Тема номера: p-адические числа

Удивительные арифметические свойства биномиальных коэффициентов

Э. Б. Винберг

1. Вступление

Хорошо известные формулы

$$(a+b)^2 = a^2 + 2ab + b^2,$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

являются частными случаями формулы бинома Ньютона

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \dots + C_n^{n-1} ab^{n-1} + b^n = \sum_{k=1}^{n} C_n^k a^{n-k} b^k. \quad (1)$$

Коэффициент C_n^k в этой формуле есть «число сочетаний из n по k» — число способов выбрать k предметов из n предметов без учета порядка[1)].

Выбирая k предметов из n предметов по порядку, первый предмет мы можем выбрать n способами, второй — $n-1$ способами, третий — $n-2$ способами и т. д. Таким образом, число упорядоченных выборок k предметов из n предметов равно

$$n(n-1)(n-2)\cdot\ldots\cdot(n-k+1).$$

Если же мы не хотим учитывать порядок, то это число надо разделить на «число перестановок» k предметов — число способов упорядочить k

[1)] Вместо C_n^k используется также обозначение $\binom{n}{k}$.

предметов, которое (по тем же соображениям) равно

$$k(k-1)\cdot\ldots\cdot 2\cdot 1 = k!\,.$$

Окончательно получаем

$$C_n^k = \frac{n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)}{k!}\,. \tag{2}$$

(Обратите внимание на то, что число множителей в числителе и знаменателе одинаково.)

Формуле (2) можно придать вид

$$C_n^k = \frac{n!}{k!(n-k)!}\,,$$

откуда следует, что

$$C_n^k = C_n^{n-k}\,. \tag{3}$$

Впрочем, последнее свойство очевидно и из комбинаторного смысла числа сочетаний: выбрать k предметов из n предметов — это то же, что выбрать оставшиеся $n-k$ предметов.

Числа C_n^k, называемые также *биномиальными коэффициентами*, удобно вычислять при помощи следующего рекуррентного соотношения:

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k\,. \tag{4}$$

Для его доказательства выделим один предмет из имеющихся n предметов. Тогда число способов выбрать k предметов, включая выделенный, равно C_{n-1}^{k-1}, а число способов выбрать k предметов, отличных от выделенного, равно C_{n-1}^k, откуда и следует формула (4).

Удобно считать, что

$$C_n^k = 0 \text{ при } k < 0 \text{ или } k > n.$$

Тогда формула (4) будет справедлива и при $k = 0, n$.

Биномиальные коэффициенты можно записать в форме *треугольника Паскаля* — бесконечной треугольной таблицы, в n-й строке которой стоят числа

$$C_n^0,\ C_n^1,\ C_n^2,\ \ldots,\ C_n^{n-1},\ C_n^n\,,$$

причем строки таблицы сдвинуты таким образом, что каждое число n-й строки в соответствии с формулой (4) равно сумме двух ближайших к нему чисел $(n-1)$-й строки. Первые 10 строк (от нулевой до девятой) треугольника Паскаля показаны на рис. 1.

Биномиальные коэффициенты обладают рядом удивительных арифметических свойств. Подсчитаем, например, сколько нечетных чисел имеется в каждой строке треугольника Паскаля. Мы получим последовательность чисел

$$1,\ 2,\ 2,\ 4,\ 2,\ 4,\ 4,\ 8,\ 2,\ 4,\ \ldots$$

$$\begin{array}{ccccccccccccccccccc}
&&&&&&&&&1&&&&&&&&&\\
&&&&&&&&1&&1&&&&&&&&\\
&&&&&&&1&&2&&1&&&&&&&\\
&&&&&&1&&3&&3&&1&&&&&&\\
&&&&&1&&4&&6&&4&&1&&&&&\\
&&&&1&&5&&10&&10&&5&&1&&&&\\
&&&1&&6&&15&&20&&15&&6&&1&&&\\
&&1&&7&&21&&35&&35&&21&&7&&1&&\\
&1&&8&&28&&56&&70&&56&&28&&8&&1&\\
1&&9&&36&&84&&126&&126&&84&&36&&9&&1
\end{array}$$

Рис. 1. *Треугольник Паскаля*

Сразу трудно угадать общий закон для членов этой последовательности. Однако видно, что все выписанные числа являются степенями двойки! В следующем разделе мы опишем закон, по которому четные и нечетные числа располагаются в треугольнике Паскаля и, в частности, докажем, что число нечетных чисел в каждой строке действительно является степенью двойки.

