Задачи о линейных рекуррентах

А. Я. Канель-Белов

В «Математическом просвещении», сер. 3, вып. 12, с. 236, опубликована

Задача 12.12 (теорема Сколема — Малера — Леха[1]). *Линейной рекуррентой порядка n* называется такая последовательность $\{u_k\}$, что при всех k

$$a_0 u_{k+n} + a_1 u_{k+n-1} + \ldots + a_n u_k \equiv 0,$$

где a_i — некоторые константы, не все равные нулю одновременно. *Нулём* линейной рекурренты называется такое k, что $u_k = 0$. Докажите, что множество нулей линейной рекурренты есть объединение конечного набора точек и конечного набора арифметических прогрессий.

(*Предложил А. Я. Канель*)

Понятие линейной рекурренты играет важную роль во многих математических задачах. Первоначальные сведения о линейных рекуррентах содержатся в брошюре [4].

I. Напомним классический факт:

Теорема 1. *Дана линейная рекуррента $A = \{a_n\}$ порядка k, где*

$$a_{n+k} = b_1 a_{n+k-1} + \ldots + b_k a_n. \tag{1}$$

Тогда её общий член a_n имеет вид

$$a_n = \sum_i \lambda_i^n P_i(n), \tag{2}$$

где λ_i — корень характеристического уравнения

$$x^k = b_1 x^{k-1} + \ldots + b_k$$

некоторой кратности k_i, а P_i — многочлен степени не выше $k_i - 1$.

[1] Сколем [9] доказал эту теорему для рациональных чисел, Малер [8] — для алгебраических, Лех [7] — для любого поля характеристики 0.

Доказательство основано на следующих соображениях. Пусть τ — *оператор сдвига*, переводящий последовательность с n-м членом a_n в последовательность с n-м членом a_{n+1}. Тогда наша линейная рекуррента $A = \{a_n\}$ удовлетворяет условию

$$(\tau^k - b_1\tau^{k-1} - \ldots - b_k)A = 0.$$

Оператор $Q = \tau^k - b_1\tau^{k-1} - \ldots - b_k$ можно представить в виде

$$Q = \tau^k - b_1\tau^{k-1} - \ldots - b_k = \prod_{i=1}^{m}(\tau - \lambda_i)^{k_i}.$$

Как известно, аннулятор такого оператора состоит из последовательностей, удовлетворяющих условию (2).

С другой стороны, линейная рекуррента порядка k однозначно задаётся своими первыми k членами, которые можно выбрать произвольным образом. Поэтому пространство последовательностей, удовлетворяющих равенству (1), имеет размерность k. Но пространство последовательностей, удовлетворяющих равенству (2), имеет ту же размерность k, так что эти пространства совпадают. Теорема доказана. □

Упражнение. Пусть $\{a_n\}$ — линейная рекуррента, как в теореме 1. Тогда её *производящая функция* $f(x) = \sum_{n=0}^{\infty} a_n x^n$ имеет вид $f(x) = P(x)/Q(x)$, где $\deg(P) < \deg(Q)$, $Q(x)$ — характеристический многочлен для $\{a_n\}$.

Замечание 1. Аналогичное утверждение (с похожим доказательством) есть в матанализе. Рассмотрим дифференциальное уравнение с постоянными коэффициентами:

$$a_0 y^{(n)} + a_1 y^{(n-1)} + \ldots + a_n y = 0.$$

Тогда его решение имеет вид

$$y = \sum_i e^{\lambda_i x} P_i(x), \tag{3}$$

где λ_i — корень *характеристического уравнения*

$$x^k = b_1 x^{k-1} + \ldots + b_k$$

некоторой кратности k_i, а P_i — многочлен степени не выше $k_i - 1$.

В доказательстве теоремы 1, равно как и её родственника в теории дифференциальных уравнений, применяется идея *линейной суперпозиции*. Например, при исследовании линейных дифференциальных уравнений с ненулевой правой частью используется *функция Грина*.

Поясним её физический смысл. Пусть нам надо исследовать напряжение $T(y)$, $y \in B$, при граничной нагрузке $P(x)$, где $x \in S$ — точка поверхности. Рассматривается случай, когда нагрузка P сосредоточена в одной точке x (т. е. является дельта-функцией), находят напряжение $G(y, x)$, а потом суммируют с весами, пропорциональными значениям функции P, т. е. получают соотношение вида

$$T(y) = \int_x G(y, x)P(x).$$

Замечание 2. Приведём подборку олимпиадных задач, где эта идея также работает.

