Экспоненциальные диофантовы уравнения и сумма цифр числа

В. М. Журавлёв, П. И. Самовол

Если я смогу расширить в этом пункте границы Арифметики, то Вы даже не поверите, какие чудесные предложения мы сможем отсюда получить.

Из письма Ферма к Мерсенну

Число «66» ничем не успело зарекомендовать себя в глазах Стёпы. Оно состояло в визуальном родстве с нулём, что делало его не до конца понятным. Кроме того, «66» приходилось родственником другому известному числу, «666». Иного это напугало бы, но Стёпа гораздо сильнее опасался числа «661», которое делилось на «43» без остатка.

Виктор Пелевин. Числа

§ 1. Введение

Однажды французский композитор и теоретик музыки Филипп де Витри заказал Льву Герсониду небольшое математическое исследование. Филиппа де Витри интересовали гармонические[1)] числа, которые он использовал при написании музыкальных произведений — мотетов. В 1343 году Лев Герсонид завершил исследование и написал короткое сочинение, которое сохранилось под названием «De Numeris Harmonicis». В этой работе было доказано, что существуют только четыре пары гармонических чисел, отличающихся на единицу — это пары $(1;2)$, $(2;3)$, $(3;4)$ и $(8;9)$. На современном математическом языке можно сказать, что Герсонид решил

[1)] Числа вида 2^a3^b.

в целых неотрицательных числах уравнение

$$2^a 3^b + 1 = 2^c 3^d.$$

Если использовать свойства делимости на 2 и на 3, то легко видеть, что решение этого уравнения сводится к двум следующим случаям.

Задача 1. Найти все решения уравнений в целых неотрицательных числах n и m:

$$\text{а) } 1 + 2^n = 3^m; \quad \text{б) } 1 + 3^m = 2^n. \tag{1}$$

В такой простой формулировке задача по решению этих уравнений давно стала фольклорной, и мы можем найти её в разных источниках [3, 9, 10]. Впрочем, для решения этой задачи школьнику нужно не только уметь правильно делить с остатком (в отличие от Стёпы из эпиграфа[2)]), но также знать основы теории делимости и иметь некоторые навыки решения задач с помощью сравнений по модулю. К слову сказать, современное решение этих уравнений, доступное для понимания школьника, занимает чуть больше двух абзацев.

В современной теории чисел уравнения, решения которых ищутся в натуральных, целых или рациональных числах, называются диофантовыми уравнениями. Из дошедших до нашего времени источников можно узнать, что сам Диофант умел решать не только линейные и квадратные уравнения, но также некоторые уравнения третьей, четвёртой и даже шестой степени. Если неизвестные величины находятся в показателях степеней членов диофантового уравнения, то такие уравнения называются экспоненциальными или показательными диофантовыми уравнениями. Уравнения такого вида гораздо труднее поддаются изучению в отличие от полиномиальных диофантовых уравнений. Таким образом, с большой долей уверенности можно сказать, что Герсонид первым начал исследование экспоненциальных диофантовых уравнений.

§ 2. Некоторые обобщения

Вышеуказанные уравнения являются частными случаями диофантового уравнения

$$a^x - b^y = k, \tag{2}$$

где a и b — натуральные параметры, $k \neq 0$ — целое число.

Поисками решений этого диофантового уравнения математики активно занимались в середине прошлого века и доказали, что количество его

[2)] Элементарная проверка показывает, что $661 = 43 \cdot 15 + 16 \equiv 16 \pmod{43}$, т. е. 661 нацело на 43 не делится.

решений конечно (см., например, [13, с. 51]). Более того, если $k = 1$, то это уравнение имеет не более одного решения за исключением случая $a = 3$ и $b = 2$, в котором имеется ровно два решения, указанных Герсонидом.

На рубеже веков удалось решить ещё одно из известных обобщений уравнения (1) — *уравнение Каталана*

$$x^u - y^v = 1, \quad \text{где } u, v > 1.$$

Подробно об этом уравнении можно прочитать в статье [8].

В рамках этой статьи мы хотим провести небольшое математическое исследование. Будем обобщать уравнения из задачи 1, увеличивая количество слагаемых в левой части. Мы решим несколько таких уравнений и по ходу исследования попытаемся ответить на возникающие вопросы.

Для начала нас будет интересовать, в каких случаях степень тройки можно представить в виде суммы единицы и двух различных степеней двойки?

Задача 2. Найти все решения уравнения в натуральных числах a, b, m

$$1 + 2^a + 2^b = 3^m, \quad \text{где } a < b. \tag{3}$$

Отметим, что в условии задачи мы оставляем строгое неравенство $a < b$, поскольку при $a = b$ мы просто попадаем в случай задачи 1. Затем попробуем узнать, в каких случаях степень тройки можно представить в виде суммы единицы и трёх различных степеней двойки.

Задача 3. Найти все решения уравнения в натуральных числах

$$1 + 2^a + 2^b + 2^c = 3^m, \quad \text{где } a < b < c. \tag{4}$$

Общий случай с k слагаемыми подразумевает серьёзное знание темы. Поэтому попытаемся его конкретизировать.

Диофантовы уравнения могут иметь и конечное число решений (в частности, ни одного), и бесконечное. Исходя из этого сформулируем следующую задачу.

Задача 4. Зафиксируем натуральное число k. Конечно или бесконечно количество решений в натуральных числах уравнения

$$1 + 2^{a_1} + 2^{a_2} + 2^{a_3} + \ldots + 2^{a_k} = 3^m, \quad \text{где } a_1 < a_2 < \ldots < a_k? \tag{5}$$

Этот общий вопрос на сегодняшний день не имеет простого решения. Он связан с очень серьёзными фундаментальными теоремами, и его подробное обсуждение выходит за рамки этой небольшой заметки. Тем не менее, мы попытаемся поработать с большим числом слагаемых, чтобы определить возможные подходы к решению этой задачи элементарными методами.

§ 3. Несколько частных случаев

Любое исследование начинается с рассмотрения частных случаев. Мы не будем отступать от этого принципа и поэтому приведём решение п. а) первой задачи. Итак, решаем уравнение $1 + 2^n = 3^m$. Как мы и обещали, попытаемся втиснуть решение в два абзаца, сконцентрировавшись на математической идее и опуская излишние подробности.

Решение задачи 1а). Если m нечётно, т. е. $m = 2q+1$, то $3^m \equiv 3^{2q+1} \equiv 3 \pmod 8$, откуда $1 + 2^n \equiv 3 \pmod 8$. Последнее сравнение выполняется только для $n = 1$, тогда $m = 1$.

Если m чётно, то $m = 2q$. Тогда $2^n = (3^q - 1)(3^q + 1)$. Последнее равенство возможно, только если каждый сомножитель в правой части является степенью двойки. Имеем для некоторых натуральных b, c

$$\begin{cases} 3^q - 1 = 2^b, \\ 3^q + 1 = 2^c \end{cases} \quad\Rightarrow\quad 2 = 2^c - 2^b \quad\Rightarrow\quad c = 2,\ b = 1,\ q = 1.$$

Откуда $m = 2$, $n = 3$.

Итак, ответ для задачи 1а) состоит из двух пар: $(n; m) \in \{(1; 1), (3; 2)\}$.

Надеемся, что подобным образом читатели решат уравнение $1 + 3^m = 2^n$ и подтвердят результат, полученный Герсонидом.

Упражнение 1. Найти все решения уравнений в натуральных числах m, n и $q > 7$:

$$\begin{array}{lll} \text{а) } 1 + 2^n = 5^m; & \text{б) } 1 + 2^n = 7^m; & \text{в) } 1 + 2^n = q^m; \\ \text{г) } 2^n - 1 = 5^m; & \text{д) } 2^n - 1 = 7^m; & \text{е) } 2^n - 1 = q^m. \end{array}$$

Перейдём теперь к уравнению $1 + 2^a + 2^b = 3^m$, где $1 \leqslant a < b$.

Решение задачи 2 (I способ). Правая часть уравнения делится на три, следовательно, и левая часть делится на три. Это возможно только в том случае, когда оба показателя степеней двоек — чётные числа. Значит, $a = 2a_1$ и $b = 2b_1$. Тогда имеем $4^{a_1} + 4^{b_1} = 3^m - 1$. Поскольку левая часть полученного уравнения делится на 4, то и правая его часть должна делиться на 4. Поэтому m чётно, т. е. $m = 2q$. Разложив на множители, получим

$$2^{2a_1} \cdot (1 + 4^{b_1 - a_1}) = (3^q - 1)(3^q + 1).$$

Числа $3^q - 1$ и $3^q + 1$ — последовательные чётные числа. Поэтому одно из них делится на 2 только в первой степени. Рассмотрим два возможных случая.

В первом случае имеем

$$\begin{cases} 3^q - 1 = 2^{2a_1-1} \cdot t, \\ 3^q + 1 = 2^{2a_1-1} \cdot t + 2, \end{cases} \quad \text{где } t \text{ — нечётное число.}$$

Тогда

$$2^{2a_1} \cdot (1 + 4^{b_1-a_1}) = 2^{2a_1} t(2^{2a_1-2}t + 1).$$

Разделив обе части уравнения на 2^{2a_1}, получим

$$1 + 4^{b_1-a_1} = t(2^{2a_1-2}t + 1).$$

Далее,

$$t - 1 = 4^{b_1-a_1} - 2^{2a_1-2}t^2 = (2^{b_1-a_1} - 2^{a_1-1}t)(2^{b_1-a_1} + 2^{a_1-1}t).$$

Если нечётное число $t \geqslant 3$, то левая часть уравнения положительна, следовательно, и правая положительна, и мы имеем $2^{b_1-a_1} - 2^{a_1-1}t \geqslant 1$. Но тогда $t - 1 \geqslant 1 \cdot (1 + t)$. Получаем противоречие. Остаётся $t = 1$.

