Math-Net.Ru

Общероссийский математический портал

Н. Сафаеи, Об одной задаче В.А. Сендерова, *Квант*, 2021, номер 10, 2–11

DOI: <https://doi.org/10.4213/kvant20211001>

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: 3.85.183.62

26 апреля 2023 г., 18:21:50

Об одной задаче В.А.Сендерова

Н.САФАЕИ

Памяти моего так и не увиденного
учителя Валерия Анатольевича Сендерова

ВВЕДЕНИЕ

В старших классах я стал постоянным читателем журнала «Квант». Особенно важным для меня был «Задачник «Кванта» по математике, и со временем мой интерес к этому разделу постоянно рос. Несколько задач, опубликованных в журнале, заставили меня обратить на них пристальное внимание. Одной из самых сложных среди них была задача M2159, предложенная известным российским задачным композитором Валерием Анатольевичем Сендеровым. Формулировка задачи была следующая:

Найдите все натуральные числа k , с такими, что выражение

$$n(n+1)(n+2)\dots(n+k-1)+c$$

является точной степенью для всех натуральных чисел n , кроме, быть может, конечного их числа.

Поначалу задача казалась мне совершенно недоступной, и, чтобы подступиться к ней, я прочитал много книг и статей. В некоторых из них были предприняты шаги по ее исследованию. Но, насколько мне известно, полное решение никогда не публиковалось ни в «Кванте», ни в других журналах.

В этой статье я приведу решение задачи, а также некоторые другие результаты, которые помогут читателю улучшить свои знания о многочленах с целыми коэффициентами и их применении к теории чисел. Кроме того, статья призвана объяснить, как возникла идея решения этой задачи, показать шаги доказательства, объясняя при этом логику их возникновения, наконец, расширить и углубить основную идею для решения некоторых новых задач.

ВСПОМОГАТЕЛЬНЫЕ ФАКТЫ

В этом разделе я перечислю набор инструментов, который понадобится в дальнейшем для решения задачи, а также некоторые ссылки для дальнейшего чтения.

Китайская теорема об остатках

Теорема (китайская теорема об остатках).

Пусть $a_1, a_2, \dots, a_n$ – попарно взаимно простые целые числа. Тогда система сравнений

$$x \equiv b_1 \pmod{a_1},$$

$$x \equiv b_2 \pmod{a_2},$$

...

$$x \equiv b_n \pmod{a_n}$$

имеет единственное решение по модулю $a_1 a_2 \dots a_n$ для любых целых $b_1, b_2, \dots, b_n$. В частности, у этой системы гарантированно существует натуральное решение x .

Следствие 1. При тех же допущениях о попарной взаимной простоте чисел a_i верен следующий факт: если x пробегает ровно c_i остатков по каждому модулю a_i , то по модулю $a_1 a_2 \dots a_n$ число x пробегает ровно $c_1 c_2 \dots c_n$ остатков.

Наибольший общий делитель многочленов

Под *наибольшим общим делителем* двух многочленов $A(x)$, $B(x)$ с рациональными коэффициентами, из которых хотя бы один не равен тождественно нулю, мы понимаем приведенный многочлен (т.е. многочлен, старший коэффициент которого равен единице) $D(x)$ с рациональными коэффициентами наибольшей степени, который делит одновременно и $A(x)$, и $B(x)$. Для многочленов с рациональными коэффициентами, как и для целых чисел, работает алгоритм Евклида, благодаря которому можно доказать представление $D(x)$ в следующем виде:

$$D(x) = R(x)A(x) + S(x)B(x),$$

где $R(x)$, $S(x)$ – некоторые многочлены с рациональными коэффициентами.

Если же многочлен $D(x)$ тождественно равен 1, многочлены $A(x)$ и $B(x)$ с рациональными коэффициентами называются *взаимно простыми*. Многочлены с целыми коэффициентами считаются взаимно простыми, если они взаимно просты как многочлены с рациональными коэффициентами. Взяв вышеупомянутое разложение для НОД двух взаимно простых многочленов $A(x)$, $B(x)$ с целыми коэффициентами и домножив его на НОК знаменателей коэффициентов $R(x)$, $S(x)$, мы получим следующее утверждение:

Лемма 1. Для любых двух взаимно простых многочленов $A(x)$, $B(x)$ с целыми коэффициентами существует целое ненулевое число M и другие многочлены $C(x)$, $D(x)$ с целыми коэффициентами такие, что

$$M = A(x)C(x) + B(x)D(x).$$

Алгебраические числа и минимальные многочлены

Комплексное число α называется *алгебраическим*, если существует ненулевой многочлен $P(x)$ с целыми коэффициентами такой, что $P(\alpha) = 0$. Например, $\sqrt{2} + \sqrt{3}$ — алгебраическое число, поскольку $P(\sqrt{2} + \sqrt{3}) = 0$, где $P(x) = x^4 - 10x^2 + 1$. Очевидно, что множество алгебраических чисел содержит как подмножество множество рациональных чисел. Среди чисел, не являющихся алгебраическими, наиболее известна константа *Лиувилля*, определяемая так:

$$\sum_{n=1}^{\infty} 10^{-n!} = 0,11000100000000000000000010000\dots$$

Ненулевой многочлен $P(x)$ с целыми коэффициентами минимальной степени, для которого $P(\alpha) = 0$, называется *минимальным многочленом* алгебраического числа α . Несложно понять, что минимальный многочлен любого алгебраического числа нельзя разложить на множители в множестве $\mathbb{Z}[x]$ всех многочленов с целыми коэффициентами. Кроме того, если существует другой многочлен $R(x)$ с целыми коэффициентами, имеющий α в качестве корня, то из предположения о минимальности степени следует, что $\deg P \leq \deg R$. Разделим многочлен $R(x)$ на многочлен $P(x)$ с остатком:

$$R(x) = P(x)Q(x) + S(x),$$

причем $\deg S < \deg P$. Умножая обе части на наименьший общий знаменатель коэффициентов многочленов $Q(x)$, $S(x)$, мы можем считать, что $Q(x)$ и $S(x)$ имеют целые коэффициенты. Подставив $x = \alpha$ в уравнение выше, найдем, что $S(\alpha) = 0$. Следовательно, из условия минимальности степени следует, что $S(x)$ тождественно равен 0, т.е. $R(x)$ делится на $P(x)$. Таким образом, все многочлены с целыми коэффициентами и корнем α кратны минимальному многочлену. Из доказанного немедленно вытекает

Следствие 2. Каждый неприводимый (т.е. не разложимый на множители) многочлен $P(x)$ с рациональными коэффициентами является минимальным многочленом своих корней.