1. В клетки шахматной доски записаны числа от 1 до 64 (в первой горизонтали слева направо идут числа от 1 до 8, во второй — от 9 до 16, и т. д.). Перед некоторыми числами поставлены плюсы, перед остальными — минусы, так что в каждой вертикали и в каждой горизонтали 4 плюса и 4 минуса. Докажите, что сумма всех чисел равна нулю.
2. По кругу расставлены 128 натуральных чисел. За один ход между всеми соседними числами записывают их сумму, а старые числа стирают. Докажите, что через несколько ходов все числа будут делиться на 128.
3. В вершинах правильного 100-угольника расставлены целые числа. Каждую минуту каждое из чисел заменяется на свою разность с числом, следующим за ним по часовой стрелке. Докажите, что через 5 минут сумма чисел в вершинах любого правильного 20-угольника с вершинами в вершинах нашего 100-угольника будет делиться на 5.
4. Правильный треугольник разбит прямыми, параллельными его сторонам, на равные между собой правильные треугольники. Один из маленьких треугольников чёрный, остальные — белые. Разрешается перекрашивать одновременно все треугольники, пересекаемые прямой, параллельной любой стороне исходного треугольника. Всегда ли можно с помощью нескольких таких перекрашиваний добиться того, чтобы все маленькие треугольники стали белыми?
5. В правильном десятиугольнике проведены все диагонали. Возле каждой вершины и каждой точки пересечения диагоналей поставлено число +1 (рассматриваются только сами диагонали, а не их продолжения). Разрешается одновременно изменить все знаки на одной стороне или одной диагонали. Можно ли с помощью нескольких таких операций изменить все знаки на противоположные?

6. Стороны правильного треугольника разделены на n частей. Через получившиеся точки проведены прямые, параллельные сторонам. Внутри получившихся треугольников записаны ± 1 так, что каждое число внутри исходного треугольника равно произведению соседей (по сторонам маленького треугольника). Покажите, что в треугольниках при вершинах записаны одинаковые числа.
7. а) Рассмотрим множество непрерывных функций на отрезке $[0, 2n]$, таких, что $F(0) = 0$ и на любом интервале $(k, k+1)$, где k целое, производная равна либо $+1$, либо -1. Каких функций больше: неотрицательных или таких, что $F(2n) = 0$?
   б) Как подсчитать число таких функций, что $-n/3 < F(x) < n/3$?
   (См. задачи 11.7, вып. 11, с. 163, и 11.7′, вып. 26, с. 269, а также их решения, вып. 27, с. 251–254).
8. Бесконечная в обе стороны полоса клетчатой бумаги состоит из чёрных и белых клеток. Каждую секунду клетка, имеющая чётное число чёрных соседей, становится белой, а имеющая нечётное число чёрных соседей — чёрной. Докажите, что:
   а) если через 2^n секунд исходная раскраска повторится, то она периодична с периодом $3 \cdot 2^n$;
   б) исходная раскраска периодически повторяется тогда и только тогда, когда она сама периодична (т. е. периодичность во времени равносильна периодичности в пространстве).
   в) Что можно сказать о полосе произвольной ширины? Или о всей клетчатой плоскости?
9. В каждой вершине пятиугольника записано некоторое число, меньшее 1000, причём сумма всех этих чисел равна 0. Каждое число заменяется полусуммой соседних чисел, и эта операция проводится 1000 раз. Докажите, что после этого каждое из чисел будет меньше 1.
10. На плоскости дано 239 прямых общего положения. Докажите, что в областях, на которые эти прямые разбивают плоскость, можно расставить ненулевые целые числа так, чтобы для каждой из прямых было выполнено следующее условие: сумма чисел в каждой из полуплоскостей, определяемых этой прямой, равна нулю.
11. Правильный $4k$-угольник разрезан на параллелограммы. Докажите, что среди них не менее k прямоугольников. Найдите их общую площадь, если сторона $4k$-угольника равна a.

II. Приведём теперь несколько полезных фактов про линейные рекурренты.

Предложение 2. *Пусть линейная рекуррента удовлетворяет системе линейных рекуррентных соотношений порядков* k_i:

$$b_0^{(i)} a_n + b_1^{(i)} a_{n-1} + \ldots + b_{k_i}^{(i)} a_{n-k_i} = 0, \quad i = 1, \ldots, s.$$

Тогда все эти соотношения следуют из одного:

$$c_0 a_n + b_1 a_{n-1} + \ldots + c_k a_{n-k} = 0.$$

Если коэффициенты исходной системы рациональны, то и коэффициенты c_i *тоже рациональны.*

Доказательство. Рассмотрим характеристические многочлены

$$P_i(x) = b_0^{(i)} x^{k_i} + b_1^{(i)} x^{k_i - 1} + \ldots + b_{k_i}^{(i)} = 0, \quad i = 1, \ldots, s.$$

Заметим следующее.