2. Биномиальные коэффициенты по модулю p

Пусть p — простое число. Займемся вычислением биномиальных коэффициентов C_n^k по модулю p.

Разделим n и k на p с остатком:

$$n = n'p + n_0, \quad k = k'p + k_0, \quad (0 \leqslant n_0, k_0 < p). \tag{5}$$

Докажем, что

$$C_n^k \equiv C_{n'}^{k'} C_{n_0}^{k_0} \pmod{p}. \tag{6}$$

Среди имеющихся n предметов выделим n' блоков по p предметов в каждом блоке, оставив n_0 предметов вне блоков. Выборку k предметов будем называть *блочной*, если она состоит из k' целых блоков и k_0 предметов вне блоков. Число блочных выборок равно $C_{n'}^{k'} C_{n_0}^{k_0}$. Поэтому нам достаточно доказать, что число остальных выборок делится на p.

Отметим, что, как видно из (2), C_p^l при $0 < l < p$ делится на p.

Рассмотрим выборки, содержащие соответственно l_1, l_2, $\ldots$, l_s предметов ($0 < l_1, \ldots, l_s < p$) из каких-то фиксированных s блоков ($s > 0$) и, кроме того, целиком какие-то фиксированные блоки и какие-то фиксированные предметы вне блоков. (Общее число выбираемых предметов, естественно, должно быть равно k.) Число таких выборок равно

$$C_p^{l_1} C_p^{l_2} \cdot \ldots \cdot C_p^{l_s}$$

и согласно предыдущему делится на p^s. Суммируя, получаем, что число всех неблочных выборок делится на p. Тем самым сравнение (6) доказано.

Разделим теперь n' и k' на p с остатком:

$$n' = n''p + n_1, \quad k' = k''p + k_1 \quad (0 \leqslant n_1, k_1 < p).$$

Подставляя в (5), получаем

$$n = n''p^2 + n_1 p + n_0, \quad k = k''p^2 + k_1 p + k_0.$$

Продолжая так дальше, мы в конце концов получим p-ичное представление чисел n и k:

$$n = n_d p^d + n_{d-1} p^{d-1} + \cdots + n_1 p + n_0,$$
$$k = k_d p^d + k_{d-1} p^{d-1} + \cdots + k_1 p + k_0.$$

(Число цифр в p-ичной записи чисел n и k, конечно, не обязано быть одинаковым, но мы можем для удобства сделать его формально одинаковым, приписав спереди к одному из чисел несколько нулей.)

Применив несколько раз сравнение (6), мы получим следующую теорему.

Теорема 1 (Люка́ (Lucas), 1878).

$$C_n^k \equiv C_{n_d}^{k_d} C_{n_{d-1}}^{k_{d-1}} \cdot \ldots \cdot C_{n_1}^{k_1} C_{n_0}^{k_0} \pmod p.$$

Следствие. *C_n^k не делится на p тогда и только тогда, когда $k_i \leqslant n_i$ при всех $i = 0, 1, \ldots, d$.*

В частности, число нечетных биномиальных коэффициентов в n-й строке треугольника Паскаля равно числу таких k, в двоичной записи которых единицы стоят лишь там, где они стоят в двоичной записи числа n. Число таких k равно 2^r, где r — число единиц в двоичной записи числа n.

На рис. 2 изображены первые 16 строк треугольника Паскаля по модулю 2. Для большей наглядности нули заменены кружками, а единицы — крестиками.

В следующих трех задачах n_i и k_i $(i = 0, 1, \ldots, d)$ обозначают цифры в двоичной записи чисел n и k.

