ВЕСТНИК ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2023 Математика и механика № 84
Tomsk State University Journal of Mathematics and Mechanics

Научная статья
УДК 511.17 + 519.682 MSC: 11B65, 11A07
doi: 10.17223/19988621/84/2

Последовательности биномиальных коэффициентов по простому модулю

Валентин Михайлович Зюзьков

Томский государственный университет, Томский государственный университет систем управления и радиоэлектроники, Томск, Россия, vmz@math.tsu.ru

Аннотация. Рассматривается поведение бесконечных последовательностей биномиальных коэффициентов $\binom{x}{y} \bmod p$, $x = 0, 1, 2, \ldots$ по простому модулю p. В поисках закономерностей предварительно проводятся математические эксперименты с помощью Wolfram Mathematica. Доказывается периодичность данных последовательностей и определяется длина периода как p в степени $\lfloor \log_p(y) \rfloor + 1$.

Ключевые слова: экспериментальная математика, последовательности биномиальных коэффициентов, периоды, сравнения, система Mathematica

Для цитирования: Зюзьков В.М. Последовательности биномиальных коэффициентов по простому модулю // Вестник Томского государственного университета. Математика и механика. 2023. № 84. С. 14–22. doi: 10.17223/19988621/84/2

Original article

Sequences of binomial coefficients modulo prime

Valentin M. Zyuz′kov

Tomsk State University, Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russian Federation, vmz@math.tsu.ru

Abstract. The behavior of infinite sequences of binomial coefficients $\binom{x}{y} \bmod p$, $x = 0, 1, 2, \ldots$; p is a prime number) is considered. In the search of regularities, preliminary mathematical experiments are carried out using Wolfram Mathematica. The periodicity of these sequences is proved and the length of the period is determined as p to the power of $\lfloor \log_p(y) \rfloor + 1$.

Keywords: experimental mathematics, sequences of binomial coefficients, periods, congruences, Mathematica system

© В.М. Зюзьков, 2023

For citation: Zyuz'kov, V.M. (2023) Sequences of binomial coefficients modulo prime. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics*. 84. pp. 14–22. doi: 10.17223/19988621/84/2

Экспериментальная математика – это тип математического исследования, в котором вычисления используются для изучения математических структур и определения их основных свойств и закономерностей. Как и экспериментальная наука, экспериментальная математика может использоваться для составления математических предсказаний, которые затем подтверждаются или опровергаются на основе дополнительных вычислительных экспериментов. Такие исследования должны завершаться доказательством. Разработка широкого спектра математических программных продуктов, таких как Mathematica [1] с языком программирования Wolfram, позволила математикам с разным опытом и интересами использовать компьютер в качестве важного инструмента в своей повседневной работе. Современное состояние экспериментальной математики описано в [2]. Примеры экспериментов в теории чисел, подтверждений и опровержений приведены в [3]. Современной экспериментальной математике свойственно изложение результатов, следуя Эйлеру, который в своих работах показывал все подробности: каким образом он приходил к формулировкам теорем, на каких предположениях основывался [3. Гл. VI; 4].

В тексте статьи присутствуют написанные на языке Wolfram фрагменты программ, каждый из которых отмечается слева вертикальной чертой. Входные выражения, которые Mathematica вычисляет, выделяются полужирным шрифтом и являются (1) определениями новых функций или (2) вызовами встроенных функций (либо ранее определенных функций) с аргументами. Во втором случае выходное выражение – значение вычисленного выражения – помещается сразу после входа без выделения жирности. Имена функций языка Wolfram, введенные пользователем, пишутся с маленькой буквы курсивом как в программных фрагментах, так и в остальном тексте. Имена встроенных функций языка Wolfram в соответствии с синтаксисом пишутся с большой буквы прямым шрифтом.

Начинаем исследование с рассмотрения бесконечных последовательностей $\binom{n}{p^t} \bmod p$ остатков биномиальных коэффициентов при делении на простое p, $n = 0, 1, 2, 3, \ldots$, с неотрицательным целым t. В данном контексте обозначение mod используется для арифметической операции нахождения остатка при целочисленном делении. Элементы последовательности на языке Wolfram можно определить функцией

```
h[p_, t_, n_]: = Mod[Binomial[n, p^t], p]
```

с фиксированными натуральными параметрами $t \geq 0$ и p.

