УДК 51-37+519.61
DOI: 10.25559/SITITO.15.201902.283-289

Быстрое вычисление чисел Бернулли

Р. Р. Айдагулов[1,2], С. Т. Главацкий[1*]
[1] Московский государственный университет имени М.В. Ломоносова, г. Москва, Россия
119991, Россия, г. Москва, ГСП-1, Ленинские горы, д. 1
[*] glavatsky_st@mail.ru
[2] Институт машиноведения РАН имени А.А. Благонравова, г. Москва, Россия
119334, Россия, г. Москва, ул. Бардина, д. 4

Аннотация

Числа Бернулли часто встречаются в математическом анализе, теории чисел, комбинаторике и в других областях математики. В некоторых монографиях по теории чисел имеются отдельные главы, посвященные только числам Бернулли и их свойствам. Алгоритмы вычисления чисел Бернулли встроены во все популярные математические пакеты: Mathematica, Matlab, Magma, Pari GP и т.д.

В настоящей работе предлагается более быстрый, по сравнению с известными, алгоритм для вычисления чисел Бернулли. Суть нашего подхода заключается в усовершенствовании мультимодулярного метода Харвея за счет разрежения больших вычисляемых сумм, когда мы выражаем суммы по половине интервала через суммы в интервалах длины 1/12 или даже 1/15 длины интервала суммирования. В работе доказано, что такого сокращения интервалов суммирования удается достичь для подавляющего большинства простых чисел. При этом неудобные простые числа (а их не больше 0.01% при больших значениях n) можно просто исключить из списка тех, по модулю которых считается очередное число Бернулли.

Предлагаемый нами в статье алгоритм быстрого вычисления (ускорение более чем втрое, по сравнению с алгоритмом Харвея) чисел Бернулли по модулям простых чисел может быть успешно использовано и для нахождения иррегулярных простых чисел, иррегулярных пар , а также при вычислении инвариантов Ивасавы. При вычислении иррегулярных пар и инвариантов Ивасавы приведенный в нашей работе алгоритм значительно (более чем в 10 раз) более эффективен.

Ключевые слова: числа Бернулли, алгоритм, эффективность, модулярное вычисление, разреженные суммы.

Для цитирования: *Айдагулов Р. Р., Главацкий С. Т.* Быстрое вычисление чисел Бернулли // Современные информационные технологии и ИТ-образование. 2019. Т. 15, № 2. С. 283-289. DOI: 10.25559/SITITO.15.201902.283-289

Calculation of Bernoulli Numbers

R. R. Aidagulov[a,b], S. T. Glavatsky[a*]
[a] Lomonosov Moscow State University, Moscow, Russia
1, Leninskie gory, Moscow 119991, Russia
[*] glavatsky_st@mail.ru
[b] Institute of Mechanical Engineering RAS after A.A. Blagonravov, Moscow, Russia
4 Bardina St., Moscow 119334, Russia

Abstract

Bernoulli numbers are often found in mathematical analysis, number theory, combinatorics, and other areas of mathematics. In some monographs on number theory there are separate chapters devoted only to Bernoulli numbers and their properties. Algorithms for calculating Bernoulli numbers are built into all popular mathematical packages: Mathematica, Matlab, Magma, Pari GP, etc.
In this paper, we propose an algorithm for calculating Bernoulli numbers, which is faster than the known ones. The essence of our approach is to improve the Harvey multimodular method due to making sparse of large calculated sums, when we express the sums in half the interval in terms of sums in the intervals of length 1/12 or even 1/15 of the length of the summation interval. It is proved in the paper that such a reduction in the summation intervals can be achieved for the vast majority of prime numbers. At the same time, inconvenient prime numbers (and there are them no more than 0.01% for large values of n) can be simply excluded from the list those by modulo of which the current Bernoulli number is calculated.
The algorithm of fast calculation proposed by us in the article (acceleration is more than three times as compared with the Harvey algorithm) of Bernoulli numbers modulo prime numbers can also be successfully used to find irregular prime numbers, irregular pairs, and also when calculating Iwasawa invariants. When calculating the irregular pairs and Iwasawa invariants, the algorithm presented in our work is significantly (more than 10 times) more efficient.

Keywords: Bernoulli numbers, algorithm, efficiency, modular calculation, sparse sums.