Задача 1. *Рассмотрим n-ю строку треугольника Паскаля по модулю 2 как двоичную запись некоторого натурального числа P_n. Докажите, что*

$$P_n = F_{i_1} \cdot \ldots \cdot F_{i_s},$$

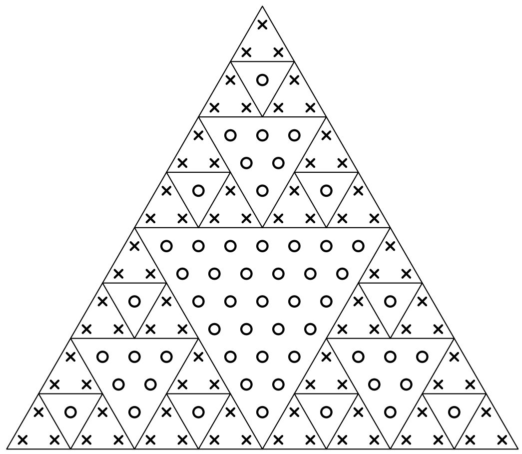

Рис. 2.

где $i_1, \ldots, i_s$ — номера разрядов, в которых в двоичной записи числа n стоят единицы, а $F_i = 2^{2^i} + 1$ — i-е число Ферма.

Например, $P_5 = F_0 F_2 = 3 \cdot 17 = 51 = 2^5 + 2^4 + 2 + 1$.

Задача 2. *Докажите, что если биномиальный коэффициент C_n^k нечетен (т. е. $k_i \leqslant n_i$ при всех $i = 0, 1, \ldots, d$), то*

$$C_n^k \equiv \prod_{i=1}^{d} (-1)^{k_{i-1} n_i + k_i n_{i-1}} \pmod 4.$$

Выведите отсюда, что если в двоичной записи числа n нет двух единиц подряд, то все нечетные числа в n-й строке треугольника Паскаля сравнимы с 1 по модулю 4, а в противном случае ровно половина из них сравнима с 1 по модулю 4.

Задача 3. *Докажите, что если биномиальный коэффициент C_n^k четен, то он не делится на 4 тогда и только тогда, когда имеется ровно одно значение i, для которого $k_i > n_i$, и при этом $k_{i+1} < n_{i+1}$.*

3. Делимость биномиальных коэффициентов на степени простых чисел

Мы уже научились определять, делится ли биномиальный коэффициент C_n^k на простое число p. Но, если он делится на p, как узнать, делится ли он на p^2 и, вообще, на какую максимальную степень p он делится? Ответ на этот вопрос дается приводимой ниже теоремой Куммера.

Для любого целого числа N и простого числа p будем обозначать через $\operatorname{ord}_p N$ показатель максимальной степени p, на которую делится N.

Теорема 2 (Куммер (Kummer), 1852). *Показатель* $\operatorname{ord}_p C_n^k$ *равен числу переносов при сложении «столбиком» чисел* k *и* $l = n - k$ *в* p*-ичной записи.*

Доказательство. Будем доказывать теорему индукцией по n. При $n = 0$ утверждение очевидно. При $n > 0$ рассмотрим два случая.

1-й случай. Числа k и l (а значит, и n) делятся на p:

$$n = n'p, \quad k = k'p, \quad l = l'p.$$

Делимость числа C_n^k на степени p определяется теми множителями в выражении (2), которые делятся на p. Число этих множителей в числителе и знаменателе одинаково и равно k'. Если мы оставим только их и сократим полученную дробь на $p^{k'}$, то мы получим $C_{n'}^{k'}$. Следовательно,

$$\operatorname{ord}_p C_n^k = \operatorname{ord}_p C_{n'}^{k'}. \tag{7}$$

С другой стороны, p-ичные записи чисел k' и l' получаются из p-ичных записей чисел k и l отбрасыванием нулей, стоящих в нулевом разряде (и сдвигом остальных разрядов). Поэтому число переносов при сложении k и l такое же, как и при сложении k' и l'. По предположению индукции оно равно $\operatorname{ord}_p C_{n'}^{k'}$, что в силу (7) равно $\operatorname{ord}_p C_n^k$.

2-й случай. Хотя бы одно из чисел k и l не делится на p. Для определенности будем считать, что k не делится на p, т. е. $k_0 > 0$.