При $t = 1$ мы получаем уравнение $3^q - 1 = 2^{2a_1-1}$, которое мы решали выше. Для $q = 1$, $m = 2$ получим противоречие с неравенством $1 \leqslant a < b$. Значит, $q = 2$ и $m = 4$. Тогда $a_1 = 2$, $a = 4$, откуда $b = 6$.

Во втором случае мы должны записать

$$\begin{cases} 3^q - 1 = 2^{2a_1-1} \cdot t - 2, \\ 3^q + 1 = 2^{2a_1-1} \cdot t, \end{cases} \quad \text{где } t \text{ — нечётное число.}$$

Аналогично получаем $1 + 4^{b_1-a_1} = t(2^{2a_1-2}t - 1)$ и далее

$$t + 1 = 2^{2a_1-2} \cdot t^2 - 4^{b_1-a_1} = (2^{a_1-1}t - 2^{b_1-a_1})(2^{a_1-1}t + 2^{b_1-a_1}).$$

Последнее равенство для нечётных значений t возможно при $a < b$ только в случае $a_1 = 1$. Но тогда $t + 1 \geqslant 1 \cdot (t + 2)$. Получаем противоречие.

В результате мы нашли единственное решение диофантова уравнения: $(a; b; m) \in \{(4; 6; 4)\}$.

Упражнение 2 (LXI ММО, 1998, задача 11.4, [11]). Решите в натуральных числах уравнение $3^x + 4^y = 5^z$.

Упражнение 3 (47 IMO, задача 4, Словения 2006). Найдите все пары (x, y) целых чисел такие, что $1 + 2^x + 2^{2x+1} = y^2$.

Решение задачи 2 не кажется слишком сложным и экстраординарным. Мы использовали те же методы, что и при решении задачи 1, а именно сравнения по модулю и разложение на множители. Кроме того, на одном из этапов решения задачи 2 нам удалось свести её к задаче 1, что наталкивает на мысль о возможности применения метода математической индукции. Именно поэтому вначале у авторов возникло ложное чувство, что трудности, возникающие при дальнейшем увеличении числа слагаемых, будут преодолимыми. Однако уже при попытках рассмотреть следующий случай, а именно представление степени тройки в виде суммы единицы и трёх различных степеней двойки, обнаружилось много сюрпризов.

Авторы предлагают пытливым читателям хотя бы на пару часов отложить чтение этой статьи и попробовать самостоятельно решить задачу 3, а затем сравнить результаты.

Итак, продолжим.

Нам понадобятся некоторые классические результаты, которые мы приведём без доказательства со ссылкой на источники. Кроме того, мы сформулируем и докажем в виде лемм несколько важных вспомогательных утверждений.

§ 4. Очень важная лемма

О малой теореме Ферма и теореме Эйлера написано немало, см., например, подборку статей [1, 2, 7]. В этом разделе мы приведём формулировки теорем, а чуть позже применим теоремы при решении наших задач.

Теорема 1 (Малая теорема Ферма). *Если числа a и p взаимно просты и p простое, то $a^{p-1} \equiv 1 \pmod{p}$.*

При решении задач 1 и 2 мы столкнулись с необходимостью выяснить, на какую степень двойки делится число $3^m - 1$. Частичный ответ на этот вопрос мы можем почерпнуть из теоремы Эйлера.

Теорема 2 (Эйлер). *Если числа a и m взаимно просты, то $a^{\phi(m)} \equiv 1 \pmod{m}$, здесь $\phi(m)$ — функция Эйлера.*

Возьмём $m = 2^{n+1}$, тогда $\phi(m) = 2^n$. Поэтому $3^{2^n} \equiv 1 \pmod{2^{n+1}}$ и, более того, для любого натурального t выполняется $(3^t)^{2^n} \equiv 1 \pmod{2^{n+1}}$, поскольку числа 3^t и 2^{n+1} взаимно просты. Следовательно, число $3^{2^n t} - 1$ делится на 2^{n+1} и, конечно, делится на степени двойки с меньшими показателями.

И всё же в нашем случае ответ, полученный с помощью теоремы Эйлера, не является исчерпывающим. Фактически мы хотим узнать, на какую *максимальную* степень двойки делится число $3^m - 1$. Такой показатель степени 2 называется 2-адическим (диадическим) показателем для числа $3^m - 1$. Нам поможет следующая

Лемма 1. *Для $i \geqslant 1$ выполняется равенство $3^{2^i} = 1 + 2^{i+2} + 2^{i+3}q$, где $q \in \mathbb{Z}$.*

Доказательство.

$$\frac{3^{2^i}-1}{2^{i+2}} = \frac{(3-1)(3+1)(3^2+1)\ldots(3^{2^{i-1}}+1)}{2^{i+2}} = \frac{3^2+1}{2}\cdot\frac{3^4+1}{2}\cdot\ldots\cdot\frac{3^{2^{i-1}}+1}{2} = r.$$

Каждый сомножитель представляет собой нечётное число, поскольку является половиной суммы квадрата нечётного числа и 1:

$$\frac{(2x+1)^2+1}{2} = 1 + 2(x^2+x)$$

— нечётное число. Следовательно, число r также нечётно: $r = 2q+1$, где $q \in \mathbb{Z}$. Тогда $\dfrac{3^{2^i}-1}{2^{i+2}} = 2q+1$, откуда $3^{2^i} = 1 + 2^{i+2} + 2^{i+3}q$, ч. т. д. □

Из леммы 1 вытекает очевидное

Следствие 1. *Для $i \geqslant 1$ выполняется*
а) $3^{2^i} \equiv 1 \pmod{2^{i+2}}$; б) $3^{2^i} \equiv 1 + 2^{i+2} \pmod{2^{i+3}}$.

Рассмотрим выражение $3^{2^n t} - 1$ для нечётного числа t. Мы можем разложить его на множители:

$$3^{2^n t} - 1 = (3^{2^n})^t - 1 = (3^{2^n} - 1)\big((3^{2^n})^{t-1} + (3^{2^n})^{t-2} + \ldots + 3^{2^n} + 1\big).$$

Множитель $(3^{2^n})^{t-1} + (3^{2^n})^{t-2} + \ldots + 3^{2^n} + 1$ является нечётным числом как сумма нечётного числа нечётных слагаемых. Следовательно, максимальная степень двойки, на которую делится число $3^{2^n t} - 1$, совпадает с максимальной степенью двойки, на которую делится число $3^{2^n} - 1$. Таким образом, лемма улучшает результат, полученный из теоремы Эйлера, а именно: если t — нечётное число, то число $3^{2^n t} - 1$ делится на 2^{n+2} и не делится на 2^{n+3}. Другими словами, число $n+2$ является 2-адическим (диадическим) показателем числа $3^{2^n t} - 1$.

Фактически мы доказали следующее утверждение:

Лемма 2. *Если $3^m - 1$ делится на 2^a и не делится на 2^{a+1}, то $m = 2^{a-2}t$, где t — нечётное число.*

В такой формулировке этот результат мы будем часто применять в дальнейшем. Интересные примеры нахождения p-адических показателей для случая простого числа $p \geqslant 3$ читатели могут найти в статье [4].

Опираясь на лемму 2, мы можем получить другой способ решения задачи 2.

Решение задачи 2 (II способ). По условию $1 + 2^a + 2^b = 3^m$. Правая часть уравнения делится на три, следовательно, и левая часть делится на три. Это возможно только в том случае, когда оба показателя степеней двоек — чётные числа. Значит, $a = 2a_1 \geqslant 2$ и $b = 2b_1 \geqslant 2$. Перепишем наше уравнение в виде

$$2^a(1 + 2^{b-a}) = 3^m - 1.$$

Поскольку $1 + 2^{b-a}$ — нечётное число, получаем, что $3^m - 1$ делится на 2^a и не делится на 2^{a+1}. Тогда из леммы 2 следует, что $m = 2^{a-2}t$, где t нечётно и $a = 2a_1 > 3$. Предположим, что $a > 5$. Тогда $3^{2^{a-3}t} \geqslant 3^{2^{a-3}} > 2^a$. Имеем

$$1 + 2^a = 3^m - 2^b = (3^{2^{a-3}t})^2 - (2^{b_1})^2 = (3^{2^{a-3}t} - 2^{b_1})(3^{2^{a-3}t} + 2^{b_1}).$$

Значит, $3^{2^{a-3}t} - 2^{b_1} \geqslant 1$. Далее,

$$1 + 2^a = (3^{2^{a-3}t} - 2^{b_1})(3^{2^{a-3}t} + 2^{b_1}) \geqslant 1 \cdot (3^{2^{a-3}t} + 2^{b_1}) > 2^a + 2^{b_1}.$$

Получаем, что $1 + 2^a > 2^a + 2^{b_1}$, что невозможно. В силу чётности a, остаётся только $a = 4$. Имеем

$$17 = 1 + 2^4 = 3^m - 2^b = (3^{2t} - 2^{b_1})(3^{2t} + 2^{b_1}),$$

откуда $1 = 3^{2t} - 2^{b_1}$ и $17 = 3^{2t} + 2^{b_1}$. Получаем $b = 6$, $m = 4$.

