Н. К. Верещагин, Эффективные верхние оценки числа нулей линейной рекуррентной последовательности, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 1986, номер 1, 25–30

или

$$\sum_{i=1}^{m} c_i \sum_{j=0}^{m-1} P_j(z)\, y_i^{(j)} = 0,$$

где не все c_i $(i=1, \ldots, m)$ равны нулю. Так как все разности $m\lambda_i - m\lambda_j$ отличны от целых чисел, а внутренние суммы в последнем равенстве суть умноженные на $z^{-m\lambda_i}$ ряды по целым степеням z, то для каждого индекса i, при котором $c_i \neq 0$, получаем

$$\sum_{j=0}^{m} P_j(z)\, y_i^{(j)} = 0. \tag{13}$$

Легко убедиться, что последнее равенство равносильно линейной зависимости ряда $\left(\frac{z}{m}\right)^{m\lambda_i} y_i$ и его производных до $m-1$ включительно над полем $\mathbf{C}(z)$. Однако этот ряд имеет такой же вид, какой и ряд $\varphi(z)$ в доказанной выше лемме, если числа $\lambda_1, \ldots, \lambda_m$ в последнем заменить числами $\lambda_1 - \lambda_i - 1, \ldots, \lambda_m - \lambda_i - 1$. Из доказанной леммы следует, что функции $y_i, \ldots, y_i^{(m-1)}$ линейно независимы над $\mathbf{C}(z)$, а из (13) — что $P_1(z) = \ldots = P_m(z) = 0$. Теорема 2 доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Siegel C. L. Über einige Anwendungen Diophantische Approximationen. — Abh. Press. Akad. Wiss., 1929—1930, 1, 1—70.
2. Шидловский А. Б. О критерии алгебраической независимости значений одного класса целых функций. — Изв. АН СССР. Сер. матем., 1959, **23**, 35—66.
3. Олейников В. А. О трансцендентности и алгебраической независимости значений некоторых целых функций. — Изв. АН СССР. Сер. матем., 1968, **32**, 63—92.
4. Олейников В. А. Об алгебраической независимости значений E-функций. — Матем. сб., 1969, **78(120)**, № 2, 301—306.
5. Frobenius G. Über den Begriff der Irreducibilität in den Theorie der linearen Differentialgleichungen. — Journ. f. d. r. u. a. Math., 1873, **76**, 236—270.
6. Нестеренко Ю. В. Об алгебраической независимости значений E-функций, удовлетворяющих линейным неоднородным дифференциальным уравнениям. — Матем. заметки, 1969, **5**, № 5, 587—598.
7. Салихов В. Х. О дифференциальной неприводимости одного класса дифференциальных уравнений. — Изв. АН СССР. Сер. матем., 1980, **44**, № 1, 176—202.

Поступила в редакцию
29.03.84

УДК 511.216

Н. К. Верещагин

ЭФФЕКТИВНЫЕ ВЕРХНИЕ ОЦЕНКИ ЧИСЛА НУЛЕЙ ЛИНЕЙНОЙ РЕКУРРЕНТНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

В 1935 г. К. Малер [1], использовав p-адический метод Т. Сколема, доказал, что множество нулей любой линейной рекуррентной последовательности (л. р. п.) полулинейно, то есть является объединением конечного множества и конечного числа арифметических прогрессий. Из доказательства Малера можно извлечь алгоритм, позволяющий по любой данной л.р.п. определить, конечно ли ее множество нулей. Другой такой алгоритм, основанный на результате [1], но не на его доказа-

тельстве, построен в [2] Берстелем и Миньоттом. Оба алгоритма, однако, не дают верхней оценки числа нулей. В настоящей работе предлагается алгоритм, определяющий, конечно ли число нулей данной л. р. п., и дающий верхнюю оценку этого числа, если оно конечно (следствие 2), что усиливает результат Берстеля и Миньотта. Эффективная оценка нулей дана теоремой 1. Заметим, что проблема существования алгоритма, вычисляющего по данной л.р.п. описание ее множества нулей, открыта. Доказываемые результаты получены модификацией рассуждений Малера [1] с помощью конструкции Сколема из [3]. Теорема 2 настоящей работы дает возможность при получении верхней оценки обойтись без вычислений, связанных с идеалами в кольце целых алгебраических чисел, требуемых теоремой 1, ценой сильного огрубления самой оценки. Наконец, следствие 3 дает совсем грубую и наглядную оценку.