Лемма 2. Пусть $P(x)$ — неприводимый многочлен с рациональными коэффициентами, тогда $P(x)$ и его производная $P'(x)$ взаимно просты.

Доказательство. Предположим противное, т.е. что существует непостоянный многочлен $D(x)$ с рациональными коэффициентами, который делит как $P(x)$, так и $P'(x)$. Поскольку $P(x)$ неприводим, то $D(x) = cP(x)$, следовательно, $P(x)$ должен делить $P'(x)$, что, очевидно, неправда. Это доказывает лемму 2.

Любознательный читатель может найти много интересных фактов об алгебраических числах и минимальных многочленах, а также рассказ об одном важном классе алгебраических чисел, называемых числами Пизо, в прекрасной статье [2].

Лемма Гаусса

Назовем *содержанием* многочлена $P(x) = a_0 + a_1x + \dots + a_nx^n$ с целыми коэффициентами наибольший общий делитель $d = d(P)$ всех его коэффициентов. Если $d(P) = 1$, то многочлен $P(x)$ называют *примитивным*.

Лемма 3. Пусть $P(x), Q(x) \in \mathbb{Z}[x]$. Тогда $d(PQ) = d(P)d(Q)$. В частности, произведение двух примитивных многочленов снова будет примитивным многочленом.

Доказательство. Начнем с последнего утверждения. Пусть $P(x) = a_0 + a_1x + \dots + a_nx^n$ и $Q(x) = b_0 + b_1x + \dots + b_nx^n$ — примитивные многочлены из $\mathbb{Z}[x]$, произведение которых не является примитивным, т.е. для некоторого простого числа p верна делимость $p \mid d(PQ)$.

Выберем наименьшие индексы s, t , для которых $p \nmid a_s, p \nmid b_t$. Такие индексы найдутся в силу примитивности P и Q . Коэффициент при x^{s+t} в многочлене $P(x)Q(x)$ будет равен

$$c_{s+t} = a_s b_t + (a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \dots) + \\ + (a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \dots).$$

Так как a_{s-i} и b_{t+i} при $i > 0$ делятся на p по условию и $p \mid c_{s+t}$ по предположению, то $p \mid a_s b_t$, а это противоречит выбору индексов s и t .

Переходя к общему случаю, запишем произвольные многочлены $P(x), Q(x) \in \mathbb{Z}[x]$ в виде

$$P = d(P)P_0, Q = d(Q)Q_0,$$

где P_0, Q_0 – примитивные многочлены. Так как $PQ = d(P)d(Q)P_0Q_0$ и по доказанному $d(P_0Q_0) = 1$, то $d(PQ) = d(P)d(Q)$, что и требовалось доказать.

Лемма 4 (лемма Гаусса). Целочисленный многочлен, неприводимый над $\mathbb{Z}$, также неприводим над $\mathbb{Q}$.

Доказательство. Предположим, что для некоторых многочленов $R(x) \in \mathbb{Z}[x], P(x), Q(x) \in \mathbb{Q}[x]$ выполняется равенство $R(x) = P(x)Q(x)$. После умножения обеих частей этого равенства на НОК знаменателей и сокращения на НОД числителей всех коэффициентов у P и Q , оно переписывается в виде

$$aR(x) = bP_0(x)Q_0(x),$$

где $a, b \in \mathbb{Z}$, а $P_0(x)$ и $Q_0(x)$ – примитивные многочлены над $\mathbb{Z}$. По лемме 3 имеем $ad(R) = b$, так что после сокращения получается разложение $R(x) = d(R)P_0(x)Q_0(x)$, поэтому многочлен $R(x)$ приводим также и над $\mathbb{Z}[x]$.

Лемма Гензеля

В этом подразделе я опишу очень важный результат, который не один раз пригодится в решении. Для начала заметим, что для любого многочлена $P(x)$ степени 0, т.е. тождественно равного константе, верно следующее равенство: $P(x+y) = P(x)$.

Дальше, для любого линейного многочлена $P(x)$ верно соотношение $P(x+y) = P(x) + cy$, где константа c равна коэффициенту при x или, другими словами, первой производной многочлена P .

Вышесказанное несложно обобщить на случай произвольного многочлена с помощью метода математической индукции по степени многочлена. Верен следующий факт: если $P(x)$ – многочлен степени d с целыми коэффициентами, то справедливо равенство

$$P(x+y) = P(x) + f_1(x)y + f_2(x)y^2 + \dots + f_d(x)y^d,$$

где $f_i(x) = \frac{P^{(i)}(x)}{i!}$, $i = 1, 2, \dots, d$ – многочлены с целыми коэффициентами степени не выше $d-1$, а $P^{(i)}(x)$ – i -я производная $P(x)$.

Непосредственным следствием этого утверждения является следующий очень полезный факт.

Лемма 5 (лемма Гензеля). Пусть $P(x)$ – многочлен с целыми коэффициентами. Тогда для любого простого q , натурального s и целых r, n верно следующее сравнение:

$$P(n + rq^s) \equiv P(n) + rq^s P'(n) \pmod{q^{2s}}.$$

МНОГОЧЛЕНЫ, ЗНАЧЕНИЯ КОТОРЫХ В ЦЕЛЫХ ТОЧКАХ СУТЬ ПОЛНЫЕ КВАДРАТЫ

В этой части статьи я расскажу о некоторых полезных фактах, которые возникли в результате моих попыток решить задачу. Я разместил эти факты до самого доказательства, чтобы предоставить читателю предисторию решения задачи, а также придать ему достаточно энергии для прочтения остальной части статьи. Начнем со следующей леммы.

