Math-Net.Ru

Общероссийский математический портал

А. Ю. Нестеренко, Об одном подходе к разложению иррациональных чисел,
Матем. вопр. криптогр., 2018, том 9, выпуск 1, 89–106

DOI: <https://doi.org/10.4213/mvk248>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.81.55.215

26 апреля 2023 г., 07:00:47

**Об одном подходе
к разложению иррациональных чисел**

А. Ю. Нестеренко

Национальный исследовательский университет «Высшая школа экономики», Москва

Получено 11.V.2017

Аннотация. Рассматривается новый подход к представлению иррациональных чисел, задаваемых быстро сходящимися рядами, в произвольной системе счисления. Приведены алгоритмы представления чисел, принадлежащих двум большим классам, а также оценки числа шагов в предложенных алгоритмах и объема используемой при вычислениях памяти. Проведено исследование возможности эффективной реализации этих алгоритмов.

Ключевые слова: разложения иррациональных чисел, быстро сходящиеся ряды

On an approach to the expansion of irrational numbers

A. Yu. Nesterenko

National Research University Higher School of Economics, Moscow

Abstract. We consider a new approach to the representation of irrational numbers defined by rapidly convergent series in an arbitrary base. For two large classes of such numbers some algorithms of their representation are described; also the number of operations and the memory volume used are estimated. The possibility of efficient realization of these algorithms is studied.

Key words: irrational numbers expansions, rapidly convergent series

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 1, pp. 89–106 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

В настоящее время известно несколько различных подходов к выработке псевдослучайных последовательностей. Одним из таких подходов является представление иррациональных чисел в заданной системе счисления. В его основе лежит следующий хорошо известный результат, см., например, [6, п. 4.6].

Пусть $b > 1$ — целое число, а действительное число α представлено в системе счисления по основанию b , т. е.

$$\alpha = \sum_{n=0}^{\infty} a_n b^{-n} = [a_0; a_1, a_2, \dots]_b, \quad (1)$$

где $a_0 \in \mathbb{Z}$, $a_n \in \{0, 1, \dots, b-1\}$, $n = 1, 2, \dots$. Последовательность коэффициентов $a_1, a_2, \dots$ является периодической тогда и только тогда, когда α рационально.

Следовательно, для любого целого $b > 1$ последовательность коэффициентов представления иррационального числа α может рассматриваться как псевдослучайная непериодическая последовательность элементов кольца $\mathbb{Z}_b$.

Согласно результатам Э. Бореля [2, 12] (см. также [4, гл. 1, § 8]) элементы определенной равенством (1) последовательности для почти всех действительных чисел α имеют равномерное распределение на $\mathbb{Z}_b$. Хотя в настоящее время не существует результатов, позволяющих говорить о равномерном распределении коэффициентов $a_1, a_2, \dots$ представления произвольно заданного иррационального числа α , результаты практических экспериментов говорят о статистической неотличимости вырабатываемых последовательностей от равномерно распределенных последовательностей для большого количества иррациональных чисел α , см. [7].

В настоящей работе рассматриваются алгоритмические вопросы представления иррациональных чисел, задаваемых быстро сходящимися рядами, в заданной системе счисления по основанию $b > 1$. Рассмотрим класс чисел вида

$$\alpha = \sum_{n=0}^{\infty} \omega_n, \quad \text{где } \omega_n \in \mathbb{Q}. \quad (2)$$

Пусть существует такое число $n_0 \in \mathbb{N}$, что для любого $n \geq n_0$ выполнено неравенство $0 < |\omega_n| < b^{-n}$. В [7–9] исследовались два подмножества из рассматриваемого класса.

Первое подмножество было образовано числами вида

$$\alpha = \sum_{n=0}^{\infty} \frac{c_n}{n!}, \quad (3)$$

где $\{c_n\}_{n=0}^{\infty}$ — периодическая последовательность рациональных чисел.

Второе подмножество состояло из чисел вида

$$\alpha = \sum_{n=0}^{\infty} R(n) \frac{1}{b^n}, \quad (4)$$

где $R(n)$ есть рациональная функция вида

$$R(n) = \frac{u_1}{(dn + x_1)^s} + \dots + \frac{u_m}{(dn + x_m)^s}, \quad d, s, m \in \mathbb{N}, \quad (5)$$

величины $u_1, \dots, u_m$ — рациональные числа, а $x_1, \dots, x_m$ — различные натуральные числа. Известно, что перечисленные в (3), (4) подмножества содержат в себе большое число математических констант (см. [10, 11]), например, $\ln 2$, e или

$$\pi = \sum_{n=0}^{\infty} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right) \frac{1}{16^n}. \quad (6)$$

1. Алгоритм представления чисел в заданной системе счисления

Начнем с описания простого алгоритма представления действительного числа α вида (2) в системе счисления по основанию $b > 1$. Этот алгоритм обобщает алгоритм, предложенный в [7].

Определим начальное значение $\delta_{-1} = 0$, последовательность рациональных величин

$$\alpha_n = b\delta_{n-1} + \omega_n b^n, \quad a_n = \lfloor \alpha_n \rfloor, \quad \delta_n = \alpha_n - a_n, \quad n = 0, 1, \dots, \quad (7)$$

а также частичную сумму

$$s_k(\alpha) = \sum_{n=0}^k a_n b^{-n}, \quad k = 0, 1, \dots \quad (8)$$

Верна следующая лемма.