Определение 1. *Последовательность алгебраических чисел* $\{u_n\}$ *называется л. р. п., если найдутся такие алгебраические числа* $a_1, a_2, \ldots, a_d$, *что при всех* $n \geqslant d$

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \ldots + a_d u_{n-d}. \tag{1}$$

Наименьшее такое d, *что при подходящих* $a_1, \ldots, a_d$ *выполнено* (1) *при всех* $n \geqslant d$, *называется порядком л.р.п., а многочлен* $x^d - a_1 x^{d-1} - \ldots - a_d$ — *собственным многочленом. Множество* $\{n \mid u_n = 0\}$ *называется множеством нулей л. р. п.* $\{u_n\}$.

Л. р. п. $\{u_n\}$ будем считать данной, если даны числа $a_1, \ldots, a_d$, для которых выполнено (1) при всех $n \geqslant d$, и числа $u_0, \ldots, u_{d-1}$. Алгебраическое число задаем своим минимальным многочленом и окрестностью, отделяющей его от других корней этого многочлена.

Если $u_n \in \mathbf{Z}$ для всех n, то будем называть $\{u_n\}$ целочисленной последовательностью. Известно [4], что собственный многочлен целочисленной л. р. п. имеет целые коэффициенты.

В основе всех наших результатов лежит следующая лемма, доказанная Т. Сколемом [3] для идеалов в кольце целых рациональных чисел. Доказательство с несущественными изменениями переносится на кольцо целых алгебраических чисел, и мы его опустим.

Пусть K — поле алгебраических чисел; $\mathfrak{p}$ — простой идеал в кольце целых чисел поля K, обозначаемом $\mathbf{Z}_K$; π — простой элемент кольца $\mathfrak{p}$-целых чисел $\mathfrak{O}_\mathfrak{p}$. Кольцо целых $\mathfrak{p}$-адических чисел обозначим $\mathfrak{T}_\mathfrak{p}$.

Лемма. *Пусть* $\{f_i\}$ — *последовательность многочленов с* $\mathfrak{p}$-*целыми коэффициентами из* K, *причем* $f_0(x)$ *имеет коэффициент, не делящийся на* $\mathfrak{p}$. *Тогда количество решений уравнения*

$$f_0(x) + \pi f_1(x) + \ldots + \pi^i f_i(x) + \ldots = 0 \tag{2}$$

в кольце $\mathfrak{T}_\mathfrak{p}$ *(следовательно, и в целых числах) не превосходит степени* $f_0(x)$.

Следствие 1. *Пусть* $\{f_i\}$ — *последовательность многочленов с коэффициентами из* $\mathfrak{O}_\mathfrak{p}$ *и* l — *наименьшее число, такое, что выполнено*

$$f_0(x) + \pi f_1(x) + \ldots + \pi^l f_l(x) \not\equiv 0 \pmod{\pi^{l+1}}.$$

Тогда количество решений уравнения (2) в $\mathfrak{T}_\mathfrak{p}$ *не превосходит степени многочлена* $f_0(x) + \pi f_1(x) + \ldots + \pi^l f_l(x)$.

Доказательство. Применим лемму к последовательности $\{\tilde{f}_i\}$, определенной так:

$$\tilde{f}_0(x)=\pi^{-l}\sum_{k=1}^{l}\pi^k f_k(x),\quad \tilde{f}_i(x)=f_{i+l}(x)\ \text{при}\ i\geqslant 1.$$

Пусть $\{u_n\}$ — л. р. п. Тогда, как известно [4], значение u_n определяется формулой

$$u_n=\sum_{i=1}^{m}P_i(n)\,\alpha_i^n, \tag{3}$$

где $\alpha_1, \ldots, \alpha_m$ — корни собственного многочлена, $P_i\in\mathbf{Q}(\alpha_1, \ldots, \alpha_m)[x]$, степень P_i равна кратности α_i без единицы. Для формулировки основной теоремы нам понадобится еще одно определение.