Лемма 6. Про многочлен $P(x)$ четной степени с целыми коэффициентами известно, что его значения при любых достаточно больших натуральных n и старший коэффициент являются квадратами целых чисел. Тогда существует многочлен $Q(x)$ с целыми коэффициентами такой, что $P(x) = Q(x)^2$.

Доказательство. Пусть данный в условии леммы многочлен имеет вид

$$P(x) = x^{2k} + a_{2k-1}x^{2k-1} + \dots + a_0.$$

Я хочу переписать его в виде

$$P(x) = Q(x)^2 + r(x) = \\ = (b_k x^k + b_{k-1} x^{k-1} + \dots + b_0)^2 + r(x),$$

где $\deg r(x) \leq k-1$. Чтобы понять, что это возможно, я сравню коэффициенты при x^{k+t} для $t=0,1,\dots, k-1$ у двух разных

форм записи: $a_{k+t} = 2b_k b_t + \sum_{i=1}^{k-1-t} b_{t+i} b_{k-i}$.

Легко видеть, что по этим соотношениям последовательно и однозначно восстанавливаются $b_{k-1}, b_{k-2}, \dots, b_1, b_0$. Также видно, что все b_i являются рациональными числами; обозначим через M наибольший общий делитель их знаменателей. По условию для всех достаточно больших натуральных n мы имеем $P(n) = y_n^2$, где $y_n \in \mathbb{Z}$. После домножения на M^2 мы получим следующее соотношение: $(My_n)^2 = Q_1(n)^2 + M^2 r(n)$, где $Q_1(x) = MQ(x) \in \mathbb{Z}[x]$. Если у $r(x)$ положительный старший коэффициент, то при достаточно больших натуральных n верно неравенство $(My_n)^2 > Q_1(n)^2$ и, следовательно, $(My_n)^2 \geq (1 + Q_1(n))^2$. Аналогично, если старший коэффициент многочлена $r(x)$ отрицательный, то $(My_n)^2 \leq (-1 + Q_1(n))^2$. В обоих случаях выполняется неравенство $2|Q_1(n)| \leq |M^2 r(n) - 1|$ при всех достаточно больших натуральных n , что, очевидно, неверно, так как степень многочлена $Q_1(x)$ меньше, чем степень многочлена $r(x)$. Следовательно, многочлен $r(x)$ тождественно равен нулю, и $P(x) = Q(x)^2$. Осталось доказать, что многочлен $Q(x)$ имеет целые коэффициенты, в этом мне поможет следующая лемма.

Лемма 7. Многочлен $Q(x)$ с комплексными коэффициентами таков, что его старший коэффициент рациональный, и для некоторого натурального k все коэффициенты многочлена $Q(x)^k$ целые. Тогда $Q(x) \in \mathbb{Z}[x]$.

Доказательство. Пусть $Q(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, тогда $Q(x)^k$ можно записать в виде $b_{kn} x^{kn} + b_{kn-1} x^{kn-1} + \dots + b_0$.

Докажем по индукции, что все коэффициенты a_i являются рациональными. Старший коэффициент a_n лежит в множестве рациональных чисел по условию; предположим, что $a_n, a_{n-1}, \dots, a_{n-s}$ рациональны, и докажем, что $a_{n-s-1} \in \mathbb{Q}$. Для этого в равенстве

$$b_{kn} x^{kn} + b_{kn-1} x^{kn-1} + \dots + b_0 = (a_n x^n + a_{n-1} x^{n-1} + \dots + a_0)^k$$

сравним коэффициенты при x^{kn-s-1} :

$$b_{kn-s-1} = k a_{n-s-1} a_n^{k-1} + S,$$

где $S = S(a_n, a_{n-1}, \dots, a_{n-s})$ — значение рациональной функции в рациональных точках $a_n, a_{n-1}, \dots, a_{n-s}$ и, следовательно, рациональное число. Отсюда, следует, что

коэффициент $a_{n-s-1} = \frac{b_{kn-s-1} - S}{k a_n^{k-1}}$ также

является рациональным, что и требовалось доказать.

Представим теперь многочлен $Q(x)^k$ с целыми коэффициентами в виде произведения двух многочленов $Q(x)$ и $Q(x)^{k-1}$ с рациональными коэффициентами. По лемме Гаусса существует такое рациональное число q , что многочлены $qQ(x)$ и $q^{-1}Q(x)^{k-1}$ имеют целые коэффициенты. Предположим, что $q = a/b$, где a, b — целые взаимно простые числа, тогда многочлены $aQ(x)$, $bQ(x)^{k-1}$ также имеют целые коэффициенты. Следовательно, многочлен $a^{k-1}Q(x)^{k-1} \in \mathbb{Z}[x]$. По алгоритму Евклида для нахождения наибольшего общего делителя существуют целые числа s, t такие, что $a^{k-1}s + bt = (a, b) = 1$. Таким образом, многочлен $a^{k-1}sQ(x)^{k-1} + bsQ(x)^{k-1} = Q(x)^{k-1}$ имеет целые коэффициенты. Продолжая этот процесс, легко приходим к тому, что $Q(x)$ будет иметь целые коэффициенты. Это завершает доказательство леммы 7.

Наконец, докажем обобщение леммы 6.

Лемма 8. Про многочлен $P(x)$ с целыми коэффициентами известно, что его значения при любых достаточно больших натуральных n являются квадратами целых чисел. Тогда для некоторого многочлена $Q(x)$ с целыми коэффициентами верно тождество $P(x) = Q(x)^2$.