Лемма 1. Для введенных в (7) коэффициентов a_n , $n = 0, 1, \dots$, выполнено равенство

$$\alpha = \sum_{n=0}^{\infty} \frac{a_n}{b^n}.$$

Более того,

$$\alpha - s_k(\alpha) = \frac{1}{b^k} \left(\delta_k + b^k \sum_{n=1}^{\infty} \omega_{k+n} \right). \quad (9)$$

Доказательство. Для любого $n > 0$ из (7) следует равенство

$$\frac{\alpha_n}{b^n} = \frac{\alpha_{n-1} - a_{n-1}}{b^{n-1}} + \omega_n, \quad \text{или} \quad \frac{\alpha_{n-1}}{b^{n-1}} - \frac{\alpha_n}{b^n} = \frac{a_{n-1}}{b^{n-1}} - \omega_n.$$

Просуммировав полученные равенства по всем $n = 1, 2, \dots$, получим

$$\alpha_0 = \sum_{n=0}^{\infty} \frac{a_n}{b^n} - \sum_{n=1}^{\infty} \omega_n.$$

Поскольку $\alpha_0 = \omega_0$ и ряд $\sum_{n=0}^{\infty} \omega_n$ сходится, получим искомое равенство.

Для доказательства второго утверждения леммы заметим, что из равенства $\delta_n = \alpha_n - a_n$ следует равенство $\delta_n - b\delta_{n-1} = \omega_n b^n - a_n$. Пользуясь этим, находим

$$\begin{aligned} \alpha - s_k &= \sum_{n=0}^k \left(\omega_n - \frac{a_n}{b^n} \right) + \sum_{n=k+1}^{\infty} \omega_n = \\ &= \sum_{n=0}^k (\omega_n b^n - a_n) \frac{1}{b^n} + \sum_{n=k+1}^{\infty} \omega_n = \sum_{n=0}^k \left(\frac{\delta_n}{b^n} - \frac{\delta_{n-1}}{b^{n-1}} \right) + \sum_{n=k+1}^{\infty} \omega_n = \\ &= \frac{1}{b^k} \left(\delta_k + b^k \sum_{n=1}^{\infty} \omega_{k+n} \right). \end{aligned}$$

Лемма доказана. $\square$

Отметим, что равенства (7) не дают окончательного представления числа α в виде (1). Действительно, пусть для всех $n \geq n_0$ выполнено неравенство $0 < |\omega_n| < b^{-n}$. Тогда, учитывая, что величины δ_n принимают значения в интервале $0 \leq \delta_n < 1$, и окаймляющие неравенства в

$$-1 < \omega_n b^n \leq \alpha_n = \delta_{n-1} b + \omega_n b^n < b + 1, \quad (10)$$

получаем, что величины $a_n = \lfloor \alpha_n \rfloor$, вычисленные в соответствии с равенствами (7), удовлетворяют неравенствам $-1 \leq a_n \leq b$ при $n \geq n_0$.

Рассмотрим два граничных случая, в которых при $n \geq n_0$ эти условия не выполняются.

1. Если $a_n = b$, то в представлении (1) возникает равенство

$$\dots + a_{n-1}b^{-n+1} + b \cdot b^{-n} + \dots = \dots + (a_{n-1} + 1)b^{-n+1} + 0 \cdot b^{-n} + \dots,$$

т.е. для выполнения условия $a_n < b$ необходимо изменить значения коэффициентов a_{n-1}, a_n : сделать замену $a_{n-1} = a_{n-1} + 1$, $a_n = 0$. Очевидно, что если новое значение коэффициента $a_{n-1} \geq b$, то процедуру переноса единицы нужно повторить для индекса $n - 1$.

2. Если $a_n = -1$, то в представлении (1) возникает равенство

$$\dots + a_{n-1}b^{-n+1} + (-1) \cdot b^{-n} + \dots = \dots + (a_{n-1} - 1)b^{-n+1} + (b - 1) \cdot b^{-n} + \dots,$$

т.е. для выполнения условия $0 \leq a_n$ необходимо изменить значения коэффициентов a_{n-1}, a_n : сделать замену $a_{n-1} = a_{n-1} - 1$, $a_n = b - 1$. Поскольку

$$-1 = -1 \cdot b + (b - 1), \quad 0 \leq b - 1 < b,$$

можно объединить два случая в один на основе следующего условия. Если

$$a_n = qb + r, \quad q \in \{-1, 1\}, \quad r \in \{b - 1, 0\},$$

то $a_{n-1} = a_{n-1} + q$, $a_n = r$.

Отметим, что для $n < n_0$ коэффициенты $a_1, \dots, a_{n_0}$ могут принимать произвольные значения. Приведем пример: первые десять знаков разложения числа e в системе счисления по основанию $b = 16$, вычисленные с помощью соотношений (7), имеют вид

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = [1; 16, 128, 682, 2741, 8743, 23309, 53263, 106529, 189386, \dots]_{16} \quad (11)$$

Из сказанного следует, что для получения точного равенства (1) может потребоваться корректировка значений, полученных с помощью соотношений (7). При этом для индексов $n \geq n_0$ корректировка значений потребует переноса единицы, как было сказано выше, а для индексов $0 < n < n_0$, как в приведенном выше примере, может потребоваться перенос больших значений: если $a_n = qb + r \geq 0$, где $q \in \mathbb{Z}$ и $0 \leq r < b$, то необходимо перенести величину q в разряд с индексом, меньшим на единицу, т.е. сделать замену $a_n = r$, $a_{n-1} = a_{n-1} + q$. После чего повторить указанную процедуру для индекса $n - 1$.