В итоге имеем единственное решение $(a; b; m) \in \{(4; 6; 4)\}$.

Упражнение 4. Найти все решения уравнений в целых неотрицательных числах a, b, m, где $1 \leqslant a < b$:

а) $1 + 2^a + 2^b = 5^m$;   б) $1 + 2^a + 2^b = 7^m$;   в)* $1 + 2^a + 2^b = 2015^m$.

После удачного рассмотрения нескольких частных случаев хочется попробовать решить задачу в целом.

§ 5. Сумма цифр

Из признаков делимости на 3 и на 9, изучаемых в школе, несложно вывести, что сумма цифр в десятичной записи числа 3^m равна 3 для $n = 1$ и будет делиться на 9 для $n \geqslant 2$.

А что мы можем сказать о сумме цифр числа 3^n в двоичной записи?

Перепишем уравнения (1), (3), (5) немного по-другому, поменяв местами правую и левую части:

$$3^m = 2^n + 2^0;$$
$$3^m = 2^b + 2^a + 2^0;$$
$$3^m = 2^{a_k} + \ldots + 2^{a_2} + 2^{a_1} + 2^0.$$

Мы записали степень тройки в двоичной системе. Суммы цифр в правой части записанных уравнений соответственно равны 2, 3 и $k+1$.

Поскольку мы решили задачу 1, то тем самым ответили на вопрос: «Какие степени числа 3 имеют сумму цифр в двоичной записи, равную 2?» Это будут только две степени тройки: 3 и 9. Соответственно решения задач 2 и 3 отвечают на вопрос: «Какие степени числа 3 имеют сумму цифр в двоичной записи равную 3 или 4?»

Вопрос, поставленный в исследовательской задаче 4, теперь можно переформулировать по-другому: *«Конечно ли количество степеней троек, у которых сумма цифр в двоичной записи равна некоторому постоянному числу k?»*

Сразу же возникает и другой вопрос: если конечно, то можно ли как-то оценить количество таких степеней троек, т. е. понять, сколько различных решений имеет диофантово уравнение (5)?

Если мы обозначим через $\nu(n)$ сумму цифр в двоичной записи числа n, то наш вопрос сводится к решению уравнения

$$\nu(3^m) = k. \tag{6}$$

Конечно, такая упрощённая запись не означает, что новое уравнение легче решается. Но порой, переформулировав задачу и посмотрев на неё с другой стороны, удаётся увидеть некоторые скрытые закономерности.

Такая переформулировка позволила нам подключить к исследованию задачи компьютер. Нужно было написать программу, которая записывает степени тройки в двоичной системе, считает сумму цифр и сводные данные заносит в таблицу. Школьник Влад Сергиенко написал такую программу, дополнив её графиками функции $y = \nu(3^x)$. На самом деле мы имеем дело с последовательностью $s_m = \nu(3^m)$, а программа по имеющейся последовательности значений построила кусочно-линейную функцию. Расчёты были произведены для всех целых $0 \leqslant m \leqslant 299$.

Приведём результаты этих вычислений, где q обозначает количество различных решений для различных значений суммы цифр s (см. таблицу на стр. 176).

Начало таблицы соответствует тому, что мы уже получили. Имеется только одна степень тройки с суммой цифр в двоичной записи, равной 1, — при $m = 0$. Только две степени тройки с суммой цифр в двоичной записи, равной 2, — при $m = 1$ и $m = 2$. Только одна степень тройки с суммой цифр в двоичной записи, равной 3, — при $m = 4$. По одной степени тройки с суммами цифр в двоичной записи, равными 4 и 5.

Расчёты также показали, что при $m \leqslant 299$ уравнение $\nu(3^m) = 6$ и, соответственно, уравнение $1 + 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} = 3^m$, где $1 \leqslant a_1 < a_2 <$

s	q	s	q	s	q	s	q	s	q	s	q	s	q	s	q
1	1	25	3	49	1	75	2	106	2	130	2	158	1	187	1
2	2	26	2	51	1	77	3	109	1	131	1	159	1	189	2
3	1	27	1	52	1	79	2	110	1	132	1	160	2	190	1
4	1	28	1	55	2	81	3	111	2	133	1	162	3	191	2
5	1	29	1	56	3	82	2	112	1	136	1	165	1	192	1
6	3	30	1	57	1	83	2	114	1	138	2	166	1	194	2
8	1	32	2	58	3	84	1	115	2	140	1	170	4	195	2
9	1	33	1	61	1	85	2	116	1	143	1	171	7	196	4
10	1	34	4	63	1	87	3	118	1	145	1	172	1	197	1
11	2	35	1	64	2	89	1	119	4	146	2	173	1	198	5
13	1	36	1	65	1	90	2	120	2	147	2	174	1	199	1
14	3	38	2	66	1	91	2	121	1	148	1	175	2	200	1
15	1	39	4	67	3	92	1	122	1	149	1	178	1	201	2
16	1	40	1	68	2	93	2	123	2	150	1	179	3	203	1
17	2	41	2	69	1	94	1	124	3	151	2	180	3	204	2
18	1	42	3	70	2	95	1	125	2	153	1	181	2	206	3
19	1	45	2	71	2	97	5	126	1	154	2	182	1	208	1
20	1	46	1	72	2	98	2	127	2	155	1	183	3	209	2
22	1	47	1	73	1	100	1	128	1	156	2	185	1	210	3
24	1	48	1	74	1	105	1	129	4	157	1	186	1	212	2

$< a_3 < a_4 < a_5$, имеет три решения. Уравнение $\nu(3^m) = 7$ и, соответственно, уравнение $1 + 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} + 2^{a_6} = 3^m$, где $1 \leqslant a_1 < a_2 < a_3 < a_4 < a_5 < a_6$, не имеет ни одного решения.

Последний факт явился неожиданностью, поскольку на первый взгляд казалось, что с увеличением числа слагаемых и, соответственно, количества независимых переменных решения всегда должны быть. Из таблицы также видно, что этот факт не единичный и, например, уравнения $\nu(3^m) = 12$ или $\nu(3^m) = 21$ также не имеют решений при $m \leqslant 299$. Взглянув на график функции $y = \nu(3^x)$ и на аналогичные графики по другим ос-

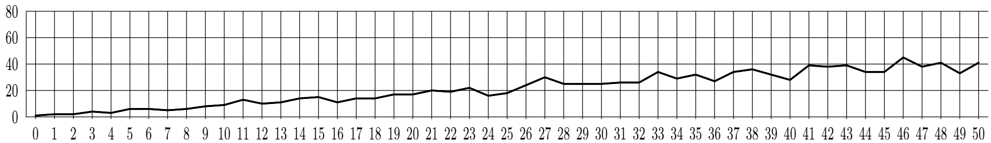

Рис. 1. *Сумма цифр числа* 3^n *по основанию* 2

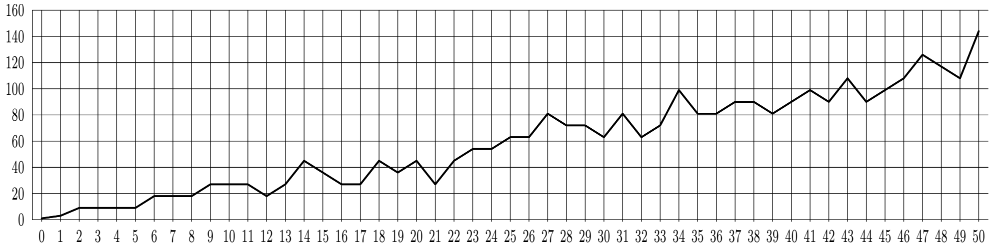

Рис. 2. *Сумма цифр числа* 3^n *по основанию* 10

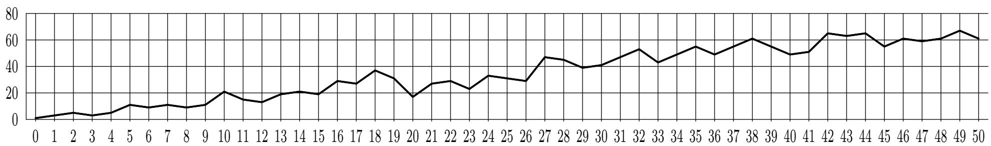

Рис. 3. *Сумма цифр числа* 3^n *по основанию* 5

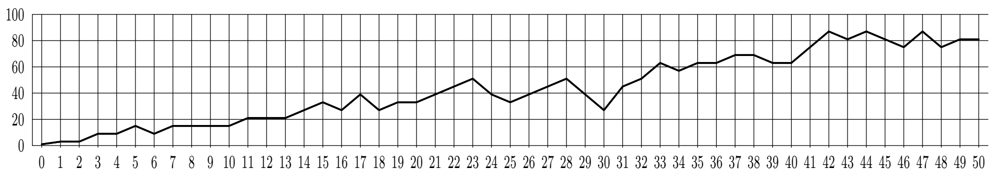

Рис. 4. *Сумма цифр числа* 3^n *по основанию* 7

нованиям систем счисления на расчётном интервале (рис. 1–4), мы видим функции, в среднем возрастающие с ростом рассматриваемого интервала.

Получив такие данные, мы вполне можем переформулировать наши вопросы в виде эквивалентных утверждений в следующей теореме (одно из них является ответом на вопрос задачи 4).