For citation: Aidagulov R.R., Glavatsky S.T. Calculation of Bernoulli Numbers. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2019; 15(2):283-289. DOI: 10.25559/SITITO.15.201902.283-289

Введение. Определение чисел Бернулли

В математических формулах и теоремах часто появляются числа Бернулли. В некоторых монографиях по теории чисел имеются отдельные главы, посвященные только числам Бернулли и их свойствам [1, 2]. Первый в мире опубликованный компьютерный алгоритм, созданный леди Адой Лавлейс, осуществлял вычисление чисел Бернулли.

Обычно числа Бернулли определяются через производящую их функцию:

$$\sum_{m\geq 0}\frac{B_m t^m}{m!}=\frac{t}{e^t-1}=e^{Bt}\ (0!=1) \tag{1}$$

Здесь последнее равенство есть удобная формальная запись для ряда:
$f(x)=\sum_n a_n x^n, f(B)=\sum_n a_n B_n$.

С использованием этой формальной записи кратко записывается рекуррентная формула для вычисления чисел Бернулли, имеющаяся во всех учебниках:
$(1+B)^m-B^m=0, m>1$.

В развернутом виде эта формула имеет вид:

$$\sum_{k=0}^{m-1}C_m^k B_k=0 \tag{2}$$

Доказательство этой формулы получается непосредственно из определения
$t=e^{(1+B)t}-e^{Bt}$.

Формула (2) позволяет легко вычислить начальные значения чисел Бернулли. Используя чётность функции $f(t)=\frac{t}{e^t-1}+\frac{t}{2}$ получаем, что все числа Бернулли с нечетными номерами, кроме первого, равны нулю.

В приложениях часто используются многочлены [1, 2]:

$$B_m(x)=\sum_{k=0}^{m}C_m^k B_k x^{m-k}=(x+B)^m,$$

называемые многочленами Бернулли. Имеет место формула:
$B_m(x+1)-B_m(x)=mx^{m-1}$.

С её использованием легко получаются решения разностных уравнений типа:
$F(x+1)-F(x)=f(x)=\sum_n a_n x^n$.

и их решения, как сумматорные формулы Эйлера-Маклорена, легко записываются через многочлены Бернулли:
$F(x)=\sum_n \frac{a_{n-1}}{n}B_n(x)$.

Таким образом, получается (уточненная) формула Стирлинга:

$$n!=\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \exp\left[\sum_{k=1}^{m}\frac{B_{2k}}{2k(2k-1)}n^{1-2k}+\theta_{m.n}\frac{B_{2m+2}n^{-2m-1}}{(2m+2)(2m+1)}\right],$$

где $0<\theta_{m,n}<1$.

Числа Бернулли впервые появились в сумматорных формулах для степеней натуральных чисел:

$$S_m(q)=\sum_{k=1}^{q-1}k^m=\frac{B_{m+1}(q)-B_{m+1}}{m+1}= \tag{3}$$

$$=B_m q+\frac{m}{2}B_{m-1}q^2+\frac{m(m-1)}{6}B_{m-2}q^3$$

Для оценки величины B_k обычно используют явную формулу для значений дзета-функции:

$$B_k=(-1)^{\frac{k}{2}+1}\frac{2\varsigma(k)k!}{(2\pi)^k}\ \ k-четное \tag{4}$$

Эта формула может использоваться и для вычисления самих чисел Бернулли через приближенное вычисление:

$$\varsigma(k)=\sum_{n=1}^{\infty}\frac{1}{n^k}=\prod_p\frac{1}{1-\frac{1}{p^k}}$$

Знаменатель чисел Бернулли легко вычисляется как произведение соответствующих простых чисел (согласно теореме Staudt-Clausen):

$$Q_k=\prod_{(p-1)|k}p.$$

Соответственно, числитель чисел Бернулли может быть вычислен из формул (4), после предварительного вычисления $\varsigma(k)$ с необходимой точностью, как ближайшее целое к произведению с Q_k 3]. На такое вычисление B_k потребуется $O(k^2 ln^2 k)$ операций. При этом вычисление дзета-функции $\varsigma(k)$ через произведение уменьшает количество операций за счет того, что в произведении участвуют числа, близкие к 1. Это облегчает вычисление произведения заменой на сумму логарифмов, которые вычисляются с необходимой точностью [4, 5]. Оно легло в основу алгоритмов в пакетах Mathematica[1] [6] и Pari GP[2] [7].