Таким образом, если для некоторого заданного значения индекса $k \geq 1$ требуется вычислить частичную сумму $s_k(\alpha)$ или, другими словами, точные значения коэффициентов $a_0, \dots, a_k$, то необходимо с помощью соотношений (7) вычислить значения коэффициентов $a_0, a_1, \dots, a_h$, где индекс h удовлетворяет условиям

$$a_h < b - 1, \quad h \geq \max\{k + 1, n_0\}. \quad (12)$$

Условие $a_h < b - 1$ означает, что даже в случае переноса из $(h + 1)$ -го разряда в h -й разряд переноса в $(h - 1)$ -й разряд не произойдет. Далее надо провести процедуру коррекции в соответствии с описанными выше правилами для всех коэффициентов $a_{h-1}, a_{h-2}, \dots, a_0$.

Изложенное выше приводит к следующему алгоритму.

Алгоритм 1. Алгоритм представления иррационального числа
в заданной системе счисления

Вход: $\alpha = \sum_{n=0}^{\infty} \omega_n$, где $b, k, n_0 \in \mathbb{N}$, $\omega_n \in \mathbb{Q}$, а также
 $0 < |\omega_n| < b^{-n}$ при $n \geq n_0$.

Выход: $s_k(\alpha) = [a_0; a_1, \dots, a_k]_b$, где $a_0 \in \mathbb{Z}$ и $0 \leq a_n < b \quad \forall n = 1, \dots, k$.

- 1 Положить $h = \max\{k + 1, n_0\}$ и $\delta_{-1} = 0$.
- 2 /* Вычисляем последовательность коэффициентов */
- 3 Для всех $n = 0, \dots, h$ выполнять
 - 4 Вычислить $\alpha_n = b \delta_{n-1} + \omega_n b^n$.
 - 5 Положить $a_n = \lfloor \alpha_n \rfloor$ и $\delta_n = \alpha_n - a_n$.
- 6 **конец**
- 7 Пока $a_h \geq b - 1$, выполнять
 - 8 Вычислить $h = h + 1$ и $\alpha_h = b \delta_{h-1} + \omega_h b^h$.
 - 9 Положить $a_h = \lfloor \alpha_h \rfloor$ и $\delta_h = \alpha_h - a_h$.
- 10 **конец**
- 11 /* Выполняем процедуру коррекции вычисленных значений */
- 12 Для всех $n = h - 1, h - 2, \dots, 1$ выполнять
 - 13 Если $a_n < 0$ или $a_n \geq b$, то
 - 14 Найти такие q, r , что $a_n = qb + r$, $q \in \mathbb{Z}$, $0 \leq r < b$.
 - 15 Положить $a_n = r$, $a_{n-1} = a_{n-1} + q$.
 - 16 **конец**
- 17 **конец**

Отметим, что все операции в алгоритме 1 производятся только с целыми числами, представляющими собой числители и знаменатели чисел α_n, δ_n и ω_n . Изложенный алгоритм прост, но обладает рядом недостатков: он не допускает параллельной реализации и, кроме того, использует очень большой объем памяти. Для оценки используемого объема памяти получим оценку величины знаменателя величины δ_n , принимающей максимальное значение среди всех величин, используемых в алгоритме. Используя (2), представим $\omega_n = p_n/q_n$ при $n = 0, 1, \dots$, где $\text{НОД}(p_n, q_n) = 1$. Тогда из (7) для некоторого натурального ν_n получаем равенство

$$\delta_n = \frac{\nu_n}{q_0 \cdots q_n} = \frac{b \nu_{n-1} q_n + q_0 \cdots q_{n-1} p'_n b^n \pmod{q_0 \cdots q_n}}{q_0 \cdots q_n},$$

где $\nu_{-1} = 0$ и $p'_n = p_n \pmod{q_n}$ при $p_n \geq 0$, $p'_n = q_n - (|p_n| \pmod{q_n})$ при $p_n < 0$. Поскольку $\text{НОД}(\nu_n, q_0 \cdots q_n)$ может быть отличен от единицы, то полученное равенство, с учетом неравенства $0 < |\omega_n| < b^{-n}$ при $n \geq n_0$, дает приближительную оценку снизу роста знаменателей дробей δ_n :

$$q_0 \cdots q_n > b \cdot b^2 \cdots b^{n-1} \cdot b^n = b^{n(n+1)/2}, \quad n \geq n_0.$$

2. Модификации алгоритма 1

При проведении вычислений можно использовать тот факт, что возникающие в приложениях числа α вида (3) и (4) могут быть представлены в виде линейной формы с рациональными коэффициентами от действительных чисел, также представимых в виде (2). Это позволяет свести вычисление частичной суммы для исходного числа α к операциям с частичными суммами входящих в α слагаемых. Нам потребуется следующая лемма.

Лемма 2. Пусть $k, b > 1, m \geq 1$ — натуральные числа, $u_1, \dots, u_m$ — произвольные рациональные числа и $\xi_1, \dots, \xi_m$ — положительные действительные числа, определенные рядом (2). Обозначим

$$\begin{aligned} \mu &= \lceil \log_b m \rceil, \\ l &= \max\{0, \lceil \log_b |u_1| \rceil, \dots, \lceil \log_b |u_m| \rceil\}, \\ z &= \max\{0, \lceil \log_b \xi_1 \rceil, \dots, \lceil \log_b \xi_m \rceil\}. \end{aligned} \tag{13}$$

Тогда для величины $\alpha = \sum_{i=1}^m u_i \xi_i$ выполнено неравенство

$$\left| \alpha - \sum_{i=1}^m \text{sgn}(u_i) s_{k+3+z+\mu}(|u_i|) s_{k+3+l+\mu}(\xi_i) \right| < \frac{1}{b^k},$$

где частичные суммы s_k определены равенством (8).

