Решения задач из прошлых выпусков

16.4. Условие. (Исправленный текст см. МП № 18, с. 270.) Ограничена ли последовательность $\{a_n\}$, заданная рекуррентно: $a_1 = 1$, $a_2 = x$; $a_{n+1} = \dfrac{a_n^2 - 1}{a_{n-1}}$, $x \in (-2, 2)$? (*К. Н. Игнатьев*)

Ответ: ограничена.

Решение (см. Б. Рабинович, Об одной последовательности. Вестник трудов ДНТТМ. Москва, 1990, стр. 4–6). Положим $\varphi = \arccos(x/2)$. Заметим, что $\sin\varphi \neq 0$, поскольку $x \in (-2, 2)$. Достаточно показать, что $a_n = \dfrac{\sin n\varphi}{\sin\varphi}$, тогда $|a_n| \leqslant \dfrac{1}{\sin\varphi}$. При $n = 1, 2$ равенство проверяется непосредственно. Пусть $n \geqslant 2$, проведём переход к $n + 1$. Нужно показать, что

$$\sin(n+1)\varphi = \frac{\sin^2 n\varphi - \sin^2\varphi}{\sin(n-1)\varphi}.$$

Преобразуем числитель правой части:

$$\begin{aligned}&(\sin n\varphi + \sin\varphi)(\sin n\varphi - \sin\varphi) = \\ &\qquad = 2\sin\frac{(n+1)\varphi}{2}\cdot\cos\frac{(n-1)\varphi}{2}\cdot 2\sin\frac{(n-1)\varphi}{2}\cdot\cos\frac{(n+1)\varphi}{2} = \\ &\qquad\qquad = \sin(n+1)\varphi\cdot\sin(n-1)\varphi,\end{aligned}$$

что и требовалось. (*Б. Рабинович*)

16.9. Условие. В алфавите анчурского языка есть лишь три буквы: A, B и C. Два разных слова обозначают одно и то же понятие, если одно из них может быть получено из другого с помощью следующих операций, которые можно проводить в любой последовательности и в любых количествах:

1) в любом месте слова можно заменять друг на друга следующие комбинации букв: ABA на BAB, ACA на CAC или BC на CB (и наоборот);

2) из любого места можно выкидывать две одинаковые буквы, идущие подряд, а также в любое место можно вставлять две одинаковые буквы.

а) Конечное или бесконечное количество понятий можно выразить с помощью этого языка? Если конечное, то сколько?

б) Тот же вопрос, если замена BC на CB запрещена, однако разрешена замена BCB на CBC. (*В. О. Бугаенко*)

в) Тот же вопрос, если в алфавите всего две буквы A и B, свойство 2 сохраняется и из любого места можно выкидывать $(AB)^n$ и в любое место вставлять это выражение. (*А. Я. Канель-Белов*)

Ответ: а) 24; б) бесконечное; в) $2n$.

Решение. Для удобства начнём с пункта б).

б) Рассмотрим разбиение плоскости на равные правильные треугольники тремя семействами параллельных прямых, образующих углы 60° друг с другом. Выделим один из треугольников и назовём его **исходным**. Прямые, содержащие стороны исходного треугольника, обозначим a, b, c и будем считать их соответствующими буквам A, B и C алфавита соответственно. Каждому слову поставим в соответствие треугольник, получающийся из исходного треугольника последовательными зеркальными отражениями относительно прямых, соответствующих буквам слова.

Оказывается, при этом словам, выражающим одинаковые понятия, будет соответствовать один и тот же треугольник. Действительно, фрагмент слова, состоящий из одинаковых букв, означает двойное отражение относительно одной прямой, т. е. тождественное преобразование. Фрагмент ABA означает отражение относительно прямой, проходящей через точку пересечения прямых a и b и образующей с каждой из них угол $\pi/3$. То же самое означает фрагмент BAB. Аналогично рассматриваются пары (ACA, CAC) и (BCB, CBC).