Определение 2. *Пусть* $K=\mathbf{Q}(\alpha_1, \ldots, \alpha_m)$, φ — *функция Эйлера на идеалах в* $\mathbf{Z}_K$ (*см.* [5]), $\mathfrak{p}$ — *простой идеал в* $\mathbf{Z}_K$, p — *простое число из* $\mathfrak{p}$, q — *любое простое число. Через* $\nu_{\mathfrak{p}}$ *обозначим показатель идеала* $\mathfrak{p}$. *Положим* $r_{\mathfrak{p}}$ *равным* $\varphi(\mathfrak{p}^t)$, *где* $t=\left[\dfrac{\nu_{\mathfrak{p}}(p)}{p-1}\right]+2$. *Определим числа* $m_{\mathfrak{p}}^i$, $0\leqslant i<r_{\mathfrak{p}}$, *так:* $m_{\mathfrak{p}}^i=\min\{\nu_{\mathfrak{p}}(u_{i+jr_{\mathfrak{p}}})\,|\,0\leqslant j<d\}$ *и аналогично для целочисленной л. р. п.:* $m_q^i=\min\{\nu_q(u_{i+jr_{(q)}})\,|\,0\leqslant j<d\}$ ($m_{\mathfrak{p}}^i$, *как и* $m_q{}^i$, *могут быть равны* ∞). *Наибольшую из степеней* P_i *обозначим* a.

Заметим, что если хотя бы одно из чисел $m_{\mathfrak{p}}^i$ или m_q^i равно ∞, то есть $\forall n<d$ $(u_{i+nr_{\mathfrak{p}}}=0)$, то множество нулей бесконечно, так как $u_{i+nr_{\mathfrak{p}}}=v_n$ — л. р. п. порядка, не большего d (см. [4]), и имеет d первых нулей; следовательно, $v_n\equiv 0$. Поэтому для л. р. п. с конечным множеством нулей все $m_{\mathfrak{p}}^i$ и m_q^i конечны. Обратно, если все $m_{\mathfrak{p}}^i$, m_q^i конечны, то справедлива

Теорема 1. *Пусть* $\{u_n\}$ — *л. р. п. с собственным многочленом* $Q(x)$. *А. Если* $\mathfrak{p}$ — *простой идеал в* $\mathbf{Z}_K$, *взаимно простой с идеалами* $(\alpha_1), \ldots, (\alpha_m)$, *и* $\forall i\nu_{\mathfrak{p}}(P_i(x))\geqslant 0$, $\nu_{\mathfrak{p}}(Q(x))\geqslant 0$, *то*

$$|\{n\,|\,u_n=0\}|\leqslant\sum_{i=0}^{r_{\mathfrak{p}}-1}m_{\mathfrak{p}}^i+r_{\mathfrak{p}}a.$$

Б. Если $\{u_n\}$ — *целочисленная л. р. п., если* q — *простое число, большее двух, и если для любого простого идеала* $\mathfrak{q}$, *делящего* q, *имеет место:* $\nu_q(P_i)\geqslant 0$ *для любого* i *и* $\nu_{\mathfrak{q}}(\alpha_j)=0$ *для любого* j, *то*

$$|\{n\,|\,u_n=0\}|\leqslant 2\sum_{i=0}^{r_q-1}m_q^i+r_qa.$$

Доказательство. А. Известно [5], что $\alpha_i^{r_{\mathfrak{p}}}\equiv 1\ (\mathrm{mod}\,\mathfrak{p}^t)$, то есть $\alpha_i^{r_{\mathfrak{p}}}=1+\beta_i\pi^t$, где β_i — $\mathfrak{p}$-целое число. Имеет место цепочка равенств

$$u_{j+xr_{\mathfrak{p}}}=\sum_i P_i(j+xr_{\mathfrak{p}})\,\alpha_i^j\alpha_i^{r_{\mathfrak{p}}x}=\sum_i Q_{ij}(x)\,(1+\pi^t\beta_i)^x=$$

$$=\sum_{k=0}^{\infty}\pi^{tk}\binom{x}{k}\sum_i Q_{ij}(x)\,\beta_i^k.$$

Легко убедиться, что

$$v_{\mathfrak{p}}\left(\binom{x}{k}\right)=v_{\mathfrak{p}}(p)\cdot v_p\left(\binom{x}{k}\right)\geqslant v_{\mathfrak{p}}(p)\,v_p\left(\frac{1}{k!}\right)\geqslant -\frac{v_{\mathfrak{p}}(p)}{p-1}\cdot k.$$

Поэтому $v_{\mathfrak{p}}\left(\pi^{tk}\binom{x}{k}\right)\geqslant k$ и $u_{j+xr_{\mathfrak{p}}}$ представляется рядом, удовлетворяющим условиям следствия 1:

$$u_{j+xr_{\mathfrak{p}}}=\sum_{k=0}^{\infty}\pi^k g_k^j(x), \tag{4}$$

где

$$g_k^j=\pi^{tk-k}\binom{x}{k}\sum_i Q_{ij}(x)\,\beta_i^k.$$

Для каждого $j<r_{\mathfrak{p}}$ оценим сверху число l из условия следствия 1. Докажем, что $l\leqslant m_{\mathfrak{p}}^j$. Действительно, найдется такое n, что $u_{j+nr_{\mathfrak{p}}}\not\equiv 0 \pmod{\pi^{m_{\mathfrak{p}}^j+1}}$; для этого n

$$\sum_{k=0}^{\infty}\pi^k g_k^j(n)\not\equiv 0 \pmod{\pi^{m_{\mathfrak{p}}^j+1}},$$