Изучим поведение при некоторых небольших p и t. Диапазон изменения n задается с помощью встроенной функции Range:

```
h[2, 1, #] & /@ Range[0, 15]
{0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1}
```

```
h[2, 2, #] & /@ Range[0, 15]
{0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1}
```

```
h[2, 3, #] & /@ Range[0, 31]
{0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1}
```

```
h[3, 0, #] & /@ Range[0, 15]
{0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, 0}
```

```
h[3, 1, #] & /@ Range[0, 15]
{0, 0, 0, 1, 1, 1, 2, 2, 2, 0, 0, 0, 1, 1, 1, 2}
```

```
h[3, 2, #] & /@ Range[0, 27]
{0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0}
```

```
h[5, 2, #] & /@ Range[0, 50]
{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2}
```

Чтобы высказать правдоподобную догадку о периодичности элементов в последовательностях, потребовалось изучить значительно больше примеров значений t и p и также рассмотреть более длинные диапазоны значений n.

Выскажем следующее предположение о поведении рассмотренных последовательностей.

Гипотеза 1. Последовательность $\binom{n}{p^t}$, $n = 0, 1, 2, 3, \ldots$, является периодической с длиной периода равной p^{t+1}.

После точной формулировки гипотезы можно проверять уже ее справедливость программным путем без просмотра результатов вычислений. Для этого определим на языке Wolfram две булевы функции. В первой функции *test*1[*p*, *t*, *ns*] с фиксированными значениями p и t проверяем истинность гипотезы для диапазона значений *ns* параметра n:

```
test1[p_, t_, ns_] :=
And @@ (Mod[h[p, t, #], p] = = Mod[h[p, t, # + p^(t + 1)], p] & /@ ns)
```

Следующее вычисление показывает, что $\binom{n}{7^5} \bmod 7 = \binom{n+7^6}{7^5} \bmod 7$ для n от 0 до 1 000. Длина периода равна $7^6 = 117\,649$.

```
test1[7, 5, Range[0, 1000]]
True
```

Следующее вычисление показывает, что $\binom{n}{17^4} \bmod 17 = \binom{n+17^5}{17^4} \bmod 17$ для n от 0 до 1 000. Длина периода равна $17^5 = 1\,419\,857$.

```
test1[17, 4, Range[0, 1000]]
True
```

Вторая функция *test*2[*ps*, *t*, *ns*] при фиксированном *t* проверяет истинность гипотезы для диапазонов значений *ns* и *ps*:

```
test2[ps_, t_, ns_] := And @@ (test1[#, t, ns] & /@ ps)
```

Следующее вычисление показывает, что $\binom{n}{p^4} \bmod p = \binom{n+p^5}{p^4} \bmod p$ для всех *n* от 0 до 100 и для всех первых десяти простых чисел. Выражение Prime[Range[10]] задает список первых 10 простых чисел:

```
test2[Prime[Range[10]], 4, Range[0, 100]]
True
```

Приступим к доказательству гипотезы 1.

Лемма 1. Если *p* – простое число, то

$$\binom{x}{y} \equiv \binom{\lfloor x/p \rfloor}{\lfloor y/p \rfloor}\binom{x \bmod p}{y \bmod p} \pmod p$$

при любых целых неотрицательных *x* и *y*.

Формулировку утверждения см.: [5. С. 278], доказательство приведено в работе [5. С. 586].

Лемма 2. Пусть натуральные числа $t > 0$, $s \geq 0$ и *p* – простое число. Тогда

$$\binom{\lfloor n/p^s \rfloor}{p^t} \equiv \binom{\lfloor n/p^{s+1} \rfloor}{p^{t-1}} \pmod p$$

Доказательство. Применяя лемму 1, имеем

$$\binom{\lfloor n/p^s \rfloor}{p^t} \equiv \binom{\lfloor \lfloor n/p^s \rfloor / p \rfloor}{\lfloor p^t/p \rfloor}\binom{\lfloor n/p^s \rfloor \bmod p}{p^t \bmod p} \equiv \binom{\lfloor n/p^{s+1} \rfloor}{p^{t-1}}\binom{\lfloor n/p^s \rfloor \bmod p}{0} \equiv$$

$$\equiv \binom{\lfloor n/p^{s+1} \rfloor}{p^{t-1}} \times 1 \equiv \binom{\lfloor n/p^{s+1} \rfloor}{p^{t-1}} \pmod p.$$

Следующая теорема в частности (утверждение 2) доказывает гипотезу 1.

Теорема 1. Если *p* – простое, $t > 0$, то

1) $\binom{n}{p^t} \equiv \lfloor n/p^t \rfloor \pmod p$.