Подставив в формулу (3) значение $q=1$, получаем рекуррентные формулы:

$$B_0=1, 0=B_m+\frac{m}{2}B_{m-1}+\frac{m(m-1)}{6}B_{m-2}+ \tag{5}$$

$$+\ldots+C_m^k\frac{B_{m-k}}{k+1}+\ldots, m>0$$

Однако вычисление значения каждого из чисел Бернулли по этим формулам потребует ещё большего количества операций из-за необходимости вычисления больших биномиальных коэффициентов. Они полезны для модулярных вычислений. Рекордное вычисление произвел David Harvey на основе мультимодулярного алгоритма [8]. Ниже выводятся формулы разреженных сумм для модулярного вычисления чисел Бернулли, которые ускоряют вычисление более чем в три раза по сравнению с алгоритмом Harvey.

[1] Pavlyk O. Today We Broke the Bernoulli Record: From the Analytical Engine to Mathematica // Wolfram Blog. April 29, 2008. [Электронный ресурс]. URL: https://blog.wolfram.com/2008/04/29/today-we-broke-the-bernoulli-record-from-the-analytical-engine-to-mathematica/ (дата обращения: 6.05.2019).

[2] The Pari Group, Pari/GP build A2019b. [Электронный ресурс]. URL: https://pari.math.u-bordeaux.fr/doc.html дата обращения: 6.05.2019).

Разреженные модулярные суммы

В основе модулярного вычисления $B_m, m>2$ лежит следствие формулы (3):

$$B_m=\frac{1}{q}S_m(q)-\frac{m(m-1)}{6}B_{m-2}q^2-\dots$$

гда $q=p^l$, эта формула дает хорошее *p*-адическое приближение. Если $p>3$ и $(p-1)$ не делит $(m-2)$, то аппроксимация имеет точность

$$B_m=\frac{1}{q}S_m(q)+O(q^2),q=p^l \qquad (6)$$

В противном случае точность уменьшается до $O(p^{2l-1})$. В правой части равенства (3) члены суммы, делящиеся на *p*, дают величину $p^{m-l}S_m(p^{l-1})=O(p^{2l})$ при $m>2l$ и (*p-1*), не делящем *m*. Таким образом, можно считать, что в формуле (6) используются только члены, не делящиеся на *p*:

$$B_m+O(p^{2l})=\frac{1}{q}S'_m(q)=\frac{1}{p}S'_m(p)+\sum_{k=1}\frac{C_m^k}{p^{l-k}}S'_{m-k}(p)S_k(p^{l-1}) \qquad (7)$$

Анализ модулярной формулы (7) показал, что, увеличив точность l в два раза при степенях простых чисел, можно уменьшить количество используемых простых чисел примерно в два раза. Однако при этом приходится вычислять суммы степеней в два раза больше, и для первых сумм степеней их надо вычислять с двойной точностью. Соответственно, увеличение точности не дает эффекта экономии числа операций в вычислении чисел Бернулли, разве что за исключением случая малых простых оснований.

Пусть $(a,q)=1$. Умножим члены суммирования на a и обозначим вычеты:

$$r_x=ax-q\left[\frac{ax}{q}\right]:$$

Таким образом,

$$(a^m-1)\frac{S'_m(q)}{mq}-a^{m-1}\sum_{(x,p)=1}x^{m-1}\left[\frac{ax}{q}\right]-\frac{(m-1)qa^{m-2}}{2}\sum_{(x,p)=1}x^{m-2}\left[\frac{ax}{q}\right]^2+O(q^2),p>3.$$

Обозначим далее

$$B'_m=\frac{B_m}{m},X_{a,j}=\sum_{\frac{jq}{a}<x<\frac{(j+1)q}{a}}x^{m-1},Y_{a,j}=\sum_{\frac{jq}{a}<x<\frac{(j+1)q}{a}}x^{m-2}$$

Известно [1], что модифицированные коэффициенты B'_m являются *p*-адическими целыми при условии, что $(p-1)$ не делит *m*. Поделив полученное выражение на a^{m-1}, и используя введенные обозначения, перепишем равенство в виде:

$$(e_a-a)B'_m=-\sum_{j=1}^{a-1}jX_{a.j}+\frac{m-1}{2a}q\sum_{j=1}^{a-1}j^2Y_{a,j}+R \qquad (8)$$

Здесь $e_a=a^{1-m}(modq^2),R=O(q^2)$, когда $m\neq 2mod(p-1)$.

Расчет второго порядка точности по формулам (8) может сократить общее количество операций при вычислении чисел Бернулли.