и потому хотя бы один из коэффициентов многочлена $\pi^0 g_0^j(x)+\ldots$ $\ldots+\pi^{m_{\mathfrak{p}}^j}g_{m_{\mathfrak{p}}^j}(x)$ не делится на $\pi^{m_{\mathfrak{p}}^j+1}$. По определению l из этого следует, что $l\leqslant m_{\mathfrak{p}}^j$. Остается заметить, что степень $\sum_{k=0}^{l} f_k^j(x)\pi^k$ не превышает $a+m_{\mathfrak{p}}^j$, и просуммировать эти оценки по j.

Б. Для целочисленных л.р.п. $\{u_n\}$ многочлены P_i в формуле (3) обладают следующим свойством: для любого изоморфизма Ψ поля K над $\mathbf{Q}$ из $\alpha_j=\Psi(\alpha_i)$ следует $P_j=\Psi(P_i)$. Действительно,

$$\sum_i \Psi(\alpha_i^n)\,\Psi(P_i(n))=\Psi(u_n)=u_n=\sum_j \alpha_j^n P_j(n)$$

и известно [4], что выражения вида (3) определяют одну и ту же функцию, только если они совпадают. Опять выполнено сравнение $\alpha_i^{r_q}\equiv 1 \pmod q$ в кольце $\mathbf{Z}_K$, то есть $\alpha_i^{r_q}=1+q\beta_i$, причем если $\alpha_j=\Psi(\alpha_i)$, то, очевидно, $\beta_j=\Psi(\beta_i)$. Произведем те же преобразования, что и при доказательстве А, с заменой $\mathfrak{p}^t$ на (q) и p на q. Теперь многочлены $\sum_i Q_{ij}(x)\beta_i^k$ имеют рациональные коэффициенты, так как они неподвижны при всех изоморфизмах K над $\mathbf{Q}$. Для получения формулы (4) применим оценку $v_q\left(q^k\binom{x}{k}\right)\geqslant k-\frac{k}{2}=\frac{k}{2}$ и положим $g_k{}^j(x)$ равным $q^{k-1}\binom{x}{2k-1}\sum_i Q_{ij}\beta_i^{2k-1}+q^k\binom{x}{2k}\sum_i Q_{ij}\beta_i^{2k}$. Далее рассуждаем, как в пункте А, учитывая, что степень $g_k{}^j$ равна $2k+a$. Следствие 1 применим для случая $K=\mathbf{Q}$, $\mathfrak{p}=(q)$. Доказательство закончено.

Следствие 2. *Имеется алгоритм, определяющий по данной л. р. п., конечно ли множество ее нулей, и вычисляющий верхнюю границу числа ее нулей, если оно конечно.*

Доказательство. Идеал $\mathfrak{p}$ и все числа $r_{\mathfrak{p}}$, $m^i_{\mathfrak{p}}$ можно найти эффективно по данной л. р. п. Если хотя бы одно $m^i_{\mathfrak{p}}$ бесконечно, то и множество нулей бесконечно, если же все $m^i_{\mathfrak{p}}$ конечны, то применим оценку из пункта А теоремы.

Вычисление идеала $\mathfrak{p}$ и чисел $r_{\mathfrak{p}}$, $m^i_{\mathfrak{p}}$ требует много времени. Хотелось бы иметь способ вычисления верхних оценок, не требующий вычислений в кольцах алгебраических чисел. Такой способ дает теорема 2, используемая вместе с пунктом Б теоремы 1.

Теорема 2. *Пусть* $Q(x)=\varphi_1^{\nu_1}\cdot\ldots\cdot\varphi_s^{\nu_s}$ — *разложение собственного многочлена на неприводимые над* $\mathbf{Q}[x]$ *множители,* $f(x)=\varphi_1\cdot\ldots\cdot\varphi_s$, q — *простое число, не делящее дискриминант* D *многочлена* $f(x)$ *и свободный коэффициент* b *многочлена* $f(x)$, $q\geqslant\max\{3,a\}$. *Если* r_q *в определении 2 заменить числом* $S=q^{d!}\prod_{i=1}^{d!}(q^i-1)^{\left[\frac{d!}{i}\right]}$ *и соответственно изменить* $m_q{}^i$, *то выполнена оценка пункта Б теоремы 1.*

Доказательство. Допустим, главный идеал (q) имеет общие множители с (α_i), тогда (q) имеет общие множители и с $(b)=(\alpha_1)\cdot\ldots\cdot(\alpha_m)$. Но идеалы (q) и (b) взаимно просты, поэтому (q) и (α_i) взаимно просты.