Докажем, что каждому из треугольников разбиения соответствует по крайней мере одно слово. Для этого нужно показать, что для любого треугольника разбиения существует композиция отражений относительно прямых a, b и c, переводящая исходный треугольник в него. Как было замечено выше, если s_a, s_b и s_c — симметрии относительно трёх прямых, пересекающихся в одной точке под углом $\pi/3$, то каждая из них выражается в виде композиции двух других (а именно, $s_c = s_a \circ s_b \circ s_a$, аналогично s_a и s_b). Из этого наблюдения легко вывести, что симметрия относительно любой прямой разбиения выражается в виде композиции симметрий относительно сторон исходного треугольника. Поэтому достаточно найти композицию симметрий относительно любых прямых разбиения (а не только сторон исходного треугольника), переводящую исходный треугольник в произвольно заданный. Соединим эти два треугольника цепочкой смежных треугольников. Для каждой пары смежных треугольников отражение относительно их общей стороны переводит один из них в другой. Значит, композиция этих отображений переводит начальный треугольник цепочки в конечный.

Взяв по слову, соответствующему каждому из треугольников разбиения, получаем бесконечное число слов, обозначающих различные понятия.

а) Теперь покажем, что в случае (а) количество различных понятий не превосходит 24. Так же как и в случае (б) поставим в соответствие буквам сло́ва некоторые осевые симметрии. Оси, соответствующие буквам A и B, а также буквам A и C, должны образовывать между собой угол 60°. Оси, соответствующие буквам B и C, должны быть перпендикулярны. Таким образом, образуемый ими треугольник должен иметь углы 60°, 60° и 90°. Разумеется, такого треугольника не существует на евклидовой плоскости, однако его можно построить на сфере. Отражая этот треугольник относительно сторон, получим замощение сферы равными треугольниками, подобно тому как в случае (б) мы получили замощение плоскости равными правильными треугольниками. Как и в случае (б), слова, означающие одинаковые понятия, соответствуют одному и тому же треугольнику разбиения. Различие в том, что количество треугольников разбиения в этом случае конечно, а именно равно 24. Таким образом, количество различных понятий языка не меньше 24.

Выпишем по одному слову, соответствующему каждому из треугольников разбиения: $\varnothing$, A, B, C, AB, BA, AC, CA, BC, ABA, ACA, ABC, BAC, BCA, CAB, $ABAC$, $ABCA$, $ACAB$, $BACA$, $BCAB$, $ABACA$, $ABCAB$, $BACAB$, $ABACAB$. Доказательство того, что любое слово эквивалентно одному из перечисленных, оставляем читателю в качестве самостоятельного упражнения. (*В. О. Бугаенко*)

в) Назовём слово *неуменьшаемым*, если оно не эквивалентно никакому слову меньшей длины. Неуменьшаемые слова не содержат подслов вида AA и BB, значит, они — подслова периодической последовательности $(AB)^\infty = \ldots ABABABABA \ldots$ Далее, в неуменьшаемом слове подслово AB не может повторяться n раз подряд. При этом

$$(BA)^n = A^2(BA)^n = A(AB)^n A = A^2 = \varnothing.$$

Поэтому все неуменьшаемые слова есть подслова в $(AB)^{n-1}A$ или $B(AB)^{n-1}$. Всего таких подслов $2n$.

Остаётся показать, что все они различны. Пусть A обозначает осевую симметрию правильного n угольника, B — симметрию относительно оси, повёрнутой на угол π/n. Легко видеть, что A и B порождают все движения n-угольника, а всего таких движений $2n$. Задача решена.

(*А. Я. Канель-Белов*)

17.10. Условие. Дано векторное пространство W, $\dim W = m$, два его подпространства U и V такие, что $U \cap V = 0$ ($\dim U = n_1$, $\dim V = n_2$), и обратимый оператор $A\colon W \to W$. Докажите, что $A^n(U) \cap V = 0$ при некотором $n \leqslant \min\left(\binom{m}{n_1}, \binom{m}{n_2}\right)$. (*Фольклор*)

Решение. Пусть $n = n_1$, и пусть $\{e_1, \ldots, e_m\}$ — базис пространства W, причём векторы $e_1, \ldots, e_n$ составляют базис подпространства U. Рассмотрим пространство внешних форм порядка n над W, т.е. n-линейных кососимметричных функций на W со значениями в основном поле. В этом пространстве имеется базис B из $r := \binom{m}{n}$ форм вида $e_{i_1} \wedge \ldots \wedge e_{i_n}$, $1 \leqslant i_1 < \ldots < i_n \leqslant m$, которые равны 1 на $\{e_{i_1}, \ldots, e_{i_n}\}$ и 0 на любом наборе $\{e_{j_1}, \ldots, e_{j_n}\}$, где хотя бы одно из $j_1, \ldots, j_n$ не равно ни одному из $i_1, \ldots, i_n$.

