ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.17+519.114 DOI 10.22405/2226-8383-2018-19-3-257-269

Об алгебре и арифметике биномиальных и гауссовых коэффициентов

Пачев Урусби Мухамедович — доктор физико-математических наук, доцент, профессор кафедры геометрии и высшей алгебры, Кабардино-Балкарский государственный университет имени Х. М. Бербекова.
e-mail: urusbi@rambler.ru

Аннотация

В работе рассматриваются вопросы, касающиеся алгебраических и арифметических свойств таких комбинаторных чисел как биномиальные, полиномиальные и гауссовы коэффициенты.

Для центральных биномиальных коэффициентов $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ установлено новое свойство сравнимости по модулю $p^3 \cdot (2p-1)$, не равному степени простого числа, где p и $(2p-1)$ — простые числа, при этом используется теорема Волстенхолма о том, что при $p \geqslant 5$ эти коэффициенты соответственно сравнимы с числами 2 и 1 по модулю p^3.

В части, относящейся к гауссовым коэффициентам $\binom{n}{k}_q$ исследованы алгебраические и арифметические свойства этих чисел. Пользуясь алгебраической интерпретацией гауссовых коэффициентов, установлено, что число k-мерных подпространств n-мерного векторного пространства над конечным полем из q элементов равно числу $(n-k)$-мерных его подпространств, при этом число q от которого зависит гауссовый коэффициент должно быть степенью простого числа, являющегося характеристикой этого конечного поля.

Получены оценки снизу и сверху для суммы $\sum_{k=0}^{n} \binom{n}{k}_q$ всех гауссовых коэффициентов, достаточно близкие к ее точному значению (формула для точного значения такой суммы пока ещё не установлена), а также асимптотическая формула при $q \to \infty$. В виду отсутствия удобной производящей функции для гауссовых коэффициентов мы пользуемся исходным определением гауссового коэффициента $\binom{n}{k}_q$, при этом считаем, что $q > 1$.

При исследовании арифметических свойств делимости и сравнимости гауссовых коэффициентов используется понятие первообразного корня по данному модулю. Получены условия делимости гауссовых коэффициентов $\binom{p}{k}_q$ и $\binom{p^2}{k}_q$ на простое число p, а также вычислена сумма всех этих коэффициентов по модулю простого числа p.

В заключительной части приводятся некоторые нерешенные задачи теории чисел, связанные с биномиальными и гауссовыми коэффициентами, которые могут представлять интерес для дальнейших исследований.

Ключевые слова: центральные биномиальные коэффициенты, теорема Волстенхолма, гауссовый коэффициент, сумма гауссовых коэффициентов, делимость на простое число, сравнение по данному модулю, первообразный корень по данному модулю.

Библиография: 17 названий.

Для цитирования:
У. М. Пачев. Об алгебре и арифметике биномиальных и гауссовых коэффициентов // Чебышевский сборник, 2018, т. 19, вып. 3, с. 257–269.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.17+519.114 DOI 10.22405/2226-8383-2018-19-3-257-269

On algebra and arithmetic of binomial and gaussian coefficients

Pachev Urusbi Muhamedovich — doctor of physical and mathematical sciences, associate professor, professor of the department of geometry and higher school, Kabardino-Balkarian state university named after H.M. Berbekov.
e-mail: urusbi@rambler.ru

Abstract

In this paper we consider questions relating to algebraic and arithmetic properties of such binomial, polynomial and Gaussian coefficients.

For the central binomial coefficients $\binom{2p}{p}$ and $\binom{2p-1}{p-1}$, a new comparability property modulo $p^3 \cdot (2p-1)$, which is not equal to the degree of a prime number, where p and $(2p-1)$ are prime numbers, Wolstenholm's theorem is used, that for $p \geqslant 5$ these coefficients are respectively comparable with the numbers 2 and 1 modulo p^3.

In the part relating to the Gaussian coefficients $\binom{n}{k}_q$, the algebraic and arithmetic properties of these numbers are investigated. Using the algebraic interpretation of the Gaussian coefficients, it is established that the number of k-dimensional subspaces of an n-dimensional vector space over a finite field of q elements is equal to the number of $(n-k)$ -dimensional subspaces of it, and the number q on which The Gaussian coefficient must be the power of a prime number that is a characteristic of this finite field.

Lower and upper bounds are obtained for the sum $\sum_{k=0}^{n} \binom{n}{k}_q$ of all Gaussian coefficients sufficiently close to its exact value (a formula for the exact value of such a sum has not yet been established), and also the asymptotic formula for $q \to \infty$. In view of the absence of a convenient generating function for Gaussian coefficients, we use the original definition of the Gaussian coefficient $\binom{n}{k}_q$, and assume that $q > 1$.

In the study of the arithmetic properties of divisibility and the comparability of Gaussian coefficients, the notion of an antiderivative root with respect to a given module is used. The conditions for the divisibility of the Gaussian coefficients $\binom{p}{k}_q$ and $\binom{p^2}{k}_q$ by a prime number p are obtained, and the sum of all these coefficients modulo a prime number p.

In the final part, some unsolved problems in number theory are presented, connected with binomial and Gaussian coefficients, which may be of interest for further research.

Keywords: central binomial coefficients, Wolstenholme's theorem, Gaussian coefficient, the sum of Gaussian coefficients, divisibility by prime number, congruences modulo, primitive roots for this module.

Bibliography: 17 titles.

For citation:
U. M. Pachev, 2018, "On algebra and arithmetic of binomial and gaussian coefficients", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 257–269.

1. Введение

В работе рассматриваются некоторые вопросы, относящиеся к таким смежным областям математики как комбинаторика, алгебра и теория чисел. Многие комбинаторные числа представляют собой алгебраические выражения в общем случае дробного вида и нужно установить их целостность, а также делимость на степени простых чисел. Например, для некоторых

вопросов нужно знать наивысший показатель с которым входит данное простое число p в разложение $n!$ на простые множители. Этот показатель, как известно, оказывается равным сумме $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots$, где $[\ ]$ — целая часть числа. Отсюда получается независимое от комбинаторики доказательство целости полиномиального коэффициента $\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}$, где $n_1+n_2+\ldots+n_k=n$ и $n_i\geqslant 0$. При этом конечно нужно подсчитать сколько раз входит простое число p в числитель и знаменатель этого выражения и ещё воспользоваться очевидным свойством: $[\alpha+\beta]\geqslant[\alpha]+[\beta]$.