Докажем, что если $\mathfrak{q}$ — простой идеал, делящий q, то $\nu_{\mathfrak{q}}(P_i)\geqslant 0$. Будем считать P_i многочленами с $(a+1)$ коэффициентом (a — наибольшая из степеней). Тогда эти коэффициенты однозначно определяются по $m(a+1)$ начальным значениям л. р. п. Матрица соответствующей линейной системы такова: $(x^i\alpha_j{}^x)$, $0\leqslant i\leqslant a$, $1\leqslant j\leqslant m$, $0\leqslant x<m(a+1)$, i и j определяют строку, а x — столбец. Определитель Δ этой системы (см. [6], § 7.8) равен $\left(\prod_{t=1}^{(a-1)}t!\right)^m b^{\frac{a(a-1)}{2}}D^{\frac{a^2}{2}}$.

Из условий, наложенных на q, следует, что $\mathfrak{q}$ взаимно просто с Δ, и поэтому показатели вхождения $\mathfrak{q}$ в компоненты решения системы неотрицательны (все коэффициенты расширенной матрицы системы — $\mathfrak{q}$-целые числа).

Очевидно, что если в определении 2 в качестве r_q взять любое кратное $\varphi((q))$, то теорема 1 останется верной, так как единственным использованным свойством r_q было $\alpha_i^{r_q}\equiv 1\pmod q$. Мы утверждаем, что $\varphi((q))\mid S$ и, следовательно, $\alpha^S\equiv 1\pmod q$. Пусть n есть степень $\mathbf{Q}(\alpha_1,\ldots,\alpha_m)$ над $\mathbf{Q}$. Тогда $n\mid d!$. Известно, что

$$\varphi((q))=N((q))\prod_{\mathfrak{p}_i\mid q}\left(1-\frac{1}{N(\mathfrak{p}_i)}\right)=q^n\prod\left(1-\frac{1}{q^{f_i}}\right),$$

где N обозначена норма идеала; произведение нужно взять по всем простым идеалам, делящим q; f_i — степень инерции идеала $\mathfrak{P}_i$. Так как $\Sigma f_i\leqslant n$, легко убедиться, что $\varphi((q))\mid S$.

Доказательство теоремы закончено.

Теорема 2 дает следующий алгоритм вычисления верхней оценки числа нулей л. р. п.: 1) разложение собственного многочлена на неприводимые множители и отыскание дискриминанта $f(x)$; 2) отыскание простого q, удовлетворяющего условию теоремы 2; 3) вычисление числа S и $m_q{}^i$ и вычисление верхней оценки по формуле из пункта Б теоремы 1.

Приведем без доказательства очень грубую оценку количества нулей л. р. п., получаемую путем грубой оценки r_q, $m_q{}^i$, q.

Следствие 3. *Для целочисленной л. р. п.* $\{u_n\}$ *порядка* d *с конеч ным множеством нулей имеет место неравенство*

$$|\{n \mid u_n = 0\}| \ll \log_2 C\,(6H)^{2d^2d!},$$

где H — *высота собственного многочлена,* $C = \max\{2, |u_0|, \ldots, |u_{d-1}|\}$

СПИСОК ЛИТЕРАТУРЫ

1. Mahler K. Eine arithmetische Eigenschaft Taylorschen Koeffitienten rationale Funktionen. — Koninkl. Akad. wetensch. Amst., 1935, **38**, N 1, 50—60.
2. Berstel J., Mignotte M. Deux problemes decidables des suites recurrentes li neares. — Bull. Soc. math. France, 1976, **104**, 175—184.
3. Skolem T. Ein Verfahren zur Behandlung gewisser exponentialer und diophanti scher Gleichungen. — C. r. VIII congr. math. à Stockholm, 1934, p. 163—188.
4. Salomaa A., Soittola M. Automata-theoretic aspects of formal power series Berlin, 1978.
5. Боревич З. И., Шафаревич И. Р. Теория чисел. М., 1972.
6. Фельдман Н. И. Приближения алгебраических чисел. М., 1981.

Поступила в редакцию
10.05.84