УДК 511.36+511.37

ПЛОТНОСТНАЯ ОЦЕНКА ЧИСЛА ШАГОВ В АЛГОРИТМЕ ЕВКЛИДА

Быковский В. А.– д - р физ. - мат. наук, член-корр. РАН директор Хабаровского отделения Института прикладной математики, тел. (4212)32-46-76, e-mail: vab@iam.khv.ru (ДВО РАН)

Получена новая оценка числа шагов в алгоритме Евклида

A new estimate for the number of steps in Euclidean algorithm has been found.

Ключевые слова: алгоритм Евклида

Пусть a и q – натуральные числа с $a < q$. Положим $l_a(q) = l$, где l – длина канонического разложения

$$\frac{a}{q} = [0; q_1, \ldots, q_l] \tag{1}$$

в непрерывную дробь с неполными частными q_i (натуральные числа). При этом всегда $q_l \geq 2$. Хорошо известно (см., например, [1]), что величина $l_a(q)$ совпадает с числом шагов в алгоритме Евклида для нахождения $\text{НОД}(a,q)$. Нас будет интересовать вопрос о верхней оценке

$$l(q) = \max\{l_1(q), \ldots, l_{q-1}(q)\},$$

который имеет давнюю и содержательную историю (см. по этому поводу [1]).

Пусть $\rho = 1{,}7286\ldots$ – вещественное число, для которого $\varsigma(\rho) = 2$ (речь идет о дзета-функции Римана). Положим $\psi(x) = -(1-x)\log(1-x) - x\log x$ и $\varphi(y) = \rho(1 + 2\log_G \Phi)y + \psi(y\log_G \Phi)\log^{-1}\Phi$, где $\Phi = (1+\sqrt{5})/2$ (золотое сечение) и $G = (2+\sqrt{3})\Phi^{-2}$. Функция $\varphi(y)$ монотонно возрастает на интервале $\left(0, \frac{1}{2}\log_\Phi G\right)$ от 0 до $\varphi\left(\frac{1}{2}\log_\Phi G\right) > \rho + \log 2 > 1$ и поэтому $\varphi(\alpha) = 1$ при некотором $\alpha = 0{,}06213\ldots$

Пусть $0 < \varepsilon < \alpha$, $P \geq 2$, $M_\varepsilon(P)$ – множество всех натуральных чисел q из отрезка $[2, P]$, для которых *не выполняется* неравенство

$$l(q) \leq (1 - \alpha + \varepsilon)\log_\Phi q, \tag{2}$$

В работе доказывается следующая

Теорема. *Для любого* $\varepsilon \in (0, \alpha)$, $\#M_\varepsilon(P) \underset{\varepsilon}{<<} P^{1-\rho(1-\alpha)\varepsilon}$.

Замечание 1. Здесь и в дальнейшем под $\#X$ подразумевается количество элементов множества X.

Замечание 2. *Записи* $f(x) = O\big(g(x)\big)$ *и* $f(x) << g(x)$ *означают, что во всей области определения переменных* x *(одной и той же для* f *и* g*) выполняется неравенство* $|f(x)| \leq Cg(x)$ *с некоторой абсолютной положительной константой* C. *Если* $C = C(\varepsilon)$ *(константа зависит от* ε*), то будем писать* $f(x) = O_\varepsilon\big(g(x)\big)$ *и* $f(x) \underset{\varepsilon}{<<} g(x)$.

Замечание 3. *Из теоремы следует, что для* **почти всех** *натуральных* q *выполняется неравенство (2), которое уточняет неулучшаемую оценку* $l(q) \leq \log_\Phi q + O(1) \quad \forall q \in \mathrm{N}$, *восходящую к Э. Леже [2] (см. по этому поводу [1]).*

Замечание 4. *В работе [3] (см. также [1], задача 38 из 4.5.3) доказано, что для любого натурального* q *выполняется неравенство* $l(q) \geq \frac{1}{2}\log_\Phi q + O(1)$.