Доказательство. В условии этой леммы у нас нет дополнительных ограничений, как в лемме 6, но я применю следующий красивый трюк. Очевидно, что существуют целые l_1, l_2 такие, что многочлены $P(x+l_1)$ и $P(x+l_2)$ не имеют общих корней. Многочлен $H(x) = P(x+l_1) \cdot P(x+l_2)$ гарантированно имеет четную степень и стар

ший коэффициент, являющийся точным квадратом, а также точными квадратами являются и его значения во всех достаточно больших целых точках. По лемме 6 существует многочлен $P_1(x) \in \mathbb{Z}[x]$ такой, что $P(x+l_1) \cdot P(x+l_2) = P_1(x)^2$. Так как многочлены $P(x+l_1)$ и $P(x+l_2)$ не имеют общих корней, то существуют многочлены $R(x)$, $S(x)$ такие, что $P(x+l_1) = R(x)^2$, $P(x+l_2) = S(x)^2$, причем по лемме 7 все коэффициенты $R(x)$, $S(x)$ – целые числа. Следовательно, $P(x)$ является квадратом многочлена с целыми коэффициентами, что и требовалось доказать.

Исходя из доказанного выше, можно заключить, что если многочлен с целочисленными коэффициентами является полным квадратом во всех целых точках, кроме, может быть, конечного их числа, то он представляется в виде квадрата многочлена с целочисленными коэффициентами. Для этого достаточно заметить, что утверждение леммы 8 остается в силе, если заменить в условии «при любых достаточно больших натуральных n » на «при любых достаточно малых целых n ». Возможно, аналогичным образом можно вывести похожий факт о третьей, четвертой степенях и т.д. Но, как читатель может заметить, в формулировке задачи известно только то, что многочлен – точная степень натурального числа, и мы не знаем наверняка, что это за степень. Есть ли здесь какая-то закономерность? Я вернусь к этому позже.

ПЕРВАЯ ПОПЫТКА РЕШЕНИЯ

Настало время наконец подступить к решению задачи. В этой главе я свяжу воедино китайскую теорему об остатках и лемму Гензеля и получу еще несколько вспомогательных результатов. Сначала я докажу следующую лемму.

Лемма 9. Пусть $P(x)$ – неприводимый многочлен с целыми коэффициентами, не равный тождественно константе. Тогда существует бесконечно много простых чисел q таких, что для каждого из них выполняется равенство $v_q(P(n)) = 1$ при некотором целом $n = n(q)$.

Здесь v_q – функция, значение которой на ненулевом целом числе m определяется так:

$$v_p(m) = \max \{k \in \mathbb{N} : p^k \mid m\}.$$

Доказательство. Доказательство я проведу в

два этапа. На первом я докажу, что существует бесконечно много простых делителей значений в целых точках данного в условии многочлена. Это известное в олимпиадной среде утверждение, которое носит название теоремы Шура. Если у $P(x)$ свободный коэффициент равен 0, то $x \mid P(x)$, и утверждение, очевидно, верное. В случае $P(0) = a \neq 0$ предположим противное, существует только конечное множество $M = \{p_1, \dots, p_l\}$ простых делителей чисел вида $P(n)$, где n – целое. Рассмотрим многочлен $Q(x) = P(a + p_1 \dots p_l P(a)x)$; по лемме Гензеля при любых целом n и простом $p_i \in M$ выполняется равенство $v_{p_i} Q(n) = v_{p_i} P(a)$. Так как числа $Q(n)$ и $P(a)$ имеют один и тот же набор простых множителей, входящий в их разложение в одинаковых степенях, то

$$|P(a + p_1 \dots p_l P(a)n)| = |Q(n)| = P(a).$$

Такое может быть, только если многочлен $P(x)$ тождественно равен константе. Следовательно, наше предположение неверно, а теорема Шура, в свою очередь, верна.

Так как многочлен $P(x)$ неприводим, то по лемме 2 существуют многочлены $A(x)$ и $B(x)$ с целыми коэффициентами такие, что $A(x)P(x) + B(x)P'(x) = C$ для некоторого целого C . Это означает, что каждое простое q , большее $|C|$ (мы уже знаем по теореме Шура, что их бесконечно много), делящее $P(n)$ при каком-то целом n , не является делителем числа $P'(n)$. Поэтому из леммы Гензеля следует, что для таких q , n верно следующее:

$$P(n+q) - P(n) \equiv qP'(n) \not\equiv 0 \pmod{q^2}.$$

Значит, по крайней мере одно из чисел $P(n)$ и $P(n+q)$ делится на q , но не делится на q^2 , что и требовалось.

Теперь я докажу лемму, применение которой значительно приблизит нас к решению задачи. Это утверждение (с небольшими изменениями) позаимствовано из замечательной статьи [3].

Лемма 10. Пусть $P(x)$ – многочлен с целыми коэффициентами такой, что при каждом натуральном n , кроме, быть может, конечного их числа, значение многочлена $P(n)$ является нетривиальной точной

степенью некоторого натурального числа, т.е. $P(n) = m(n)^{s(n)}$, где $m(n)$, $s(n)$ – натуральные числа, большие 1. Тогда существуют натуральное $s > 1$ и многочлен $Q(x) \in \mathbb{Z}[x]$ такие, что $P(x) = Q(x)^s$.

Доказательство. Пусть $P(x) = aP_1^{\alpha_1} \dots P_t^{\alpha_t}$, где $a \in \mathbb{Z}$, а $P_1, \dots, P_t$ – различные неприводимые многочлены с целыми коэффициентами. Для каждой пары различных индексов i, j существует целая ненулевая константа c_{ij} такая, что

$$P_i(x)A_{ij}(x) + P_j(x)B_{ij}(x) = c_{ij}$$

при некоторых многочленах $A_{ij}(x)$, $B_{ij}(x)$ с целыми коэффициентами. По лемме 9 существуют простые $q_1, \dots, q_t > |a| \cdot \max_{1 \leq j \leq t} |c_{ij}|$ такие, что $v_{q_i}(P_i(n_i)) = 1$ при некоторых натуральных n_i . Согласно выбору простых q_i (напомню, что, в частности, $q_i > |c_{ij}|$ для всех $1 \leq j \leq t$) выполняется равенство $v_{q_i}(P_j(n_i)) = 0$, иначе левая часть равенства $P_i(n_i)A_{ij}(n_i) + P_j(n_i)B_{ij}(n_i) = c_{ij}$ делится на q_i , в отличие от правой части.