Многочисленные подобные утверждения о целости различных выражений составленных из факториалов можно найти в книге P. Bachmann [1].

В теории чисел большое внимание уделяется вопросу делимости и сравнимости центральных биномиальных коэффициентов $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$, для простого числа p. Первый результат в этом вопросе был получен Волстенхолмом [2] в 1862 г., установившим, что выполняются сравнения $\binom{2p}{p}\equiv 2 \pmod{p^3}$ или что то же самое $\binom{2p-1}{p-1}\equiv 1 \pmod{p^3}$. С помощью этого результата мы в теореме 1 устанавливаем ещё одно свойство сравнимости центральных биномиальных коэффициентов по модулю не равному степени простого числа.

Ближайшим обобщением биномиальных коэффициентов являются полиномиальные коэффициенты, которые появляются в полиномиальной формуле

$$(x_1+\ldots+x_k)^n=\sum_{x_1+\ldots+x_k=n}\binom{n}{n_1,n_2,\ldots,n_k}x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k},$$

где

$$\binom{n}{n_1,n_2,\ldots,n_k}=\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}$$

есть полиномиальный коэффициент.

Для них по сравнению с биномиальными коэффициентами мало известных результатов, имеющих приложения особенно в теории чисел. В связи с этим мы в теореме 2 переносим результат предложения 1 о делимости биномиальных коэффициентов на простое число на полиномиальные коэффициенты и как следствие получаем ещё одно доказательство малой теоремы Ферма (относительно трёх имеющихся доказательств этой теоремы см. [3]).

Ещё одним из обобщений биномиальных коэффициентов являются гауссовы коэффициенты, называемые ещё q-биномиальными коэффициентами. Они были введены Гауссом в [4] для решения некоторых важных вопросов теории чисел, в частности для определения знака так называемой гауссовой суммы. Мы будем пользоваться современным обозначением гауссовых коэффициентов, а именно гауссовый коэффициент $\binom{n}{k}_q$ определяется равенством

$$\binom{n}{k}_q=\frac{\left(q^n-1\right)\left(q^{n-1}-1\right)\cdot\ldots\cdot\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdot\ldots\cdot(q-1)}$$

При $q=1$ получаем неопределённость вида $\frac{0}{0}$, но если перейти к пределу то

$$\lim_{q\to 1}\binom{n}{k}_q=\binom{n}{k}=\frac{n!}{k!\,(n-k)!}$$

и значит, $\binom{n}{k}_q$ есть обобщение биномиального коэффициента.

Несмотря на то, что гауссовый коэффициент задаётся дробью, тем не менее при каждом значении q, n и k этот коэффициент получается целым числом, иначе говоря, $\binom{n}{k}_q$ есть целочисленный многочлен от q см. [5]. Относительно гауссовых коэффициентов и их применении в алгебре, точнее в теории p-групп, см. [6, 7].

С помощью гауссовых коэффициентов удаётся решить один вопрос о числе k-мерных и $(n-k)$-мерных подпространств n-мерного векторного пространства над конечным полем F_q из

q элементов. Особый интерес представляет вопрос о сумме $\sum_{k=0}^{n} \binom{n}{k}_q$ гауссовых коэффициентов. Для неё не удаётся получить точное значение как в случае биномиальных коэффициентов, ввиду чего мы даём только оценки сверху и снизу и её асимптотику при $q \to \infty$.

Пользуясь понятием первообразного корня по данному модулю p мы доказываем свойство делимости гауссовых коэффициентов $\binom{p}{k}_q$ на простое число p, а также вычисляем сумму всех гауссовых коэффициентов по модулю простого числа p.

2. Арифметические свойства биномиальных и полиномиальных коэффициентов

Биномиальные коэффициенты являются самыми известными среди всех комбинаторных чисел. Сначала они определяются как число k-элементных подмножеств n-элементного множества, называемое числом сочетаний без повторений из n элементов по k элементов. Оно обозначается через C_n^k и равно $\frac{n!}{k!(n-k)!}$, где $0 \leqslant k \leqslant n$.

Эти же числа появляются в биномиальной формуле для $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$, где $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ есть биномиальный коэффициент из n по k.

Биномиальные коэффициенты могут быть изучены с различных точек зрения, например, с выявлением интересных алгебраических и арифметических свойства этих чисел.

Мы не будем рассматривать широко известные алгебраические тождества с биномиальными коэффициентами. Гораздо больший интерес представляют исследования арифметических свойств делимости биномиальных коэффициентов.

Самый простейший факт, связанный с делимостью биномиальных коэффициентов на простое число, содержится в следующем утверждении.

Предложение 1. *Если p — простое число и $1 \leqslant k \leqslant p-1$, то биномиальный коэффициент $\binom{p}{k}$ делится на p.*

Доказательство см. [8], где даются два доказательства.

Особый интерес представляют свойства сравнимости для центральных биномиальных коэффициентов вида $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ по модулю степеней числа p. Относительно них известен следующий результат.

Теорема (Волстенхолм). *Пусть простое число $p \geqslant 5$. Тогда $\binom{2p}{p} \equiv 2 \pmod{p^3}$ или, что то же самое, $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$.*

Доказательство было дано Волстенхолмом [2] в 1862 г.

Доказательство также приводится в [3], опираясь на понятие сравнения по любому модулю степеней простого числа p для рациональных чисел, при этом используются также свойства поля классов вычетов $\mathbb{Z}_p$.

Заметим, что без указанных этих дополнительных средств легко доказывается более слабый результат о том, что $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

Действительно, воспользуемся известным соотношением для биномиальных коэффициентов $\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \ldots + \binom{p}{p}^2$.