Напомним, что введенные Л. Эйлером континуанты $K_l(x_1, \ldots, x_l)$ (многочлены от l переменных $x_1, \ldots, x_l$ определяются по правилу: $K_0 = 1$ и $K_1(x_1) = x_1$; для $l \geq 0$

$$K_{l+2}(x_1, \ldots, x_{l+2}) = K_{l+1}(x_1, \ldots, x_{l+1})x_{l+2} + K_l(x_1, \ldots, x_l).$$

Хорошо известно (см., например, [1]), что $K_l(x_1, \ldots, x_l) = K_l(x_l, \ldots, x_1)$ и для натуральных n и m

$$K_{n+m}(x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}) =$$
$$= K_m(x_1, \ldots, x_m)K_n(x_{m+1}, \ldots, x_{m+n}) + K_{m-1}(x_1, \ldots, x_{m-1})K_{n-1}(x_{m+2}, \ldots, x_{m+n}).$$

Далее, для любых натуральных $q_1, \ldots, q_l$

$$K_l(q_1, \ldots, q_l) \geq K_l(1, \ldots, 1) = u_{l+1},$$

где u_n – последовательность Фибоначчи, определяемая начальными условиями $u_1 = u_2 = 1$ и рекуррентным соотношением $u_{n+2} = u_{n+1} + u_n$.

Замечание 5. *Индукцией по* n *легко доказывается двусторонняя оценка* $\Phi^{n-2} \le u_n \le \Phi^{n-1}$.

Замечание 6. *Для канонического разложения (1) с* $\text{НОД}(a,q)=1$, $K_l(q_1,\ldots,q_l)=q$ *и* $K_{l-1}(q_2,\ldots,q_l)=a$.

Положим $V_{n+1}=K_{2n}(2,1,\ldots,2,1,\ldots,2,1)=K_{2n}(1,2,\ldots,1,2,\ldots,1,2)$. Для этой последовательности $V_1=1$, $V_2=K_2(2,1)=3$ и $V_{n+2}-4V_{n+1}+V_n=0$. Также справедливо

Замечание 7. *Для любого натурального* n, $\left(2+\sqrt{3}\right)^{n-2} \le V_n \le \left(2+\sqrt{3}\right)^{n-1}$.

Доказательство теоремы

Пусть $s\in[1,\infty)$ и $\text{N}_\varepsilon^2(s)$ – множество пар натуральных чисел (a,q), для которых:

$1\le a<q\le\Phi^s$; $\text{НОД}(a,q)=1$; $l_a(q)>(1-\alpha+\varepsilon)s$.

Для любой такой пары с каноническим разложением (1) величина $r=r_a(q)$ – количество неполных частных q_i *больших* 1. Положим $r_1=[r/2]$. Очевидно, что $q=K_l(q_1,\ldots,q_l)\ge K_l(q_1',\ldots,q_l')$, где $q_i'=\min\{2,q_i\}\in\{1,2\}$. Предположим, что $2r\le l$. Согласно [4] (см. также [1], упражнение 37 из 4.5.3)

$$K_l(q_1',\ldots,q_l')\ge K_l(t_1,\ldots,t_l)$$

с $t_{2i-1}=1$ и $t_{2i}=2$ для $1\le i\le r-r_1$, $t_i=1$ для $2(r-r_1)<i\le l-2r$, $t_{l-2i}=1$, и $t_{l-2i-1}=2$ для $0\le i<r_1$. Поэтому

$$q\ge K_{2(r-r_1)}(1,2,\ldots,1,2)\cdot K_{l-2r}(1,\ldots,1)K_{2r_1}(2,1,\ldots,2,1)=V_{r-r_1}u_{l-2r}V_{r_1}\ge\left(2+\sqrt{3}\right)^{r-4}\Phi^{l-2r-1}.$$

Следовательно, при $s\ge s_0(\varepsilon)$

$$\Phi^s\ge q\ge\left(2+\sqrt{3}\right)^r\Phi^{(1-\alpha)s-2r}=\Phi^{s-\alpha s+r\log_\Phi G}.$$

То есть

$$r\le\alpha s\log_G\Phi \quad\text{при}\quad s\ge s_0(\varepsilon). \tag{3}$$

В случае $2r>l$ по тем же причинам

$$\Phi^s\ge q\ge K_{2[l/2]}(2,1,\ldots,2,1)>>\left(2+\sqrt{3}\right)^{\frac{l}{2}}>\Phi^{\frac{l}{2}\log_\Phi\left(2+\sqrt{3}\right)}.$$