По китайской теореме об остатках существует такое натуральное n , что

$$n \equiv n_1 \pmod{q_1^2},$$

$$n \equiv n_t \pmod{q_t^2}.$$

Из леммы Гензеля следует, что $v_{q_i}(P_i(n)) = 1$; также очевидно, что при всех отличных от i индексах j простое число q_i не делит $P_j(n)$, так как оно не делит $P_j(n_i)$. Следовательно, для каждого индекса i верно равенство

$$v_{q_i}(P(n)) = v_{q_i}(a) + \alpha_1 \cdot v_{q_i}(P_1(n)) + \dots + \alpha_t \cdot v_{q_i}(P_t(n)) = \alpha_i.$$

Поскольку $v_{q_i}(P(n)) = s(n) \cdot v_{q_i}(Q(n))$, следовательно, $s(n) | \alpha_i$ для каждого $1 \leq i \leq t$. Значит, у чисел α_i есть общий делитель $s = s(n) > 1$, т.е. $P_1^{\alpha_1} \dots P_t^{\alpha_t} = Q_1^s$ для некоторого многочлена $Q_1 \in \mathbb{Z}[x]$. Так как $P(n)$ является точной s -й степенью, то s -й степенью является также и число a , поэтому многочлен $Q(x) = a^{1/s} Q_1(x)$ удовлетворяет условиям леммы, что и требовалось найти.

ВТОРАЯ ПОПЫТКА РЕШЕНИЯ

Как уже наверняка заметил читатель, путь к решению задачи оказался непростым. В конце концов, все предыдущие результа-

ты указывают нам на то, что мы должны выяснить, существуют ли многочлен $Q(x)$ с целыми коэффициентами и некоторое натуральное число $s \geq 2$, удовлетворяющие следующему тождеству:

$$x(x+1) \dots (x+k-1) + c = Q(x)^s.$$

Насколько мне известно, в существующей литературе была предпринята попытка решить задачу в случае $s = 2$, которая, однако, не имеет ничего общего с нашим подходом, но заслуживает упоминания здесь. Решение можно найти, например, в статье [1].

Следствие 3. Пусть $P_{k,c}(x) = x(x+1) \dots (x+k-1) + c$, тогда $P_{k,c}(x)$ при $k \neq 2, 4$ не является квадратом многочлена.

Доказательство. Предположим, что $P_{k,c}(x) = Q(x)^2$, $k = 2n$. Тогда $P_{k,c}(x+1) - P_{k,c}(x) = k(x+1)(x+2) \dots (x+k-1) = Q(x+1)^2 - Q(x)^2$.

$$\begin{aligned} \text{Следовательно,} \\ (Q(x+1) - Q(x))(Q(x+1) + Q(x)) &= \\ &= k(x+1)(x+2) \dots (x+k-1). \end{aligned}$$

Сравнивая степени многочленов из вышеприведенного равенства, несложно заметить, что многочлен $Q(x+1) - Q(x)$ имеет ровно $n-1$ действительный корень, в то время как ровно n различных действительных чисел являются корнями многочлена $Q(x+1) + Q(x)$. Поскольку график многочлена $y = Q(x+1)$ получается из графика $y = Q(x)$ сдвигом на единицу влево, каждое из $(n-1)$ -го решения уравнения $Q(x+1) = Q(x)$ лежит между парой корней многочлена $Q(x) + Q(x+1)$. Значит,

$$\begin{aligned} Q(x+1) - Q(x) &= \\ &= n(x+2)(x+4) \dots (x+2n-2), \\ Q(x+1) + Q(x) &= \\ &= 2(x+1)(x+3) \dots (x+2n-1). \end{aligned}$$

Складывая эти выражения, получаем $2Q(x+1) = 2(x+1)(x+3) \dots (x+2n-1) + n(x+2)(x+4) \dots (x+2n-2)$. Вычитая и подставляя в результат $x+1$ вместо x , найдем, что $2Q(x+1) = 2(x+2)(x+4) \dots (x+2n) - n(x+3)(x+5) \dots (x+2n-1)$.

Два полученных выражения для $2Q(x+1)$ несовместны при $n > 2$. В этом можно убедиться, например, так. Подставим в эти

равенства $x = 0$ и вычтем одно из другого. Мы получим соотношение

$$(n+2)(1 \cdot 3 \cdot \dots \cdot (2n-1)) = 3n(2 \cdot 4 \cdot \dots \cdot (2n-2)),$$

в котором правая часть делится на большую степень двойки, чем левая.

ГЛАВНЫЕ РЕЗУЛЬТАТЫ

Итак, теперь мы полностью готовы для того, чтобы получить главный результат нашей статьи. В предыдущих разделах рассказывалось, как я искал баланс между алгеброй и теорией чисел, и доказал несколько результатов, которые призваны облегчить понимание того, что будет написано ниже.

Пусть $P(x) = x(x+1)\dots(x+m-1)$, тогда верна следующая лемма.

Лемма 11. Для каждого комплексного a степень НОД многочленов $P(x) - a$ и $P'(x)$ не превосходит 2; более того, если m нечетно, то она не превосходит 1.