1. Если линейная рекуррента удовлетворяет характеристическому уравнению с многочленом P, то для любого многочлена Q она удовлетворяет характеристическому уравнению с многочленом PQ.
2. Если линейная рекуррента удовлетворяет характеристическим уравнениям с многочленами P_1, P_2, то для любых коэффициентов λ_1, λ_2 она удовлетворяет характеристическому уравнению с многочленом $\lambda_1 P_1 + \lambda_2 P_2$.
3. И, следовательно, если линейная рекуррента удовлетворяет характеристическим уравнениям с многочленами P_1, P_2, то для любых многочленов Q_1, Q_2 она удовлетворяет характеристическому уравнению с многочленом $Q_1 P_1 + Q_2 P_2$.

Действительно, соотношения можно естественным образом умножать на константы и складывать. Соответствующие операции производятся и с характеристическими многочленами. Кроме того, соотношение можно *сдвигать*, т. е. переходить от соотношения

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0$$

к его следствию

$$d_0 a_{n+1} + d_1 a_{n-1} + \ldots + d_m a_{n-m+1} = 0.$$

Этому переходу отвечает умножение характеристического многочлена на переменную x. Осуществляя сдвиги последовательно, мы можем умножать характеристический полином и на x^k.

Остаётся отметить, что (как и у целых чисел) наибольший общий делитель D системы многочленов P_i от одного переменного есть их линейная комбинация $D = \sum_i Q_i P_i$ для некоторых многочленов Q_i. Предложение доказано. □

Предложение 3. *Если все члены линейной рекурренты рациональны, то и все коэффициенты d_i задающего её соотношения*

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0$$

тоже рациональны.

Первое доказательство. В силу предыдущего предложения достаточно рассмотреть соотношение минимальной степени. Условие, что *фиксированная последовательность* $\{a_n\}$ удовлетворяет соотношению

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0,$$

можно записать как (бесконечную) систему линейных уравнений с коэффициентами из множества $\{a_n\}$ (где d_i — неизвестные, a_i — коэффициенты). Предложение вытекает из следующей леммы:

Лемма 4. (*а*) *Любая система линейных уравнений от конечного числа переменных равносильна своей конечной подсистеме.*

(*б*) *Пусть дана* (*вообще говоря бесконечная*) *система линейных уравнений с рациональными коэффициентами. Если она имеет ненулевое решение, то она имеет и ненулевое рациональное решение.*

Доказательство. (а) Рассмотрим первое уравнение, выразим одну из неизвестных через другие и подставим в остальные уравнения. Те уравнения, в которых все коэффициенты окажутся нулевыми, вычеркнем. Далее берём любое из оставшихся уравнений и опять выразим какую-либо неизвестную через другие, и т. д. Поскольку число неизвестных конечно, процесс остановится на некотором шаге. Система равносильна совокупности тех уравнений, которые мы использовали для выражения неизвестных.

Замечание. То же верно и для системы полиномиальных уравнений. *Теорема Гильберта о базисе* утверждает, что любая система полиномиальных уравнений произвольной степени от ограниченного числа переменных равносильна конечной подсистеме. См. решение задачи 4.12 (выпуск 18, с. 265), а также задачу 11.12 (выпуск 11, с. 164).

(б) В силу п. (а) достаточно рассмотреть систему из конечного числа уравнений. Как и при решении п. (а), последовательно исключаем переменные. При этом рациональность коэффициентов сохраняется. В конце концов мы избавимся от всех уравнений, но так как по условию система имеет ненулевое решение, при этом останутся *свободные параметры*, т. е. неизвестные, через которые остальные выражаются как линейные функции с рациональными коэффициентами. Остаётся

придать этим свободным параметрам ненулевые рациональные значения. Лемма доказана, а вместе с ней и предложение 3. □

□

Упражнение. В стаде 101 корова. Любые 100 из них можно разделить на два стада по 50 коров так, что общие веса стад будут равны. Докажите, что веса всех коров равны.

Упражнение. Решите задачу сперва для целых, потом для рациональных, потом для вещественных весов.

Второе доказательство. Выберем базис $\{e_i\}$ в векторном пространстве V над $\mathbb{Q}$, порождённом коэффициентами d_i нашей линейной рекурренты

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0.$$

Раскладывая выражение $d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m}$ по базису $\{e_i\}$, мы получаем набор коэффициентов при базисных векторах e_i. Поскольку все a_i рациональны, а векторы линейно независимы над $\mathbb{Q}$, сумма коэффициентов при каждом таком e_i должна равняться нулю, т. е.

$$d_0^{(i)}a_n + d_1^{(i)}a_{n-1} + \ldots + d_m^{(i)}a_{n-m} = 0, \tag{4}$$

где $d_j^{(i)}$ есть i-я координата числа d_j, рассматриваемого как вектор из V. Таким образом, рекуррентное соотношение

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0$$

равносильно системе линейных рекуррентных соотношений (4). А эта система в свою очередь, в силу предложения 2, равносильна одному линейному соотношению с рациональными коэффициентами. Предложение доказано. □