Теорема 3. (i) *Уравнение* $1 + 2^{a_1} + 2^{a_2} + 2^{a_3} + \ldots + 2^{a_k} = 3^m$, *где* $1 \leqslant a_1 < a_2 < a_3 < \ldots < a_k$, *при фиксированном натуральном* k *имеет конечное число решений.*

(ii) *Последовательность* $s_m = \nu(3^m)$ *возрастает неограниченно вместе с* m, *т. е.*

$$\varliminf_{m \to \infty} s_m = \infty.$$

Элементарное доказательство приведённой теоремы авторам неизвестно. Известно, что теорема может быть доказана разными, но, как мы отметили, не элементарными способами. Ввиду их сложности оставим решение этой теоремы за рамками статьи.

Следует добавить, что приведённая теорема является следствием серьёзной теоремы Шмидта о подпространстве (см. [15]). При таком подходе можно получить неэффективную оценку на рост суммы цифр. Эффективную оценку с помощью метода Бейкера получил Стюарт. Заинтересованный читатель может ознакомиться с указанными результатами, изучив источники [14, 16, 17, 20].

§ 6. О теореме Шинцеля

Если рассмотреть десятичную систему счисления, то аналог теоремы 3 удаётся доказать с помощью непростых, но вполне элементарных рассуждений.

Задача 5 [9, задача 207]. Доказать, что сумма цифр числа 2^n (записанного в десятичной системе счисления) неограниченно возрастает вместе с n.

На самом деле имеет место более сильное утверждение.

Теорема 4 (А. Шинцель). *Если g — чётное натуральное число, не делящееся на 10, то сумма цифр числа g^n (записанного в десятичной системе счисления) возрастает неограниченно вместе с n.*

Мы приведём доказательство теоремы А. Шинцеля по книге [9].

Доказательство. Определим бесконечную последовательность целых чисел a_i, $i = 0, 1, 2, \ldots$, следующим образом: $a_0 = 0$ и для $k = 0, 1, 2, \ldots$ пусть a_{k+1} означает наименьшее натуральное число, такое что $2^{a_{k+1}} > 10^{a_k}$ (таким образом, $a_1 = 1$, $a_2 = 4$, $a_3 = 14$ и т. д.). Имеем $a_0 < a_1 < a_2 < \ldots$

Докажем, что если при натуральном k выполнено $n \geqslant a_k$, то сумма цифр числа g^n будет не меньше чем k. Пусть c_j — цифра десятичного разложения числа g^n, стоящая при 10^j. Так как g есть чётное число, получаем, что $2^n \mid g^n$, и так как $n \geqslant a_k$, получаем $2^{a_i} \mid g^n$ для $i = 0, 1, 2, \ldots, k$. Поэтому, учитывая, что $2^{a_i} \mid 10^{a_i}$, имеем:

$$2^{a_i} \mid (c_{a_i-1}10^{a_i-1} + \ldots + c_0).$$

Если бы для $a_{i-1} \leqslant j < a_i$ все цифры c_j были равны нулю, то мы имели бы:

$$2^{a_i} \mid (c_{a_{i-1}-1}10^{a_{i-1}-1} + \ldots + c_0)$$

и, так как $c_0 \neq 0$, также

$$2^{a_i} \leqslant c_{a_i-1}10^{a_{i-1}-1} + \ldots + c_0 < 10^{a_{i-1}}.$$

Откуда $2^{a_i} \leqslant 10^{a_{i-1}}$, что противоречит определению числа a_i. Следовательно, по крайней мере одна из цифр c_j, где $a_{i-1} \leqslant j < a_i$, отлична от нуля.

Но последнее заключение справедливо для $i = 0, 1, 2, \ldots, k$. Следовательно, число g^n имеет по крайней мере k цифр отличных от нуля. Поэтому для достаточно больших n (для $n \geqslant a_k$) сумма цифр числа g^n не меньше произвольно заданного натурального числа k и, значит, сумма цифр числа g^n возрастает неограниченно вместе с n. Что и требовалось доказать. $\square$

Упражнение 5 (А. Шинцель). Если g — нечётное натуральное число, делящееся на 5, то сумма цифр числа g^n (записанного в десятичной системе счисления) возрастает неограниченно вместе с n.

В частности, из доказанной теоремы следует для $g = 2$, что сумма цифр числа 2^n возрастает неограниченно вместе с n. Однако она не возрастает монотонно, например сумма цифр 2^3 есть 8, а сумма цифр 2^4 есть 7 или сумма цифр 2^{16} есть 25, а сумма цифр 2^{17} есть 14.

Для сравнения на рис. 5–8 приведены графики суммы цифр числа 2^n в системах счисления по основаниям 10, 3, 5, 7. Неограниченность роста

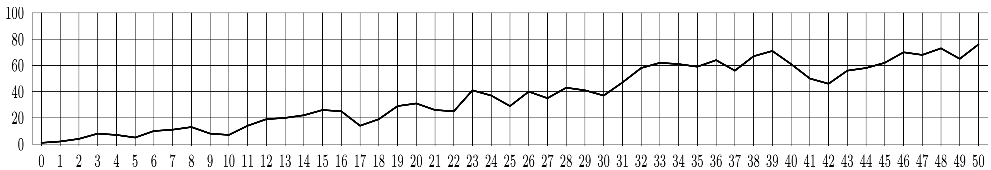

Рис. 5. Сумма цифр числа 2^n по основанию 10

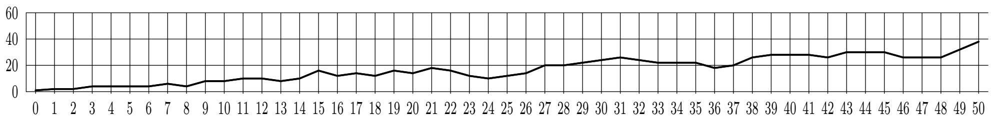

Рис. 6. Сумма цифр числа 2^n по основанию 3

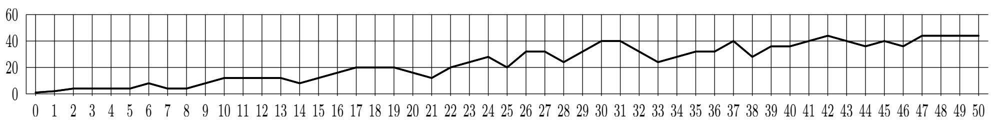

Рис. 7. Сумма цифр числа 2^n по основанию 5

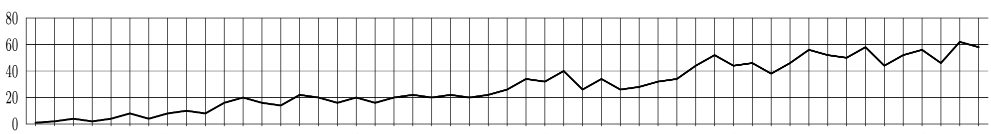

Рис. 8. Сумма цифр числа 2^n по основанию 7

суммы цифр числа 2^n по основанию 10 следует из теоремы Шинцеля. Для оснований 3, 5, 7 она следует из уже упоминавшейся теоремы Шмидта о подпространстве. Элементарное доказательство этого факта авторам неизвестно.

К сожалению, мы не смогли адаптировать имеющееся доказательство теоремы Шинцеля для случая теоремы 3. Дело в том, что в этом доказательстве существенную роль играет тот факт, что основание степени и основание системы счисления имеют общий делитель. В исследуемом нами случае числа 2 и 3 взаимно просты.

§ 7. В поисках формулы для суммы цифр

На каком-то этапе нам показалось, что утверждение (ii) теоремы 3 поддаётся элементарному доказательству и с ним можно «поработать». А что если найти явную формулу для вычисления суммы цифр числа?

Рассмотрим двоичную запись числа n. Пусть

$$n = b_q 2^q + b_{q-1}2^{q-1} + \ldots + b_1 2 + b_0, \quad \text{где } b_q = 1,\ b_i \in \{0, 1\}.$$

Как и прежде, $\nu(n)$ обозначает сумму цифр двоичной записи числа n, т. е. количество тех чисел b_i, которые равны 1. Понятно, что $q = [\log_2 n]$.

Через $\tau(n)$ обозначим максимальное количество единиц в конце двоичной записи числа n, т. е. $b_i = 1$, если $0 \leqslant i \leqslant \tau(n) - 1$, и $b_{\tau(n)} = 0$.

Задача 6. Докажите, что для всех натуральных n выполнены соотношения:

а) $\nu(n+1) = \nu(n) + 1 - \tau(n)$;

б) $\nu(n) = n - \sum\limits_{k=1}^{q} k\left[\dfrac{n+2^k}{2^{k+1}}\right]$, где $q = [\log_2 n]$.

Решение. а) Если n чётное, т. е. $b_0 = 0$ и поэтому $\tau(n) = 0$, имеем очевидное равенство $\nu(n+1) = \nu(n) + 1$.

Если n нечётное, то, поскольку у n на конце $\tau(n)$ единиц и $b_{\tau(n)} = 0$, то у $n+1$ на конце будет $\tau(n)$ нулей, при этом на $(\tau(n)+1)$-м месте появится 1, остальные цифры не изменятся. Следовательно, $\nu(n+1) = \nu(n) + 1 - \tau(n)$. Что и требовалось доказать.

