Решения задач из предыдущих выпусков

6.11. Условие. Рассматриваются слова из букв русского алфавита. Слова вида SUT и $SUUT$ имеют одинаковый смысл (здесь S, U, T — произвольные слова, возможно, пустые). Докажите, что количество различных смыслов конечно.

Решение. Назовём слова A и B *эквивалентными* (обозначение: $A \sim B$), если одно можно получить из другого цепочкой замен вида $U \leftrightarrow UU$. Обозначим через $|A|$ длину слова A.

Докажем сначала следующие две леммы.

Лемма 1. *Пусть A — произвольное слово, содержащее все буквы алфавита X, а B — произвольное слово в этом алфавите. Тогда $A \sim ABC$ для некоторого слова C.*

Доказательство. Индукция по длине $|B|$ слова B. Если $|B| = 0$, утверждение тривиально. Пусть теперь $|B| > 0$, и b — первая буква слова B, то есть $B = bB'$.

Буква b встречается в A, то есть $A = UbV$ для некоторых слов U, V; тогда $A \sim UbVbV = AbV$. Применяя предположение индукции к словам $A' = Ab$ и B', находим слово C' такое, что $A' \sim A'B'C' = ABC'$; тогда $A \sim A'V \sim ABC'V$, и можно положить $C = C'V$. Лемма доказана. □

Лемма 2. *Существует такое число $f(n)$, что любое слово в n-буквенном алфавите длины, не меньшей $f(n)$, эквивалентно слову меньшей длины.*

Доказательство. Индукция по n. База индукции при $n = 1$ тривиальна: можно положить $f(1) = 2$. Для шага индукции докажем, что можно положить $f(n) = (n^{f(n-1)} + 1)f(n-1)$. Действительно, рассмотрим слово W длины, не меньшей $f(n)$, и выделим в нём $n^{f(n-1)}+1$ непересекающихся подслов длины $f(n-1)$. По принципу Дирихле, два из этих подслов будут одинаковыми, то есть $W = UABAV$, где A — слово длины $f(n-1)$. Если слово A содержит не все n букв нашего алфавита, то по предположению индукции $A \sim A'$, где $|A'| < f(n-1)$; тогда $W \sim UA'BA'V$, и утверждение доказано.

Пусть теперь A содержит все буквы алфавита. Тогда, применяя лемму, получаем, что $A \sim ABC$ для некоторого слова C. Отсюда имеем

$ABA \sim ABABC \sim ABC \sim A$, то есть $W = UABAV \sim UAV$, и $|UAV| < |W|$, что и требовалось доказать. $\square$

Теперь легко доказать утверждение задачи. Рассмотрим произвольное слово в n-буквенном алфавите; будем применять к нему лемму 2, пока его длина не меньше $f(n)$. В итоге получим, что наше слово эквивалентно слову длины, меньшей $f(n)$, то есть одному из конечного набора слов.

(*И. И. Богданов*)

11.3. Условие. $A_1, \ldots, A_n$ и $B_1, \ldots, B_n$ — два разбиения единичного квадрата на непересекающиеся измеримые множества. S_{ij} — пересечение множеств A_i и B_j, $|G|$ — площадь множества G. Докажите неравенство:

$$\sum_{ij} |S_{ij}| \cdot \ln(|S_{ij}|) \geqslant \sum_i |A_i| \cdot \ln(|A_i|) + \sum_j |B_j| \cdot \ln(|B_j|).$$

Решение. Неравенство задачи — это (с точностью до знака) стандартный факт из теории информации: энтропия совместного распределения не превосходит суммы энтропий. Приведём стандартное доказательство этого факта.