Доказательство. В силу (2) и (8) для любого положительного действительного числа $\xi = \sum_{n=0}^{\infty} a_n b^{-n}$

$$s_{k+1}(\xi) = \sum_{n=0}^{k+1} \frac{a_n}{b^n}, \quad \varepsilon_\xi = \xi - s_{k+1}(\xi),$$

где $a_0 \in \mathbb{N}$, $0 \leq a_n < b$ для всех $n = 1, 2, \dots$. Тогда

$$\begin{aligned} 0 \leq \xi - s_{k+1}(\xi) &= \sum_{n=k+2}^{\infty} \frac{a_n}{b^n} = \frac{1}{b^{k+2}} \left(a_{k+2} + \frac{a_{k+3}}{b} + \frac{a_{k+4}}{b^2} \dots \right) < \\ &< \frac{b}{b^{k+2}} \sum_{n=0}^{\infty} \frac{1}{b^n} = \frac{1}{b^k(b-1)} \leq \frac{1}{b^k}, \end{aligned}$$

и из условия $b > 1$ получаем неравенство

$$0 \leq \xi - s_{k+1}(\xi) = \varepsilon_\xi < \frac{1}{b^k}. \quad (14)$$

Так как для всех $i = 1, \dots, m$ и для любого $k \geq 0$ величины $\xi_i > 0$ удовлетворяют неравенствам

$$s_{k+1}(\xi_i) < \xi_i \leq b^z, \quad s_{k+1}(|u_i|) < |u_i| \leq b^l,$$

то из (14) следует, что

$$\begin{aligned} &\left| \alpha - \sum_{i=1}^m \operatorname{sgn}(u_i) s_{k+3+z+\mu}(|u_i|) s_{k+3+l+\mu}(\xi_i) \right| = \\ &= \left| \sum_{i=1}^m \operatorname{sgn}(u_i) (|u_i| \xi_i - s_{k+3+z+\mu}(|u_i|) s_{k+3+l+\mu}(\xi_i)) \right| = \\ &= \left| \sum_{i=1}^m \operatorname{sgn}(u_i) (s_{k+3+l+\mu}(\xi_i) \varepsilon_{u_i} + s_{k+3+z+\mu}(|u_i|) \varepsilon_{\xi_i} + \varepsilon_{u_i} \varepsilon_{\xi_i}) \right| \leq \\ &\leq \sum_{i=1}^m (s_{(k+2+l+\mu)+1}(\xi_i) \varepsilon_{u_i} + s_{(k+2+z+\mu)+1}(|u_i|) \varepsilon_{\xi_i} + \varepsilon_{u_i} \varepsilon_{\xi_i}) < \\ &< m \left(\frac{b^z}{b^{k+2+z+\mu}} + \frac{b^l}{b^{k+2+l+\mu}} + \frac{1}{b^{2(k+1)+l+z+2\mu}} \right) \leq \\ &\leq b^\mu \cdot \frac{1}{b^{k+\mu}} \cdot \frac{1}{b^2} \left(2 + \frac{1}{b^{k+\mu+l+z}} \right) \leq \frac{3}{4} \frac{1}{b^k} < \frac{1}{b^k}. \end{aligned}$$

Лемма 2 доказана. □

Доказанная лемма позволяет свести вычисление частичной суммы $s_k(\alpha)$ к элементарным операциям сложения и умножения для частичных сумм действительных чисел ξ_i , через которые выражается число α . При перемножении частичных сумм можно воспользоваться любым из известных в настоящее время алгоритмов быстрого умножения больших чисел. Детальные описания таких алгоритмов можно найти в [1, 3, 5].

Лемма 2 позволяет также оценить количество слагаемых в частичных суммах, необходимых для вычисления величины α с заданной точностью. В утверждении леммы 2 возникают приближения $s_k(u)$ для положительных рациональных чисел u . Рассмотрим способ вычисления указанных приближений подробнее.

2.1. Представление рациональных чисел

Дадим детальное описание алгоритма представления рациональных чисел в заданной системе счисления, т. е. алгоритма построения равенства

$$u = \sum_{n=0}^{\infty} u_n b^{-n} = [u_0; u_1, \dots]_b,$$

где $u_0 \in \mathbb{Z}$ и $0 \leq u_n < b$ для всех $n = 1, 2, \dots$

Если u является целым числом, то, очевидно, $u = [u_0]_b$. Далее, если $u < 0$, то

$$-u = -[v_0; v_1, \dots]_b, \quad \text{где} \quad |u| = \sum_{n=0}^{\infty} \frac{v_n}{b^n}.$$

Тогда из равенств

$$0 = u + (-u) = \sum_{n=0}^{\infty} (u_n - v_n) b^n$$

получаем, что частичную сумму $s_k(u)$ можно вычислить по частичной сумме

$$s_k(|u|) = \sum_{n=0}^k \frac{v_n}{b^n}$$

при помощи равенств

$$u_k = b - v_k, \quad u_n = v_n - 1, \quad n = k-1, \dots, 1, 0.$$

Таким образом, достаточно рассмотреть случай положительного рационального нецелого числа $u \in \mathbb{Q}$.