Лемма 5. *Рассмотрим линейную рекурренту, заданную соотношением*

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0 \tag{5}$$

минимальной степени. С каждым n свяжем вектор $f_n = (a_n, \ldots, a_{n-m+1})$. Пусть имеет место равенство

$$\sum_i \lambda_i f_i = 0. \tag{6}$$

Тогда при любом k справедливо равенство

$$\sum_i \lambda_i f_{i+k} = 0. \tag{7}$$

Доказательство. Поскольку равенство (5) устойчиво относительно сдвигов (справедливо для всех n), из него следует и соотношение

$$d_0 f_n + d_1 f_{n-1} + \ldots + d_m f_{n-m} = 0. \qquad (8)$$

Преобразуя выражение (6) с помощью соотношения (8), мы получим соотношение, в котором индексы i при всех f_i меньше m. А тогда, в силу минимальности m и, как следствие, линейной независимости f_i, $i = 1, \ldots, m-1$, все они окажутся нулями. Поскольку процесс преобразования остаётся тем же при сдвиге нумерации, аналогичное преобразование выражения (7) также приведёт к нулевому результату, что и доказывает лемму 5. □

Существует несколько другое доказательство леммы 5, основанное на том, что все соотношения между f_i следуют из соотношения (5), а подстановка $f_i \to f_{i+1}$, отвечающая сдвигу, сохраняет эти соотношения.

Нам потребуется ещё одна

Лемма 6. *В любой системе целочисленных m-мерных векторов $\{f_i\}$ можно указать конечную подсистему $\{f_j\}$ такую, что каждый вектор f_i будет целочисленной линейной комбинацией векторов из $\{f_j\}$.*

Доказательство. Проведём индукцию по m. Пусть $m = 1$, т. е. векторы — это целые числа. Пусть d — их НОД. Тогда в системе существует такая конечная совокупность элементов, что d является их целочисленной линейной комбинацией. Но тогда и любой элемент системы представляется в виде целочисленной линейной комбинации этих элементов.

Пусть $m > 1$ и для меньших размерностей лемма верна. Пусть НОД первых координат векторов системы равен d'. Найдётся конечная подсистема векторов, через первые координаты которых d' выражается в виде целочисленной линейной комбинации. Вычитая из каждого вектора исходной системы эту комбинацию, умноженную на подходящий коэффициент, получим систему, в которой первая координата каждого вектора равна нулю. По предположению индукции векторы этой системы выражаются через их конечную подсистему. А эта подсистема выражается через конечную совокупность векторов исходной системы, что и требовалось.

Лемма доказана. □

Замечания. (а) Верен аналог леммы при замене чисел на многочлены. При этом вместо целочисленной комбинации многочленов $P_i(x)$ следует рассматривать полиномиальную комбинацию $\sum P_i(x)Q_i(x)$.

(б) Для линейных комбинаций с неотрицательными коэффициентами аналогичное утверждение для одномерного случая имеет место (упражнение), а для многомерного — нет (тоже упражнение).

Предложение 7. *Если все члены линейной рекурренты целые, то в некотором задающем её минимальном соотношении*

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0$$

все коэффициенты d_i тоже целые и при этом $d_0 = 1$.

Доказательство. Коэффициенты d_i можно считать взаимно простыми в совокупности. Рассмотрим систему векторов $\{f_i\}$ (см. лемму 5). Применив лемму 6, найдём конечную подсистему $\{f_j\}$, $j < M$, через которую выражаются все f_i, в том числе f_M. Итак, имеет место равенство

$$f_M = \sum_{i=1}^{M-1} \lambda_j f_j.$$

Ввиду леммы 5 получаем при всех k:

$$f_{M+k} = \sum_{i=1+k}^{M-1+k} \lambda_j f_j.$$

Это означает, что наша линейная рекуррента обладает соотношением нужного типа:

$$a_{n+M} = \sum_{i=1}^{M} a_{n+M-i}c_i. \tag{9}$$

При этом характеристический многочлен для минимального соотношения

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0$$

делит характеристический многочлен для соотношения (9). Поскольку старший коэффициент последнего равен единице, а старший член произведения есть произведение старших членов, коэффициент d_0 тоже равен единице. Предложение 7 доказано. □

Рассмотрим линейную рекурренту

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0.$$

Пусть $a_k^{(\lambda)} = \lambda^k a_k$. Тогда

$$d_0a_n^{(\lambda)} + \lambda \cdot d_1a_{n-1}^{(\lambda)} + \ldots + \lambda^m \cdot d_ma_{n-m}^{(\lambda)} = 0,$$

так что характеристические многочлены для последовательностей $\{a_n\}$ и $\{a_n^{(\lambda)}\}$ будут равны соответственно

$$P(x) = d_0x^n + d_1x^{n-1} + \ldots + \cdot d_m$$

и

$$P_\lambda(x) = d_0x^n + \lambda \cdot d_1x^{n-1} + \ldots + \lambda^m \cdot d_m$$

и корни многочлена P_λ получаются из корней многочлена P умножением на λ.