Обозначим $|S_{ij}| = s_{ij}$, $a_i = |A_i| = \sum_j s_{ij}$, $b_j = |B_j| = \sum_i s_{ij}$. Запишем разность

$$\sum_{ij} |S_{ij}| \cdot \ln(|S_{ij}|) - \sum_i |A_i| \cdot \ln(|A_i|)$$

в виде

$$\sum_{i,j} s_{ij} \ln s_{ij} - \sum_{i,j} s_{ij} \ln a_i = \sum_{i,j} a_i \frac{s_{ij}}{a_i} \ln \frac{s_{ij}}{a_i}\,. \qquad (*)$$

Заметим, что функция $f(x) = x \ln x$ выпукла при $x > 0$ (вторая производная положительна). Из неравенства Йенсена получаем при каждом j следующее неравенство

$$\sum_i a_i \frac{s_{ij}}{a_i} \ln \frac{s_{ij}}{a_i} \geqslant \left(\sum_i a_i \frac{s_{ij}}{a_i}\right) \ln \left(\sum_i a_i \frac{s_{ij}}{a_i}\right) = b_j \ln b_j\,.$$

Отсюда оцениваем правую часть $(*)$ снизу как

$$\sum_j b_j \ln b_j\,,$$

откуда и следует неравенство задачи. (*М. Н. Вялый*)

11.10. Условие. Пусть A, B — целочисленные матрицы. Известно, что $\det(A) = 1$, $\det(B) \neq 0$. Докажите, что существует $n \in \mathbb{N}$ такое, что $B^{-1} A^n B$ — целочисленная матрица.

Решение. Поскольку $\det(A)=1$, матрица A обратима по любому целому модулю.

Обозначим $\Delta=\det B$. Тогда $B^{-1}=\Delta^{-1}B'$, где B — целочисленная матрица. С другой стороны, при некотором n выполняется $A^n=1 \bmod \Delta$. Это означает, что $A^n=I+\Delta A_n$, где I — единичная, а A_n — целочисленная матрица. Но тогда матрица

$$B^{-1}A^nB=\Delta^{-1}B'(I+\Delta A_n)B=I+B'A_nB$$

также целочисленная. (*М. Н. Вялый*)

12.3. Условие. Вершины A и B графа G назовём *эквивалентными*, если существует такая последовательность вершин $A=A_0,A_1,\ldots,A_n=B$, что любые две соседние вершины A_i и A_{i+1} можно соединить k путями без общих промежуточных вершин. Докажите, что любые две эквивалентные вершины можно соединить k путями без общих рёбер.

Решение. Утверждение задачи вытекает из следующего факта.

Вершины A и B графа назовём эквивалентными, *если существует такая последовательность вершин $A=A_0,A_1,\ldots,A_n=B$, что любые две соседние вершины A_i и A_{i+1} можно соединить k путями без общих рёбер. Любые две эквивалентные вершины можно соединить k путями без общих рёбер.*

Доказательство факта. Если удалить любые $k-1$ рёбер, то для любого i вершины A_i и A_{i+1} окажутся в одной компоненте связности. Значит, вершины A_0 и A_n также окажутся в одной компоненте связности. Остается применить рёберную теорему Менгера.

Примечание. Это решение изоморфно первому решению, приведённому в прошлом выпуске сборника «Математическое просвещение». Действительно, теорема Форда – Фалкерсона для единичных пропускных способностей есть просто рёберная теорема Менгера. (*Б. Мохар*)

15.10. Условие. На грани правильного тетраэдра отмечена точка. Докажите, что тетраэдр можно разрезать на четыре равных выпуклых многогранника так, чтобы эта точка была вершиной одного из них.

Решение. Пусть $A_1A_2A_3A_4$ — исходный тетраэдр, O — его центр, а X_1 — данная точка на грани $A_2A_3A_4$. Обозначим через φ_{12} отражение относительно прямой ℓ_{12}, проходящей через середины рёбер A_1A_2 и A_3A_4, через φ_{13} и φ_{14} — два аналогичных отражения относительно прямых ℓ_{13} и ℓ_{14}. Тогда $\varphi_{1i}\circ\varphi_{1j}=\varphi_{1k}$, если $\{i,j,k\}=\{1,2,3\}$. Таким образом, отражения φ_{12}, φ_{13}, φ_{14} вместе с тождественным отображением образуют подгруппу в группе S_4 всех самосовмещений тетраэдра (эта подгруппа называется *группой Клейна*).