Доказательство. Структура многочлена $P(x)$ такова, что его производная $P'(x)$ имеет ровно $m-1$ корень $r_1, \dots, r_{m-1}$, причем эти корни можно упорядочить так, чтобы выполнялось неравенство

$$-(m-1) < r_{m-1} < -(m-2) < \dots < -1 < r_1 < 0.$$

Кроме того, функция $y = |P(x)|$ симметрична относительно вертикальной оси $x = -\frac{m-1}{2}$, поэтому

$|P(r_i)| = |P(r_{m-i})|$ при $1 \leq i < m$. Из свойств производной следует, что $|P(x)|$ достигает своего максимума на каждом отрезке вида $[-i; -i+1]$ в точке r_i . Следовательно,

$$\frac{|P(r_{i-1})|}{|P(r_i)|} \geq \frac{|P(r_{i+1})|}{|P(r_i)|} = \frac{|r_i+1||r_i+2|\dots|r_i+m|}{|r_i||r_i+1|\dots|r_i+m-1|} = \frac{|r_i+m|}{|r_i|},$$

и при $i \leq \frac{m}{2}$ выполняется неравенство

$$|P(r_{i-1})| > |P(r_i)|.$$

По симметрии для $i \geq \frac{m+2}{2}$ выполняется

обратное неравенство $|P(r_{i-1})| < |P(r_i)|$. Таким образом, для каждого комплексного a уравнение $P(x) = a$ имеет не более двух корней из множества $\{r_1, \dots, r_{m-1}\}$

корней $P'(x)$. Далее, если m нечетно, то $P(r_i) = -P(r_{m-i})$, следовательно, количество этих корней в этом случае не больше одного, что и требовалось доказать.

Мне осталось доказать последнюю ключевую лемму, необходимую для решения задачи.

Лемма 12. Пусть m – натуральное число. Предположим, что существуют многочлены $Q(x)$, $R(x)$ степени не меньше 2, с комплексными коэффициентами такие, что

$$P(x) = x(x+1)\dots(x+m-1) = R(Q(x)).$$

Тогда m четно, и степень многочлена $Q(x)$ равна ровно 2.

Доказательство. Заметим, что $P'(x) = R'(Q(x)) \cdot Q'(x)$. Пусть r – какой-либо комплексный корень многочлена $R'(x)$. Тогда многочлен $Q(x) - r$ делит как многочлен $P'(x)$, так и многочлен $R(Q(x)) - R(r) = P(x) - R(r)$, а следовательно, и их НОД. Из леммы 11 следует, что степень многочлена $Q(x) - r$, как и многочлена $Q(x)$ должна быть ровно 2, причем m должно быть четно, что и требовалось доказать.

Пусть теперь $Q(x)$ имеет вид $a(x-b)^2 + c$, тогда

$$P(x) = x(x+1)\dots(x+m-1) = R(a(x-b)^2 + c) = S((x-b)^2)$$

для некоторого многочлена $S(x)$ с комплексными коэффициентами. Так как $P(x)$ симметричен относительно b , то $b = \frac{m-1}{2}$.

Окончательно мы получаем, что $m = 2k$ для некоторого натурального k ,

$$P(x) = S\left(\left(x - \frac{m-1}{2}\right)^2\right),$$

$$S(x) = \left(x - \frac{1}{4}\right)\left(x - \frac{9}{4}\right)\dots\left(x - \frac{(2k-1)^2}{4}\right).$$

РЕШЕНИЕ ЗАДАЧИ

Теперь мы совсем близки к решению. По правде говоря, был проделан долгий путь, но терпеливые читатели сейчас будут вознаграждены.

Пусть $x(x+1)\dots(x+k-1) + c = Q(x)^s$ для некоторого натурального числа $s \geq 2$ и некоторого многочлена $Q(x)$ с комплексными коэффициентами. Пусть стар-

ший коэффициент $Q(x)$ равен a , тогда, поскольку $a^s = 1$, можно заменить $Q(x)$

на $\frac{1}{a}Q(x)$ и считать, что многочлен $Q(x)$

является приведенным. Не умаляя общности, можно считать, что $Q(x)$ не является степенью другого многочлена, в противном случае мы можем заменить s на другое подходящее натуральное число.

Далее, корни $Q(x)$ имеют в левой части кратность не менее s , следовательно, они все появляются в производной многочлена $P(x) + c = x(x+1)\dots(x+k-1) + c$, а значит, степень наибольшего общего делителя многочленов $P(x) + c$ и $P'(x)$ не меньше T , где T – количество различных корней $Q(x)$. По лемме 11 имеем $T \leq 1$ при нечетном k и $T \leq 2$ при четном k . Иными словами, либо $Q(x) = x + a$, либо $Q(x) = x^2 + ax + b$. В любом случае $Q(x) \in \mathbb{Z}[x]$ по лемме 7.

$$\text{Если } Q(x) = x + a, \text{ то} \\ x(x+1)\dots(x+k-1) + c = (x+a)^s.$$

Из сравнения степеней многочленов в левой и правой частях равенства получаем, что $k = s$, а сравнение свободных коэффициентов дает нам $c = a^s$. Перепишем равенство в следующем виде

$$x(x+1)\dots(x+s-1) = (x+a)^s.$$

Корни многочлена в правой части имеют вид

$$a \left(\cos \frac{2r\pi}{s} + i \sin \frac{2r\pi}{s} \right), \text{ где } r = 0, 1, \dots, s-1.$$

Легко понять, что при $s > 1$ множество этих корней не совпадает с $\{0, -1, \dots, -s+1\}$, что приводит к противоречию.

Во втором случае верно равенство

$$x(x+1)\dots(x+k-1) + c = (x^2 + ax + b)^s$$

Снова сравнивая степени и коэффициенты обеих частей, мы получаем, что $k = 2s$ и $c = b^s$, следовательно

$$x(x+1)\dots(x+k-1) = (x^2 + ax + b)^s - b^s.$$

Корни правой части уравнения являются корнями одного из уравнений

$$x^2 + ax + b = \sqrt[s]{b \left(\cos \frac{2r\pi}{s} + i \sin \frac{2r\pi}{s} \right)}$$

для некоторого $r \in \{0, \dots, s-1\}$. Заметим, что правая часть этих уравнений вещественна, только если $2r$ делится на s , и равна либо b , либо $-b$. Таким образом, существует не более четырех подходящих корней упомянутых выше уравнений. Следовательно, либо $k = 2$ и $s = 1$, либо $k = 4$ и $s = 2$. Первый случай невозможен по выбору s , во втором случае

$$\begin{aligned} x(x+1)\dots(x+k-1) &= \\ &= x(x+1)(x+2)(x+3) = \\ &= (x^2 + 3x + 1)^2 - 1, \end{aligned}$$

следовательно, $c = 1$. Таким образом, двойка натуральных чисел $(k, c) = (4, 1)$ является единственным ответом к задаче.

