Math-Net.Ru

Общероссийский математический портал

А. В. Устинов, О среднем числе шагов в алгоритме Евклида с выбором минимального по модулю остатка, *Матем. заметки*, 2009, том 85, выпуск 1, 153–156

DOI: <https://doi.org/10.4213/mzm4517>

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: 54.237.206.68

26 апреля 2023 г., 18:07:07

О среднем числе шагов в алгоритме Евклида с выбором минимального по модулю остатка

А. В. Устинов

Классический алгоритм Евклида, в котором при делении выбирается наименьший неотрицательный остаток

$$a = bq + r, \quad q = \left[\frac{a}{b} \right], \quad 0 \leq r < q,$$

соответствует разложению числа в стандартную цепную дробь

$$\frac{a}{b} = t_0 + \frac{1}{t_1 + \frac{1}{\ddots + \frac{1}{t_s}}}$$

длины $s = s(a/b)$, в которой t_0 – целое, $t_1, \dots, t_s$ – натуральные и $t_s \geq 2$ при $s \geq 1$. Алгоритм Евклида, в котором при делении выбирается наименьший по модулю остаток

$$a = bq + r, \quad q = \left[\frac{a}{b} + \frac{1}{2} \right], \quad -\frac{q}{2} \leq r < \frac{q}{2},$$

приводит к разложению в дробь

$$\frac{a}{b} = t_0 + \frac{\varepsilon_1}{t_1 + \frac{\varepsilon_2}{t_2 + \frac{\varepsilon_l}{\ddots + \frac{\varepsilon_l}{t_l}}}} \quad (1)$$

длины $l = l(a/b)$, где t_0 – целое, $t_1, \dots, t_l$ – натуральные,

$$\varepsilon_k = \pm 1, \quad t_k \geq 2, \quad k = 1, \dots, l, \quad t_k + \varepsilon_{k+1} \geq 2, \quad k = 1, \dots, l-1.$$

Существует простой алгоритм (см. [1; § 39]), который превращает обычную цепную дробь в дробь вида (1). К первому неполному частному t_j , $j \geq 1$, равному единице, нужно применить тождество

$$t_{j-1} + \frac{1}{1 + \frac{1}{t_{j+1} + \frac{1}{\ddots}}} = t_{j-1} + 1 - \frac{1}{t_{j+1} + 1 + \frac{1}{\ddots}}.$$

То есть первая единица в разложении вычеркивается, соседние неполные частные увеличиваются на единицу и между ними ставится знак “минус”. Затем находится следующая единица и процедура повторяется. Если в разложении имеется цепочка из подряд идущих единиц, то преобразование применяется к единицам, стоящим на нечетных местах в этой цепочке. Например,

$$[0; 2, 1, 3, 1, 1, 6] = \frac{1}{3 - \frac{1}{5 - \frac{1}{2 + \frac{1}{6}}}}.$$

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 07-01-00306) и проекта ДВО РАН (грант № 06-III-A-01-017).

Для среднего числа шагов в алгоритме Евклида известны следующие результаты (см. [2], [3]):

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \leq a \leq b \\ (a,b)=1}} s\left(\frac{a}{b}\right) = \frac{2 \log 2}{\zeta(2)} \cdot \log b + C_1 + O_\varepsilon(b^{-1/6+\varepsilon}), \quad (2)$$

$$\frac{2}{R(R+1)} \sum_{b \leq R} \sum_{a \leq b} s\left(\frac{a}{b}\right) = \frac{2 \log 2}{\zeta(2)} \cdot \log R + C_2 + O(R^{-1} \log^4(R+1)) \quad (3)$$

с абсолютными константами

$$C_1 = \frac{2 \log 2}{\zeta(2)} \left(\frac{3 \log 2}{2} + 2\gamma - 2 \frac{\zeta'(2)}{\zeta(2)} - 1 \right) - \frac{3}{2}, \quad C_2 = C_1 + \frac{2 \log 2}{\zeta(2)} \left(\frac{\zeta'(2)}{\zeta(2)} - \frac{1}{2} \right),$$

