор Δ с учётом соотношения $f(x)=f(1-x)$. Для этого перепишем части суммы S в виде

$$\sum_{j=0}^{n}(-1)^j\binom{2n}{j}f(n+1-j)=\sum_{i=-n}^{0}(-1)^{n+i}\binom{2n}{n+i}f(i),$$

$$\sum_{j=0}^{n}(-1)^{j+1}\binom{2n}{j-1}f(n+1-j)=\sum_{i=1}^{n+1}(-1)^{n+i}\binom{2n}{n+i}f(i).$$

Получаем, что

$$S=\sum_{i=-n}^{n}(-1)^{n+i}\binom{2n}{n+i}f(i)=\frac12\sum_{i=-n}^{n}(-1)^{n+i}\binom{2n}{n+i}\big(f(i)+f(1-i)\big)= \\ =\frac12\sum_{i=-n}^{n}(-1)^{n+i}\binom{2n}{n+i}\big(f(i)+f(i+1)\big)=\Delta^{2n}\big(f(x)-f(-x)\big)\big|_{x=-n}.$$

Так как функция $f(x)-f(-x)$ нечётная, то оператор Δ^{2n} уничтожит все степени до $2n+1$, следовательно, S делится на $p^{(2n+1)\nu_p(m)}$. □

Докажем теперь следствие 2.

Доказательство следствия 2. Теорема 1 для $m=p$ даёт делимость

$$\sum_{i=1}^{n+1}(-1)^{i-1}\cdot t_i\cdot\binom{ip}{p}$$

на p^{2n+1} для всех простых $p>2n+1$, где коэффициенты

$$t_i=\binom{2n+1}{n+1-i}\frac{2i-1}{(2n+1)i}$$

уже не всегда являются целыми. В частности,

$$t_{n+1}=\frac{1}{n+1}.$$

Заметим, что для $i \leqslant n$, мы также имеем, что

$$t_i = \binom{2n}{n-i} \frac{2i-1}{(n+1-i)i}.$$

Для всякого простого r обозначим

$$\ell_r = \max_{1 \leqslant i \leqslant n+1} -\nu_r(t_i). \tag{18}$$

Так как числа $i \cdot t_i$ (с точностью до знака представляющие собой коэффициенты в (5)) являются целыми, то при $r > n+1$ выполняется $\ell_r \geqslant 0$, а при $r \leqslant n+1$ имеет место $\ell_r \geqslant -\nu_r(t_{n+1}) \geqslant 0$. Чтобы превратить коэффициенты t_i в целые, их необходимо умножить на целое положительное число

$$L = \prod_{r \leqslant n+1} r^{\ell_r},$$

причём L является минимальным таким числом, и коэффициенты $c_i = L \cdot t_i$ будут взаимно просты в совокупности. Нашей целью является нахождение явного выражения для L, что эквивалентно нахождению явного выражения для ℓ_r для всех простых $r \leqslant n+1$.

Рассмотрим простое число $r \leqslant n+1$. Заметим, что для всякого $i = 1, 2, \ldots, n$ выполняется

$$-\nu_r(t_i) = \nu_r(i) - \nu_r\left(\binom{2n+1}{n+1-i}\right) - \nu_r\left(\frac{2i-1}{2n+1}\right), \tag{19}$$

в то время как $-\nu_r(t_{n+1}) = \nu_r(n+1)$.

Пусть $i = i_0 + i_1 r + \ldots + i_k r^k$ и $n+1 = n_0 + n_1 r + \ldots + n_k r^k$ — представление чисел i и $n+1$ в r-ичной системе счисления, где целое число $k \geqslant 1$ таково, что $r^k \leqslant n+1 < r^{k+1}$. Ясно, что $-\nu_r(t_i) \leqslant -\nu_r(t_{j_l})$, где $l = \nu_r(i)$, $j_s = n+1-\big((n+1-i) \bmod r^{s+1}\big)$. При замене i на j_l первый и последний члены в (19) не изменятся, а средний член может только увеличиться. Поэтому при поиске максимума в (18) достаточно рассмотреть только случаи, когда r-ичные цифры чисел i и $n+1$ удовлетворяют следующим соотношениям: $i_s = n_s$ для $s \geqslant l$ и $i_s = 0$ для $s < l$.