Учитывая, что $\binom{p}{0} = \binom{p}{p} = 1$ в силу предложения 1 получим $\binom{2p}{p} = 2 + p^2 k$ при некотором целом k, оттуда $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

Согласно теореме Волстенхолма центральные биномиальные коэффициенты $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ при простом p содержатся в классах вычетов $2 \pmod{p^3}$ и $1 \pmod{p^3}$ соответственно, а в силу предложения 1 $\binom{p}{k}$ при $1 \leqslant k \leqslant p-1$ лежит в классе $0 \pmod{p}$. Возникает вопрос в каких классах вычетов будут содержатся $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ по модулю $p^3\,(2p-1)$, если $2p-1$ также есть простое число. Ответ даёт следующая

Теорема 1. *Если p и $2p-1$ являются простыми числами, то для центральных биномиальных коэффициентов выполняются следующие условия сравнения*

1) $\binom{2p}{p} \equiv 2\left(1-8p^3\right) \pmod{p^3\cdot(2p-1)}$;

2) $\binom{2p-1}{p-1} \equiv 1-8p^3 \pmod{p^3\cdot(2p-1)}$.

Доказательство.

1) Пусть p и $2p-1$ простые числа. В силу теоремы Волстенхолма имеем сравнение $\binom{2p}{p} \equiv 2 \pmod{p^3}$ и ещё выполняется сравнение $\binom{2p}{p} \equiv 0 \pmod{2p-1}$. Поэтому рассматриваем систему сравнений

$$\begin{cases} x \equiv 2 \pmod{p^3}, \\ x \equiv 0 \pmod{2p-1}, \end{cases}$$

единственным решением которой по модулю $p^3\cdot(2p-1)$ в силу китайской теоремы об остатках является класс вычетов, содержащий число $\binom{2p}{p}$. Следуя доказательству китайской теоремы об остатках в случае двух сравнений по модулям $m_1 = p^3$ и $m_2 = 2p-1$ имеем $x \equiv c_1M_1M_1' + c_2M_2M_2' \pmod{p^3\cdot(2p-1)}$, где в нашем случае $c_1 = 2$, $c_2 = 0$ — правые части этой системы, при этом $M_1 = m_2 = 2p-1$, $M_2 = m_1 = p^3$. Находим обратные для M_1 и M_2 соответственно по модулям p^3 и $2p-1$. Имеем $M_1M_1' \equiv 1 \pmod{m_1}$, т. е. $(2p-1)\,M_1' \equiv 1 \pmod{p^3}$. Решая это сравнение по способу Эйлера получаем $M_1' \equiv (2p-1)^{\varphi\left(p^3\right)-1} \pmod{p^3}$, т. е. $M_1' \equiv (2p-1)^{p^3-p^2-1} \pmod{p^3}$. Применяя биномиальную формулу имеем $M_1' \equiv \sum\limits_{k=0}^{p^3-p^2-1} \binom{p^3-p^2-1}{k}(2p)^k(-1)^{p^3-p^2-1-k} \pmod{p^3}$ и, оставляя в правой части слагаемые при $0 \leqslant k \leqslant 2$, получаем $M_1' \equiv -1+\left(p^3-p^2-1\right)2p-\binom{p^3-p^2-1}{2}4p^2 \pmod{p^3}$, откуда $M_1' \equiv -1-2p-4p^2 \pmod{p^3}$, т. е. можем взять $M_1' = -4p^2-2p-1$.

Аналогично устанавливается, что $M_2' \equiv 8 \pmod{2p-1}$, т. е. $M_2' = 8$.

Тогда по формуле $x \equiv c_1M_1M_1'+c_2M_2M_2' \pmod{p^3\cdot(2p-1)}$, получаем, что $x \equiv 2\left(1-8p^3\right) \pmod{p^3\cdot(2p-1)}$, и значит, $\binom{2p}{p} \equiv 2\left(1-8p^3\right) \pmod{p^3\cdot(2p-1)}$.

2) Так как $\binom{2p-1}{p-1} = \frac{(p+1)\cdot(p+2)\cdot\ldots\cdot(2p-1)}{(p-1)!}$ и при этом по условию $2p-1$ — простое число, то $\binom{2p-1}{p-1} \equiv 0 \pmod{2p-1}$. Тогда как и в предыдущем случае рассматриваем систему сравнений

$$\begin{cases} x \equiv 1 \pmod{p^3}, \\ x \equiv 0 \pmod{2p-1}, \end{cases}$$

единственным решением которой по модулю $p^3\,(2p-1)$ является класс вычетов, содержащий число $\binom{2p-1}{p-1}$. Следуя предыдущим рассуждениям, получаем, что $\binom{2p-1}{p-1} \equiv 1-8p^2 \pmod{p^3\cdot(2p-1)}$.

Теорема 1 доказана. □

Относительно других результатов, связанных с теоремой Волстенхолма, см. [9], а что касается вопросов разложимости центральных биномиальных коэффициентов в произведение таких же коэффициентов см. [10, 11].

Перейдём теперь к рассмотрению полиномиальных (мультиномиальных) коэффициентов, при этом мы не будем затрагивать их комбинаторные интерпретации.

Полиномиальные коэффициенты появляются в полиномиальной формуле

$$(x_1+x_2+\ldots+x_k)^n = \sum_{\substack{n_1+n_2+\ldots+n_k=n \\ n_1\geqslant 0,\, n_2\geqslant 0,\,\ldots,\, n_k\geqslant 0}} \binom{n}{n_1, n_2, \ldots, n_k} x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k},$$

где

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$$

— есть полиномиальный коэффициент из n по $n_1, n_2, \ldots, n_k$. В частном случае $k = 2$ получаем биномиальные коэффициенты $\binom{n}{n_1,n_2} = \binom{n}{n_1} = \binom{n}{n_2}$.

На полиномиальные коэффициенты мы переносим результат предложения 1 о делимости на простое число p.