Из наших рассмотрений следует

Предложение 8. *Дана целочисленная линейная рекуррента*

$$A\colon\ a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0.$$

Пусть p — простое число. Тогда при некотором рациональном μ линейная рекуррента $A^\mu\colon a_n^\mu = p^{n\mu}a_n$ задаётся соотношением

$$A^\mu\colon\ a_n^\mu + d_1^\mu a_{n-1} + \ldots + d_m^\mu a_{n-m} = 0,$$

где ${d_k}^\mu = d_k\mu^k$. При этом можно подобрать такое μ, для которого:

- *хотя бы один коэффициент d_i^μ является целым числом, не делящимся на p;*
- *все нецелые коэффициенты d_i^μ представимы в виде произведения целого числа на p в положительной рациональной степени.* □

III. Под *прополкой с шагом m* последовательности $\{a_n\}$ будем понимать последовательность $\{w_{m,k} = a_{m\cdot k+q_0}\}$, где k пробегает целые числа, а q_0 фиксированное целое. Прополка также является линейной рекуррентой, и при переходе к прополке собственные числа характеристического уравнения возведутся в m-ю степень, а кратность их не уменьшится, ибо

$$w_{m,k} = \sum_i P_i(m\cdot k + q_0)\lambda_i^{q_0}(\lambda_i^m)^k = \sum_i Q_i(k)\delta_i^k,$$

где

$$\delta_i = \lambda_i^m, \quad Q_i(x) = \lambda_i^{q_0}P_i(m\cdot x + q_0), \quad \deg(Q_i) = \deg(P_i).$$

При подходящем m (равном количеству ненулевых элементов факторкольца по модулю p) они будут сравнимы с 1 по модулю p.

При этом возможно уменьшение степени Q_i после сокращения членов, но это не может происходить при всех q_0, ибо полный набор всех таких прополок с фиксированным шагом m однозначно определяет исходную линейную рекурренту.

Будем считать, что выполнено следующее.

1. Числа λ_i не являются корнями из единицы, кроме случая $\lambda_i = 1$.
2. Отношение λ_i/λ_j не есть корень из единицы при всех $i \neq j$.
3. Любая прополка является линейной рекуррентой порядка строго больше 1.

Предложение 9. (*а*) *Пусть p — простое число, $A = \{a_n\}$ — целочисленная линейная рекуррента, хотя бы два коэффициента которой не делятся на p и при этом один из её членов не делится на p. Тогда в ней найдётся прополка, все члены которой не делятся на p.*

(*б*) *Пусть p — простое число, $A = \{a_n\}$ — линейная рекуррента, члены и коэффициенты которой принадлежат $\mathbb{Z}[p^{1/n}]$, хотя бы два коэффициента не делятся на p и при этом один из её членов не делится на $p^{1/n}$. Тогда в ней найдётся прополка, все члены которой не делятся на $p^{1/n}$.*

Доказательство. Утверждение сводится к следующему очевидному факту: дана линейная рекуррента над $\mathbb{Z}_p$ хотя бы с двумя ненулевыми коэффициентами и хотя бы одним ненулевым членом. Тогда члены в ней повторяются периодически и найдётся прополка, состоящая из ненулевых членов. □

Из вышеприведённого следует

Предложение 10. *Дана ненулевая линейная рекуррента с соотношением*

$$A\colon\ a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0.$$

Тогда для любого простого p найдётся её прополка вида $W\colon w_{k,n} = a_{k\cdot n+r}$ и целочисленная линейная рекуррента $C = \{c_n\}$, все члены которой взаимно просты с p, причём

$$w_{k,n} = D \cdot p^{q\cdot n} c_n, \quad D \in \mathbb{Z},\ q \geqslant 0,\ q \in \mathbb{Z}^+.$$

Если при этом все характеристические корни A не равны собственному корню из единицы, их отношения не являются корнями из единицы и их хотя бы два, то тем же свойством обладает и линейная рекуррента $\{b_n\}$.

IV. Вернёмся к задаче 12.12. Проведём подготовительную работу.

1. Среди коэффициентов a_i выберем *базис трансцендентности*, т. е. максимальное множество M алгебраически независимых в совокупности элементов. Любой другой коэффициент a_j выражается как корень некоторого неприводимого многочлена P_j с коэффициентами из $\mathbb{Q}[M]$. Выберем простое число p, достаточно большое в следующем смысле:

можно выбрать M так, что каждый многочлен P_j взаимно прост со своей производной и все его ненулевые коэффициенты остаются ненулевыми по модулю p.

Некоторые способы выбора базиса неэквивалентны, ибо есть соотношения на a_j, выполняющиеся при одном выборе базиса и не выполняющиеся при другом. Мы берём такое большое p, чтобы все эти неэквивалентности сохранить.