б) Используем доказанное равенство. Имеем:

$$\begin{aligned} \nu(n) &= \nu(n-1) + 1 - \tau(n-1), \\ \nu(n-1) &= \nu(n-2) + 1 - \tau(n-2), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

$$\nu(2) = \nu(1) + 1 - \tau(1),$$
$$\nu(1) = 1.$$

Сложив все равенства, после упрощения получим

$$\nu(n) = n - \sum_{i=1}^{n-1} \tau(i).$$

Пусть t_k — количество чисел, меньших n и имеющих на конце k единиц. Нетрудно видеть, что числа вида $2^k - 1 + 2^{k+1}t$, где $t = 0, 1, 2, \ldots$, и только они, имеют на конце k единиц. Решив неравенство

$$2^k - 1 + 2^{k+1}t \leqslant n - 1,$$

получаем

$$t_k = 1 + \left[\frac{n - 2^k}{2^{k+1}}\right] = \left[\frac{n + 2^k}{2^{k+1}}\right].$$

Имеем

$$\nu(n) = n - \sum_{i=1}^{n-1} \tau(i) = n - \sum_{k=0}^{q} k\left[\frac{n + 2^k}{2^{k+1}}\right].$$

Что и требовалось доказать.

Теперь мы можем записать

$$\nu(3^m) = 3^m - \sum_{k=1}^{q} k\left[\frac{3^m + 2^k}{2^{k+1}}\right], \quad \text{где } q = [m \log_2 3].$$

Итак, формулу мы нашли!

Эта формула позволяет упростить процедуру программирования, позволяя избежать процедуры разложения степени тройки в двоичную запись. Однако такая формула не помогла ответить на ряд, казалось бы, простых вопросов. Например: «Какие степени числа 3 имеют сумму цифр в двоичной записи, равную 5?» Чтобы ответить на этот вопрос, приходится поступать как раньше, а именно решать в натуральных числах соответствующее экспоненциальное диофантово уравнение.

Искушённый читатель может встретить эту формулу в другом (возможно более простом) виде, восходящем к Лежандру (см., например, [18]):

$$s_b(n) = (b-1)\sum_{i=1}^{\infty}\left\{\frac{n}{b^i}\right\}, \quad \text{или} \quad s_b(n) = n - (b-1)\sum_{i=1}^{\infty}\left\lfloor\frac{n}{b^i}\right\rfloor,$$

где $s_b(n)$ обозначает сумму цифр b-ичной записи числа n.

На этом этапе мы вынуждены опять вернуться к частному случаю пока не разобранной задачи 3.

§ 8. Ещё несколько примеров

При попытках решить задачу 3 порой мы оказывались в ситуации уравнения (2). Поэтому для дальнейшего движения вернёмся к уравнению (2) и рассмотрим несколько частных случаев.

Задача 7. Решить уравнение $19 + 2^n = 3^m$ в натуральных числах.

Решение. Докажем, что у этого уравнения нет решений при $n \geqslant 5$. Действительно, если $n \geqslant 5$, то $m > 3$. Перепишем наше уравнение в виде

$$2^4(1 + 2^{n-4}) = 3(3^{m-1} - 1).$$

Поскольку $1 + 2^{n-4}$ — нечётное число, из леммы 2 получаем, что $m - 1 = 2^2(2t + 1) = 4(2t + 1)$. Кроме того, поскольку правая часть делится на 3, то и левая часть уравнения делится на 3, что возможно только при нечётном n. Имеем $19 + 2^n = 3 \cdot 81^{2t+1}$. Очевидно, что число в правой части равенства оканчивается цифрой 3. Однако поскольку n нечётно, то число в левой части может заканчиваться только цифрами 1 и 7. Получаем противоречие. Итак $n \leqslant 4$. Непосредственным перебором убеждаемся, что подходит только $n = 3$, тогда $m = 3$.

Ответ: $(n; m) \in \{(3; 3)\}$.

Задача 8. Решить уравнение $11 + 2^n = 3^m$ в натуральных числах.

Попробуем поступить так же, как и при решении предыдущей задачи.

Решение. Докажем, что у этого уравнения нет решений при $n \geqslant 5$. Действительно, если $n \geqslant 5$, то $m > 3$. Перепишем наше уравнение в виде

$$2^4(1 + 2^{n-4}) = 27(3^{m-3} - 1).$$

Поскольку $1 + 2^{n-4}$ — нечётное число, из леммы 1 получаем, что $m - 3 = 2^2(2t + 1) = 4(2t + 1)$. Имеем $11 + 2^n = 27 \cdot 81^{2t+1}$. Очевидно, что число в правой части равенства оканчивается цифрой 7. Число в левой части может заканчиваться на 7, только если 2^n оканчивается на 6. Следовательно, n делится на 4, т. е. $n = 4q$. Далее, $11 + 16^q = 27 \cdot 81^{2t+1}$. Однако $11 + 16^q \equiv 11 + (-1)^q \pmod{17}$. Значит, левая часть уравнения даёт остатки 10 или 12 при делении на 17. С другой стороны,

$$27 \cdot 81^{2t+1} \equiv 10 \cdot (-4)^{2t+1} \equiv -40 \cdot 16^t \equiv 11 \cdot (-1)^t \pmod{17}.$$

Значит, правая часть уравнения даёт остатки 6 или 11 при делении на 17. Получаем противоречие. Итак, $n \leqslant 4$. Непосредственным перебором убеждаемся, что подходит только $n = 4$, тогда $m = 3$.

Ответ: $(n; m) \in \{(4; 3)\}$.

Упражнение 6. Докажите, что следующие уравнения не имеют решений в натуральных числах m и n:

$$\text{а) } 35+2^n=3^m; \quad \text{б) } 37+2^n=3^m; \quad \text{в) } 41+2^n=3^m.$$

Упражнение 7. Решить уравнения в натуральных числах m и n:

а) $3+2^n=5^m$; б) $9+2^n=5^m$; в) $17+2^n=5^m$; г) $3+2^n=7^m$; д) $17+2^n=7^m$; е) $49+2^n=3^m$; ж) $65+2^n=3^m$.

Как видим, при решении уравнений нам приходилось использовать несколько модулей. При этом если в задаче 7 нам хватило сравнений по модулю 10, то в задаче 8 нам дополнительно пришлось привлекать сравнения по модулю 17. Фактически мы решали системы сравнений.

§ 9. Системы сравнений

Следующая лемма выглядит несколько искусственно, и всё же она оказывается мощным орудием для решения задачи 3 и других подобных задач.

Лемма 3. *Система сравнений*

$$\begin{cases} 2^a+2^b+2^c \equiv 5 \pmod{15}, \\ 2^a+2^b+2^c \equiv 0 \pmod{17} \end{cases}$$

не имеет решений в целых неотрицательных числах a, b, c.

Потратив небольшие усилия, читатели смогут найти несколько различных доказательств этой леммы. Известные нам доказательства отличаются вариантами перебора остатков. Перебор вариантов можно сделать вручную или поручить компьютеру. Мы предложим вариант доказательства, в котором опустим рутинный перебор.

Доказательство. Предположим, что решение существует. Пусть $a = 4a_1 + r_1$, $b = 4b_1 + r_2$, $c = 4c_1 + r_3$, где $r_1, r_2, r_3 = 0, 1, 2, 3$. Имеем

$$2^a+2^b+2^c = 2^{r_1}16^{a_1}+2^{r_2}16^{b_1}+2^{r_3}16^{c_1} \equiv 2^{r_1}+2^{r_2}+2^{r_3} \pmod{15},$$

кроме того

$$2^a+2^b+2^c = 2^{r_1}16^{a_1}+2^{r_2}16^{b_1}+2^{r_3}16^{c_1} \equiv \\ \equiv 2^{r_1}(-1)^{a_1}+2^{r_2}(-1)^{b_1}+2^{r_3}(-1)^{c_1} \pmod{17}.$$

Если существует какое-нибудь решение, то очевидно, что существует решение, для которого $r_1 \leqslant r_2 \leqslant r_3$.

Это замечание сокращает перебор возможных вариантов. Перебрав их, получаем, что сравнение $2^{r_1} + 2^{r_2} + 2^{r_3} \equiv 5 \pmod{15}$ имеет решение в следующих двух случаях: 1) $0 = r_1 < r_2 = r_3 = 1$; 2) $2 = r_1 < r_2 = r_3 = 3$.

Разберём оба случая.

1) $0 = r_1 < r_2 = r_3 = 1$. Имеем

$$2^a + 2^b + 2^c \equiv (-1)^{a_1} + 2(-1)^{b_1} + 2(-1)^{c_1} \pmod{17}.$$

Поскольку $(-1)^{a_1} + 2(-1)^{b_1} + 2(-1)^{c_1} \equiv \pm 1, \pm 3, \pm 5 \pmod{17}$, в этом случае сравнение $2^a + 2^b + 2^c \equiv 0 \pmod{17}$ не выполняется.

2) $2 = r_1 < r_2 = r_3 = 3$. Имеем

$$\begin{aligned} 2^a + 2^b + 2^c &\equiv 4(-1)^{a_1} + 8(-1)^{b_1} + 8(-1)^{c_1} \equiv \\ &\equiv 4((-1)^{a_1} + 2(-1)^{b_1} + 2(-1)^{c_1}) \pmod{17}. \end{aligned}$$

Поскольку $4((-1)^{a_1} + 2(-1)^{b_1} + 2(-1)^{c_1}) \equiv \pm 3, \pm 4, \pm 5 \pmod{17}$, то и в этом случае сравнение $2^a + 2^b + 2^c \equiv 0 \pmod{17}$ не выполняется. Пришли к противоречию. Итак, система сравнений неразрешима. Что и требовалось доказать. □

Следствие 2. *Система сравнений*

$$\begin{cases} 2^a + 2^b \equiv 5 \pmod{15}, \\ 2^a + 2^b \equiv 0 \pmod{17} \end{cases}$$

не имеет решений в целых неотрицательных числах a, b.