Теорема 2. *Если p — простое число и $n_i \neq p$ при всех $i = 1, 2, \ldots, k$, то справедлива делимость $p \mid \binom{n}{n_1,n_2,\ldots,n_k}$.*

Доказательство. По определению полиномиального коэффициента имеем

$$n_1 + n_2 + \ldots + n_k = p, \quad n_1 \geqslant 0, n_2 \geqslant 0, \ldots, n_k \geqslant 0,$$

и значит, в силу условия $n_i \neq 0$ получаем, что $0 \leqslant n_i < p$. Тогда $p \nmid n_i!$ и значит, $p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!$.

Но так как $\frac{p!}{p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!} = p \frac{(p-1)!}{p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$ и учитывая, что $\binom{n}{n_1,n_2,\ldots,n_k}$ есть целое число получаем $\frac{(p-1)!}{p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$ также есть целое число и, при этом, p не сокращается с $n_1! \cdot n_2! \cdot \ldots \cdot n_k!$. Следовательно, $p \mid \binom{n}{n_1,n_2,\ldots,n_k}$, ч. т. д. $\square$

Опираясь на теорему 2 в сочетании с тождеством

$$\sum_{\substack{n_1+n_2+\ldots+n_k=n \\ n_1 \geqslant 0,\, n_2 \geqslant 0,\, \ldots,\, n_k \geqslant 0}} \binom{n}{n_1, n_2, \ldots, n_k} = k^n$$

получаем малую теорему Ферма о том, что $p \mid k^p - k$ (относительно трёх других её доказательств см. [3]).

3. Алгебраические свойства гауссовых коэффициентов

Гауссовы коэффициенты впервые появились в работе Гаусса [4] по теории деления круга при вычислении значений периодов длины $\frac{n-1}{2}$, где n — простое число, т. е. когда совокупность корней уравнения деления круга $x^{n-1} + x^{n-2} + \ldots + 1 = 0$ распадается на два периода, являющиеся корнями некоторого квадратного уравнения с некоторыми коэффициентами из кругового поля корней n-ой степени из 1.

Рассматриваемый вопрос был применён Гауссом к определению знака так называемой гауссовой квадратичной суммы

$$G = \sum_r e^{\frac{2\pi i}{n} r},$$

где суммирование проводится по всем квадратичным вычетам r по простому модулю n, лежащим в границах от 1 до $\frac{n-1}{2}$.

Установление знака гауссовой суммы G проводится Гауссом при помощи исследования двух особых рядов:

$$f(x, m) = \sum_{\mu=1}^{\infty} (-1)^{\mu} (m, \mu) \text{ и } F(x, m) = \sum_{\mu=1}^{\infty} x^{\frac{\mu}{2}} (m, \mu),$$

где

$$(m, \mu) = \frac{(1 - x^m)\left(1 - x^{m-1}\right) \cdot \ldots \cdot \left(1 - x^{m-\mu+1}\right)}{(1 - x)\left(1 - x^2\right) \cdot \ldots \cdot \left(1 - x^{\mu}\right)}, \tag{1}$$

при этом (m, μ) в дальнейших исследованиях был назван гауссовым коэффициентом.

Правая часть (1) несмотря на её дробное выражение является многочленом от x с целыми коэффициентами (см. [5]).

Соотношение (1) можно преобразовать следующим образом

$$(m,\mu)=\frac{\left(x^m-1\right)\left(x^{m-1}-1\right)\cdot\ldots\cdot\left(x^{m-\mu+1}-1\right)}{\left(x^\mu-1\right)\left(x^{\mu-1}-1\right)\cdot\ldots\cdot(x-1)}.$$

По аналогии с биномиальными коэффициентами мы будем пользоваться современным обозначением гауссовых коэффициентов

$$\binom{n}{k}_q=\frac{\left(q^n-1\right)\left(q^{n-1}-1\right)\cdot\ldots\cdot\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdot\ldots\cdot(q-1)}. \tag{2}$$

Для гауссового коэффициента (2) при $q=1$ получается неопределённость вида $\frac{0}{0}$ и именно в этом неопределённом случае гауссовый коэффициент будет совпадать с биномиальным коэффициентом, т. е. $\binom{n}{k}_1=\binom{n}{k}=\frac{n!}{k!(n-k)!}$.

Действительно, разделив каждый сомножитель числителя и знаменателя левой части (2) на $q-1$, получаем следующее представление гауссового коэффициента

$$\binom{n}{k}_q=\frac{1+q+q^2+\ldots+q^{n-1}}{1}\cdot\frac{1+q+q^2+\ldots+q^{n-2}}{1+q}\cdot\ldots\cdot\frac{1+q+q^2+\ldots+q^{n-k}}{1+q+q^2+\ldots+q^{k-1}}, \tag{3}$$

откуда при $q=1$ имеем

$$\binom{n}{k}_1=\frac{n(n-1)\cdot\ldots\cdot(n-(k-1))}{1\cdot2\cdot\ldots\cdot k}=\frac{n!}{k!(n-k)!}=\binom{n}{k},$$

т. е. получился биномиальный коэффициент $\binom{n}{k}$. Из (2) и (3) получаем $\binom{n}{0}_q=1$ и $\binom{n}{n}=1$.

Рассмотрим смысл гауссовых коэффициентов в теории векторных пространств над конечным полем F_q из q элементов.

Пусть q есть степень простого числа. Через $V_n(q)$ обозначим n-мерное векторное пространство над полем F_q, при этом $V_n(q)=\{(\alpha_1,\alpha_2,\ldots,\alpha_n)\in F_q^n\mid\alpha_i\in F_q\}$.

Предложение 2. *Число k-мерных подпространств n-мерного пространства $V_n(q)$ равно гауссовому коэффициенту $\binom{n}{k}_q$.*

Доказательство см. [12].

Гауссовы коэффициенты $\binom{n}{k}_q$ мы будем рассматривать как q-аналоги биномиальных коэффициентов и в отношении их свойств.