Положим $X_2 = \varphi_{12}(X_1)$, $X_3 = \varphi_{13}(X_1)$, $X_4 = \varphi_{14}(X_1)$. Тогда точка X_i лежит на грани $A_{i+1}A_{i+2}A_{i+3}$ (все индексы берутся по модулю 4, то есть, например, $A_5 = A_1$). Заметим, что четвёрка точек (X_1, X_2, X_3, X_4) переходит в себя при любом отражении φ_{1i}. Поэтому и сумма векторов $\vec{s} = \overrightarrow{OX_1} + \overrightarrow{OX_2} + \overrightarrow{OX_3} + \overrightarrow{OX_4}$ переходит в себя при действии нашими отражениями; значит, $\vec{s} = 0$. Таким образом, либо точка O лежит внутри тетраэдра $X_1X_2X_3X_4$, либо точки X_1, X_2, X_3, X_4 компланарны.

Если тетраэдр $X_1X_2X_3X_4$ невырожден, то всё пространство разбивается на четыре трёхгранных угла $C_1 = OX_2X_3X_4$, $C_2 = OX_1X_3X_4$, $C_3 = OX_1X_2X_4$, $C_4 = OX_1X_2X_3$. Наши отражения переставляют эти трёхгранные углы и переводят тетраэдр в себя. Значит, если мы обозначим через T_i пересечение нашего тетраэдра с C_i, то $\varphi_{1i}(T_1) = T_i$, поэтому все многогранники T_i равны. Кроме того, T_i выпуклы как пересечения выпуклых множеств, и точка X_1 является вершиной T_1. Итого, наше разбиение построено.

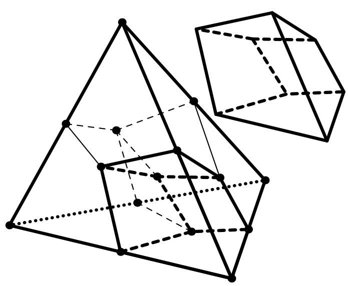

Рис. 1

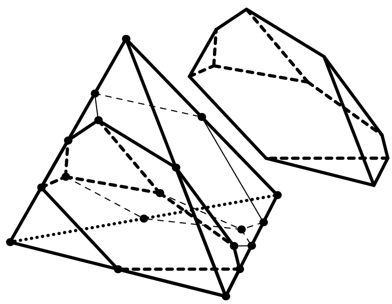

Рис. 2

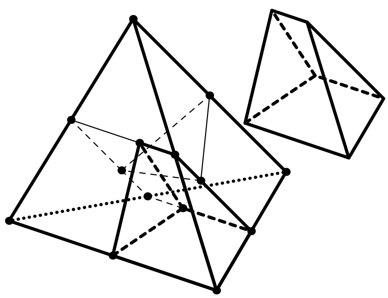

Рис. 3

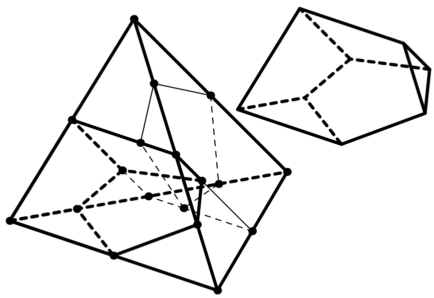

Рис. 4

Пусть, наконец, точки X_1, X_2, X_3, X_4 компланарны. Тогда четырёхугольник $X_1X_2X_3X_4$ имеет (в пространстве) три попарно перпендикулярных оси симметрии; значит, это — прямоугольник (возможно, вырожденный), его стороны параллельны двум из прямых ℓ_{1i} (скажем, ℓ_{12} и ℓ_{13}) и пересекают их. Таким образом, эти четыре точки лежат в «срединной» плоскости, равноудалённой от рёбер A_1A_4 и A_2A_3. В этом случае построение может быть получено, например, предельным переходом из невырожденного случая.