Пусть $\operatorname{ord}_p n = s \geqslant 0$. Из формулы (2) следует, что

$$\operatorname{ord}_p C_n^k = \operatorname{ord}_p C_{n-1}^{k-1} + s. \tag{8}$$

С другой стороны, нетрудно видеть, что при сложении k и l в первых s разрядах происходят переносы, а при сложении $k-1$ и l в этих разрядах переносов не происходит; все же остальные переносы происходят в тех же разрядах. Следовательно, число переносов при сложении k и l ровно на s больше, чем при сложении $k-1$ и l. Учитывая предположение индукции и равенство (8), получаем требуемое утверждение. $\square$

4. «Сокращение» биномиальных коэффициентов на p

Из теоремы Люка следует, что

$$C_{np}^{kp} \equiv C_n^k \pmod{p}.$$

Это сравнение можно улучшить. Разобьем np предметов на n блоков по p предметов в каждом блоке. Выборку из kp предметов назовем блочной (как и в п. 2), если она состоит из k целых блоков. Число блочных выборок равно C_n^k. Число выборок, содержащих соответственно $l_1, l_2, \ldots, l_s$ предметов ($0 < l_1, \ldots, l_s < p$) из каких-то фиксированных s блоков ($s > 0$) и, кроме того, целиком какие-то фиксированные блоки, равно $C_p^{l_1} C_p^{l_2} \cdot \ldots \cdot C_p^{l_s}$ и, следовательно, делится на p^s. Заметим, что $s > 1$, поскольку общее число выбираемых предметов кратно p. Следовательно, общее число неблочных выборок делится на p^2 и, значит,

$$C_{np}^{kp} \equiv C_n^k \pmod{p^2}.$$

При $p \geqslant 5$ верно еще более сильное сравнение

$$C_{np}^{kp} \equiv C_n^k \pmod{p^3}. \tag{9}$$

Рассуждая, как выше, мы видим, что для его доказательства достаточно рассмотреть случай, когда имеется всего два блока. Именно этот случай составляет предмет следующей теоремы.

Теорема 3 (Волстенхолм (Wolstenholme), 1862). *При* $p \geqslant 5$

$$C_{2p}^{p} \equiv 2 \pmod{p^3} \tag{10}$$

или, что то же самое,

$$C_{2p-1}^{p-1} \equiv 1 \pmod{p^3}. \tag{11}$$

(Легко видеть, что при $p = 2, 3$ сравнение (11) не выполняется.)

Доказательство. Распространим сравнения по модулю степеней p на рациональные числа, знаменатели которых не делятся на p, считая, что такое число делится на p^s, если числитель в его несократимой записи делится на p^s. Все основные свойства сравнений между целыми числами при этом останутся в силе.

Имеем:

$$C_{2p-1}^{p-1} = \frac{(2p-1)(2p-2)\cdot\ldots\cdot(p+1)}{p!} = \left(\frac{2p}{1} - 1\right)\left(\frac{2p}{2} - 1\right)\cdot\ldots\cdot\left(\frac{2p}{p-1} - 1\right).$$

Произведя умножение и выделив члены, содержащие p не более, чем во второй степени, получим сравнение

$$C_{2p-1}^{p-1} \equiv 1 - 2p\sum_{i=1}^{p-1}\frac{1}{i} + 4p^2 \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \frac{1}{ij} \pmod{p^3}. \tag{12}$$

Далее,

$$2\sum_{i=1}^{p-1}\frac{1}{i} = \sum_{i=1}^{p-1}\left(\frac{1}{i} + \frac{1}{p-i}\right) = p\sum_{i=1}^{p-1}\frac{1}{i(p-i)}.$$

Подставляя в (12), получаем:

$$C_{2p-1}^{p-1} \equiv 1 - p^2 \sum_{i=1}^{p-1} \frac{1}{i(p-i)} + 4p^2 \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{ij} \pmod{p^3}.$$

Таким образом, нам достаточно доказать, что

$$\sum_{i=1}^{p-1} \frac{1}{i(p-i)} \equiv \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{ij} \equiv 0 \pmod{p}.$$

Перейдя к полю вычетов

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\},$$

мы можем переписать предыдущие сравнения в виде равенств

$$\sum_{i=1}^{p-1} \frac{1}{\bar{\imath}^2} = \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{\bar{\imath}\bar{\jmath}} = 0. \tag{13}$$