Предложение 3. *Гауссовы коэффициенты обладают свойством симметрии, т. е.* $\binom{n}{k}_q=\binom{n}{n-k}_q$.

Доказательство непосредственно следует из определения.

Из предложений 2 и 3 выводится свойство подпространств конечномерного векторного пространства над конечным полем.

Теорема 3. *Число k-мерных подпространств n-мерного векторного пространства над конечным полем из q элементов рано числу $(n-k)$-мерных его подпространств.*

Доказательство. В силу предложения 2 имеем, что число $G_q(n,k)$ k-мерных подпространств n-мерного векторного пространства $V_n(q)$ над полем F_q из q элементов равно гауссовому коэффициенту $\binom{n}{k}_q$, т. е. $G_q(n,k)=\binom{n}{k}_q$. Но так как по предложению 3 справедливо равенство $\binom{n}{k}_q=\binom{n}{n-k}_q$, то $G_q(n,k)=G_q(n,n-k)$, ч. т. д. □

Как и биномиальные коэффициенты гауссовы коэффициенты обладают свойством унимодальности, т. е. имеет место следующее.

Предложение 4. *Пусть $n\in\mathbb{N}$. Последовательность $\left\{\binom{n}{k}_q\mid k=0,\ldots,n\right\}$ гауссовых коэффициентов удовлетворяет свойствам:*

а) $\binom{n}{0}_q < \binom{n}{1}_q < \ldots < \binom{n}{\frac{n}{2}}_q > \binom{n}{\frac{n}{2}+1}_q > \ldots > \binom{n}{n}_q$ *при чётном* n*;*

б) $\binom{n}{0}_q < \binom{n}{1}_q < \ldots < \binom{n}{\frac{n-1}{2}}_q = \binom{n}{\frac{n-1}{2}}_q > \ldots > \binom{n}{n}_q$ *при нечётном* n*.*

Доказательство проводится аналогично случаю биномиальных коэффициентов изложенному в [14].

Рассмотрим ещё вопрос о сумме $\sum\limits_{k=0}^{n}\binom{n}{k}_q$ всех гауссовых коэффициентов. Для суммы всех биномиальных, так и полиномиальных коэффициентов имеются точные значения.

Насколько нам известно, в математической литературе нигде не встречается решение этого вопроса в случае гауссовых коэффициентов.

Для биномиальных коэффициентов имеется производящая функция равная $(1+x)^n$, т. е. $(1+x)^n = \sum\limits_{k=0}^{n}\binom{n}{k}x^k$. Приведём имеющийся q-аналог для этого равенства.

Предложение 5. (q-бином Ньютона). *При любом натуральном* q *справедливо равенство* $\prod\limits_{k=1}^{n}\left(1+xq^k\right) = \sum\limits_{k=0}^{n}\binom{n}{k}_q q^{\frac{k(k+1)}{2}}x^k$*, где* $\binom{n}{k}_q$ *— гауссовый коэффициент.*

Доказательство см. [13]. Довольно простой вывод этого равенства имеется в [6].

Приведённое равенство представляет собой обобщение биномиальной формулы так как при подстановке $q=1$ оно переходит в обычный бином Ньютона вида $(1+x)^n$.

Из предложения 5 следует, что произведение $(1+xq)\left(1+xq^2\right)\cdot\ldots\cdot(1+xq^n)$ является производящей функцией для $\binom{n}{k}_q q^{\frac{k(k+1)}{2}}$.

Пользуясь предложением 5 можно получить следующее неравенство $\sum\limits_{k=0}^{n}\binom{n}{k}_q \leqslant 2^n q^{\frac{n(n+1)}{2}}$.

Для получения более точной оценки сверху мы воспользуемся исходным определением гауссового коэффициента.

Теорема 4. *Для суммы всех гауссовых коэффициентов при* $q>1$ *справедливы неравенства*

$$\frac{1}{2^{\frac{n}{2}}}q^{\frac{n^2}{4}-\frac{1}{4}} < \sum_{k=0}^{n}\binom{n}{k}_q \leqslant 2^n q^{\frac{n^2}{4}}.$$

Доказательство. Сначала доказываем верхнюю оценку. Имеем $\sum_{k=0}^{n}\binom{n}{k}_q = 2+\sum_{k=1}^{n-1}\binom{n}{k}_q$. Получим оценку сверху для каждого гауссового коэффициента.

Из $\binom{n}{k}_q = \frac{(q^n-1)\left(q^{n-1}-1\right)\cdot\ldots\cdot\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdot\ldots\cdot(q-1)}$ получаем $\binom{n}{k}_q < \frac{q^n\cdot q^{n-1}\cdot\ldots\cdot q^{n-k+1}}{\frac{1}{2}q^k\cdot\frac{1}{2}q^{k-1}\cdot\ldots\cdot\frac{1}{2}q} = 2^k\cdot q^{nk-k^2} < 2^k\cdot q^{\frac{n^2}{4}}$, при этом учитывается, что $nk-k^2 \leqslant \frac{n^2}{4}$ при $0\leqslant k\leqslant n$.

Тогда, включая и случай $q=1$, будем иметь $\sum_{k=0}^{n}\binom{n}{k}_q \leqslant (2^n-2)\,q^{\frac{n^2}{4}} \leqslant 2^n q^{\frac{n^2}{4}}$, тем самым верхняя оценка доказана.

Теперь перейдём к нижней оценке. Имеем $\sum_{k=0}^{n}\binom{n}{k}_q > \max\limits_{0\leqslant k\leqslant n}\binom{n}{k}_q$.