На рис. 1 и 2 показаны два возможных невырожденных разрезания, полученных описанным способом (справа от каждого тетраэдра показан один из многогранников разбиения). На рис. 3 и 4 — «вырожденные» разрезания, полученные из них предельным переходом.

Замечание. Вместо группы Клейна можно бы было рассмотреть движение пространства, переставляющее все вершины тетраэдра циклически, и группу, порождённую этим движением. Аналогичное построение, естественно, тоже работает. На рис. 5 и 6 показаны два разрезания, полученные таким образом.

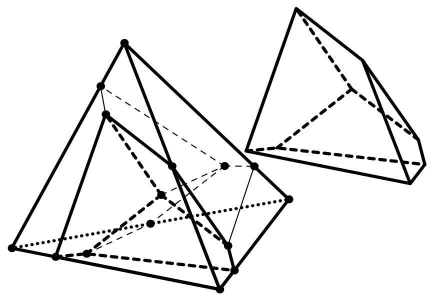

Рис. 5

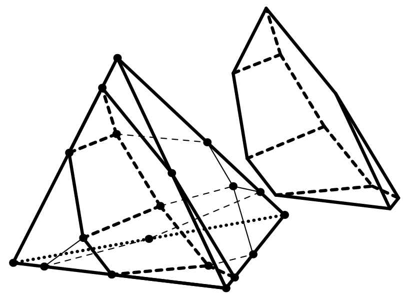

Рис. 6

Нетрудно видеть, что эта вариация допускает также обобщение на n-мерный случай.

(*И. И. Богданов*)

16.2. Условие. В Черноморске во время обсуждения вопроса о том, когда же наконец Черноморск объявят вольным городом, сложилась занятная ситуация. Все черноморцы разбились на партии, а все партии на фракции так, что: 1) существует партия, в которой объединились все n жителей города; 2) каждая партия состояла ровно из двух непересекающихся фракций; 3) каждая фракция численностью более одного человека считала себя партией. Каждый житель города платит членский взнос (1 руб.) в каждой партии, членом которой является. Как им надо было организоваться, чтобы сумма взносов была: а) максимальной; б) минимальной?

Решение. Пусть $\mathrm{Mx}(n)$ — максимально возможная сумма членских взносов, $\mathrm{Mn}(x)$ — минимально возможная. Пусть k — оптимальное число изначального деления черноморцев на две партии, так чтобы сумма членских взносов была бы, скажем, минимальна. Тогда $\mathrm{Mn}(n) = \mathrm{Mn}(k) + \mathrm{Mn}(n-k) + n$, ибо внутри фракций черноморцы делятся оптимальным образом. Таким образом, имеет место равенство:

$$\mathrm{Mn}(n) = \min_k(\mathrm{Mn}(k) + \mathrm{Mn}(n-k)) + n. \tag{1}$$

Аналогичным образом, для задачи о максимума членских взносов имеет место равенство

$$\mathrm{Mn}(n) = \max_k(\mathrm{Mn}(k) + \mathrm{Mn}(n-k)) + n. \tag{2}$$

Из формулы (2) непосредственной индукцией легко проверить, что $\mathrm{Mx}(n) = n(n+1)/2 - 1$.

Равенство для минимума членских взносов несколько сложнее. Пусть $n = 2^k + l$; $0 \leqslant l \leqslant 2^k$. Тогда $\mathrm{Mn}(n) = kn + 2l$. Это равенство также с помощью индукции выводится из формулы (1). Соответственно, $\mathrm{Mn}(2047) = 11 \cdot 2047$.