Доказательство. Поскольку $a = b = 0$ не является решением системы, не теряя общности, можно считать $a \geqslant 1$. Тогда имеем эквивалентную систему

$$\begin{cases} 2^{a-1} + 2^{a-1} + 2^b \equiv 5 \pmod{15}, \\ 2^{a-1} + 2^{a-1} + 2^b \equiv 0 \pmod{17}. \end{cases}$$

Согласно лемме 3 последняя система сравнений не имеет решений. Что и требовалось доказать. □

Упражнение 8. Система сравнений

$$\begin{cases} 2^a + 2^b + 2^c \equiv 5 \pmod{15}, \\ 2^a + 2^b + 2^c \equiv 15 \pmod{17} \end{cases}$$

не имеет решений в целых неотрицательных числах a, b, c.

Упражнение 9. Системы сравнений

$$1)\ \begin{cases} 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}\equiv 170 \pmod{255},\\ 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}\equiv 0 \pmod{257}; \end{cases}$$

$$2)\ \begin{cases} 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}\equiv 170 \pmod{255},\\ 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}\equiv 0 \pmod{257} \end{cases}$$

не имеют решений в целых неотрицательных числах a_1, a_2, a_3, a_4, a_5.

Теперь мы готовы решить задачу 3.

§ 10. Уравнение $1+2^a+2^b+2^c=3^m$

Итак, решаем уравнение $1+2^a+2^b+2^c=3^m$, где $1\leqslant a<b<c$.

Решение задачи 3. Докажем, что уравнение $1+2^a+2^b+2^c=3^m$ не имеет решений в целых неотрицательных числах m, $a<b<c$ при $a\geqslant 6$. Действительно, если $a\geqslant 6$, то перепишем наше уравнение в виде

$$2^a(1+2^{b-a}+2^{c-a})=3^m-1.$$

Поскольку $1+2^{b-a}+2^{c-a}$ — нечётное число, из леммы 1 получаем, что $m=2^{a-2}q=16d$. Так как для любого натурального k выполняется $6^k\equiv 6 \pmod{15}$, получаем

$$3^m=3^{16d}=81^{4d}\equiv 6^{4d}\equiv 6 \pmod{15}.$$

Используя малую теорему Ферма, получим $3^{16}\equiv 1 \pmod{17}$, следовательно,

$$3^m=3^{16d}=(3^{16})^d\equiv 1^d\equiv 1 \pmod{17}.$$

Но тогда мы приходим к системе сравнений

$$\begin{cases} 2^a+2^b+2^c=3^m-1\equiv 5 \pmod{15},\\ 2^a+2^b+2^c=3^m-1\equiv 0 \pmod{17}. \end{cases}$$

Как следует из леммы 3, эта система не имеет решений. Итак, $a\leqslant 5$.

Разберём случай $a=2$. Поскольку $2=a<b<c$, получаем

$$5+2^b+2^c\equiv 5 \pmod 8.$$

С другой стороны, 3^m при делении на 8 может дать остатки 1 и 3. Значит, в этом случае решений нет.

Случаи $a=1$, $a=3$, $a=4$, $a=5$ составляют содержание упражнений. Разобрав их, мы получим единственное решение $a=1$, $b=3$, $c=4$, $m=3$.

Ответ: $(a; b; c; m)\in\{(1; 3; 4; 3)\}$.

Упражнение 10. Найти все решения уравнений в натуральных числах b, c, m, где $b < c$:

$$\text{а) } 3 + 2^b + 2^c = 3^m; \quad \text{в) } 17 + 2^b + 2^c = 3^m;$$

$$\text{б) } 9 + 2^b + 2^c = 3^m; \quad \text{г) } 33 + 2^b + 2^c = 3^m.$$

Упражнение 11. Доказать, что при $10 \leqslant a_1 < a_2 < a_3 < a_4 < a_5$ уравнение $1 + 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} = 3^m$ не имеет решений в натуральных числах.

§ 11. Простые числа Ферма

При решении нашей задачи потребовалось выбрать удобный модуль для сравнений. Простые модули, которые мы использовали, образуют начало одной из известных последовательностей — последовательности чисел Ферма:

$$F_n = 2^{2^n} + 1, n = 0, 1, 2, \ldots$$

Начальные члены этой последовательности следующие: 3, 5, 17, 257, 65 537, 4 294 967 297, … В своё время Ферма считал, что все члены этой последовательности — простые числа. Однако в 1732 году Эйлер нашёл разложение

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

и опроверг гипотезу Ферма. На сегодняшний момент известно лишь 5 простых чисел Ферма: 3, 5, 17, 257, 65 537; при этом существует гипотеза, что других простых чисел Ферма нет.

Однако вернёмся к нашей задаче. Давайте посмотрим на упражнение 9, в котором появляются модули $2^{2^3} - 1 = 255$ и $2^{2^3} + 1 = 257$. Используя те же рассуждения, что и при решении задачи 3, можно решить упражнение 10. На самом деле указанные модули работают и для большего числа слагаемых. С помощью компьютера авторы проверили, что верна

Теорема 5. *Система сравнений*

$$\begin{cases} 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} + 2^{a_6} + 2^{a_7} \equiv 170 \pmod{255}, \\ 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} + 2^{a_6} + 2^{a_7} \equiv 0 \pmod{257} \end{cases}$$

не имеет решений в целых неотрицательных числах a_i, $i = \overline{1, 7}$.

В то же время при выбранных модулях, увеличивая количество слагаемых, мы уже не приходим к противоречию.

Упражнение 12. Найдите хотя бы одно решение системы сравнений

$$\begin{cases} 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} + 2^{a_6} + 2^{a_7} + 2^{a_8} \equiv 170 \pmod{255}, \\ 2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} + 2^{a_6} + 2^{a_7} + 2^{a_8} \equiv 0 \pmod{257}. \end{cases}$$

По всей видимости, чтобы получить результат, аналогичный теореме 5 или лемме 3 для восьми слагаемых (и, возможно, более восьми), мы должны взять модуль $2^{2^4}-1=65\,535$ и модуль, соответствующий следующему простому числу Ферма $2^{2^4}+1=65\,537$. Авторам не показалось возможным провести такую проверку на домашних компьютерах.

Гипотеза 1. *Система сравнений*

$$\begin{cases} 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}+2^{a_6}+2^{a_7}+2^{a_8}\equiv 3^{65\,536}-1 \pmod{65\,535},\\ 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}+2^{a_6}+2^{a_7}+2^{a_8}\equiv 0 \pmod{65\,537}\end{cases}$$

не имеет решений в целых неотрицательных числах a_i, $i=\overline{1,8}$.

Однако следующее число Ферма уже не является простым, и что будет происходить с системами сравнений в этом случае — авторам не ясно.

Может быть, читатели присоединятся к этому исследованию?

§ 12. Задачи для исследования

Задача 9. Решить уравнения в натуральных числах n, $m\neq 1$ и $q>7$: а) $3+2^n=q^m$; б) $5+2^n=q^m$.

Задача 10. Решить уравнение $3^n+100=7^m$ в натуральных числах.

Задача 11. Найти все решения уравнения $1+2^a+2^b=y^2$ в целых неотрицательных числах a, b, y, где $1\leqslant a<b$.

Задача 12. Найти все решения уравнения $1+2^a+2^b=q^m$ в целых неотрицательных числах a, b, m, q, где $1\leqslant a<b$, $m\geqslant 3$ и $q>7$.

Задача 13 (Э. Б. Винберг, [5]). При каких натуральных n число $\dfrac{3^n-1}{2}$ есть квадрат натурального числа?

В заключение отметим, что задача о росте суммы цифр успешно решалась не только для последовательности, состоящей из степеней натурального числа, но и для некоторых других последовательностей (см., например, [19]). Для искушённых читателей, вероятно, будет полезна книга [13].

§ 13. Ответы, указания, решения

Решения упражнений

Упражнение 1.

а) Ответ: $n=2$, $m=1$. б) Ответ: нет решений. в) Ответ: $q=1+2^n$ и $m=1$.

Решение. Решаем уравнение $1 + 2^n = q^m$. Очевидно, что q нечётно. Если m нечётно, то имеем $2^n = q^m - 1 = (q-1)(q^{m-1} + q^{m-2} + \ldots + q + 1)$. Множитель $q^{m-1} + q^{m-2} + \ldots + q + 1$ является суммой нечётного числа нечётных слагаемых и, следовательно, нечётен. Это возможно только при $m = 1$, тогда $q = 1 + 2^n$.

Если m чётно, то $m = 2t$. Тогда $2^n = (q^t - 1)(q^t + 1)$. Последнее равенство возможно, только если каждый из сомножителей в правой части является степенью двойки. Имеем

$$\begin{cases} q^t - 1 = 2^b, \\ q^t + 1 = 2^c \end{cases} \quad \Rightarrow \quad 2 = 2^c - 2^b \quad \Rightarrow \quad c = 2,\ b = 1,\ q = 3.$$

г) Ответ: нет решений. д) Ответ: $n = 3$, $m = 1$. е) Ответ: $q = 2^n - 1$ и $m = 1$.

Решение. Решаем уравнение $-1 + 2^n = q^m$. Очевидно, что q нечётно. Если m нечётно, то имеем

$$2^n = q^m + 1 = (q+1)(q^{m-1} - q^{m-2} + q^{m-3} - \ldots - q + 1).$$

Множитель $q^{m-1} - q^{m-2} + q^{m-3} - \ldots - q + 1$ является суммой нечётного числа нечётных слагаемых и, следовательно, нечётен. Это возможно только при $m = 1$, тогда $q = 2^n - 1$. Если m чётно, то $q^m \equiv 1 \pmod 4$. Если $n \geqslant 2$, то $-1 + 2^n \equiv 3 \pmod 4$. Противоречие. При $n = 1$ остаётся только $q = 1$.