Представим рациональное число Бернулли в виде дроби:

$$B_m=\frac{V_m}{Q_m},Q_m=\prod_{p-1|m}p,V_m=\frac{-Q_m}{p}(modp),(p-1)\,|\,m.$$

Зная Q_m, мы вычисляем V_m. В случае, если $(p-1)\,|\,m$, указанного значения по модулю *p* нам достаточно. Но таких простых чисел мало, и нет смысла считать по неудобным простым числам с большей точностью. Для остальных простых чисел можно производить вычисления с точностью до второго порядка по формулам (8), предварительно сделав суммы более разреженными.

Обозначим

$$S_{k,a,j}=\sum_{\frac{jq}{a}<x<\frac{(j+1)q}{a}}x^k.$$

Переходя к дополнениям, получаем соотношения:

$$S_{k,a,a-1-j}=\sum_{\frac{jq}{a}<x<\frac{(j+1)q}{a}}(q-x)^k=(-1)^kS_{k,a,j}+(-1)^{k-1}kqS_{k-1,a,j}+O(q^2).$$

Для наших переменных эти соотношения выглядят так:

$$X_{a,a-1-i}=-X_{a,i}+q(m-1)Y_{a,i},Y_{a,a-i-1}=Y_{a,i},$$

Здесь $\delta=\frac{(p-1)}{2}p^{l-1}$, если $(p-1)\,|\,(m-2)$, иначе $\delta=0$. Используя эти соотношения, можно оставить в наших выражениях только $X_{a,i},Y_{a,i}$ с индексами $i<\left[\frac{a}{2}\right]$:

$$(e_a-a)B'_m=\sum_{j<\frac{a}{2}}(a-1-2j)X_{a,j}-\frac{q(m-1)}{2a}\sum_{j<\left[\frac{a}{2}\right]}(a^2-1-2j^2-2j)Y_{a,j}$$
$$-\frac{q(m-1)(a^2-1)(a\ mod\ 2)}{4a}Y_{2a,a-1}. \qquad (9)$$

Пусть $a=bd$, тогда $X_{b,j}=X_{a,dj}+X_{a,dj+1}+\dots+X_{a,d(j+1)-1}$. аналогично получаем и для переменной $Y_{b,j}$. Возьмем некоторое составное число a, и для всех делителей запишем формулу через переменные с индексом a:

$$\left(de_{\frac{a}{d}}-a\right)B'_m=\sum_{i<\frac{a}{2}}\left(a-\left(1+2\left[\frac{i}{d}\right]\right)d\right)X_{a,i}-$$
$$-\frac{q(m-1)}{2a}\sum_{i<\left[\frac{a}{2}\right]}\left(a^2-1-2\left[\frac{i}{d}\right]^2-2\left[\frac{i}{d}\right]\right)Y_{a,i}-$$
$$-\frac{q(m-1)d(b^2-1)(b\ mod\ 2)}{4b}Y_{2b,b-1},$$

Комбинируя разными делителями числа a, мы можем сделать большинство коэффициентов перед величинами $X_{a,i}$ равными нулю. При $a=2$ получаем:

$$(*2)(e_2-2)B'_m=X_{2,0}-\frac{3}{8}q(m-1)Y_{2,0}.$$

Здесь и далее через $(*a)$ будем обозначать формулы разреженного суммирования с разделением области суммирования на a частей.

При $a=4$ олучаются две сокращенные формулы:

$$(*4)\frac{(e_2-2)(1+e_2)}{2}B'_m=X_{4,0}-\frac{1}{4}q(m-1)Y_{4,0},$$
$$(*4)\frac{(e_2-2)(1+e_2)}{2}B'_m=X_{4,1}-\frac{1}{4}q(m-1)Y_{4,1},$$

и $a=6$ лучаются три сокращенные формулы:

$$(*6)\frac{e_6-e_2-e_3-1}{2}B'_m=X_{6,0}-\frac{1}{6}q(m-1)Y_{6,0},$$
$$(*6)\frac{e_2+2e_3-e_6-2}{2}B'_m=X_{6,1}-\frac{2e_2}{6}q(m-1)Y_{6,1},$$

$$(*6)\frac{(2e_2-e_3-1)}{2}B'_m = X_{6,2} - \frac{1}{3}q(m-1)Y_{6,2},$$

Учитывая, что $X_{12,2} = X_{4,0} - X_{6,0}, X_{12,3} = X_{3,0} - X_{4,0}$ из этих формул получаем более разреженные суммы:

$$(*12)\frac{(e_2-1)(e_2+1-e_3)}{2}B'_m = X_{12,2} - \frac{q(m-1)}{24e_2}\left[(4e_2-1)Y_{12,2} - (2e_2+1)Y_{12,3}\right],$$

$$(*12)\frac{(e_3+e_2-1+e_4)}{2}B'_m = X_{12,3} - \frac{q(m-1)}{24e_2}\left[(6e_2-1)Y_{12,2} - Y_{12,3}\right],$$