Далее, рассмотрим набор из $r + 1$ форм $e_1 \wedge \ldots \wedge e_n$, $Ae_1 \wedge \ldots \wedge Ae_n$, $\ldots$, $A^r e_1 \wedge \ldots \wedge A^r e_n$. Некоторая их линейная комбинация, в которой не все коэффициенты нулевые, равна 0. Если $e_1 \wedge \ldots \wedge e_n$ входит в неё с нулевым коэффициентом, применим к ней оператор A^{-1}. Повторяя, если нужно, эту процедуру и добавляя слагаемые с нулевыми коэффициентами, придём к соотношению вида

$$e_1 \wedge \ldots \wedge e_n = \sum_{k=1}^{r+1} \lambda_k A^k e_1 \wedge \ldots \wedge A^k e_n. \qquad (*)$$

Пусть при любом $k = 1, \ldots, r$ найдутся такие коэффициенты $c_{k1}, \ldots, c_{kn}$, не все равные 0, что

$$\sum_{i=1}^{n} c_{ki} A^k e_i \in V.$$

При каждом k один из ненулевых коэффициентов можно взять равным 1. Например, пусть $c_{k1} = 1$. Тогда

$$A^k e_1 \wedge \ldots \wedge A^k e_n = \left(\sum_{i=1}^{n} c_{ki} A^k e_i\right) \wedge \ldots \wedge A^k e_n.$$

Выражение в скобках является линейной комбинацией векторов e_j, $j > n$, и потому левая часть равенства есть линейная комбинация выражений вида $e_{j_1} \wedge \ldots \wedge e_{j_n}$, где хотя бы одно из $j_1, \ldots, j_n$ больше n. Это верно для каждого слагаемого в правой части $(*)$. Следовательно, $e_1 \wedge \ldots \wedge e_n$ является линейной комбинацией других элементов из B, что невозможно. Полученное противоречие означает, что $A^k U \cap V = 0$ при некотором k, $1 \leqslant k \leqslant r = \binom{m}{n_1}$.

Заменив A на A^{-1} и поменяв местами U и V, получаем, что $A^{-\ell} V \cap U = 0$ при некотором ℓ, $1 \leqslant \ell \leqslant \binom{m}{n_2}$. Поскольку отображение A обратимо, $A^\ell U \cap V = A^\ell(U \cap A^{-\ell} V) = 0$. Этим доказано утверждение задачи. (*А. Скутин*)

18.2. Условие. Последовательность функций задана следующим образом: $Q_1(x) = x$, $Q_{n+1}(x) = Q_n(x+1)/Q_n(x)$. Пусть $Q_n(x) - 1 = A(x)/B(x)$, где $A(x)$, $B(x)$ — многочлены. Найдите отношение старших членов этих многочленов. (*А. А. Шапиро*)

Ответ: $(-1)^{n-2}(n-2)!x^{1-n}$.

Решение. Пусть c_n/x^k — отношение старших членов $A(x)$ и $B(x)$ (где c_n — коэффициент). Тогда

$$Q_n(x) = 1 + \frac{c_n}{x^k} + o\Big(\frac{1}{x^k}\Big) \quad \text{при } x \to \infty.$$

Следовательно,

$$\ln(Q_n(x)) = \frac{c_n}{x^k} + o\Big(\frac{1}{x^k}\Big) \quad \text{при } x \to \infty,$$

поскольку $\dfrac{\ln(1+t)}{t} \to 1$ при $t \to 0$.