2) последовательность биномиальных коэффициентов по модулю $\binom{n}{p^t} \bmod p$, $n = 0, 1, 2, \ldots$, является периодической с длиной периода p^{t+1}.

Доказательство первого утверждения. Представим $\binom{n}{p^t}$ в виде $\binom{\lfloor n/p^s \rfloor}{p^t}$, где $s = 0$, и применим лемму 2. Получаем сравнение

$$\binom{n}{p^t} \equiv \lfloor n/p^t \rfloor \pmod p.$$

Если $t - 1 \neq 0$, то снова воспользуемся леммой 2 для новой левой части $\binom{\lfloor n/p \rfloor}{p^{t-1}}$ сравнения и будем продолжать, создавая новые цепочки сравнений, пока показатель степени числа p у нижнего индекса биномиального коэффициента не станет равным 0. Таким образом, окончательно получаем

$$\binom{n}{p^t} \equiv \lfloor n / p^t \rfloor (\mathrm{mod}\ p). \quad (1)$$

Для наглядности рассмотрим, как это доказывается для случая $t = 3$:

$$\binom{n}{p^3} \equiv \binom{\lfloor n/p \rfloor}{\lfloor p^3/p \rfloor}\binom{n \bmod p}{p^t \bmod p} \equiv \binom{\lfloor n/p \rfloor}{p^2}\binom{n \bmod p}{0} \equiv \binom{\lfloor n/p \rfloor}{p^2} \times 1 \equiv \binom{\lfloor n/p \rfloor}{p^2} \equiv$$

$$\equiv \binom{\lfloor \lfloor n/p \rfloor / p \rfloor}{\lfloor p^2/p \rfloor}\binom{\lfloor n/p \rfloor \bmod p}{p^2 \bmod p} \equiv \binom{\lfloor n/p^2 \rfloor}{p}\binom{\lfloor n/p \rfloor \bmod p}{0} \equiv \binom{\lfloor n/p^2 \rfloor}{p} \times 1 \equiv$$

$$\equiv \binom{\lfloor n/p^2 \rfloor}{p} \equiv \binom{\lfloor \lfloor n/p^2 \rfloor / p \rfloor}{\lfloor p/p \rfloor}\binom{\lfloor n/p^2 \rfloor \bmod p}{p \bmod p} \equiv \binom{\lfloor n/p^3 \rfloor}{1}\binom{\lfloor n/p^2 \rfloor \bmod p}{0} \equiv$$

$$\equiv \binom{\lfloor n/p^3 \rfloor}{1} \times 1 \equiv \binom{\lfloor n/p^3 \rfloor}{1} \equiv \lfloor n/p^3 \rfloor (\mathrm{mod}\ p).$$

Доказательство второго утверждения. Из первого утверждения следует

$$\binom{n+p^{t+1}}{p^t} \equiv \lfloor (n+p^{t+1})/p^t \rfloor \equiv \lfloor n+p^t \rfloor + p \equiv \lfloor n+p^t \rfloor (\mathrm{mod}\ p).$$

То есть имеем

$$\binom{n+p^{t+1}}{p^t} \equiv \lfloor n/p^t \rfloor (\mathrm{mod}\ p). \quad (2)$$

Сравнения (1) и (2) вместе дают

$$\binom{n}{p^t} \equiv \binom{n+p^{t+1}}{p^t} (\mathrm{mod}\ p). \quad (3)$$

что доказывает второе утверждения теоремы.

Следующий результат был также найден с помощью экспериментов в системе Wolfram Mathematica. Исследовалось поведение последовательности

$$\binom{x}{y} (\mathrm{mod}\ p), x = 0,1,2,3, ...,$$

где $x \geq 1$ – целое, p – простое число, и натуральное положительное y было произвольно.

Определим функцию для вычисления $\binom{x}{y} (\mathrm{mod}\ p)$:

```
b[p_, y_, x_] := Mod[Binomial[x, y], p]
```

Мы будем применять ее для диапазона значений $x = 0, 1, 2, 3, \ldots, m$, где величина m выбирается таким образом, чтобы можно было визуально обнаружить перио-

дическое повторение значений функции *b*. Для этой же цели также список полученных значений каждого вызова функции *b*[*p*, *y*, *x*] разбивается на подсписки с помощью встроенных функций Partition и Column языка Wolfram:

Partition[*b*[3, 3^0, #]& /@ Range[0, 9], 3] // Column
{0, 1, 2}
{0, 1, 2}
{0, 1, 2}