При $a = 30$ получается ещё более сокращенная формула:

$$(*30)e_2\frac{e_6-e_5+1-e_2}{2}B'_m = X_{30,9} - (e_2+1)X_{30,5} - \frac{q(m-1)}{180e_3}$$
$$\left[(4e_4+6e_6)Y_{30.4} + (4e_4+6e_2-30e_6-27e_3)Y_{30/5} + (6e_6+63e_3)Y_{30.9}\right]$$

Назовем разреженностью отношение всей длины суммирования к общей длине фактически используемых интервалов суммирования. В последних формулах интервалы суммирования для $Y_{a,i}$ в два раза длиннее, чем для переменных $X_{a,i}$, соответственно, их разреженность в два раза меньше. Разреженность суммирования для X в формулах $(*12)$ равна 12, а в формуле $(*30)$ равна 15. Когда $e_2 = -1(modp)$, разреженность этой формулы достигает 30 для вычислений первого порядка точности.

Приведем еще пару формул такого типа без второго порядка точности (без $Y_{a,i}$):

$$(*42)\frac{e_7-e_6-e_2+1}{2}B'_m = -\left(1+\frac{1}{e_2}+\frac{1}{e_3}\right)X_{42,6} + \frac{1}{e_3}(X_{42,7} - X_{42,20}) + \frac{1}{e_2}X_{42,14} + O(q)$$

с разреженностью 10.5 и

$$(*132)\frac{e_{12}(e_{11}-e_6-e_4-1)}{2}B'_m = X_{132,0} + X_{132,22} - X_{132,43} + (1+e_2)(X_{132,33} - X_{132,10}) +$$
$$+(1+e_3)(X_{132,44} - X_{132,21}) + (1+e_4+e_6)X_{132,55} - (1+e_4+e_3)X_{132,32} -$$
$$-(1+e_2+e_3+e_6)X_{132,54} + (1+e_2+e_3+e_4+e_6)X_{132,11} + O(q)$$

с разреженностью 12. Существуют формулы с еще большим разрежением. Однако у таких формул количество интервалов суммирования растет экспоненциально, а разреженность растет медленно, как в приведенных примерах. Соответственно, проверка попадания в нужный интервал суммирования требует большего количества операций, и алгоритм теряет свою эффективность. Даже использование формул (*30) взамен формул (*12) с разреженностью выше на 25% увеличивает производительность только на 5% из-за увеличения интервалов проверки от одного до двух интервалов.

Во всех формулах коэффициент перед B'_m обращается в 0 (по модулю p), если все $e_i = i$. В этом случае $i^m = 1(mod\ p)$ для всех используемых e_i. В большинстве формул B'_m бращается в 0 (по модулю p) и в случае $e_i = 1$ для всех используемых i, т.е. при $i^{m-1} = 1(mod\ p)$ для всех i.

Алгоритм вычисления с разреженными суммами

Одним из авторов реализован на языке *C* алгоритм вычисления $V_m = Q_m mB'_m$ по модулю простых чисел p.

В случае $(p-1)\,|\,m$, получаем $V_m = -\frac{Q_m}{p}(modp)$. В случае, когда $(p-1)$ не делит m, вычисляем по модулю p величины $e_2, e_3, e_5, e_6 = e_2e_3\,(modp)$.

Если все они равны 1 или все $e_i = i(mod\ p)$, то это просто пропускается. Только в этих случаях ни одна из формул (*12), (*30) не работает.

Если $e_6 + 1 \neq e_5 + e_2$, то величина V_m по модулю p вычисляется из формулы (*30), иначе – из одной из (*12).

Для быстрого суммирования по этим формулам используется порождение всех вычетов по формуле $x = g^i 2^j, i = 0,1,\ldots,k-1, j = 0,1,\ldots,\frac{p-1}{k}-1$

Здесь $\frac{p-1}{k} = ord_p(2), g$ — образующая. На самом деле, рассматривая x, мы пробегаем не по всем вычетам, а только по половине – при четном k индекс i пробегает до $\frac{k}{2}-1$, а при нечетном – индекс j о половине вычетов как в [8]. Соответственно, проверяем, попадает ли вычет x или $-x$ интервал суммирования для переменной X.