Таким образом, $l=l_\alpha(q)<\log_\Phi^{-1}\left(2+\sqrt{3}\right)s+O(1)$, что при достаточно больших s противоречит условию

$$l>(1-\alpha+\varepsilon)s>(1-\alpha)s>2\log_\Phi^{-1}\left(2+\sqrt{3}\right)s.$$

Значит, для всех пар (a,q) из $\mathrm{N}_{\varepsilon}^{2}(s)$ выполняется оценка (3).

По заданному набору натуральных $Q_a(q)=(q_1,\ldots,q_l)$ с $q_1\ge 2$ построим новый набор

$Q'_a(q)=(q_{k_1},\ldots,q_{k_r})=(q'_1,\ldots,q'_r)$.

Вычеркиванием из $Q_a(q)$ всех $q_i=1$. При этом $k_r=l$ и будем считать, что $k_0=0$. Итерируя очевидные неравенства

$K_n(q_1,\ldots,q_{n-1},q_n)\ge K_{n-1}(q_1,\ldots,q_{n-1})q_n$,

$K_{n+t}(q_1,\ldots,q_n,1,\ldots,1)\ge K_n(q_1,\ldots,q_n)K_t(1,\ldots,1)$,

получим оценку

$$K_l(q_1,\ldots,q_l)\ge\prod_{i=1}^{r}q_{k_i}u_{k_{i-1}}\ge\Phi^{l-2r}\cdot\prod_{i=1}^{r}q_{k_i}\ .$$

Но тогда для (a,q) из $\mathrm{N}_{\varepsilon}^{2}(s)$

$$\prod_{i=1}^{r}q'_i=\prod_{i=1}^{r}q_{k_i}\le\Phi^{s-l+2r}\le\Phi^{(\alpha-\varepsilon)s+2r},$$

и в соответствии с неравенством (3)

$$\prod_{i=1}^{r}q'_i<<_{\varepsilon}\Phi^{\alpha(1+2\log_G\Phi)\varepsilon-\varepsilon s}.$$

Заметим также, что

$$l\le 1+\log_{\Phi}u_{l+1}=1+\log_{\Phi}K_l(1,\ldots,1)\le$$

$$\le 1+\log_{\Phi}K_l(q_1,\ldots,q_l)\le 1+\log_{\Phi}\Phi^{s}\le s+1.$$

Для фиксированных l и $Q'=(q'_1,\ldots,q'_r)$ набор $(q_1,\ldots,q_l)$, из которого получается Q' вычеркиванием единиц, можно выбрать C_{l-1}^{r-1} способами. При этом по формуле Стирлинга

$$C_{l-1}^{r-1}\le C_{s}^{r-1}<<\mathrm{e}^{\psi\left(\frac{r}{s}\right)s+O(\log s)}.$$

Обозначим через $T(P)$ $(P\ge 2)$ количество всех наборов натуральных чисел $(q'_1,\ldots,q'_r)$, для которых

$$\prod_{i=1}^{r}q'_i\le P \quad\text{и}\quad q'_i\ge 2\quad(1\le i\le r).$$

С помощью очевидного рекуррентного соотношения

$$T(P)=[P]-1+\sum_{2\le q\le P/2}T\left(\frac{P}{Q}\right)$$

легко показать, что $T(P) < P^{\rho}$ с числом ρ, определенным в начале работы.

Подытоживая вышесказанное, окончательно находим, что с учетом неравенства (3)

$$\#\mathrm{N}_{\varepsilon}^{2}(s) \underset{\varepsilon}{<<} s^{2} C_{l-1}^{r-1} T\left(\Phi^{\alpha(1+2\log_{G}\Phi)s-\varepsilon s+O_{\varepsilon}(1)}\right) \underset{\varepsilon}{<<} \Phi^{(\varphi(\alpha)-\varepsilon\rho)s+O(\log s)},$$

где $\varphi(\alpha) = 1$. Поэтому

$$\#\mathrm{N}_{\varepsilon}^{2}(s) \underset{\varepsilon}{<<} \Phi^{(1-\varepsilon\rho)s+O(\log s)}. \qquad (4)$$