Заметим, что $\frac{1}{\bar{1}}, \frac{1}{\bar{2}}, \ldots, \frac{1}{\overline{p-1}}$ — это те же элементы $\bar{1}, \ldots, \overline{p-1}$ поля $\mathbb{Z}_p$, взятые в каком-то другом порядке. Поэтому

$$\sum_{i=1}^{p-1} \frac{1}{\bar{\imath}^2} = \sum_{i=1}^{p-1} \bar{\imath}^2, \quad \sum_{\substack{i,j=1\\ i<j}}^{p-1} \frac{1}{\bar{\imath}\bar{\jmath}} = \sum_{\substack{i,j=1\\ i<j}}^{p-1} \bar{\imath}\bar{\jmath}.$$

Известно, что все ненулевые элементы поля $\mathbb{Z}_p$ — это корни многочлена $x^{p-1} - 1$ (малая теорема Ферма). При $p > 3$ по формулам Виета получаем:

$$\sum_{i=1}^{p-1} \bar{\imath} = 0, \quad \sum_{\substack{i,j=1\\ i<j}}^{p-1} \bar{\imath}\bar{\jmath} = 0,$$

$$\sum_{i=1}^{p-1} \bar{\imath}^2 = \left(\sum_{i=1}^{p-1} \bar{\imath}\right)^2 - 2 \sum_{\substack{i,j=1\\ i<j}}^{p-1} \bar{\imath}\bar{\jmath} = 0.$$

Тем самым равенства (13), а с ними и теорема Волстенхолма доказаны. □

Примеры. При $p = 5$ имеем

$$C_9^4 = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126 \equiv 1 \pmod{5^3},$$

а при $p = 7$ —

$$C_{13}^6 = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 1716 \equiv 1 \pmod{7^3}.$$

Отметим, что по ходу доказательства теоремы мы установили, что (при $p \geqslant 5$)

$$\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^2},$$
$$\frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p}.$$

Пример. При $p = 5$ имеем

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12} \equiv 0 \pmod{5^2},$$
$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} = \frac{205}{144} \equiv 0 \pmod{5}.$$

Возникает естественный вопрос: существуют ли простые числа p, для которых сравнение (11) выполняется по модулю p^4?

Задача 4. *Докажите эквивалентность следующих сравнений:*

$$1)\quad C_{2p-1}^{p-1} \equiv 1 \pmod{p^4};$$
$$2)\quad \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^3};$$
$$3)\quad \frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p^2}.$$

Простые числа p, для которых выполняются эти сравнения, называются *числами Волстенхолма*. Путем вычислений на компьютерах установлено, что в пределах первого миллиарда имеется ровно два таких числа: 16843 и 2124679. Существуют ли другие числа Волстенхолма, неизвестно.

Сравнение (9) может быть, однако, улучшено, если известно, что n, k, $l = n - k$ или C_n^k делятся на p.

Теорема 4 (Якобсталь (Jacobsthal), 1945). *При* $p \geqslant 5$

$$C_{np}^{kp} : C_n^k \equiv 1 \pmod{p^{3+\operatorname{ord}_p n+\operatorname{ord}_p k+\operatorname{ord}_p l}}$$

или, что то же,

$$C_{np}^{kp} \equiv C_n^k \pmod{p^{3+\operatorname{ord}_p n+\operatorname{ord}_p k+\operatorname{ord}_p l+\operatorname{ord}_p C_n^k}}.$$

Например, при $p \geqslant 5$

$$C_{p^3}^{p^2} \equiv C_{p^2}^{p} \pmod{p^8} \tag{14}$$

(учитывая, что $\operatorname{ord}_p C_{p^2}^p = 1$).

Заметим, что проверить сравнение (14) непосредственным вычислением без помощи компьютера весьма затруднительно даже при $p = 5$.

Задача 5. *Докажите сравнение* (14) *самостоятельно, не опираясь на теорему Якобсталя.*

Список литературы

[1] Granville, A. *Arithmetic properties of binomial coefficients.* I: *Binomial coefficients modulo prime powers* // Canad. Math. Soc. Conference Proc., 1997. Vol. 20. P. 253–275.

[2] Стенли Р. *Перечислительная комбинаторика*. М.: Мир, 1990. (Упражнение 6 к гл. 1, с. 72–73.)

[3] Fuchs D., Tabachnikov S. *Mathematical Omnibus. Thirty lectures on classic mathematics*, 2006. Lecture 2, pp. 24–40.
`http://www.math.psu.edu/tabachni/Books/taba.pdf`

Э. Б. Винберг, механико-математический факультет МГУ