Если порожденный вычет попадает в интервал суммирования, то вычисляем $x_{r+1}^{m-1} = x_r^{m-1}c^{(j(r+1)-j(r))}, c = 2^{(m-1)}$ [через ранее попавшийся вычет или через случай j=0. В формулах суммирования (*30) из-за разреженности суммирования разница $j(r+1) - j(r)$ может быть большой. Соответственно, для быстрого вычисления величины $c^{(j(r+1)-j(r))}$ значения табулируются, т.е. вычисляются предварительно значения $c^1, c^2, \ldots, c^{30}, c^{60}, c^{90}, \ldots, c^{900}$. Это позволяет вычислить значение $x_{r+1}^{m-1} = x_r^{m-1}c^{(j(r+1)-j(r))}$ одним умножением для подавляющего большинства возможных разниц $j(r+1) - j(r)$, или двумя умножениями в редко встречающихся случаях. Предусматриваются и исключительные (не встречавшиеся до этого) случаи $j(r+1) - j(r) > 900$. За счет разреженности сумм модулярное вычисление (вычисление по простым модулям) производится более чем в 3 раза быстрее, нежели по алгоритму Harvey [8]. Найдя значения

$$V_m = v_1(modq_1), V_m = v_2(modq_2), (q_1, q_2) = 1,$$

Вычисляем

$V_m = v_{12}(modq_1q_2), v_{12} = v_1q_2\left(q_2^{-1}(modq_1)\right) + v_2q_1\left(q_1^{-1}(modq_2)\right)$.

Когда q_1, q_2 — k-битные числа, вычисление v_{12} производится за *O(klog k)* операций. Имея вначале значения вычетов по n простым числам, вычисляем вначале вычеты по попарным произведениям, далее – по произведениям четверок и т.д., по схеме бинарного дерева. Общее количество операций для вычисления по модулю произведения всех включенных простых чисел составит $O(mlog^2m)$, в то время как на вычисление всех вычетов требуется $O(m^2log^2m)$ операций. При больших значениях m последняя часть вычислений занимает не более одного процента времени. Поэтому приведенный алгоритм останется быстрее, более чем в 3 раза, нежели алгоритм Harvey [8]. Harvey отмечает, что его алгоритм вычисляет в 3-4 раза быстрее, чем Pari GP, и в 10 раз быстрее, чем пакет Mathematica (Wolfram). Поэтому приведенный в нашей работе алгоритм будет вычислять более чем в 10 раз быстрее лучших алгоритмов (Pari GP), реализованных в математических пакетах.

Заключение

Числа Бернулли появляются в анализе (через формулы Эйлера-Маклорена) и достаточно часто – в теории чисел (см. [9–18]). В математических пакетах, содержащих их вычисление, разумно было бы использовать более эффективные алгоритмы. При вычислении иррегулярных пар (p,n) и инвариантов Ивасавы приведенный в нашей работе алгоритм весьма (более чем в 10 раз) эффективен. Из формул (*30) сразу получается, что при $p<37$ все простые числа регулярны вследствие попадания только одного члена в интервал суммирования.

В процессе создания нашего алгоритма выводились формулы разреженных сумм с высокой точностью, как за счет степени $q=p^l$, так и за счет приближения $O\left(q^2\right)$. Тем не менее, в окончательном варианте пока реализована только точность первого порядка. Дело в том, что при вычислении одного коэффициента B_m использование высокой точности дает незначительный выигрыш. Они эффективны, когда требуется вычислить одновременно серии коэффициентов $B_m, B_{m-2}, B_{m-4}, \ldots$ частности, в случае исследования на регулярность и вычисления инвариантов Ивасавы.

Список использованных источников

[1] *Боревич З. И., Шафаревич И. Р.* Теория чисел. М.: Наука. 3-е изд. доп.1985. 504 с.

[2] *Ireland K., Rosen M.* A Classical Introduction to Modern Number Theory. Second Edition // Graduate Texts in Mathematics / S. Axler, K. Ribet (eds). Springer-Verlag, New York, 1990. Vol. 84. 389 p. DOI: 10.1007/978-1-4757-2103-4

[3] *Chowla S., Hartung P.* An “exact” formula for the m-th Bernoulli number // Acta Arithmetica. 1972. Vol. 22. Pp. 113-115. DOI: 10.4064/aa-22-1-113-115

[4] *Fillebrown S.* Faster computation of Bernoulli numbers // Journal of Algorithms. 1992. Vol. 13, Issue 3. Pp. 431-445. DOI: 10.1016/0196-6774(92)90048-H

[5] *Fee G., Plouffe S.* An efficient algorithm for the computation of Bernoulli numbers. 2007. arXiv:math/0702300. URL: https://arxiv.org/pdf/math/0702300.pdf (дата обращения: 6.05.2019).