где γ – постоянная Эйлера. В то же время для среднего числа шагов в алгоритме Евклида с выбором минимального по модулю остатка известен лишь результат

$$\frac{2}{R(R+1)} \sum_{b \leq R} \sum_{a \leq b} l\left(\frac{a}{b}\right) = \frac{2 \log \varphi}{\zeta(2)} \cdot \log R + C_3 + O(R^{-\beta}),$$

где $\varphi = (1 + \sqrt{5})/2$ – золотое сечение, C_3 – абсолютная постоянная и $\beta > 0$ (см. [4]). Оказывается, что формулы, аналогичные (2) и (3), справедливы и для величины $l(a/b)$.

Для фиксированного $x \in (0, 1]$ и рационального $r = [t_0; t_1, \dots, t_s]$ через $s_x(r)$ будем обозначать статистики Гаусса–Кузьмина

$$s_x(r) = \#\{j = 1, \dots, s : [0; t_j, \dots, t_s] \leq x\}.$$

В частности, $s_1(r) = s(r)$ – длина цепной дроби для числа r .

ЛЕММА. Для любого рационального числа a/b

$$l\left(\frac{a}{b}\right) = s_{\varphi-1}\left(\frac{a}{b}\right).$$

ДОКАЗАТЕЛЬСТВО. Пусть $a/b = [t_0; t_1, \dots, t_s]$. Обозначим через $s'(a/b)$ количество остатков $r_j = [0; t_j, \dots, t_s]$, $1 \leq j \leq s$, разложение которых начинается с нечетного числа единиц. Соответственно $s''(a/b)$ будет обозначать количество остатков, начинающихся с четного (возможно нулевого) числа единиц. Очевидно, выполняется равенство $s(a/b) = s'(a/b) + s''(a/b)$.

Согласно приведенному выше алгоритму при переводе обычной цепной дроби в дробь вида (1) каждый отрезок из k подряд идущих единиц заменяется на $[k/2]$ неполных частных. Поэтому исчезает в точности $s'(a/b)$ неполных частных:

$$l\left(\frac{a}{b}\right) = s\left(\frac{a}{b}\right) - s'\left(\frac{a}{b}\right) = s''\left(\frac{a}{b}\right).$$

Но цепная дробь для числа $r \in (0, 1)$ начинается с четного числа единиц тогда и только тогда, когда $r \in (0, \varphi - 1)$. Следовательно, $s''(a/b) = s_{\varphi-1}(a/b)$.

Формулы (2) и (3) обобщаются на случай статистик Гаусса–Кузьмина (см. [3], [5]). В равенстве (7) оценка остаточного члена равномерна по x в предположении, что $x \in [x_0, 1]$ для некоторого фиксированного $x_0 > 0$.

Подставляя в них результат леммы, приходим к следующему утверждению.

ТЕОРЕМА 1. При любом $R \geq 2$

$$\frac{2}{R(R+1)} \sum_{b \leq R} \sum_{a \leq b} l\left(\frac{a}{b}\right) = \frac{2 \log \varphi}{\zeta(2)} \cdot \log R + C_3 + O(R^{-1} \log^4 R).$$

ДОКАЗАТЕЛЬСТВО. Формула (3) обобщается на случай статистик Гаусса–Кузьмина (см. [3])

$$\frac{2}{R(R+1)} \sum_{b \leq R} \sum_{a \leq b} s_x \left(\frac{a}{b} \right) = \frac{2}{\zeta(2)} (\log(1+x) \log R + C_2(x)) + O(R^{-1} \log^4 R).$$