В силу предложения 4 имеем

$$\max_{0\leqslant k\leqslant n}\binom{n}{k}_q = \begin{cases}\binom{n}{\frac{n}{2}}_q & \text{если } n\text{ — чётно,}\\ \binom{n}{\frac{n-1}{2}}_q & \text{если } n\text{ — нечётно,}\end{cases}$$

Соответственно этому рассмотрим два случая:

а) $\binom{a}{\frac{n}{2}}_q > \frac{\frac{1}{2}q^n\cdot\frac{1}{2}q^{n-1}\cdot\ldots\cdot\frac{1}{2}q^{n-\frac{n}{2}+1}}{q^{\frac{n}{2}}\cdot q^{\frac{n}{2}-1}\cdot\ldots\cdot q} = \frac{1}{2^{\frac{n}{2}}}q^{\frac{n}{2}\cdot\frac{n}{2}} = \frac{1}{2^{\frac{n}{2}}}q^{\frac{n^2}{4}}$

б) $\left(\frac{a}{\frac{n-1}{2}}\right)_q > \frac{\frac{1}{2}q^n\cdot\frac{1}{2}q^{n-1}\cdot\ldots\cdot\frac{1}{2}q^{n-\left(\frac{n-1}{2}-1\right)}}{q^{\frac{n-1}{2}}\cdot q^{\frac{n-1}{2}-1}\cdot\ldots\cdot q} = \frac{1}{2^{\frac{n-1}{2}}}q^{n-\frac{n-1}{2}\cdot\frac{n-1}{2}} = \frac{1}{2^{\frac{n-1}{2}}}q^{\frac{n^2}{4}-\frac{1}{4}}$

Объединяя теперь случаи а) и б), получаем $\sum_{k=0}^{n}\binom{n}{k}_q > \frac{1}{2^{\frac{n-1}{2}}}q^{\frac{n^2}{4}-\frac{1}{4}}$. Теорема 4 доказана. □

Несмотря на то, что гауссовы коэффициенты не обладают производящей функцией с удобным алгебраическим описанием, тем не менее, для суммы всех гауссовых коэффициентов удаётся получить асимптотическую формулу при $q\to\infty$ (комбинаторное описание коэффициентов производящей функции для $\binom{n}{k}_q$ даётся в [13]).

Теорема 5. *Для суммы всех гауссовых коэффициентов справедлива асимптотическая формула*

$$\sum_{k=0}^{n}\binom{n}{k}_q \sim \begin{cases} q^{\frac{n^2}{4}} & \text{при чётных } n,\\ 2q^{\frac{n^2}{4}-\frac{1}{4}} & \text{при нечётных } n>1,\end{cases}$$

где $\sim$ — знак асимптотической эквивалентности.

Доказательство.

1) Сначала рассматриваем случай чётного n. Так как $\binom{n}{k}_q$ есть многочлен относительно q, то для степени такого многочлена имеем $\deg\binom{n}{k}_q = nk-k^2$. Но учитывая, что $\sum\limits_{k=0}^{n}\binom{n}{k}_q$ также есть многочлен от q, будем иметь

$$\deg\sum_{k=0}^{n}\binom{n}{k}_q = \max_{0\leqslant k\leqslant n}\left\{\deg\binom{n}{k}_q\right\} = \max_{0\leqslant k\leqslant n}\left\{nk-k^2\right\} = \frac{n^2}{4}.$$

Тогда многочлен $\sum\limits_{k=0}^{n}\binom{n}{k}_q$ можно представить в следующем виде

$$\sum_{k=0}^{n}\binom{n}{k}_q = q^{\frac{n^2}{4}} + a_1q^{\frac{n^2}{4}-1} + \ldots + a_s,$$

где $a_1, a_2, \ldots, a_s$ — целые числа зависящие только от n; $s=\frac{n^2}{4}$. Запишем эту сумму ещё в следующем виде $\sum\limits_{k=0}^{n}\binom{n}{k}_q = q^{\frac{n^2}{4}}\left(1+\frac{a_1}{q}+\ldots+\frac{a_s}{q^{\frac{n^2}{4}}}\right)$, откуда при $q\to\infty$ получаем, что $\sum\limits_{k=0}^{n}\binom{n}{k}_q \sim q^{\frac{n^2}{4}}$.

2) Пусть теперь n — нечётное число. В этом случае $\deg\sum\limits_{k=0}^{n}\binom{n}{k}_q = \frac{n^2}{4}-\frac{1}{4}$. Учитывая, что в случае нечётного n имеются два равных центральных гауссовых коэффициентов, являющихся наибольшими из всех этих коэффициентов (это следует из предложения 4), получаем $\deg\sum\limits_{k=0}^{n}\binom{n}{k}_q = \frac{n^2}{4}-\frac{1}{4}$ и используя теперь предыдущие рассуждения из первого случая, получаем $\sum\limits_{k=0}^{n}\binom{n}{k}_q \sim 2q^{\frac{n^2}{4}-\frac{1}{4}}$.

Теорема 5 доказана. □

Относительно оценок и асимптотик для разных видов сумм, содержащих биномиальные коэффициенты см. [15].

4. Арифметические свойства гауссовых коэффициентов

Распространим на гауссовы коэффициенты арифметические свойства делимости и сравнимости. Рассмотрение таких свойств для гауссовых коэффициентов опирается на понятие первообразного корня по простому модулю p, при этом целое число g называется первообразным корнем по простому модулю p, если $g^{p-1} \equiv 1 \pmod p$, но $g^k \not\equiv 1 \pmod p$ при $1 \leqslant k < p-1$. В теории чисел доказывается, что первообразные корни существуют только по модулю m вида $m = 2; 4; p^\alpha; 2p^\alpha$, где p — простое число, α — натуральное число.

Следующий результат о делимости гауссовых коэффициентов даёт q-аналог предложения 1, относящиеся к биномиальным коэффициентам.