В этом случае выполнено равенство

$$u = u_0 + \frac{P}{Q}, \quad u_0 = \lfloor u \rfloor, \quad 0 < P < Q, \quad \text{НОД}(P, Q) = 1, \quad (15)$$

и для представления числа u в системе счисления по основанию b необходимо определить коэффициенты $u_1, u_2, \dots$, удовлетворяющие условию

$$\frac{P}{Q} = \sum_{n=1}^{\infty} \frac{u_n}{b^n}, \quad 0 \leq u_n < b, \quad n = 1, 2, \dots$$

Как уже отмечалось, последовательность коэффициентов $u_1, u_2, \dots$ периодична. Для определения периода, который будем обозначать символом τ , можно воспользоваться следующими рассуждениями.

Пусть основание системы счисления b имеет вид

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s},$$

где $p_1, \dots, p_s$ — простые числа, а $\beta_1, \dots, \beta_s$ — натуральные. Отметим, что в практических приложениях часто выполнено равенство $s = 1$, а величина b имеет вид $b = 2^\beta$.

Для всех $i = 1, \dots, s$ определим величины

$$\alpha_i = \nu_{p_i}(Q), \quad \lambda_i = \left\lceil \frac{\alpha_i}{\beta_i} \right\rceil, \quad \lambda = \text{НОК}(\lambda_1, \dots, \lambda_s), \quad (16)$$

где $\nu_{p(Q)}$ — максимальная степень, в которой p в точности делит Q . Тогда $\lambda_i \beta_i \geq \alpha_i$ и

$$\frac{P}{Q} = \frac{P}{q \prod_{i=1}^s p_i^{\alpha_i}} = \frac{1}{b^{\lambda} q} \cdot P \prod_{i=1}^s p_i^{\lambda(\lambda_i \beta_i - \alpha_i)/\lambda_i} = \frac{P'}{b^{\lambda} q},$$

где $\text{НОД}(b, q) = 1$.

Если $q = 1$, то $Q = b^{\lambda}$ и искомое представление найдено. Действительно, поскольку из (15) следует неравенство $P/Q < 1$, имеем

$$P' < b^{\lambda} \quad \text{и} \quad P' = u_{\lambda} + u_{\lambda-1}b + \dots + u_1b^{\lambda-1}.$$

Тогда

$$\frac{P}{Q} = \frac{P'}{b^{\lambda}} = \sum_{n=1}^{\lambda} \frac{u_n}{b^n}.$$

В этом случае представление числа P/Q в системе счисления по основанию b конечно и содержит в точности λ коэффициентов.

Далее будем считать, что $q > 1$. Определим величины t, r равенствами

$$t = \left\lfloor \frac{P'}{q} \right\rfloor, \quad r = P' - tq,$$

из которых следуют неравенства $0 \leq r < q$. Используя введенные обозначения, запишем равенство

$$\frac{P}{Q} = \frac{P'}{b^\lambda q} = b^{-\lambda} \left(t + \frac{r}{q} \right).$$

При этом из неравенств

$$1 > \frac{P}{Q} = \frac{1}{b^\lambda} \cdot \frac{P'}{q} \geq \frac{t}{b^\lambda}$$

следует, что $t < b^\lambda$.

Обозначим через $\tau = \text{ord}_q b$ такое минимальное натуральное число, что $b^\tau \equiv 1 \pmod{q}$. Тогда $b^\tau = 1 + zq$ для некоторого натурального числа z и

$$\frac{r}{q} = \frac{zr}{b^\tau - 1} = zr \sum_{n=1}^{\infty} \frac{1}{b^{n\tau}},$$

где $zr < zq = b^\tau - 1 < b^\tau$. Последнее равенство позволяет окончательно записать (15) в виде

$$u = u_0 + \frac{t}{b^\lambda} + \frac{zr}{b^\lambda} \sum_{n=1}^{\infty} \frac{1}{b^{n\tau}} = \sum_{n=0}^{\infty} \frac{u_n}{b^n}, \quad (17)$$

где

$$\begin{aligned} t &= u_1 b^{\lambda-1} + \dots + u_{\lambda-1} b + u_\lambda, \\ zr &= u_{\lambda+1} b^{\tau-1} + \dots + u_{\lambda+\tau-1} b + u_{\lambda+\tau}, \end{aligned}$$

и $0 \leq u_n < b$ для всех $n = 1, 2, \dots$

Легко видеть, что коэффициенты $u_{\lambda+1}, \dots, u_{\lambda+\tau}$ образуют период разложения числа α , коэффициенты $u_1, \dots, u_\lambda$ — подход к периоду, а число u может быть записано в виде

$$u = [u_0; u_1, \dots, u_\lambda, \overline{u_{\lambda+1}, \dots, u_{\lambda+\tau}}]_b.$$

В случае произвольного знаменателя q нахождение величины $\tau = \text{ord}_q b$ является сложной задачей. Поскольку $\tau | \varphi(q)$, где φ — функция Эйлера, поиск τ сводится к перебору делителей числа $\varphi(q)$, т. е. к разложению числа $\varphi(q)$ на простые сомножители, что может быть весьма трудоемким при больших значениях q .

Таким образом, вычисление представления (1) для рационального числа u с использованием равенства (17) целесообразно только в случае, когда величина $\varphi(q)$ невелика и может быть легко разложена на простые сомножители, а величина τ не превосходит количества коэффициентов в частичной сумме $s_k(u)$, т. е. $\tau \leq k$.

В качестве примера рассмотрим дробь

$$u_n = \frac{P_n}{Q_n} = \frac{1}{8n+5},$$

возникающую в формуле для числа π , см. (6). Легко видеть, что для любого $n \geq 0$ знаменатель Q_n есть нечетное число, поэтому для $b = 16$ период τ_n представления числа u_n удовлетворяет сравнению $16^{\tau_n} \equiv 1 \pmod{8n+5}$.