Замечание. Для читателя, знакомого с нестандартным анализом, достаточно сказать: выберем бесконечно большое простое число p и значения a_k, которые не имеют алгебраических зависимостей конечной степени с рациональными коэффициентами. Рекомендуем читателю книгу [5].

Рассмотрим теперь расширение $\mathbb{F}_q$, $q = p^\ell$, поля вычетов $\mathbb{Z}_p$, содержащее все выбранные коэффициенты. Построим расширение кольца *целых p-адических чисел*, связанное с $\mathbb{F}_q$. Известно, что поле $\mathbb{F}_q$ порождается одним элементом x степени ℓ над $\mathbb{Z}_p$. Это значит, что для некоторого неприводимого многочлена Q с коэффициентами из $\mathbb{Z}_p$ выполняется равенство $Q(x) = 0$. При этом Q — многочлен со старшим коэффициентом единица, не имеющий общих делителей со своей производной (можно считать $p > \ell$, поэтому $Q'(x) \neq 0$).

Коэффициенты многочлена Q равны остаткам от деления на p коэффициентов некоторого целочисленного многочлена $\widehat{Q}$ со старшим коэффициентом 1. Рассмотрим расширение кольца p-адических чисел элементом $\widehat{x}$ таким, что $\widehat{Q}(\widehat{x}) = 0$. Далее рассмотрим формальные степенные ряды

$$\sum_{i=0}^{\deg(Q)-1} \sum_{j=0}^{\infty} c_{ij} x^i p^j$$

с целыми c_{ij}. На них естественным образом определяются операции *сложения* и *умножения*, создающие структуру кольца R. Его редукция по модулю p есть $\mathbb{F}_q$. Это кольцо R по своим свойствам очень похоже на кольцо целых p-адических чисел, т. е. кольцо рядов $\sum_{k=0}^{\infty} c_k p^k$ с целыми c_k.

Теперь возьмём в качестве $a_i \in M$ произвольные элементы из R (с остатками $\bar{a}_i$ от деления на p), а в качестве остальных a_j — корни соответствующих многочленов P_j. Покажем, что они лежат в R. Для этого применим метод последовательных приближений.

В обычном вещественном анализе есть *метод Ньютона* построения корней. Пусть f — функция, z — её корень, $f'(z) \neq 0$. Возьмём

точку x, достаточно близкую к z, и из точки $(x, f(x))$ проведём касательную к графику функции f. Её пересечение с осью OX даст точку

$$x_1 = x - \frac{f(x)}{f'(x)},$$

являющуюся следующим приближением к z, и т. д. Пренебрегая изменением производной на маленьком отрезке $[z, x]$, имеем:

$$x_1 = x - \frac{f(x)}{f'(z)}.$$

Если z близко к x, то процесс достаточно быстро сойдётся к корню z функции f.

Аналогичный факт справедлив и для сравнений:

Лемма Гензеля. *Пусть* $Q(x) \equiv 0 \pmod p$, $Q'(x) \not\equiv 0 \pmod p$. *Тогда для любого* k *найдётся по модулю* p^k *единственное* y_k *такое, что* $Q(y_k) \equiv 0 \pmod{p^k}$.

Тем самым существует единственное решение уравнения $Q(y) = 0$ *в* p*-адических числах такое, что* $y \equiv x \pmod p$.

Предоставляем читателю доказать лемму Гензеля и её очевидное обобщение для кольца R.

Мы добились того, что все коэффициенты линейной рекурренты принадлежат кольцу R, причём $\bar{a}_0 \neq 0$, так что $a_0^{-1} \in R$. Поделив на a_0, можно считать, что $a_0 = 1$.

Переходя от последовательности к её прополкам, можно считать, что *все коэффициенты линейной рекурренты лежат в кольце* R, *а все корни характеристического уравнения сравнимы с единицей по модулю* p.

V. *О* p*-адической экспоненте и степенных рядах.* Следующее утверждение родственно лемме Гензеля.

Теорема 11. *Пусть* p *— простое число,* $a \equiv 1 \pmod p^k$, *но* $a \not\equiv 1 \pmod p^{k+1}$. *Тогда* $a^p \equiv 1 \pmod p^k$, *но при этом* $a^p \not\equiv 1 \pmod p^{k+2}$, *кроме случая* $p = 2$, $k = 1$.

Пример. Пусть $p = 2$, $a = 9$, $k = 3$. Тогда $a^p = a^2 = 81 \equiv 1 \pmod 8$, но $a^2 \not\equiv 1 \pmod{32}$.

Данное утверждение активно используется в олимпиадной практике. См. задачу 3.10 («Математическое просвещение», сер. 3, вып. 3, с. 233, авторы А. Ерошин и А. Белов; решение см. [3]). Приведём несколько полезных упражнений.

1. При каких n величина $2^n - 1$ делится на 5^{100}?
2. При каких n величина $5^n - 1$ делится на 2^{100}?