Подставляя сюда равенство из леммы, получаем утверждение теоремы с константой

$$C_3 = \frac{2}{\zeta(2)} C_2(\varphi) = \frac{2 \log \varphi}{\zeta(2)} \left(-\frac{\zeta'(2)}{\zeta(2)} - \frac{3}{2} \log \varphi - \frac{3}{2} \right) + \frac{2}{\zeta(2)} (h_1(\varphi) + h_2(\varphi)) + \frac{1}{\varphi^3},$$

где функции $h_1(x)$ и $h_2(x)$ задаются абсолютно сходящимися рядами

$$h_1(x) = \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{m=1}^n \frac{x}{n+mx} - \log(1+x) \right), \quad (4)$$

$$h_2(x) = \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{n/x \leq m < n/x+n} \frac{1}{m} - \log(1+x) \right). \quad (5)$$

ТЕОРЕМА 2. При любом $b \geq 2$

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \leq a \leq b \\ (a,b)=1}} l \left(\frac{a}{b} \right) = \frac{2 \log \varphi}{\zeta(2)} \cdot \log b + C_4 + O_{\varepsilon}(b^{5/6} \log^{7/6+\varepsilon} b). \quad (6)$$

ДОКАЗАТЕЛЬСТВО. Подставляя равенство из леммы в обобщение результата Портера (2) (см. [5])

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \leq a \leq b \\ (a,b)=1}} s_x \left(\frac{a}{b} \right) = \frac{2}{\zeta(2)} (\log(x+1) \log b + C_1(x)) + O_{\varepsilon,x}(b^{5/6} \log^{7/6+\varepsilon} b), \quad (7)$$

получаем нужное равенство с константой

$$C_4 = \frac{2}{\zeta(2)} C_1(\varphi) = \frac{2 \log \varphi}{\zeta(2)} \left(2\gamma - 2 \frac{\zeta'(2)}{\zeta(2)} - \frac{3}{2} \log \varphi - 1 \right) + \frac{2}{\zeta(2)} (h_1(\varphi) + h_2(\varphi)) - \frac{1}{\varphi^2},$$

где $h_1(x)$ и $h_2(x)$ задаются равенствами (4), (5).

ЗАМЕЧАНИЕ. Рассмотрим дисперсию величины $l(a/b)$

$$D_l(R) = \frac{2}{R(R+1)} \sum_{d \leq R} \sum_{c \leq d} \left(l \left(\frac{c}{d} \right) - E_l(R) \right)^2, \quad (8)$$

где $E_l(R)$ – математическое ожидание, стоящее в левой части равенства (3). Одним из результатов работы [4] является асимптотическая формула

$$D_l(R) = D_1 \cdot \log R + D_0 + O(R^{-\beta})$$

с абсолютными постоянными D_1 , D_0 и некоторым $\beta > 0$. Для аналогично определяемой дисперсии $D_s(R)$ величины $s(a/b)$ известен более точный результат (см. [3])

$$D_s(R) = D'_1 \cdot \log R + D'_0 + O(R^{-1/4+\varepsilon}).$$

Доказательство этого равенства остается справедливым, если вместо длины цепной дроби $s(a/b)$ рассматривать статистики Гаусса–Кузьмина. Отсюда с учетом доказанной леммы следует, что равенство (8) справедливо при любом $\beta < 1/4$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] О. Perron, *Die Lehre von den Kettenbrüchen*, bd I: Elementare Kettenbrüche, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1954. [2] J. W. Porter, *Mathematika*, **22**:1 (1975), 20–28. [3] А. В Устинов, *Изв. РАН. Сер. матем.*, **72**:5 (2008), 189–224. [4] V. Baladi, B. Vallée, *J. Number Theory*, **110**:2 (2005), 331–386. [5] А. В Устинов, *Алгебра и анализ*, **20**:5 (2008), 186–216.

А. В. Устинов

Хабаровское отделение Института
прикладной математики ДВО РАН
E-mail: ustinov@iam.khv.ru

Поступило
29.01.2008