Предположим, что мы хотим найти приближение $s_{1025}(u_n)$, которое, согласно (14), позволит определить значение u_n с точностью до 16^{-1024} . Легко рассчитать, что для всех $n = 0, \dots, 515$ выполнено неравенство $\tau_n < 1025$.

n	Q_n	τ_n
0	5	1
1	13	3
2	21	3
	...	
511	4093	1023
512	4101	683
513	4109	879
514	4117	979
515	4125	25
516	4133	1033

Следовательно, для всех $0 \leq n \leq 515$ использование равенства (17) позволит вычислить 1025 необходимых коэффициентов частичной суммы $s_{1025}(u_n)$ и тем самым оказаться эффективнее алгоритма 1.

В случае когда длина периода представления рационального числа u превышает количество членов частичной суммы $s_k(u)$, для вычисления $s_k(u)$ можно воспользоваться аналогом алгоритма 1.

Пусть $u = P/Q$ и $0 < u < 1$. Определим начальное значение $\delta_1 = u$ и последовательность коэффициентов $u_1, u_2, \dots$ равенствами

$$u_n = \lfloor \delta_n b \rfloor, \quad \delta_{n+1} = b\delta_n - u_n, \quad n = 1, 2, \dots \quad (18)$$

Так как для всех $n = 1, 2, \dots$ в силу определения выполнены неравенства $0 \leq \delta_n < 1$, то

$$0 \leq u_n = \lfloor b\delta_n \rfloor < b.$$

Теперь из (18) следует, что для любого $k \geq 1$

$$\begin{aligned} u &= \frac{P}{Q} = \frac{1}{b} (b\delta_1) = \frac{1}{b} (u_1 + \delta_2) = \frac{1}{b} \left(u_1 + \frac{1}{b} (b\delta_2) \right) = \\ &= \frac{1}{b} \left(u_1 + \frac{1}{b} (u_2 + \delta_3) \right) = \dots = \sum_{n=1}^k \frac{u_n}{b^n} + \frac{\delta_{k+1}}{b^k} = s_k(u) + \frac{\delta_{k+1}}{b^k}. \end{aligned}$$

Так как $0 \leq \delta_{k+1} < 1$, то

$$u - s_k(u) = \frac{\delta_{k+1}}{b^k} < \frac{1}{b^k}. \quad (19)$$

2.2. Алгоритм для второго множества чисел

Теперь можно применить полученные ранее результаты к представлению чисел α вида (4) в системе счисления по основанию $b > 1$. Верно равенство $\alpha = \sum_{i=1}^m u_i \xi_i$, где $u_i \in \mathbb{Q}$, а числа $\xi_i \in \mathbb{R}$ также имеют вид (4) для всех $i = 1, \dots, m$ и могут быть записаны в виде

$$\xi_i = \sum_{n=0}^{\infty} \frac{1}{dn + x_i} \frac{1}{b^n}.$$

Подобное представление позволяет применить утверждение леммы 2 для вычисления частичной суммы $s_k(\alpha)$, используя для этого частичные суммы, соответствующие рациональным числам $|u_1|, \dots, |u_m|$ и действительным числам $\xi_i, \dots, \xi_m$.

Остановимся на вычислении частичных сумм $s_k(\xi_i)$ более подробно, дополнительно предполагая, что значение k удовлетворяет неравенству $d(k+1) > b$. Отбрасывая индекс i , запишем равенство

$$\xi = \sum_{n=0}^{\infty} \frac{1}{dn + x} \frac{1}{b^n} = \sum_{n=0}^{\infty} \frac{R_n}{b^n}, \quad R_n \in \mathbb{Q},$$

где

$$R_0 = \frac{1}{x}, \quad R_1 = \frac{1}{d+x}, \quad R_2 = \frac{1}{2d+x}, \dots$$

Так как $0 < x \leq d$, то $0 < R_n < 1$ и $R_n > R_{n+1}$ для всех $n = 0, 1, \dots$. Воспользовавшись одним из описанных в предыдущем разделе методов, получим равенство

$$R_n = \sum_{j=1}^{\infty} \frac{r_j^{(n)}}{b^j} = [0; r_1^{(n)}, \dots, r_{\lambda_n}^{(n)}, \overline{r_{\lambda_n+1}^{(n)}, \dots, r_{\lambda_n+\tau_n}^{(n)}}],$$

где $0 \leq r_j^{(n)} < b$, $\lambda_n, \tau_n \in \mathbb{N}$ для всех возможных значений индексов n . Тогда

$$\xi = \sum_{n=0}^{\infty} \frac{R_n}{b^n} = \sum_{n=0}^{\infty} \left(\sum_{j=1}^{\infty} \frac{r_j^{(n)}}{b^j} \right) \frac{1}{b^n} = \sum_{n=1}^{\infty} \left(\sum_{j=0}^{n-1} r_{n-j}^{(j)} \right) \frac{1}{b^n}. \quad (20)$$

С другой стороны, положим $\delta = \lceil \log_b(k+1) \rceil$. Теперь, пользуясь (19) и вспоминая, что $d(k+1) > b > 1$, получаем оценку

$$\begin{aligned} \xi - \sum_{n=0}^k \frac{s_{k+2+\delta-n}(R_n)}{b^n} &= \\ &= \sum_{n=0}^k \frac{R_n - s_{k+2+\delta-n}(R_n)}{b^n} + \sum_{n=k+1}^{\infty} \frac{R_n}{b^n} < \\ &< \sum_{n=0}^k \frac{1}{b^{k+2+\delta}} + \frac{R_{k+1}}{b^{k+1}} \sum_{n=0}^{\infty} \frac{1}{b^n} < \\ &< \frac{k+1}{b^{k+2+\delta}} + \frac{b}{d(k+1)(b-1)b^{k+1}} \leq \frac{1}{b^{k+1}} \left(\frac{1}{b} + \frac{1}{b-1} \right) < \\ &< \frac{3}{2} \frac{1}{b^{k+1}} < \frac{1}{b^k}. \end{aligned} \quad (21)$$