Замечание 1. Доказать, что a, b являются рациональными числами, можно и напрямую, без использования леммы 7. Например, можно сравнить коэффициенты при x^{s-1} у левой и правой частей в равенстве $x(x+1)\dots(x+s-1) + c = (x+a)^s$ и получить, что $a = \frac{s-1}{2}$. Аналогично, сравнивая

коэффициенты при x^{2s-1} в равенстве

$$x(x+1)\dots(x+k-1) = (x^2 + ax + b)^s,$$

выводим, что $a = 2s - 1$. Далее, после сравнения коэффициентов при x^{2s-2} выясняется, что $b = (s-1)(2s-1)/3$, которое так же, как и a , является рациональным.

Замечание 2. Здесь я опишу другой подход к решению задачи. Будем считать, что результаты лемм 11, 12 нам неизвестны.

Напомним, что по лемме 10 существуют натуральное $s > 1$ и многочлен $Q(x) \in \mathbb{Z}[x]$ такие, что

$$x(x+1)\dots(x+k-1) + c = Q(x)^s.$$

Полагая $x = 0$, находим, что $c = Q(0)^s = b^s$. Таким образом, верно равенство

$$x(x+1)\dots(x+k-1) = Q(x)^s - b^s.$$

Следовательно, $Q(-j)^s = b^s$ для всех $j = 1, \dots, k-1$. Если s нечетно, то многочлен $Q(x) - b$ имеет минимум k различных корней: $0, -1, \dots, -k+1$ и степень не меньше k . Но тогда степень многочлена $Q(x)^s$ не меньше sk , что больше степени многочлена $P_k(x) = x(x+1)\dots(x+k-1)$, а это невозможно.

Предположим, что s четно, в таком случае достаточно рассмотреть случай $s = 2$. Перепишем наше равенство в виде

$$x(x+1)\dots(x+k-1) = Q(x)^2 - b^2 = (Q(x)-b)(Q(x)+b).$$

Не умаляя общности, можем считать, что многочлен $Q(x)$ является приведенным и $b > 0$. Заметим, что тогда k равно удвоенной степени многочлена $Q(x)$, следовательно, должно быть четно, также четен должен быть коэффициент при x^{k-1} у многочлена $Q(x)^2 - b^2$. Поэтому число $0 + 1 + \dots + (k-1) = k(k-1)/2$, являющееся коэффициентом при x^{k-1} у многочлена $x(x+1)\dots(x+k-1)$, также является четным, а так как k четно, то такое возможно только если $4 \mid k$.

Легко понять, что многочлены $Q(x)-b$ и $Q(x)+b$ имеют ровно по $l = k/2$ различных действительных корней, которые в объединении составляют множество $\{0, -1, \dots, -k+1\}$. Пусть $r_1 < r_2 < \dots < r_l$ и $s_1 < s_2 < \dots < s_l$ — корни многочленов $R(x) = Q(x)-b$ и $S(x) = Q(x)+b$ соответственно. Заметим, что для любого $i < l$ отрезки $[r_i; r_{i+1}]$ и $[s_i; s_{i+1}]$ имеют общую точку, так как на каждом из них лежит i -й по порядку корень производной многочлена $Q(x)$, совпадающей также с производной как многочлена $R(x)$, так и многочлена $S(x)$. Также понятно, что если между двумя последовательными корнями многочлена $R(x)$ лежит $a \geq 1$ корней $S(x)$, то $a \geq 2$, иначе бы график $y = S(x)$ касался прямой $y = 0$ и у многочлена $S(x)$ был бы кратный корень, что неверно. Аналогично устанавливается факт про последовательные корни многочлена $S(x)$. Таким образом, отрезки $[r_i; r_{i+1}]$ и $[s_i; s_{i+1}]$ не просто пересекаются, а один из них лежит внутри другого.

Так как $l = k/2$ четно, то наименьшим среди всех корней многочленов $R(x)$ и $S(x)$ будет r_1 , а наибольшим будет r_l , поэтому верна следующая цепочка неравенств: $r_1 < s_1 < s_2 < r_2 < r_3 < s_3 < \dots$

$$\dots < r_{l-1} < s_{l-1} < s_l < r_l.$$

Напомним, что $r_1, r_2, \dots, r_l, s_1, s_2, \dots, s_l = \{0, -1, \dots, -k+1\}$, поэтому корнями многочлена $Q(x)-b$ будут числа $1-k, 4-k, \dots, -3, 0$, а корнями многочлена $Q(x)+b$ будут числа $2-k, 3-k, \dots, -2, -1$. Если $k > 4$, то $l > 2$, и по теореме Виета совпадают суммы корней вышеупомянутых многочленов, а также

совпадают суммы попарных произведений этих корней. Значит, совпадают и суммы их квадратов, а именно:

$$0^2 + 3^2 + \dots + (k-4)^2 + (k-1)^2 = 1^2 + 2^2 + \dots + (k-3)^2 + (k-2)^2,$$

но это равенство не может выполняться, так как для любого t

$$(t-4)^2 + (t-1)^2 = 2t^2 - 10t + 17 > 2t^2 - 10t + 13 = (t-3)^2 + (t-2)^2.$$

Следовательно, $k = 4$, при этом

$$R(x) = x(x+3), \quad S(x) = (x+1)(x+2).$$

Значит, $b = (S(x) - R(x))/2 = 2/2 = 1$ и $c = b^2 = 1$. Пара чисел $(k, c) = (4, 1)$ является единственным решением задачи.