Пусть $\mathrm{N}'_{\varepsilon}(s)$ – множество всех натуральных q из полуинтервала $(\Phi^{s-1}, \Phi^{s}]$, для которых

$$l'(q) = \max_{\substack{1\le a<q \\ \text{НОД}(a,q)=1}} l_{a}(q) > (1-\alpha+\varepsilon)\log_{\Phi} q.$$

Из оценки (4) следует, что

$$\#\mathrm{N}'_{\varepsilon}(s) \underset{\varepsilon}{<<} \Phi^{(1-\rho\varepsilon)s+O(\log s)}. \qquad (5)$$

Пусть теперь $\mathrm{N}_{\varepsilon}(s)$ – множество всех натуральных q из полуинтервала $(\Phi^{s-1}, \Phi^{s}]$, для которых $l(q) > (1-\alpha+\varepsilon)\log_{\Phi} q$. Легко заметить, что $l(q) = l'(q_1)$, где q_1 – некоторый делитель q. При этом

$$(1-\alpha+\varepsilon)\log_{\Phi} q < l(q) = l(q') \le 1 + \log_{\Phi} q_1.$$

Поэтому

$$q_1 > \Phi^{-1} q^{1-\alpha+\varepsilon} > \Phi^{-1}\Phi^{(1-\alpha+\varepsilon)(s-1)} = \Phi^{(1-\alpha+\varepsilon)s+\theta(\varepsilon)}$$

с $\theta(\varepsilon) = -2+\alpha-\varepsilon$. Следовательно, величина $\#\mathrm{N}_{\varepsilon}(s)$ не превосходит количества пар натуральных чисел (d, q_1), для которых $q = dq_1 \le \Phi^{s}$ и

$$\Phi^{(1-\alpha+\varepsilon)s+\theta(\varepsilon)} < q_1 \le \Phi^{\varepsilon}, \quad (1-\alpha+\varepsilon)\log_{\Phi} q_1 < l'(q_1). \qquad (6)$$

Отсюда находим, что

$$\#\mathrm{N}_{\varepsilon} \le \sum_{q_1} \frac{\Phi^{s}}{q_1},$$

где суммирование проводится по всем натуральным q_1 с условиями из (6). Разбивая область суммирования на полуинтервалы $(\Phi^{s-k-1}, \Phi^{s-k}]$ с целыми k из отрезка $\left[0, (\alpha-\varepsilon)s - \theta(\varepsilon)\right]$ и применяя оценку (5), получаем

$$\#\mathrm{N}_{\varepsilon}(s) \underset{\varepsilon}{<<} \Phi^{s+O(\log s)} \cdot \sum_{0\le k\le(\alpha-\varepsilon)s} \left(\Phi^{s-k}\right)^{-\rho\varepsilon} \underset{\varepsilon}{<<} \Phi^{s-\rho\varepsilon(1-\alpha+\varepsilon)s+O(\log s)} \underset{\varepsilon}{<<} \Phi^{(1-\rho(1-\alpha)\varepsilon)s}.$$

Положив $P = \Phi^{s}$, окончательно находим, что

$$\#M_{\varepsilon}(P) = \sum_{0\le k\le s} \#\mathrm{N}_{\varepsilon}(s-k) \underset{\varepsilon}{<<} \sum_{0\le k\le s} \left(\frac{P}{\Phi_k}\right)^{1-\rho(1-\alpha)\varepsilon} \underset{\varepsilon}{<<} P^{1-\rho(1-\alpha)\varepsilon}.$$

Теорема полностью доказана.

Работа выполнена при поддержке РФФИ (грант № 07-01-0036) и проекта ДВО РАН № 06-1-П13-047.

Библиографические ссылки

1. *Кнут Д. Е.* Искусство программирования. Т. 2. М., 2001.
2. *Leger E.* Correspondance Math. et Physique. 1837. V. 9.
3. *Mikusinski J.* Ann. Polon. Math. 1954. V. 1.
4. *Motzkin T. S., Straus E. G.* Proc. Amer. Math. Soc. 1956. V. 7.