Упражнение 2.

Ответ: $(x; y; z) \in \{(2; 2; 2)\}$.

Решение. Поскольку $3^x + 4^y \equiv 1 \pmod 3$ и $5^z \equiv (-1)^z \pmod 3$, то z чётно. Положим $z = 2t$. Перепишем наше уравнение в виде

$$3^x = 5^z - 4^y = (5^t - 2^y)(5^t + 2^y).$$

Тогда

$$\begin{cases} 5^t - 2^y = 3^b, \\ 5^t + 2^y = 3^c \end{cases} \quad \Rightarrow \quad 2^{y+1} = 3^c - 3^b = 3^b(3^{c-b} - 1) \quad \Rightarrow \quad b = 0.$$

С учётом результата задачи 1а) $c = 2, y = 2, t = 1, z = 2, x = 2$.

Упражнение 3.

Ответ: $(x; y) \in \{(0; -2), (0; 2), (4; -23), (4; 23)\}$.

Решение. Если $x < 0$, имеем $1 < 1 + 2^x + 2^{2x+1} < 1 + 1 + 2 = 4$, поэтому решений нет.

При $x = 0, 1, 2$ точный квадрат получается только при $x = 0$, $y = \pm 2$.

Пусть $x \geqslant 3$. Будем искать решения для $y \geqslant 0$ (пары $(x; y)$ и $(x; -y)$ входят в множество решений одновременно). Поскольку $(2^x)^2 = 2^{2x} < 1 + 2^x + 2^{2x+1} < 2^{2x} + 2^{2x} + 2^{2x+1} = (2^{x+1})^2$ и $y^2 = 1 + 2^x + 2^{2x+1}$, получаем $2^x < y < 2^{x+1}$.

Перепишем наше уравнение в виде $2^x(1 + 2^{x+1}) = (y - 1)(y + 1)$. Числа $y - 1$ и $y + 1$ — это последовательные чётные числа. Поэтому одно из них делится на 2 только в первой степени.

Рассмотрим два возможных случая.

В первом случае имеем

$$\begin{cases} y - 1 = 2^{x-1} \cdot t, \\ y + 1 = 2^{x-1} \cdot t + 2, \end{cases}$$

где t — нечётное число. Поскольку $2^x < y < 2^{x+1}$, а t нечётно, получаем $2^x < y = 2^{x-1} \cdot t + 1 < 2^{x+1}$, откуда $t = 3$. Тогда $1 + 2^x + 2^{2x+1} = (1 + 3 \cdot 2^{x-1})^2$.

Положим $z = 2^{x-1}$. Имеем $1 + 2z + 8z^2 = (1 + 3z)^2 \;\Leftrightarrow\; 0 = 4z + z^2$, т. е. в этом случае нет решений.

Аналогично во втором случае имеем

$$\begin{cases} y + 1 = 2^{x-1} \cdot t, \\ y - 1 = 2^{x-1} \cdot t - 2, \end{cases}$$

где t — нечётное число. Поскольку $2^x < y < 2^{x+1}$, а t — нечётное число, получим $2^x < y = 2^{x-1} \cdot t - 1 < 2^{x+1}$, откуда $t = 3$. Тогда $1 + 2^x + 2^{2x+1} = (3 \cdot 2^{x-1} - 1)^2$. Положим $z = 2^{x-1}$. Имеем $1 + 2z + 8z^2 = (3z - 1)^2 \;\Leftrightarrow\; 0 = z^2 - 8z$. Получаем $z = 8 = 2^{x-1}$. Откуда имеем ещё два решения $x = 4$ и $y = \pm 23$.

Упражнение 4.

а) Ответ: $(a; b; m) \in \{(3; 4; 2)\}$.

Решение. Если $b > a = 1$, то $1 + 2 + 2^b \equiv 3 \pmod 4$. С другой стороны, $5^m \equiv 1 \pmod 4$, что невозможно.

Если $a = 2$, то $5 + 2^b = 5^m$, что невозможно, поскольку 2^b не делится на 5. Итак, $a \geqslant 3$. Тогда $1 + 2^a + 2^b \equiv 1 \pmod 8$.

Если m — нечётное число, то $5^m \equiv 5 \pmod 8$ и в этом случае уравнение не имеет решений. Значит, m чётно: $m = 2k$. Имеем $2^a + 2^b = 25^k - 1$.

Пусть k нечётно. Имеем $2^a(1 + 2^{b-a}) = 25^k - 1 = 24(25^{k-1} + 25^{k-2} + \ldots + 1)$. Поскольку число $25^{k-1} + 25^{k-2} + \ldots + 1$ нечётно, как сумма нечётного числа нечётных слагаемых, получаем $a = 3$. Тогда $9 + 2^b = 25^k$. Так как $25^k \equiv 1 \pmod 3$, получаем, что и $2^b \equiv 1 \pmod 3$. Следовательно, b чётно: $b = 2t$. Тогда

$$9 = 25^k - 2^b = 25^k - 2^{2t} = (5^k - 2^t)(5^k + 2^t).$$

Это возможно, только если $k=1$ и $t=2$, тогда получаем решение $a=3$, $b=4$, $m=2$. Остаётся рассмотреть случай чётного $k \geqslant 2$. Положим $k=2k_1$. Далее, $25^k-1 \equiv 0 \pmod 3$. С другой стороны, $2^a+2^b \equiv (-1)^a+(-1)^b \pmod 3$. Следовательно, числа a, b имеют разную чётность. Кроме того, $1+2^a+2^b \equiv 0 \pmod 5$. Это даёт нам только две возможности:

1) a делится на 4, т. е. $a=4a_1$ и $b=4b_1+3$;
2) $a=4a_1+3$ и $b=4b_1$.

В первом случае имеем

$$1+2^a+2^b = 1+16^{a_1}+8\cdot 16^{b_1} \equiv 1+(-1)^{a_1}+8\cdot(-1)^{b_1} \pmod{17}.$$

Аналогично во втором случае

$$1+2^a+2^b = 1+8\cdot 16^{a_1}+16^{b_1} \equiv 1+8\cdot(-1)^{a_1}+(-1)^{b_1} \pmod{17}.$$

Значит, и в первом, и во втором случае при делении на 17 левая часть уравнения $1+2^a+2^b=5^m$ может давать остатки $8, 9, 10, 11$. Однако, $25^k=25^{2k_1} \equiv 8^{2k_1} \equiv (64)^{k_1} \equiv 13^{k_1} \pmod{17}$, и, следовательно, правая часть $1+2^a+2^b=5^m$ уравнения может давать остатки $1, 4, 13, 16$ при делении на 17, что невозможно. Следовательно, для чётных k решений нет.

Итак, мы нашли единственное решение $(a; b; m) \in \{(3; 4; 2)\}$.

б) Ответ: $(a; b; m) \in \{(1; 2; 1), (4; 5; 2)\}$.

Решение. Очевидно, что $a=1$, $b=2$, $m=1$ — решение уравнения.

Если $a=1$ и $b \geqslant 3$, то $1+2+2^b \equiv 3 \pmod 8$, с другой стороны, $7^m \equiv (-1)^m \pmod 8$, т. е. в этом случае нет решений.

Аналогично для $a=2$ и $b \geqslant 3$ имеем $1+4+2^b \equiv 5 \pmod 8$, что также невозможно.

Рассмотрим случай $a \geqslant 3$, тогда $1+2^a+2^b \equiv 1 \pmod 8$. Как мы уже отметили, $7^m \equiv (-1)^m \pmod 8$, поэтому m должно быть чётным числом: $m=2k$. Пусть $a=4a_1+r_1$, где $r_1=0, 1, 2, 3$, и $b=4b_1+r_2$, где $r_2=0, 1, 2, 3$. Имеем $1+2^a+2^b = 1+2^{r_1}16^{a_1}+2^{r_2}16^{b_1} \equiv 1+2^{r_1}+2^{r_2} \pmod{15}$.

Занесём данные в таблицу остатков по модулю 15.

r_1	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
r_2	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
$1+2^{r_1}+2^{r_2}$	3	4	6	10	4	5	7	11	6	7	9	13	10	11	13	17

С другой стороны, $7^m=7^{2k}=49^k \equiv 4^k \pmod{15}$.

Если k — чётное число, т. е. $k=2k_1$, то $7^m \equiv 4^k = 4^{2k_1} = 16^{k_1} \equiv 1 \pmod{15}$, что невозможно, поскольку остаток 1 в таблице не встречается. Значит, k —

нечётно. В этом случае $7^m \equiv 4^k \equiv 4 \pmod{15}$. Далее, $1+2^a+2^b=7^m=49^k$, $2^a(1+2^{b-a})=49^k-1=48(49^{k-1}+49^{k-2}+\ldots+1)$.

Поскольку число $49^{k-1}+49^{k-2}+\ldots+1$ нечётно, как сумма нечётного числа нечётных слагаемых, получаем $a=4$. Кроме того, как следует из таблицы остатков, $r_2=1$. Значит, $1+2^4+2^b=49^k$. Перепишем это уравнение в виде $32(2^{b-5}-1)=49(49^{k-1}-1)$. Для $k=1$ получаем ещё одно решение $a=4$, $b=5$, $m=2$.