ДАЛЬНЕЙШИЕ ПРИЛОЖЕНИЯ

Посмотрим теперь, что мы можем сделать дальше и как можно применить накопленные знания. Ниже я приведу две задачи, которые кажутся мне интересными и вряд ли могут быть легко решены без утверждений, доказанных выше.

Задача 1. Пусть

$S(x) = (x-1^2)(x-3^2)\dots(x-(d-1)^2)$, где d — четное натуральное число. Докажите, что для каждого комплексного a степень НОД многочленов $S(x)-a$ и $S'(x)$ не превосходит 1.

Решение. Если $d = 2$, то это утверждение очевидно, поэтому ниже рассматривается случай $d > 2$. Заметим, что если $P(x) = x(x+1)\dots(x+d-1)$, то $P(x) = 2^{-d} S((2x+d-1)^2)$. Обозначим через $s_1, \dots, s_{d/2-1}$ корни производной $S(x)$. Среди них нет кратных, и их можно упорядочить следующим образом:

$$1^2 < s_{d/2-1} < 3^2 < \dots < (d-3)^2 < s_1 < (d-1)^2.$$

Вспомним обозначения из леммы 11 и заметим, что верно равенство $s_i = (2r_i + d-1)^2$ для $i = 1, \dots, d/2-1$. Следовательно, $S(s_i) = 2^d P(r_i)$, и из доказательства леммы 11 следует, что

$$|S(s_1)| > |S(s_2)| > \dots > |S(s_{d/2-1})|.$$

Таким образом, для каждого комплексного a уравнение $S(x) = a$ имеет не более одного корня из множества $\{s_1, \dots, s_{d/2-1}\}$ корней $S'(x)$, что и требовалось доказать.

Задача 2 Найдите все натуральные числа n такие, что существуют многочлены $g(x)$ и $h(x)$ с комплексными коэффициентами, степень каждого из которых не меньше 2, такие, что многочлен $f(x) = x^n + \dots + x^2 + x + 1$ можно представить в виде $g(h(x))$.

Решение. Применяя идеи из доказательства леммы 12, получим, что если бы многочлены из условия задачи существовали, то многочлены $f(x) - g(\alpha)$ и $f'(x)$ делились бы на многочлен $h(x) - \alpha$ степени не меньшей 2, где α – некоторый комплексный корень многочлена $g'(x)$. Следовательно, существует как минимум два корня r, s многочлена

$$f'(x) = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2},$$

такие, что $f(r) = f(s)$. Легко понять, что $r, s \neq 1$. Заметим, что $ns^{n+1} = (n+1)s^n - 1$ и $nr^{n+1} = (n+1)r^n - 1$. Далее, из равенства $f(r) = f(s)$ следует, что

$$s^n + \dots + s^2 + s + 1 = r^n + \dots + r^2 + r + 1.$$

С другой стороны, равенство выше можно записать как

$$\frac{s^{n+1} - 1}{s - 1} = \frac{r^{n+1} - 1}{r - 1}.$$

Пользуясь этим фактом и вспоминая равенства

$$\begin{aligned} s^{n+1} &= (1 + 1/n)s^n - 1/n, \\ r^{n+1} &= (1 + 1/n)r^n - 1/n, \end{aligned}$$

получим, что

$$\left(1 + \frac{1}{n}\right) \cdot \frac{s^n - 1}{s - 1} = \left(1 + \frac{1}{n}\right) \cdot \frac{r^n - 1}{r - 1}.$$

Отсюда легко вывести, что $\frac{s^n - 1}{s - 1} = \frac{r^n - 1}{r - 1},$

что эквивалентно равенству

$$s^{n-1} + \dots + s^2 + s + 1 = r^{n-1} + \dots + r^2 + r + 1.$$

Значит, $s^n = r^n$, а следовательно, и $s^{n+1} = (1 + 1/n)s^n - 1/n = (1 + 1/n)r^n - 1/n = r^{n+1}$. Из последних двух равенств получаем $r = s$, что невозможно, так как производная многочлена $f(x)$ не имеет кратных корней. Мы получили противоречие с предположением о существовании многочленов $g(x)$ и $h(x)$, поэтому натуральных n , удовлетворяющих условию задачи, не существует.

ЗАКЛЮЧЕНИЕ

В начале этой статьи я предоставил набор базовых инструментов из алгебры и теории чисел, которыми я пользовался при решении вышеозвученной задачи. Несмотря на то, что не все эти инструменты оказались плодотворными, они содержат в себе замечательные идеи, которые могут быть полезны в будущем. Кроме того, из них читатель может почерпнуть что-то полезное о природе процесса решения задач в целом. Этот процесс прежде всего является эволюционным и основан на методе проб и ошибок.

В основных разделах этой статьи я попытался показать читателю интересные связи между алгеброй и теорией чисел. В частности, леммы 11, 12 имеют большой потенциал для применения в более сложных и захватывающих дыхание задачах. Читатель может обдумать эти леммы и попытаться найти новые способы их применения. Также важный момент заключается в том, что приобретенный набор инструментов открывает путь к реализации различных подходов в решении задач. Это очень полезно для школьников, которые постоянно заняты решением задач и готовятся к математическим соревнованиям высокого уровня, например, таким, как международная математическая олимпиада.

Отмечу напоследок, что наше упорство завело нас очень далеко и помогло нам пройти моменты кризиса. Точнее говоря, когда мы сталкиваемся с определенными трудностями при решении сложных задач, стойкость и страсть к преодолению этих трудностей помогают увидеть и понять то, о чем бы мы никогда не могли подумать раньше.

Литература

1. В.Бугаенко и др. Произведения последовательных натуральных чисел. – Материалы Летней конференции Турнира городов 2008.
2. А.Егоров. Числа Пизо. – «Квант», 2005, № 5.
3. П.Кожевников, В.Сендеров. Делители значений многочлена. – Сборник «Задачи Санкт-Петербургской олимпиады по математике 2010 года». – СПб.: Невский Диалект, 2010, с. 121–129.