Замечание. Можно рассматривать двоичное дерево, связанное с разбиением на партии/фракции и заметить, что если есть две висячие вершины, чьи уровни отличаются не менее чем на 2, то одну из них можно перенести к другой так, чтобы общая сумма членских взносов уменьшилась.

(*А. Я. Канель-Белов*)

16.11. Условие. При каких натуральных n число $\dfrac{3^n-1}{2}$ есть квадрат целого числа?

Ответ: $n \in \{1, 2, 5\}$.

Решение. Требуется решить уравнение

$$2x^2 + 1 = 3^n \tag{1}$$

в натуральных числах n и x.

1-й способ. Этот способ решения опирается на теорию уравнений вида

$$X^2 - AY^2 = B, \tag{2}$$

где $A > 0$, $B \neq 0$ — целые числа и $\sqrt{A}$ иррационален. Частным случаем является *уравнение Пелля* с $B = 1$. Все решения уравнения (2) в целых числах X, Y могут быть найдены из формул

$$X + Y\sqrt{A} = \pm(X_j + Y_j\sqrt{A})(X_0 + Y_0\sqrt{A})^k, \quad k \in \mathbb{Z},$$

где (X_j, Y_j) — некоторые *базисные* решения, а (X_0, Y_0) — *минимальное* решение ассоциированного уравнения Пелля в натуральных числах (подробности читатель может найти, например, в статье [2] или книге [3]).

Пусть сначала n чётно, $n = 2m$. Положим $y = 3^m$. Уравнение Пелля

$$y^2 - 2x^2 = 1$$

в натуральных числах имеет единственную серию решений:

$$y + x\sqrt{2} = (3 + 2\sqrt{2})^k, \quad (k = 1,\, 2,\, \ldots).$$

Если $m \geqslant 2$, то $y \equiv 0 \pmod 9$, а это имеет место тогда и только тогда, когда $k \equiv 3 \pmod 6$.

Действительно, последовательность чисел $(3 + 2\sqrt{2})^k$ является периодической по любому модулю (подумайте, почему). Заметим, что

$$(3 + 2\sqrt{2})^6 \equiv -1 \pmod 9.$$

Поэтому если $k = 6q + r$, где $r \in \{0, 1, \ldots, 5\}$, то

$$(3 + 2\sqrt{2})^k \equiv (-1)^q (3 + 2\sqrt{2})^r \pmod 9.$$

Проверка показывает, что только при $r = 3$ рациональная часть числа $(3 + 2\sqrt{2})^r$ будет $\equiv 0 \pmod 9$.

Но для $k = 6q + 3$ имеем $y \equiv 0 \pmod{11}$, что невозможно, если $y = 3^m$.

В самом деле, поскольку $(3 + 2\sqrt{2})^6 \equiv -1 \pmod{11}$, имеем

$$(3 + 2\sqrt{2})^k \equiv (-1)^q (3 + 2\sqrt{2})^3 \equiv (-1)^q 4\sqrt{2} \pmod{11},$$

откуда и следует утверждение.

Итак, $m = 1$ — единственное возможное значение, откуда $(n, x) = (2, 2)$.

В случае нечётного $n = 2m + 1$ рассуждения аналогичны. Положим $z = 2x$, $y = 3^m$. Уравнение

$$z^2 - 6y^2 = -2$$

в натуральных числах также имеет единственную серию решений:

$$z + y\sqrt{6} = (2 + \sqrt{6})(5 + 2\sqrt{6})^k \quad (k = 0,\, 1,\, 2,\, \ldots).$$

Далее можно проверить, что сравнение $y \equiv 0 \pmod{27}$ равносильно сравнению $k \equiv 4 \pmod 9$, однако для таких k имеем $y \equiv 0 \pmod{17}$ — противоречие. Таким образом, $m \leqslant 2$, что даёт $(n, x) \in \{(1, 1), (5, 11)\}$.