3. Пусть $p > 2$, n натуральное. Докажите, что среди остатков по модулю p^n, взаимно простых с p, есть *первообразный корень по модулю* p^n, т. е. такой, что остальные являются его степенями.
4. Пусть $n > 2$. Докажите, что среди остатков по модулю 2^n нет первообразного корня.
5. Укажите такое n, что в десятичном разложении числа 5^n имеется 1000 нулей, идущих подряд. Аналогичные вопросы про девятки и про степени двойки.

Над кольцом p-адических чисел можно рассматривать степенные ряды и элементарные функции. *Близость* означает, что разность делится на высокую степень p, понятие *сходимости* определяется естественным образом. В этой топологии множество p-адических чисел компактно. *Экспонента*, *синус*, *косинус* и т. п. определяются через степенные ряды

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \sin x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{n!}, \quad \cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{n!}.$$

Эти ряды сходятся при x, делящемся на p, если $p > 2$ (при $p = 2$ надо потребовать, чтобы x делился на $4 = p^2$) и удовлетворяют тем же функциональным соотношениям, что в вещественном случае. Например, докажем, что $e^{x+y} = e^x e^y$. Распишем e^{x+y}, e^x, e^y в виде рядов и раскроем скобки. Если коэффициенты в разности $e^{x+y} - e^x e^y$ сократятся, то функциональное соотношение установлено. Если нет, то они не сократятся и для привычных нам вещественных экспонент. Но тогда равенство $e^{x+y} = e^x e^y$ не имеет места и в нашем вещественном мире, что неверно. Аналогично устанавливаются теоремы сложения для синуса и косинуса.

VI. Решение задачи 12.12. Мы закончили подготовительную работу. Как отмечено в конце п. IV, линейная рекуррента состоит из прополок, каждая из которых имеет корни характеристического уравнения, сравнимые с единицей по модулю p, а общий вид её члена согласно теореме 1 представляет собой сумму произведений полинома на экспоненту, т. е. является аналитической функцией. Если у неё конечное число нулей, то задача решена.

Если же число нулей бесконечно, то у них есть предельная точка Z, являющаяся целым p-адическим числом. Теперь заметим, что если x делится на p, то ряд для бинома Ньютона $(1 + x)^z$ сходится при всех p-адических z и определяет аналитическую функцию. Аналогичное верно в кольце R и его расширениях. Значит, ряд Тейлора

для общего члена прополки в окрестности точки Z сходится при всех целых p-адических n, причём к нулю, поскольку Z — предельная точка нулей. Но тогда коэффициенты ряда нулевые, что означает, что его сумма — тождественный нуль.

Мы разбили линейную рекурренту на конечное число прополок, в каждой из которых либо конечное множество нулей, либо все члены нулевые, что и доказывает утверждение задачи.

Замечание 1. Если основное поле конечно или, более общо, состоит из алгебраических элементов, то последовательность нулей линейной рекурренты периодична (возможно, с предпериодом). Если же основное поле имеет положительную характеристику $p>0$ и содержит трансцендентный элемент t, то утверждение задачи перестаёт быть верным.

Пусть, например, $a_n=(t+1)^n-t^n-1$. Тогда $a_n=0\Leftrightarrow n=p^k$, $k\in\mathbb{N}$. В этом случае множество нулей устроено следующим образом. Рассмотрим такие n, что $a_n=0$. Разложив n в p-ичной системе счисления, рассмотрим множество таких n как множество слов над алфавитом $A=\{0,1,\dots,p-1\}$. Это *регулярный язык*. Иными словами, имеется конечный граф с начальной O и финальной T вершинами, рёбра которого помечены буквами из A, причём каждому пути из O в T отвечает p-ичная запись числа n, для которого $a_n=0$. В этом случае существует алгоритм, распознающий принадлежность произвольного натурального n множеству нулей. См. [6].

Замечание 2. Линейную рекурренту можно рассматривать как экспоненциально-полиномиальную функцию от одной переменной. Для большего числа переменных, как показала Джулия Робинсон, проблема наличия нуля алгоритмически неразрешима. С другой стороны, если основания экспонент лежат в поле характеристики $p>0$, то ситуация меняется. Пусть F — экспоненциально-полиномиальная функция от k переменных. С набором $(n_1,\dots,n_k)$ свяжем слово над алфавитом A^k из p^k символов, состоящее из последних цифр чисел $n_1,\dots,n_k$, предпоследних и т. д. Множеству наборов $(n_1,\dots,n_k)$ таких, что $F(n_1,\dots,n_k)=0$, отвечает регулярный язык, и искомый алгоритм существует. См. [6].