Пусть $\Delta(f) = f(x+1) - f(x)$ — оператор разностной производной с шагом 1. Тогда

$$\Delta(\ln x) = \frac{1}{x} + \sum_{k=2}^{\infty} d_k \frac{1}{x^k}$$

и

$$\Delta\Big(\frac{1}{x^k}\Big) = -k\frac{1}{x^{k+1}} + \sum_{l=k+1}^{\infty} c_{k,l} \frac{1}{x^{k+l}}$$

для каких-то d_k, $c_{k,l}$ (таким образом, асимптотика разностной производной совпадает с асимптотикой обычной производной).

При $n > 1$ имеем

$$\ln Q_n(x) = \ln Q_{n-1}(x+1) - \ln Q_{n-1}(x) = \Delta(\ln Q_{n-1}(x)).$$

Спускаясь по n, получаем (с учётом предыдущих равенств и условия $Q_1(x) = x$):

$$\ln Q_n(x) = \Delta^{n-1}(\ln x) = (-1)^{n-2}(n-2)!\frac{1}{x^{n-1}} + o\Big(\frac{1}{x^{n-1}}\Big),$$

откуда следует ответ. (*А. Я. Канель-Белов*)

18.7. Условие. Пусть $P(x) \neq \text{const}$ — многочлен с целыми коэффициентами. Докажите, что существует бесконечно много простых чисел вида $4k+1$, делящих его значение в целой точке.

Замечание. При публикации эта задача была приписана И. Богданову. В действительности он предложил задачу, а авторство её неизвестно. Редакция будет благодарна читателям за любые указания по этому поводу.

Ниже в первом решении доказан именно тот факт, который содержится в задаче; при этом используются свойства гауссовых целых чисел. Второе же решение доказывает существенно более общий факт, раскрывая глубинную сущность задачи.

Решение 1. Пусть $q = a + bi$ — некоторое простое гауссово число, делящее значение многочлена $P(m+ni)$ в некоторой целой гауссовой точке $m+ni$, причём $b \neq 0$ и $q \neq \pm 1 \pm i$. Тогда, как известно, $p = q\bar{q} = a^2 + b^2$ — простое число вида $4k+1$. Далее, существует натуральное k такое, что k^2+1 делится на p (годится, например, любое целое решение сравнения $kb \equiv a \pmod{p}$). При этом $k^2 + 1 = (k-i)(k+i)$, а тогда одна из скобок делится на q.

Пусть для определённости $k + i$ делится на q. Тогда имеем

$$P(m-nk) = P(m+ni-n(k+i)) \equiv P(m+ni) \equiv 0 \pmod{q},$$

то есть $P(m-nk)$ делится на q. Поскольку это число целое, оно делится также на $\bar{q}$, а значит, оно делится на p.

Осталось показать, что у значений $P(x)$ в целых гауссовых точках есть бесконечно много простых делителей с ненулевой мнимой частью. Это рассуждение стандартно. Пусть sx^k и r — соответственно старший и свободный члены многочлена $P(x)$. Если $r = 0$, то $P(x)$ делится на x и утверждение тривиально.

В противном случае предположим, что $q_1, \ldots, q_n$ — все простые гауссовы числа, делящие значения $P(x)$. Положим $N = crq_1q_2 \ldots q_n$ для большого по модулю целого гауссового числа c. Тогда нетрудно видеть, что в разложение числа $P(N)$ простые множители q_i входят в той же степени, что и в r. Поскольку других простых сомножителей с ненулевой мнимой частью в разложении $P(N)$ быть не может, приходим к выводу, что $\arg P(N)$ может принимать конечное количество значений. Однако при больших c этот аргумент очень близок к $\arg(sN^k)$. Теперь, подобрав аргумент коэффициента c должным образом, легко прийти к противоречию. (*Д. Клюев*)

Решение 2. В первом решении доказано, что у значений многочлена $P(x)$ в целых точках есть бесконечно много простых делителей, делящих некоторое число вида n^2+1. Это утверждение является частным случаем более общего факта, который мы здесь и докажем.

Факт. *Пусть $P(x)$ и $Q(x)$ — два неконстантных многочлена с целыми коэффициентами. Тогда существует бесконечно много простых чисел p, делящих как некоторое значение $P(n)$ в целой точке, так и некоторое значение $Q(m)$ в целой точке.*

Доказательство. Ясно, что достаточно ограничиться случаем, когда $P(x)$ и $Q(x)$ неприводимы над $\mathbb{Z}$ (если они приводимы, достаточно применить факт для некоторых их неприводимых делителей).