Теорема 6. *Если p — простое число и q — первообразный корень по модулю p, то для гауссового коэффициента $\binom{p}{k}_q$ при $2 \leqslant k \leqslant p-2$ справедлива делимость $p \mid \binom{n}{k}_q$.*

Доказательство. Пусть q — первообразный корень по простому модулю p, т. е. $g^{p-1} \equiv 1 \pmod p$, но $g^m \not\equiv 1 \pmod p$ при $m \leqslant p-2$. Значит, $\left(q^k-1\right) \cdot \ldots \cdot (q-1) \not\equiv 0 \pmod p$ при $2 \leqslant k \leqslant p-2$. При этом в числителе гауссового коэффициента $\binom{p}{k}_q$ все сомножители за исключением второго сомножителя не делятся p, а второй сомножитель в силу малой теоремы Ферма делится на p. Значит, учитывая при этом $\binom{p}{1}_q$ и $\binom{p}{p-1}_q$ не делятся на p, получаем, что $p \mid \binom{p}{k}_q$ при $2 \leqslant k \leqslant p-2$, ч. т. д. $\square$

Представляют интерес вопросы, связанные с делимостью гауссовых коэффициентов вида $\binom{p^\alpha}{k}_q$ и $\binom{2p^\alpha}{k}_q$ на возможные степени простого числа p при условии, что q есть первообразный корень по модулю p^α или $2p^\alpha$. Мы рассматриваем этот вопрос в следующем частном случае.

Теорема 7. *Если p — простое число и q — первообразный корень по модулю p^2, то для гауссового коэффициента $\binom{p^2}{k}_q$ справедлива делимость $p \mid \binom{p^2}{k}_q$ при $p+1 \leqslant k \leqslant p^2-p-1$.*

Доказательство. Так как по условию $p+1 \leqslant k \leqslant p^2-p-1$ и q — первообразный корень по модулю q^2, то $p^2 \mid q^{p^2-p}-1$, но $q^k \not\equiv 1 \pmod{p^2}$. Тогда число сомножителей знаменателя $\left(q^k-1\right) \cdot \left(q^{k-1}-1\right) \cdot \ldots \cdot (q-1)$ коэффициента $\binom{p^2}{k}_q$, делящихся точно на p, будет равно целой части $\left[\frac{k}{p-1}\right]$ (это следует из того, что $p^2 \nmid q^{k-l}-1$ при всех $0 \leqslant l < k$). Поэтому получаем следующую точную делимость $p^{\left[\frac{k}{p-1}\right]} \| \left(q^k-1\right) \cdot \left(q^{k-1}-1\right) \cdot \ldots \cdot (q-1)$ на степень простого числа p.

Аналогично, числитель $\left(q^{p^2}-1\right) \cdot \left(q^{p^2-1}-1\right) \cdot \ldots \cdot \left(q^{p^2-k+1}-1\right)$ гауссового коэффициента $\binom{p^2}{k}_q$ также имеет $\left[\frac{k}{p-1}\right]$ сомножителей, делящихся на p. Но так как среди этих сомножителей есть $q^{p^2-p}-1$, который делится на p^2, то имеем делимость

$$p^{\left[\frac{k}{p-1}\right]+1} \mid \left(q^{p^2}-1\right) \cdot \left(q^{p^2-1}-1\right) \cdot \ldots \cdot \left(q^{p^2-k+1}-1\right).$$

Следовательно, $p \mid \binom{p^2}{k}_q$, ч. т. д. $\square$

Следующий результат даёт значение суммы всех гауссовых коэффициентов $\binom{p}{k}_q$ по простому модулю p.

Теорема 8. *Если q — первообразный корень по нечётному простому модулю p, то справедливо сравнение $\sum\limits_{k=0}^{p} \binom{p}{k}_q \equiv 4 \pmod p$.*

Доказательство. По свойствам гауссовых коэффициентов имеем

$$\sum_{k=0}^{p} \binom{p}{k}_q = \binom{p}{0}_q + \binom{p}{p}_q + \binom{p}{1}_q + \binom{p}{p-1}_q + \sum_{k=2}^{p-2} \binom{p}{k}_q = 2 + 2\frac{q^p-1}{q-1} + \sum_{k=2}^{p-2} \binom{p}{k}_q.$$

Отсюда, переходя к сравнению по модулю p, в силу теоремы 5, будем иметь $\sum\limits_{k=0}^{p}\binom{p}{k}_q \equiv 2+2\frac{q^p-1}{q-1} \pmod p$ или, что то же самое, $\sum\limits_{k=0}^{p} \equiv 4+\frac{q^p-q}{q-1} \pmod p$. Так как по условию q — первообразный корень по модулю p, то $p \nmid q-1$. Но по малой теореме Ферма $p \nmid q^p-q$. Следовательно, $\sum\limits_{k=0}^{p}\binom{p}{k}_q \equiv 4 \pmod p$, ч. т. д. $\square$

Замечание. *Результаты теорем 7 и 8 не являются q-аналогами биномиальных коэффициентов в виду того, что в них q выбиралось первообразным корнем по модулям p и p^2 соответственно.*

5. Заключение

В этой части мы приводим некоторые нерешенные задачи теории чисел, связанные с биномиальными гауссовыми коэффициентами, которые могут представлять интерес для дальнейших исследований.

1. Следующая гипотеза о простых делителях биномиальных коэффициентов, представлена Малышевым А. В. в [16].

Гипотеза. *Пусть n, k — целые числа, $0 \leqslant 2k \leqslant n$. Пусть биномиальный коэффициент $\binom{n}{k} = u \cdot v$, где каждый простой множитель числа u меньше чем k, а каждый простой множитель числа v не меньше, чем k.*

Доказаны [17], что $u < v$ за исключением 12 случаев:

$$\begin{gathered}\binom{8}{3}, \quad \binom{9}{4}, \quad \binom{10}{5}, \quad \binom{12}{5}, \quad \binom{21}{7}, \quad \binom{21}{8}, \\ \binom{30}{7}, \quad \binom{33}{13}, \quad \binom{33}{14}, \quad \binom{36}{13}, \quad \binom{36}{17}, \quad \binom{56}{13}.\end{gathered} \tag{$*$}$$

Немного изменим постановку задачи. Пусть $\binom{n}{k} = U \cdot V$, где каждый постой множитель числа U не больше чем k. Доказано, что и здесь $U < V$ за исключением конечного числа пар n и k. Помимо $(*)$ найдено ещё 7 исключений:

$$\binom{9}{3}, \quad \binom{10}{3}, \quad \binom{18}{3}, \quad \binom{28}{5}, \quad \binom{54}{7}, \quad \binom{82}{3}, \quad \binom{162}{3}.$$

Предположено [17], что других исключений нет. Доказать или опровергнуть эту гипотезу.