Последнее неравенство дает выражение, позволяющее вычислить приближение к числу ξ с заданной точностью b^{-k} . Заметим, что при этом с ростом n количество членов в частичной сумме $s_{k+2+\delta-n}(R_n)$ убывает. Теперь можно привести алгоритм 2, основывающийся на неравенстве (21) и позволяющий вычислять значение ξ с заданной точностью. Этот алгоритм находит приближение к числу $\xi = \sum_{n=0}^{\infty} R_n b^{-n}$ с заданной точностью b^{-k} путем последовательного вычисления приближений к рациональным числам R_n с точностью $b^{-(k+2+\delta-n)}$.

Алгоритм 2. Алгоритм вычисления представления в системе счисления по основанию b числа $\xi = \sum_{n=0}^{\infty} R_n b^{-n}$

Вход: $\xi = \sum_{n=0}^{\infty} R_n b^{-n}$, где $R_n = (dn+x)^{-1}$, а также такие числа $b, d, x, k \in \mathbb{N}$, что $d(k+1) > b$.

Выход: $s_k(\xi) = [0; c_1, \dots, c_k]_b$, где $0 \leq c_i < b$, $i = 1, \dots, k$.

- 1 Положить $\delta = \lceil \log_b(k+1) \rceil$ и $c_i = 0$ для всех $i = 0, \dots, k+2+\delta$.
- 2 Для всех $n = 0, \dots, k$ выполнять
 - 3 Вычислить $s_{k+2+\delta-n}(R_n) = \sum_{i=1}^{k+\delta-n} r_i^{(n)} b^{-i}$, используя либо представление (17), либо соотношения (18).
 - 4 Для всех $i = k+\delta-n, \dots, 1$ выполнять
 - 5 Положить $c_{i+n} = c_{i+n} + r_i^{(n)}$.
 - 6 **конец**
 - 7 /* Редукция значений c_i */
 - 8 Положить $\sigma = 0$.
 - 9 Для всех $i = k+2+\delta, \dots, 1$ выполнять
 - 10 Вычислить такие значения q, r , что $0 \leq r < b$ и $c_i + \sigma = qb + r$.
 - 11 Положить $\sigma = q$ и $c_i = r$.
 - 12 **конец**
 - 13 Положить $c_0 = \sigma$.
 - 14 **конец**
 - 15 Вернуть в качестве результата вектор $s_k(\xi) = [0; c_1, \dots, c_k]_b$.

Метод, заложенный в основу этого алгоритма, позволяет существенно уменьшить объем используемой памяти. Действительно, в случае когда период разложения числа R_n в системе счисления по основанию b не превосходит k , для получения значений, лежащих на периоде коэффициентов $r_i^{(n)}$, можно использовать представление (17) (как показано в разделе 2.1, эта ситуация возникает при небольших значениях n). В случае когда $\text{ord}_{(dn+x)} b > k$, можно последовательно применять равенства (18). Однако для больших значений n необходимо вычислить только $k+2+\delta-n$ коэффициентов разложения $r_i^{(n)}$, $i = 1, \dots, k+2+\delta-n$ (в частности, при $n = k$ только $2+\delta$ коэффициентов), что также замедляет рост знаменателей величин δ_n , участвующих в равенстве (18). Объем памяти, используемой для хранения промежуточных значений $c_1, \dots, c_{k+2+\delta}$, не слишком сильно отличается от k , поскольку $\delta = \lceil \log_b(k+1) \rceil$.

В качестве последнего замечания отметим, что в алгоритме 2 третий шаг — вычисление представления рационального числа R_n в системе счисления по основанию b — можно проводить параллельно для различных значений n .

2.3. Алгоритм для первого множества чисел

Соображения, аналогичные вышеизложенным, можно использовать для представления в системе счисления по основанию b иррациональных чисел вида (3). Действительно, согласно [9] выполнено равенство

$$\alpha = \sum_{n=0}^{\infty} \frac{c_n}{n!} = \sum_{i=0}^{m-1} c_i \xi_i(m), \quad (22)$$

где m — период последовательности рациональных чисел $\{c_n\}_{n=0}^{\infty}$, $c_0, \dots, c_{m-1}$ — числа, лежащие на периоде, и

$$\xi_i(m) = \sum_{n=0}^{\infty} \frac{1}{(nm+i)!}, \quad i = 0, \dots, m-1.$$

Легко видеть, что числа $\xi_i(m)$ также имеют вид (2) при всех возможных значениях i . Следовательно, равенство (22) также позволяет применить при вычислении числа α утверждение леммы 2.

Рассмотрим числа $\xi_i(m)$ более детально. Они обладают следующим замечательным свойством. При $m = 1$ выполнены равенства

$$\xi_0(1) = \sum_{n=0}^{\infty} \frac{1}{n!} = e, \quad \alpha = x_0 e,$$

где e — основание натурального логарифма.