В данном случае вы видим, что период значений функции *b* равен {0, 1, 2}. Рассмотрим последовательности для всех значений $y \le 9$:

Partition[*b*[3, 2, #]& /@ Range[0, 9], 3] // Column
{0, 0, 1}
{0, 0, 1}
{0, 0, 1}
Partition[*b*[3, 3, #]& /@ Range[0, 18], 9] // Column
{0, 0, 0, 1, 1, 1, 2, 2, 2}
{0, 0, 0, 1, 1, 1, 2, 2, 2}

Partition[*b*[3, 4, #]& /@ Range[0, 18], 9] // Column
{0, 0, 0, 0, 1, 2, 0, 2, 1}
{0, 0, 0, 0, 1, 2, 0, 2, 1}

Partition[*b*[3, 5, #]& /@ Range[0, 18], 9] // Column
{0, 0, 0, 0, 0, 1, 0, 0, 2}
{0, 0, 0, 0, 0, 1, 0, 0, 2}

Partition[*b*[3, 6, #]& /@ Range[0, 18], 9] // Column
{0, 0, 0, 0, 0, 0, 1, 1, 1}
{0, 0, 0, 0, 0, 0, 1, 1, 1}

Partition[*b*[3, 7, #]& /@ Range[0, 18], 9] // Column
{0, 0, 0, 0, 0, 0, 0, 1, 2}
{0, 0, 0, 0, 0, 0, 0, 1, 2}

Partition[*b*[3, 8, #]& /@ Range[0, 18], 9] // Column
{0, 0, 0, 0, 0, 0, 0, 0, 1}
{0, 0, 0, 0, 0, 0, 0, 0, 1}

Partition[*b*[3, 3^2, #]& /@ Range[0, 54], 27] // Column
{0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2}
{0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2}

Были рассмотрены и другие случаи с небольшими значениями *p* и *y*. В изученных примерах обнаружилось, что если $p^k \le y < p^{k+1}$ для натурального показателя *k*, то выполнена **гипотеза 2**:

$$\binom{x}{y} \equiv \binom{x + p^{k+1}}{y} \pmod{p}.$$

Более сложный тест для проверки гипотезы состоит в случайном выборе чисел *p, k, y, x* и выдает булевское значение. Ниже приведен код этого теста: вызов теста и полученный результат – True.

```
xs = { }; Do[p = RandomChoice[{2, 3, 5, 7, 11, 13, 17}]; k = RandomInteger[{0, 5}];
y = RandomInteger[{p^k, p^(k + 1) – 1}]; x = RandomInteger[{0, 2p^k}];
AppendTo[xs, Mod[Binomial[x, y], p] = = Mod[Binomial[x + p^(k + 1), y], p]],
1000];
And @@ xs
True
```

Тест проверяет 1 000 вариантов для случайного выбора значений *p, k, y, x*. Значение *p* выбирается среди простых чисел 2, 3, 5, 7, 11, 13 и 17. Возможные значения *k* суть 0, 1, 2, 3, 4, 5. Целое значение *y* удовлетворяет условию $p^k \le y < p^{k+1}$. Возможные значения переменной *x* удовлетворяют условию $0 \le x < 2p^{k+1}$. Логические значения True или False – результаты проверки каждого варианта, накапливаются в одном списке *xs*. После получения тысячи булевских значений тест вычисляет конъюнкцию этих значений. Тест запускался несколько раз, и после того как он выдал значение True во всех проделанных попытках, была доказана гипотеза 2.

Теорема 2 (обобщение теоремы 1). Пусть $x \ge 1$ – целое, $k \ge 0$ – целое, p – простое число, и выполнено неравенство $p^k \le y < p^{k+1}$. Тогда

$$\binom{x}{y} \equiv \binom{x + p^{k+1}}{y} (\text{mod } p). \tag{4}$$

Для доказательства нам понадобится теорема Люка и лемма 3.

Теорема Люка [6. С. 43]. Пусть p – простое число, и пусть n, m, q, r – неотрицательные числа, причем $0 \le q < p$, $0 \le r < p$. Тогда

$$\binom{pn+q}{pm+r} \equiv \binom{n}{m}\binom{q}{r} (\text{mod } p).$$

Лемма 3. Пусть $x \ge 1$ – целое, p – простое число и $0 \le y < p$. Тогда

$$\binom{x}{y} \equiv \binom{x+p}{y} (\text{mod } p). \tag{5}$$

Доказательство. Пусть n, q – неотрицательные целые, такие что $x = np + q$ и $0 \le q < p$. Применяя теорему Люка по отдельности к биномиальным коэффициентам $\binom{x}{y}$ и $\binom{x+p}{y}$ имеем

$$\binom{x}{y} = \binom{nx+q}{0\times p+y} \equiv \binom{n}{0}\binom{q}{y} \equiv \binom{q}{y} (\text{mod } p).$$

$$\binom{x+p}{y} = \binom{(n+1)p+q}{0\times p+y} \equiv \binom{n+1}{0}\binom{q}{y} \equiv \binom{q}{y} (\text{mod } p).$$

Из полученных сравнений следует сравнение (5).