VII. Задача 20.4 («Математическое просвещение», сер. 3, вып. 28, с. 236). Последовательность $\{a_n\}$ называется *линейной рекуррентой порядка k*, если для некоторых $b_1,\dots,b_k$ при всех $n\geqslant k$ выполняется равенство $b_0a_n+b_1a_{n-1}+\dots+b_ka_{n-k}=0$. Пусть $b_0=1$, $a_i,b_i\in\mathbb{Z}$ при всех i. Докажите, что либо последовательность $\{a_n\}$ содержит член,

имеющий не менее 2016 различных простых делителей, либо множество натуральных чисел разбивается на непересекающиеся арифметические прогрессии, на каждой из которых наша рекуррента пропорциональна геометрической прогрессии. (*А. Я. Канель-Белов*)

Решение задачи 20.4. Пусть рекуррента не распадается на последовательности, пропорциональные геометрическим прогрессиям. Применяя процесс, описанный в предложении 10, найдём прополку вида $B\colon b_n = a_{k\cdot n+r}$, где

$$b_n = D \cdot \prod_i p_i^{q_i \cdot n} c_n, \quad q_i \geqslant 0,\ q_i \in \mathbb{Z},$$

$\{p_i\}$ есть набор всех простых делителей коэффициентов рекурренты, числа c_n не делятся на p_i при всех i, n и $D \in \mathbb{Z}$. Пусть s — натуральное число. Существует простое $P > p_i\ \forall\, i$, делящее c_s, а значит, и $a_{k\cdot s+r}$. Поскольку P не делит характеристические коэффициенты a_i, остатки по модулю P периодически повторяются без предпериода, и мы можем взять прополку как в A, так и в C, состоящую из членов, не делящихся на P. Применив предложение 10, построим прополку

$$B_n^1 = P \cdot D_1 \cdot \prod_i p_i^{q_i \cdot n} P^j c_n^1 = a_{k_1 \cdot n + r_1},$$

где c_n^1 не делятся на p_i, а также на P. Продолжая процесс дальше, на s-м шаге получим прополку

$$B_n^s = \prod_{j=1}^{s} P_j \cdot D_s \cdot \prod_i p_i^{q_{i,s} \cdot n} \prod_{j=1}^{s} P_j^{q'_{j,s}} c_n^s = a_{k_s \cdot n + r_s}.$$

Она состоит из членов, имеющих не менее s различных простых делителей. Поскольку s может быть сколь угодно большим, задача решена.

Замечание. Предложение 7 используется в следующей теореме.

Теорема Пизо. *Если $\alpha > 1$ — алгебраическое число, то следующие свойства равносильны.*

- *Дробная часть числа $\{\alpha^n\}$ стремится к константе при $n \to \infty$.*
- *Число α есть число Пизо, т. е. является корнем уравнения $P(x) = 0$ с целыми коэффициентами и со старшим коэффициентом 1, причём $|\alpha| > 1$, а все остальные корни многочлена P по модулю строго меньше единицы.*

Числам Пизо был посвящён проект на 12 Летней конференции Международного математического Турнира городов в 2000 году, см. [10].

Позднее А. А. Егоров по мотивам этого проекта опубликовал две статьи в «Кванте» [1], [2]. Предложение 7 обсуждается в [2].

Про дробные части степеней трансцендентных чисел мало что известно. Не установлено, может ли предел дробной части степеней вообще существовать (кроме тривиального случая $|\alpha| < 1$). Известно только, что множество чисел, превосходящих единицу, дробная часть которых имеет предел, не более чем счётно. (См. задачу 24.9, вып. 24, с. 176; решение, вып. 27, с. 260–262.)

Список литературы

[1] *Егоров А.* Числа Пизо // Квант. 2005. № 5. С. 8–13.

[2] *Егоров А.* Числа Пизо (окончание) // Квант. 2005. № 6. С. 9–13.

[3] *Ерошин А. Е.* Периодические десятичные дроби // Математическое просвещение. Сер. 3. Вып. 8. М.: МЦНМО, 2004. С. 239–245.

[4] *Маркушевич А. И.* Возвратные последовательности. М.: Наука, 1983.

[5] *Успенский В. А.* Что такое нестандартный анализ? М.: Наука, 1987.

[6] *Chilikov A. A.*, *Belov A. Ya.* Exponential Diophantine equations in rings of positive characteristic // Journal of knot theory and its ramifications. 2020. Vol. 29, № 2.

[7] *Lech C.* A Note on Recurring Series // Ark. Mat. 1953. Vol. 2. P. 417–421.

[8] *Mahler K.* Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen // Proc. Akad. Wetensch. Amsterdam. 1935. Vol. 38. S. 50–60.

[9] *Skolem Th.* Einige Sätze uber gewisse Reihenentwicklungen und Exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen. Oslo Vid. akad. Skrifter, I(6). 1933.

[10] `https://www.turgor.ru/lktg/2000/index.php`.

Алексей Яковлевич Канель-Белов, университет Бар-Илана (Израиль)
`kanel@mccme.ru`