[6] Wolfram Research, Inc., Mathematica, Version 6.0, Champaign, IL, 2007.

[7] *Stein W.* Modular Forms, a Computational Approach. Graduate Studies in Mathematics. Vol. 79. American Mathematical Society, Providence, Rhode Island, 2007. 268 p. DOI: 10.1090/gsm/079

[8] *Harvey D.* A Multimodular algorithm for computing Bernoulli numbers. 2008. arXiv:0807.1347. URL: https://arxiv.org/abs/0807.1347 (дата обращения: 6.05.2019).

[9] *Постников М. М.* Теорема Ферма. Введение в теорию алгебраических чисел. М.: Наука. 1978. 128 с.

[10] *Whittaker E. T., Watson G. N.* A course of modern analysis. Fourth Edition. Camb. Univ. Press, 1928.

[11] *Онши Е.* Обобщенные числа Бернулли–Гурвица и универсальные числа Бернулли // Успехи математических наук. 2011. Т. 66, № 5(401). С. 47-108. DOI: 10.4213/rm9441

[12] *Johnson W.* Irregular prime divisors of the Bernoulli numbers // Mathematics of Computation. 1974. Vol. 28. Pp. 653-657. DOI: 10.2307/2005943

[13] *Kellner B. C.* On irregular prime powers of Bernoulli numbers. 2004. arXiv:math/0409223. URL: https://arxiv.org/abs/math/0409223v2 (дата обращения: 6.05.2019).

[14] *Koblitz N.* p-adic Numbers, p-adic Analysis and Zeta-Functions // Graduate Texts in Mathematics / S. Axler, K. Ribet (eds). Springer-Verlag, New York, 1984. Vol. 58. 153 p. DOI: 10.1007/978-1-4612-1112-9

[15] *Thangadurai R.* Adams theorem on Bernoulli numbers revisited // Journal of Number Theory. 2004. Vol. 106. Pp. 169-177. DOI: 10.1016/j.jnt.2003.12.006

[16] *Buhler J., Crandall R., Ernvall R., Mets¨ankyl¨a T., Shokrollahi M. A.* Irregular Primes and Cyclotomic Invariants to 12 Million // Journal of Symbolic Computation. 2001. Vol. 31. Pp. 89-96. DOI: 10.1006/jsco.1999.1011

[17] *Wagstaff, Samuel S., Jr.* Prime divisors of the Bernoulli and Euler numbers // Number theory for the millennium, III (Urbana, IL, 2000). A K Peters, Natick, MA, 2002. Pp. 357-374. MR1956285

[18] *Greenberg R.* Iwasawa Theory — Past and Present // Advanced Studies in Pure Mathematics. 2001. Vol. 30. Pp. 335-385. URL: https://projecteuclid.org/download/pdf_1/euclid.aspm/1536853285 (дата обращения: 6.05.2019).

Поступила 6.05.2019; принята к публикации 10.07.2019; опубликована онлайн 25.07.2019.

Об авторах:

Айдагулов Рустем Римович, старший научный сотрудник кафедры теоретической информатики, отделение математики, механико-математический факультет, Московский государственный университет имени М.В. Ломоносова (119991, Россия, г. Москва, ГСП-1, Ленинские горы, д. 1), Институт машиноведения РАН имени А.А. Благонравова (119334, Россия, г. Москва, ул. Бардина, д. 4), кандидат физико-математических наук, ORCID: http://orcid.org/0000-0002-6579-429X, a_rust@bk.ru

Главацкий Сергей Тимофеевич, доцент кафедры теоретической информатики, отделение математики, механико-математический факультет, Московский государственный университет имени М.В. Ломоносова (119991, Россия, г. Москва, ГСП-1, Ленинские горы, д. 1), кандидат физико-математических наук, доцент, ORCID: http://orcid.org/0000-0003-1857-6158, glavatsky_st@mail.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Borevich Z.I., Shafarevich I.R. Number Theory, (Pure and Applied Mathematics, Volume 20). Academic Press, 1986. 435 p. (In Eng.)