Доказательство теоремы 2. Индукция по *k*. Базис при $k = 0$ доказан в лемме 3. Для доказательства индуктивного перехода предположим, что сравнение (4) выполнено при $k = t$. Докажем выполнимость (4) для $k = t + 1$. Положим $x = np + q$

и $0 \le q < p$, где n – целое неотрицательное число, $y = p^{t+1} + r$ и $0 \le r < p$. По теореме Люка имеем

$$\binom{x}{y} = \binom{np+q}{p^t \times p + r} \equiv \binom{n}{p^t}\binom{q}{r} (\mathrm{mod}\ p).$$

Теперь начнем с правой части сравнения (4) при $k = t + 1$. По теореме Люка получаем

$$\binom{x + p^{t+2}}{y} = \binom{p(n + p^{t+1}) + q}{p^t p + r} \equiv \binom{n + p^{t+1}}{p^t}\binom{q}{r} (\mathrm{mod}\ p).$$

И заключение данной теоремы следует из сравнения (3), полученного в пункте 2 теоремы 1.

Следствие. Пусть p – простое число, y – положительное целое число, тогда последовательность

$$\binom{x}{y} \bmod p, x = 0,1,2,3,... \tag{6}$$

является периодической с длиной периода $d = p^{\lfloor \log_p(y) \rfloor + 1}$.

Доказательство. Для y существует единственное целое k, для которого $p^k \le y < p^{k+1}$. Это значение k равно $\lfloor \log_p(y) \rfloor$. Теорема 2 говорит, что последовательность (6) является периодической с длиной периода p^{k+1}.

Список источников

1. Wolfram Mathematica. URL: http://www.wolfram.com/mathematica
2. *Weisstein E.W.* Experimental Mathematics // Wolfram MathWorld. URL: https://mathworld.wolfram.com/ExperimentalMathematics.html
3. *Зюзьков В.М.* Эксперименты в теории чисел. Томск : Изд-во НТЛ, 2019. 348 с.
4. *Грэхем Р., Кнут Д., Поташник О.* Конкретная математика. Основание информатики. М. : Мир ; БИНОМ. Лаборатория знаний, 2006. 703 с.
5. *Табачников С.Л., Фукс Д.Б.* Математический дивертисмент : 30 лекций по классической математике. М. : МЦНМО, 2011. 512 с.

References

1. *Wolfram Mathematica*. URL: http://www.wolfram.com/mathematica
2. Weisstein Eric W. *Experimental Mathematics. From MathWorld – A Wolfram Web Resource*. https://mathworld.wolfram.com/ExperimentalMathematics.html
3. Zyuz'kov V.M. (2019) *Eksperimenty v teorii chisel* [Experiments in the number theory]. Tomsk: NTL.
4. Graham R., Knut D., Patashnik O. (1994) *Concrete Mathematics. A Foundation for Computer Science*. Addison-Wesley.
5. Tabachnikov S.L., Fuks D.B. (2011) *Matematicheskiy divertisment. 30 lektsiy po klassicheskoy matematike* [Mathematical divertisement. 30 lectures on classical mathemics]. Moscow: MCCME.

***Сведения об авторе*:**
Зюзьков Валентин Михайлович – старший научный сотрудник, доцент кафедры вычислительной математики и компьютерного моделирования Томского государственного

университета, профессор кафедры компьютерных систем управления и проектирования Томского государственного университета систем управления и радиоэлектроники, Томск, Россия. E-mail: vmz@math.tsu.ru

***Information about the author*:**
Zyuz′kov Valentin M. (Senior Researcher, Associate Professor of chair of Computational Mathematics and Computer Modeling, Tomsk State University, Professor of the Chair of Computer Systems in Control and Design of the Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russian Federation). E-mail: vmz@math.tsu.ru

Статья поступила в редакцию 15.09.2022; принята к публикации 10.07.2023

The article was submitted 15.09.2022; accepted for publication 10.07.2023