2. Представляет интерес исследовать сравнение для центральных биномиальных коэффициентов по модулям, содержащим два и более простых делителей.

3. Перенести изложенные результаты на q-мультиномиальные коэффициенты являющиеся q-аналогом полиномиальных коэффициентов (по поводу этого понятия см. [5]).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Bachmann P. Niedere Zahlen theorie. I und II. Teil, Leipzig, 1902 und 1912, 402 p. und 480 p.

2. Wolstenholme J., On certain properties of prime numbers. Quart. J. Pure Appl. Math. 5 (1862), 35–39.

3. Винберг Э. Б., Удивительные свойства биномиальных коэффициентов// Мат. Просвещение. Третья серия. Вып. 12. Изд.-во МЦНМО. 2008.

4. Gauss C. F., Summatio quarumdam serierum singularium, Comment. Soc. Reg. Sci. Gottingensis, 1 (1811): Werke, Vol. 2, P. 11–45

5. Стенли Р. Перечислительная комбинаторика. Изд.-во «Мир», 1990. 440 с.

6. Шокуев В. Н. Гауссовы коэффициенты. 1988. Нальчик: КБГУ. 98 с.

7. Шокуев В. Н. Основы теории перечисления для конечных нильпотентных групп // Записки научных семинаров ПОМИ. 1994. Т. 211. С. 174–183.

8. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. Изд.-во «Мир», 1987. 415 с.

9. Dzhumadil'daev A. S., Yeliussizov D. A. Wolstenholme's theorem ащк црфе binomial coefficients// Сибирские электронные математические известия. Т. 9, 2012, С. 460–463.

10. Erdös P. On some divisibility properties of $\binom{2n}{n}$. Canad. Math. Bull. 1964, Vol. 7, No 4, P. 513–518.

11. Moser R. Insolvability of $\binom{2n}{n} = \binom{2n}{a} \cdot \binom{2b}{b}$. Canad. Math. Bull. 6 (1963). Pp. 167–169.

12. Айгнер М. Комбинаторная теория. М.: «Мир», 1982. 556 с.

13. Polia G., Aalexanderson G. L. Gaussian binomial coefficients// Elemente der Mathematik, Vol. 26, N 5, 1971. pp. 102–109.

14. Липский В., Комбинаторика для программистов. М.: «Мир», 1988. 213 с.

15. Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986, 384 с.

16. Берник В. И., Ковалевская Э. И. Нерешённые задачи теории чисел. Минск. 1990. Препринт №35 (335)/ АН БССР. Ин.-т математики.

17. Ecklund (Jr) E. F., Eggleton R. B., Erdös P., Selfridge J. Z. On the prime factorisation of binomial coefficients// Austral. Math. Soc., Ser. A. 1978. Vol. 26. P. 257–269.

REFERENCES

1. Bachmann P. Niedere Zahlen theorie. I und II. Teil, Leipzig, 1902 und 1912, 402 p. und 480 p.

2. Wolstenholme J., On certain properties of prime numbers. Quart. J. Pure Appl. Math. 5 (1862), 35–39.

3. Vinberg, E. B. 2008, Udivitelnie svoistva binomialnih koeffitsientov [Amazing problems of binomial coefficients]. M. 62 pp. (Russian).

4. Gauss C. F., Summatio quarumdam serierum singularium, Comment. Soc. Reg. Sci. Gottingensis, 1 (1811): Werke, Vol. 2, P. 11–45

5. Stanley, R. Enumerative combinatorics. by Wadsworth, inc. California. Vol. 1, 1986.

6. Shokuev, V. N. 1988, "Gauusovi koeffitsienti" [Gaussian coefficients]. Nalchik. 98 p. (Russian).

7. Shokuev, V. N. 1994, "Osnovi teorii perechisleniya dlya konechnikh nilpotentnikh grupp" [Foundations of enumeration theory for finite nilpotent groups]. Zap. Nauchn. Sem. POMI. Vol. 211, pp. 174–183. (Russian).

8. Ireland, K. and Rosen, M. 1982, “Klassichesloe vvedenie v sovremennuyu teotiyu chisel” [A Classical Introduction to Modern Number Theory]. Springer. 385 p.

9. Dzhumadil'daev A. S., Yeliussizov D. A. Wolstenholme's theorem ащк црфе binomial coefficients// Сибирские электронные математические известия. Т. 9, 2012, С. 460–463.

10. Polia G., Aalexanderson G. L. Gaussian binomial coefficients// Elemente der Mathematik, Vol. 26, N 5, 1971. pp. 102–109.

11. Erdös P. On some divisibility properties of $\binom{2n}{n}$. Canad. Math. Bull. 1964, Vol. 7, No 4, P. 513–518.

12. Moser R. Insolvability of $\binom{2n}{n} = \binom{2n}{a} \cdot \binom{2b}{b}$. Canad. Math. Bull. 6 (1963). Pp. 167–169.

13. Ainger, M. Combinatorial theory. Springer–Verlang. Berlin Heidelberg New York, 1979,

14. Lipski, W. 1988, “Kombinatorika dlya progamistov” [Combinatorics for programmers]. M. Mir, 213 pp. (Russian)

15. Yablonsky S. V. 1986, “Vvedenie v diskretnuyu matematiku” M.: Nauka, 384 p. [Introduction to discrete mathematics]. (Russian)

16. Bernik, V. I., Kovalevsky, E. J. 1990, “Nereshennie zadachi v teorii chisel” [Unsolved problems in number theory]. Preprint N35 (435), Minsk. 1990. 39 p. (Russian)

17. Ecklund (Jr) E. F., Eggleton R. B., Erdös P., Selfridge J. Z. On the prime factorisation of binomial coefficients// Austral. Math. Soc., Ser. A. 1978. Vol. 26. P. 257–269.

Получено 30.07.2018
Принято к печати 15.10.2018