2-й способ. Для чётных $n = 2m$ можно рассуждать совсем элементарно, предварительно переписав уравнение в виде

$$(3^m - 1)(3^m + 1) = 2x^2.$$

Положим $x = 2x_1$, тогда

$$\frac{3^m - 1}{2} \cdot \frac{3^m + 1}{2} = 2x_1^2,$$

при этом числа $(3^m \pm 1)/2$ взаимно просты. Возможны следующие два случая: либо
$$\frac{3^m-1}{2}=2a^2, \quad \frac{3^m+1}{2}=b^2,$$
либо
$$\frac{3^m-1}{2}=a^2, \quad \frac{3^m+1}{2}=2b^2$$
(a, b — некоторые натуральные числа). Но в первом случае равенство
$$3^m=4a^2+1$$
невозможно, поскольку $4a^2+1$ не делится на 3. Во втором случае имеем
$$3^m=(2b-1)(2b+1),$$
откуда $2b-1=1$ и $2b+1=3^m$, т. е. $b=1$, $m=1$ и $x=2$.

В случае нечётных $n=2m+1$ рассуждение менее элементарно. Мы можем воспользоваться тем, что кольцо
$$\mathbb{Z}[\sqrt{-2}]=\{a+b\sqrt{-2} : a,\, b\in\mathbb{Z}\}$$
факториально, т. е. для него справедлив аналог основной теоремы арифметики об однозначном разложении в произведение простых чисел. Проще всего это доказать, заметив, что кольцо $\mathbb{Z}[\sqrt{-2}]$ *евклидово*, т. е. в нём возможно *деление с остатком* (точные формулировки соответствующих определений и фактов см., например, в учебнике [1, с. 190–197]; проверка евклидовости кольца $\mathbb{Z}[\sqrt{-2}]$ относительно нормы $N(a+b\sqrt{-2})=a^2+2b^2$ оставляется читателю в качестве несложного упражнения).

Перепишем уравнение (1) в виде
$$(1+x\sqrt{-2})(1-x\sqrt{-2})=(1+\sqrt{-2})^{2m+1}(1-\sqrt{-2})^{2m+1}. \tag{3}$$
Заметим, что числа $1\pm x\sqrt{-2}$ взаимно просты в кольце $\mathbb{Z}[\sqrt{-2}]$, а числа $1\pm\sqrt{-2}$ являются простыми в этом кольце. Поэтому из равенства (3) и свойства факториальности следует, что
$$1+x\sqrt{-2}=\pm(1\pm\sqrt{-2})^{2m+1}$$
при некотором выборе знаков. Раскрыв бином и приравняв вещественные части, получим равенство
$$1-C_{2m+1}^2 2+C_{2m+1}^4 2^2-\ldots+(-1)^m C_{2m+1}^{2m}2^m=\pm1. \tag{4}$$

При знаке «минус» в случае $m\geqslant 2$ это равенство можно переписать в виде
$$1-C_{2m+1}^2+C_{2m+1}^4 2-\ldots+(-1)^m C_{2m+1}^{2m}2^{m-1}=0.$$
Но такое равенство невозможно, поскольку при любом m число
$$1-C_{2m+1}^2+C_{2m+1}^4 2=\frac{(2m-1)(2m^3-m^2-4m-3)}{3}$$
не делится на 4.