Если $m > 1$, то

$$\begin{aligned} e &= \sum_{n=0}^{\infty} \frac{1}{n!} = \\ &= \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{m!} + \frac{1}{(m+1)!} + \dots + \frac{1}{(2m)!} + \frac{1}{(2m+1)!} + \dots = \\ &= \frac{1}{0!} + \frac{1}{m!} + \frac{1}{(2m)!} + \dots + \frac{1}{1!} + \frac{1}{(m+1)!} + \frac{1}{(2m+1)!} + \dots \\ &\quad \dots + \frac{1}{2!} + \frac{1}{(m+2)!} + \frac{1}{(2m+2)!} + \dots = \\ &= \sum_{n=0}^{\infty} \frac{1}{(nm)!} + \sum_{n=0}^{\infty} \frac{1}{(nm+1)!} + \sum_{n=0}^{\infty} \frac{1}{(nm+2)!} + \dots = \\ &= \xi_0(m) + \xi_1(m) + \xi_2(m) + \dots + \xi_{m-1}(m), \end{aligned}$$

или

$$\xi_0(m) + \dots + \xi_{m-1}(m) = e.$$

Вернемся к вычислению $\xi_i(m)$ с заданной точностью b^{-k} , предполагая, что k достаточно велико и выполнено неравенство $b^k < k!$. Пусть k_0 — такое минимальное натуральное число, что $k_0 m + i \geq k$, тогда k_0 определяет число слагаемых, необходимых для вычисления $\xi_i(m)$. Действительно, воспользовавшись неравенством

$$\begin{aligned} ((k_0 + s)m + i)! &= (k_0 m + i)! \times (k_0 m + i + 1) \cdots (k_0 m + i + m) \times \cdots \\ &\quad \cdots \times (k_0 m + i + (s-1)m + 1) \cdots (k_0 m + i + sm) > \\ &> (k_0 m + i)! (k_0 m + i)^{sm} = k! k^{sm}, \end{aligned}$$

получаем

$$\begin{aligned} \xi_i(m) - \sum_{n=0}^{k_0} \frac{1}{(nm+i)!} &= \sum_{n=k_0+1}^{\infty} \frac{1}{(nm+i)!} < \\ < \frac{1}{k!} \left(\frac{1}{k^m} + \frac{1}{k^{2m}} + \cdots \right) &= \frac{1}{k!(k^m-1)} < \frac{1}{b^k}. \end{aligned}$$

Если $Q_n = (nm+i)!$, то

$$Q_{n+1} = Q_n (nm+i+1) \cdots (nm+i+m)$$

и

$$Q_n \mid Q_{n+1} \quad \text{для всех } n=0, \dots, k_0.$$

Условие делимости позволяет использовать только равенство (17) при вычислении частичной суммы для рационального числа $1/Q_n$. Если обозначить $\tau_n = \text{ord}_{Q_n} b$, то из свойств показателей следует, что $\tau_n \mid \tau_{n+1} = \text{ord}_{Q_{n+1}} b$ и

$$\tau_{n+1} = s \tau_n, \quad \text{где } s \mid \prod_{j=1}^m \varphi(nm+i+j), \quad n=0, \dots, k_0. \quad (23)$$

Следовательно, определив начальное значение $\tau_0 = \text{ord}_{i!} b$, остальные значения можно находить, последовательно применяя условие (23).

И последнее. Если необходимо вычислять представление в системе счисления по основанию b для нескольких чисел α вида (3), то величины $\xi_0(m), \dots, \xi_{m-1}(m)$ можно определить заранее, поскольку их значения не зависят от последовательностей коэффициентов $\{c_n\}_{n=0}^{\infty}$, определяющих α .

Список литературы

- [1] Ахо А., Хопкрофт Дж., Ульман Дж., *Построение и анализ вычислительных алгоритмов*, М. : Мир, 1979, 536 с.
- [2] Борель Э., *Основные идеи алгебры и анализа*, Л. : ГИЗ, 1927.
- [3] Василенко О. Н., *Теоретико-числовые алгоритмы в криптографии*, М. : МЦМНО, 2003, 325 с.
- [4] Кейперс Л., Нидеррайтер Г., *Равномерное распределение последовательностей*, М. : Наука, 1985, 408 с.
- [5] Кнут Д. Э., *Искусство программирования для ЭВМ. Получисленные алгоритмы*. Т. 2, 3-е изд., М. : Вильямс, 2000, 788 с.
- [6] Нестеренко Ю. В., *Теория чисел*, М. : Академия, 2008, 272 с.
- [7] Нестеренко А. Ю., “О статистических свойствах некоторых трансцендентных чисел”, *Уч. зап. Орловского гос. ун-та*, № 6, часть 2 (2012), 170–176.
- [8] Нестеренко А. Ю., “Алгоритм восстановления параметров одного класса иррациональных чисел”, *Изв. Саратовского ун-та. Сер. Матем. Мех. Инф.*, **13**:4, часть 2 (2013), 89–93.
- [9] Чирский В. Г., Нестеренко А. Ю., “Об одном подходе к преобразованию периодических последовательностей”, *Дискретная математика*, **27**:4 (2015), 150–157.
- [10] Bailey D. H., Borwein P. B., Plouffe S. On the rapid computation of various polylogarithmic constants, *Math. Comput.*, **66**:218 (1997), 903–913.
- [11] Bayley D. H., “A compendium of BBP-type formulas for mathematical constants”, *Preprint* (2010), <http://crd.lbl.gov/dhbailey/dhbpapers/bbp-formulas.pdf>.
- [12] Borel E., “Les probabilités dénombrables et leurs applications arithmétiques”, *Rend. Circ. Mat. Palermo*, **27** (1909), 247–271.