Пусть $\alpha \in \mathbb{C}$ и $\beta \in \mathbb{C}$ — некоторые корни многочленов $P(x)$ и $Q(x)$ соответственно. Рассмотрим алгебраическое расширение $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}[\alpha, \beta]$; по теореме о примитивном элементе существует такое $\gamma \in \mathbb{C}$, что $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$. Значит, существуют такие многочлены $F(x), G(x) \in \mathbb{Q}[x]$, что $\alpha = F(\gamma)$ и $\beta = G(\gamma)$.

Далее, число γ также алгебраично над $\mathbb{Q}$, поэтому оно является корнем некоторого неприводимого многочлена $R(x) \in \mathbb{Z}[x]$. Тогда $\mathbb{Q}[\gamma] \cong \mathbb{Q}[x]/(R(x))$. Это значит, что для любого многочлена $S(x) \in \mathbb{Q}[x]$ мы имеем $S(\gamma) = 0$ тогда и только тогда, когда $S(x)$ делится на $R(x)$. Поскольку $P(F(\gamma)) = Q(G(\gamma)) = 0$, заключаем, что $P(F(x))$ и $Q(G(x))$ делятся на $R(x)$, то есть

$$P(F(x)) = R(x)P_1(x) \quad \text{и} \quad Q(G(x)) = R(x)Q_1(x).$$

Заметим, что многочлены $F(x)$, $G(x)$, $P_1(x)$ и $Q_1(x)$ могут иметь нецелые (но рациональные!) коэффициенты; пусть N — наибольшее простое число, на которое делится какой-нибудь из знаменателей этих коэффициентов.

Для неконстантного многочлена $R(x)$ существует бесконечно много простых чисел, делящих его значения в целых точках (доказательство этого утверждения повторяет концовку предыдущего решения, но содержит меньше технических подробностей). Пусть $p > N$ — такое простое число, и пусть $R(n)$ — соответствующее значение. Тогда числители рациональных чисел $P(F(n)) = R(n)P_1(n)$ и $Q(G(n)) = R(n)Q_1(n)$ делятся на p, поскольку знаменатели чисел $P_1(n)$ и $Q_1(n)$ на него не делятся.

Единственная оставшаяся проблема заключается в том, что числа $F(n)$ и $G(n)$ — рациональные, а не целые. Однако их знаменатели также не делятся на p. Значит, если $F(n) = a/b$ для взаимно простых целых a и b, то можно выбрать такое целое c, что $a \equiv bc \pmod{p}$. Тогда $P(c) \equiv P(a/b) \equiv 0 \pmod{p}$. Аналогично находится значение $Q(x)$ в целой точке, делящееся на p. (*И. Богданов, А. Канель-Белов*)

18.10. Условие. Какую наибольшую размерность может иметь подпространство пространства $(n \times n)$-матриц полем действительных чисел, состоящее только из вырожденных матриц? (*Фольклор*)

Ответ: $n^2 - n$.

Решение. Подпространством коразмерности n, удовлетворяющим условиям задачи, является, например, множество матриц с нулевой первой строкой.

Докажем теперь, что коразмерность подпространства, удовлетворяющего условиям задачи, не меньше n. Подпространство коразмерности k можно задать системой линейных уравнений ранга k, в которой неизвестными являются координаты в стандартном базисе матричных единиц. У этой системы есть k главных неизвестных, а остальные — свободные. Если предположить, что $k < n$, то нетрудно доказать, что с помощью перестановки строк и столбцов можно добиться, чтобы все главные неизвестные оказались под главной диагональю (оставляем читателю этот факт в качестве самостоятельного упражнения). При этом подпространство, задаваемое системой, переходит в другое подпространство той же размерности, задаваемое преобразованной системой, а условие, что оно содержит только вырожденные матрицы, сохраняется. Но свободным неизвестным можно присвоить любые значения. Поставим единицы на главной диагонали и нули над ней. Получим невырожденную матрицу в нашем подпространстве. Это противоречие доказывает утверждение. (*В. О. Бугаенко*)