Пусть теперь в равенстве (4) взят знак «плюс». Тогда при $m \geqslant 5$ оно примет вид

$$C_{2m+1}^2 - C_{2m+1}^4 2 + C_{2m+1}^6 2^2 - C_{2m+1}^8 2^3 + \ldots - (-1)^m C_{2m+1}^{2m} 2^{m-1} = 0. \quad (5)$$

Ясно, что m должно быть чётным. Положим

$$\begin{aligned} A = C_{2m+1}^2 - C_{2m+1}^4 2 + C_{2m+1}^6 2^2 - C_{2m+1}^8 2^3 = \\ = -\frac{m(m-2)(2m+1)(8m^5 - 68m^4 + 158m^3 - 139m^2 + 254m + 102)}{315}. \end{aligned}$$

Для любого целого числа $P \neq 0$ пусть $\nu_2(P)$ обозначает такое целое неотрицательное число α, что P делится на 2^α, но не делится на $2^{\alpha+1}$. Для любого рационального числа P/Q положим $\nu_2(P/Q) = \nu_2(P) - \nu_2(Q)$. Как нетрудно видеть,

$$\nu_2(A) = \nu_2(m(m-2)) + 1.$$

Для доказательства невозможности равенства (4) нам достаточно убедиться в справедливости неравенств $\nu_2(B_l) > \nu_2(A)$, где

$$B_l = C_{2m+1}^{2l} 2^{l-1}, \quad 5 \leqslant l \leqslant m.$$

Имеем $B_l = C_{2m-9}^{2l-10} B 2^{l-1}$, где

$$B = \frac{m(m-1)(m-2)(m-3)(m-4)(2m+1)(2m-1)(2m-3)(2m-5)(2m-7)}{l(l-1)(l-2)(l-3)(l-4)(2l-1)(2l-3)(2l-5)(2l-7)(2l-9)}.$$

Поэтому

$$\begin{aligned} \nu_2(B_l) \geqslant \nu_2(B2^{l-1}) = \nu_2(m(m-2)(m-4)) + a \geqslant \\ \geqslant \nu_2(m(m-2)) + 1 + a = \nu_2(A) + a, \end{aligned}$$

где

$$a = \nu_2\left(\frac{2^{l-1}}{l(l-1)(l-2)(l-3)(l-4)}\right) > 0$$

при любом $l \geqslant 5$.

Комментарии. I. Уравнения

$$x^2 + 2 = 3^n, \quad x^2 + 4 = 5^n$$

также могут быть решены двумя способами (первое из них было представлено на VIII Кубке памяти Колмогорова). Уравнение

$$7x^2 - 4 = 3^n$$

решается первым способом, а уравнение

$$x^2 + 7 = 2^n$$

(уравнение Рамануджана – Нагеля, см. [4], а также [5, p. 205–206]) — вторым, но технически более сложно. Этим же способом, но технически проще решается уравнение

$$x^2 + 1 = y^n$$

при любом целом $y > 1$ (см. материалы X Кубка памяти Колмогорова).

Есть многочисленные примеры подобных уравнений, которые можно решить школьными методами, при этом используются только основная теорема арифметики и метод остатков.

Один из неэлементарных подходов связан с эллиптическими кривыми. Решение уравнения (1) сводится к отысканию всех целых точек на кривых

$$2x^2 + 1 = 3^r y^3, \quad r \in \{0, 1, 2\}.$$

При $r = 0$ эта задача может быть решена элементарно (снова можно воспользоваться факториальностью кольца $\mathbb{Z}[\sqrt{-2}]$).

II. Решение уравнения

$$2x^2 + 1 = 3^n$$

первым способом есть на `www.artofproblemsolving.com` (см. [6]).

Список литературы

[1] Кострикин А. И. *Введение в алгебру. Часть* I. *Основы алгебры*. М.: Физико-математическая литература. 2000.

[2] Спивак А. В. *Уравнения Пелля* // Квант. №4. 2002. С. 5–11.

[3] Barbeau E. J. *Pell's equation*. New-York: Springer-Verlag. 2003.

[4] Nagell T. *The Diophantine equation* $x^2 + 7 = 2^n$ // Ark. Mat. Vol. 4. 1961. P. 185–187.

[5] Mordell L. J. *Diophantine equations*. London: Academic Press Inc. 1969.

[6] `http://.../Forum/viewtopic.php?f=56&t=346906`

(*Н. Н. Осипов*)