[2] Ireland K., Rosen M.A Classical Introduction to Modern Number Theory. Second Edition. In: Axler S., Ribet K. (eds). *Graduate Texts in Mathematics.* Springer-Verlag, New York. 1990; 84. (In Eng.) DOI: 10.1007/978-1-4757-2103-4

[3] Chowla S., Hartung P. An “exact” formula for the m-th Bernoulli number. *Acta Arithmetica*. 1972; 22:113-115. (In Eng.) DOI: 10.4064/aa-22-1-113-115

[4] Fillebrown S. Faster computation of Bernoulli numbers. *Journal of Algorithms*. 1992; 13(3):431-445. (In Eng.) DOI: 10.1016/0196-6774(92)90048-H

[5] Fee G., Plouffe S. An efficient algorithm for the computation of Bernoulli numbers. 2007. arXiv:math/0702300. Available at: https://arxiv.org/pdf/math/0702300.pdf (accessed 6.05.2019). (In Eng.)

[6] Wolfram Research, Inc., Mathematica, Version 6.0, Champaign, IL, 2007. (In Eng.)

[7] Stein W. Modular Forms, a Computational Approach. Graduate Studies in Mathematics. Vol. 79. American Mathematical Society, Providence, Rhode Island. 2007; p. 268. (In Eng.) DOI: 10.1090/gsm/079

[8] Harvey D. A Multimodular algorithm for computing Bernoulli numbers. 2008. arXiv:0807.1347. Available at: https://arxiv.org/abs/0807.1347 (accessed 6.05.2019). (In Eng.)

[9] Postnikov M.M. Fermat's Theorem: An Introduction to the Theory of Algebraic Numbers. Moscow: Nauka, 1978. (In Russ.)

[10] Whittaker E. T., Watson G. N. A course of modern analysis. Fourth Edition. Camb. Univ. Press, 1928. (In Eng.)

[11] Ônishi Y. Generalized Bernoulli-Hurwitz numbers and the universal Bernoulli numbers. *Russian Mathematical Surveys.* 2011; 66(5):871-932. (In Eng.) DOI: 10.1070/RM2011v066n05ABEH004763

[12] Johnson W. Irregular prime divisors of the Bernoulli numbers. *Mathematics of Computation*. 1974; 28:653-657. (In Eng.) DOI: 10.2307/2005943

[13] Kellner B. C. On irregular prime powers of Bernoulli numbers. 2004. arXiv:math/0409223. Available at: https://arxiv.org/abs/math/0409223v2 (accessed 6.05.2019). (In Eng.)

[14] Koblitz N. p-adic Numbers, p-adic Analysis and Zeta-Functions. In: Axler S., Ribet K. (eds). *Graduate Texts in Mathematics*. Springer-Verlag, New York. 1984; 58. (In Eng.) DOI: 10.1007/978-1-4612-1112-9

[15] Thangadurai R. Adams theorem on Bernoulli numbers revisited. *Journal of Number Theory.* 2004; 106:169-177. (In Eng.) DOI: 10.1016/j.jnt.2003.12.006

[16] Buhler J., Crandall R., Ernvall R., Mets¨ankyl¨a T., Shokrollahi M. A. Irregular Primes and Cyclotomic Invariants to 12 Million. *Journal of Symbolic Computation*. 2001; 31:89-96. (In Eng.) DOI: 10.1006/jsco.1999.1011

[17] Wagstaff, Samuel S., Jr. Prime divisors of the Bernoulli and Euler numbers. *Number theory for the millennium, III (Urbana, IL, 2000)*. A K Peters, Natick, MA, 2002. Pp. 357-374. MR1956285 (In Eng.)

[18] Greenberg R. Iwasawa Theory — Past and Present. *Advanced Studies in Pure Mathematics*. 2001; 30:335-385. Available at: https://projecteuclid.org/download/pdf_1/euclid.aspm/1536853285 (accessed 6.05.2019). (In Eng.)

Submitted 16.05.2019; revised 20.06.2019;
published online 25.07.2019.

About the authors:

Rustem R. Aidagulov, Senior Researcher of Department of Theoretical Informatics, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University (1, Leninskie gory, Moscow 119991, Russia), Institute of Mechanical Engineering RAS after A.A. Blagonravov (4 Bardina St., Moscow 119334, Russia), Ph.D. (Phys.-Math.), ORCID: http://orcid.org/0000-0002-6579-429X, a_rust@bk.ru

Sergei T. Glavatsky, Associate Professor of Department of Theoretical Informatics, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University (1, Leninskie gory, Moscow 119991, Russia), Ph.D. (Phys.-Math.), Associate Professor, ORCID: http://orcid.org/0000-0003-1857-6158, glavatsky_st@mail.ru

All authors have read and approved the final manuscript.