Если $\nu_r(i) = 0$, то из (19) следует, что

$$-\nu_r(t_i) = \nu_r(n+1) - \nu_r\left(\binom{2n}{n-i}\right) - \nu_r(2i-1) \leqslant -\nu_r(t_{n+1}) \leqslant \ell_r.$$

Если при сложении $n+1$ и n в r-ичной системе счисления не происходит переноса в l-м разряде, то $-\nu_r(t_{j_{l+1}}) \geqslant -\nu_r(t_{j_l})+1$ за счёт увеличения $\nu_r(j_{l+1}) = \nu_r(j_l)$. Если же перенос происходит, то за ним могут последовать и другие переносы, т. е. $-\nu_r(t_{j_l}) \leqslant -\nu_r(t_{j_{l+m}})$, где $l+m$ — это номер разряда, где переноса снова не происходит. Точнее, для $s = 0, 1, \ldots, m$ имеем, что

$$-\nu_r(t_{j_{l+s}}) = -\nu_r(t_{j_{l+m}}) - (m-s) = -\nu_r(t_{j_l}) + 1 - (m-s)$$

при условии, что соответствующие цифры $n+1$ отличны от нуля. Поэтому максимум $-\nu_r(t_i)$ достигается при $i = j_q$, где q — наибольший r-ичный разряд, где не происходит переноса при сложении $n+1$ и n. Отсюда следует, что

$$L = \prod_{r \leqslant n+1} r^{\ell_r} = \frac{\text{НОК}(1,2,\ldots,2n)\cdot(2n+1)}{\binom{2n+1}{n}}.$$

Так как для каждого простого $r \leqslant n+1$ существует номер i, такой что $r \nmid c_i$, коэффициенты $c_i = L \cdot t_i$ являются целыми и взаимно простыми в совокупности.

□

4. Заключительные замечания

Теорема 3 охватывает случай сумм биномиальных коэффициентов с произвольными кратными p верхними индексами, но с фиксированным нижним индексом. Наш анализ показывает, что обобщения теоремы 3 на случай произвольных нижних индексов не всегда приводит к разрешимым линейным уравнениям относительно коэффициентов y_i, а когда они разрешимы, их не удаётся выразить общей формулой.

Заметим, что существует также обобщения соотношения Якобсталя на случай составного модуля, предложенное первым автором. А именно, соотношение Якобсталя можно записать в виде

$$m^3 \mid 6 \cdot \sum_{d\mid m} \mu\left(\frac{m}{d}\right)\binom{ad}{bd} \tag{20}$$

для случая простого $m = p$, где $\mu(\cdot)$ — функция Мёбиуса. При этом оказывается, что делимость (20) верна и для произвольного положительного целого числа m. Это утверждение получается из соотношения Якобсталя рассмотрением делимости на $p^{3\nu_p(m)}$ для каждого простого делителя $p \mid m$. Из делимости (20) легко следует аналогичная делимость

$$m^3 \mid 12 \cdot \sum_{d\mid m} (-1)^{m+d} \mu\left(\frac{m}{d}\right)\binom{ad}{bd}. \tag{21}$$

Заметим, что множитель 6 в (20) можно заменить на

$$M(a,b) = \frac{12}{\text{НОД}\big(12, ab(a-b)\big)}$$

(нетрудно убедиться, что $M(a,b) \mid 6$), причём для некоторых a, b множитель может быть взят равным даже $(1/2)M(a,b)$. Аналогично множитель 12 в (21) можно заменить на

$$M'(a,b) = \frac{3}{\text{НОД}\big(3, ab(a-b)\big)} \cdot 2^{\delta},$$

где

$$\delta = \begin{cases} \min\{1, \nu_2(b)\}, & \text{если } \nu_2(a-b) = \nu_2(b), \\ 2 & \text{иначе,} \end{cases}$$

а для некоторых a, b далее уменьшить до $(1/2)M'(a,b)$. Например, для $(a,b) = (2,1)$ частные, соответствующие этим делимостям с $M(2,1) = 6$ и $M'(2,1) = 3$, представлены последовательностями `A268592` и `A254593` в онлайн-энциклопедии целочисленных последовательностей [6]. Теорема 3 позволяет обобщить делимости (20) и (21) на большие степени m.

Литература

[1] Винберг Э. Б. Удивительные арифметические свойства биномиальных коэффициентов // Матем. просвещ. Сер. 3. — 2008. — № 12. — С. 33—42.

[2] Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Высшая школа, 2000.

[3] Фукс Д. Б., Фукс М. Б. Арифметика биномиальных коэффициентов // Квант. — 1970. — № 6. — С. 17—25.

[4] Granville A. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers // Can. Math. Soc. Conf. Proc. — 1997. — Vol. 20. — P. 253—275.

[5] Meštrović R. Lucas' theorem: its generalizations, extensions and applications (1878—2014). — `arXiv:1409.3820`. — 2014.

[6] The OEIS Foundation: The On-Line Encyclopedia of Integer Sequences. — `http://oeis.org`. — 2016.