Пусть теперь $k \geqslant 3$. Поскольку k нечётно, то $k-1$ чётно. Положим $k-1=2^dq$, где $q=2q_1+1$ нечётно, а $d \geqslant 1$ — натуральное число. Тогда

$$49^{k-1}-1=49^{2^dq}-1=(49^{2^d})^q-1=(49^{2^d}-1)\big((49^{2^d})^{q-1}+(49^{2^d})^{q-2}+\ldots+1\big).$$

Но $49^{2^d}-1=(49-1)(49+1)(49^2+1)\ldots(49^{2^{d-1}}+1)$. Поэтому если $d \geqslant 2$, то правая часть уравнения делится на 64, а левая часть на 64 не делится. Значит, $d=1$. Тогда $k=2q+1$ и $17+2^b=49^{2q+1}$.

Рассмотрим остатки обеих частей уравнения по модулю 17. Имеем $17+2^b=17+2^{r_2}16^{b_1}=17+2\cdot 16^{b_1}\equiv 2\cdot(-1)^{b_1}=\pm 2 \pmod{17}$. С другой стороны, $49^{2q+1}\equiv(-2)^{2q+1}\equiv(-2)^{4q_1+3}\equiv(-8)\cdot 16^{q_1}\equiv \pm 8 \pmod{17}$. Приходим к противоречию. Таким образом, других решений, кроме двух найденных, уравнение не имеет.

в) Ответ: нет решений.

Решение. Если $a=1$, то $b>4$, тогда $1+2+2^b\equiv 3 \pmod{16}$. С другой стороны $2015^m\equiv(-1)^m=\pm 1 \pmod{16}$. Противоречие.

Если $a=2$, то $5+2^b=2015^m$, что невозможно, так как 2^b не делится на 5.

Если $a=3$ и $b>a$, то $9+2^b=2015^m$. Но $9+2^b\equiv 9 \pmod{16}$ и $2015^m\equiv$ $\equiv(-1)^m=\pm 1 \pmod{16}$. Противоречие.

Итак, $a\geqslant 4$. Тогда $1+2^a+2^b\equiv 1 \pmod{16}$. Значит, m чётно, $m=2t$. Поскольку 2015 делится на 5 и не делится на 3, правая часть уравнения даёт остаток 5 или 10 при делении на 15. Следовательно, левая часть уравнения также даёт остаток 5 или 10 при делении на 15. Как следует из таблицы остатков п. б), это возможно в трёх случаях:

1) $a=4a_1$ и $b=4b_1+3$;
2) $a=4a_1+1$ и $b=4b_1+1$;
3) $a=4a_1+3$ и $b=4b_1$.

Рассмотрим модуль 17. Имеем

$$2015^m\equiv 2015^{2t}\equiv 9^{2t}\equiv 81^t\equiv(-4)^t\equiv 1, 4, 13, 16 \pmod{17}.$$

В случае 1 имеем

$$1+2^a+2^b=1+16^{a_1}+8\cdot 16^{b_1}\equiv 1+(-1)^{a_1}+8(-1)^{b_1}\equiv 8, 9, 10, 11 \pmod{17},$$

что невозможно.

В случае 3 получаем такую же ситуацию.

В случае 2 получаем

$$1+2^a+2^b=1+2\cdot 16^{a_1}+2\cdot 16^{b_1}\equiv 1+2(-1)^{a_1}+2(-1)^{b_1}\equiv 1,5,14 \pmod{17}.$$

Возможен остаток 1, если a_1 и b_1 разной чётности, а $t=4t_1$. Пусть $a=8a_2+1$ и $b=8b_2+5$, случай $a=8a_2+5$ и $b=8b_2+1$ рассматривается аналогично. Имеем $1+2^{8a_2+1}+2^{8b_2+5}=2015^{8t_1}$. Далее

$$1+2^a+2^b=1+2\cdot 256^{a_2}+32\cdot 256^{b_2}\equiv 2 \pmod 3.$$

Но $2015^m\equiv 2015^{8t_1}\equiv 1 \pmod 3$. Поэтому решений нет.

Упражнение 5.

Доказательство. Определим бесконечную последовательность целых чисел a_i, $i=0,1,2,\ldots$, следующим образом: $a_0=0$ и для $k=0,1,2,\ldots$ пусть a_{k+1} означает такое наименьшее натуральное число, что $5^{a_{k+1}}>10^{a_k}$ (таким образом, $a_1=1$, $a_2=2$, $a_3=3$, $a_4=5$ и т. д.). Имеем $a_0<a_1<a_2<\ldots$

Докажем, что если при натуральном k выполнено $n\geqslant a_k$, то сумма цифр числа g^n будет $\geqslant k$. Пусть c_j — цифра десятичного разложения числа g^n, стоящая при 10^j. Так как g делится на 5, получаем, что $5^n \mid g^n$, и так как $n\geqslant a_k$, получаем, что $5^{a_i}\mid g^n$ для $i=0,1,2,\ldots,k$. Поэтому, учитывая, что $5^{a_i}\mid 10^{a_i}$, имеем: $5^{a_i}\mid (c_{a_i-1}\cdot 10^{a_i-1}+\ldots+c_0)$. Если бы для $a_{i-1}\leqslant j<a_i$ все цифры c_j были равны нулю, то мы имели бы: $5^{a_i}\mid (c_{a_{i-1}-1}\cdot 10^{a_{i-1}-1}+\ldots+c_0)$ и, так как $c_0\neq 0$, также $5^{a_i}\leqslant c_{a_{i-1}-1}\cdot 10^{a_{i-1}-1}+\ldots+c_0\leqslant 10^{a_{i-1}}$.

Откуда $5^{a_i}\leqslant 10^{a_{i-1}}$, что противоречит определению числа a_i. Следовательно, по крайней мере одна из цифр c_j, где $a_{i-1}\leqslant j<a$, отлична от нуля.

Но последнее заключение справедливо для $i=0,1,2,\ldots$ Следовательно, число g^n имеет по крайней мере k цифр отличных от нуля. Поэтому для достаточно больших n (для $n\geqslant a_k$) сумма цифр числа g^n не меньше произвольно заданного натурального числа k и, значит, сумма цифр числа g^n возрастает неограниченно вместе с n. Что и требовалось доказать. □

Упражнение 6.

а) При $n\leqslant 5$ решений нет. Если $n\geqslant 6$, то перепишем уравнение в виде

$$32(1+2^{n-5})=3(3^{m-1}-1).$$

Из леммы 2 получаем $m-1=2^{5-2}t=8t$, где t — нечётное число. Тогда $3^m=3^{8t+1}\equiv 3\cdot 81^{2t}\equiv 3\cdot 6\equiv 3 \pmod{15}$. С другой стороны, выражение $35+2^n$ при делении на 15 даёт остатки 6, 7, 9, 13. Противоречие.

б) При $n=1,2$ решений нет. Если $n\geqslant 3$, то $37+2^n\equiv 5 \pmod 8$, а $3^m\equiv 1,3 \pmod 8$, что невозможно.

в) При $n \leqslant 5$ решений нет. Если $n \geqslant 6$, то перепишем уравнение в виде

$$32(1 + 2^{n-5}) = 9(3^{m-2} - 1).$$

Из леммы 2 получаем $m - 2 = 2^{5-2}t = 8t$, где t — нечётное число. Тогда $3^m = 3^{8t+2} \equiv 9 \cdot 81^{2t} \equiv 9 \cdot 6 \equiv 9 \pmod{15}$. С другой стороны, выражение $41 + 2^n$ при делении на 15 даёт остатки $0, 4, 12, 13$. Противоречие.

Упражнение 7.

а) Ответ: $n = 1$, $m = 1$.

Если $n \geqslant 2$, то $3 + 2^n \equiv 3 \pmod 4$, а $5^m \equiv 1 \pmod 4$, что невозможно. Остаётся $n = 1$, $m = 1$.

б) Ответ: $n = 4$, $m = 2$.

При $n = 1, 2, 3$ решений нет. Рассмотрим случай $n \geqslant 4$.

Если m нечётно, то $8(1 + 2^{n-3}) = 5^m - 1 = 4(5^{m-1} + 5^{m-2} + \ldots + 1)$. Множитель $5^{m-1} + 5^{m-2} + \ldots + 1$ является нечётным числом, как сумма нечётного числа нечётных слагаемых. Поэтому правая часть уравнения делится на 4 и не делится на 8. Левая часть уравнения делится на 8. Противоречие.

Если m чётно, $m = 2t$, то $2^n = 5^m - 9 = (5^t - 3)(5^t + 3)$. Имеем для некоторых натуральных b, c:

$$\begin{cases} 5^t - 3 = 2^b, \\ 5^t + 3 = 2^c \end{cases} \quad \Rightarrow \quad 6 = 2^c - 2^b \quad \Rightarrow \quad c = 3,\ b = 1,\ t = 1,$$

откуда $m = 2$, $n = 4$. При решении можно также использовать результат упражнения 4а).

в) Ответ: $n = 3$, $m = 2$.

Указание. Перепишите уравнение в виде $1 + 2^4 + 2^n = 5^m$. Рассмотрите два случая $n \leqslant 4$ и $n > 4$. Используйте результат упражнения 4а).

г) Ответ: $n = 2$, $m = 1$. При $n = 1$ решений нет. При $n = 2$ получаем $m = 1$. Если $n \geqslant 3$, то $3 + 2^n \equiv 3 \pmod 8$, а $7^m \equiv \pm 1 \pmod 8$. Противоречие.

д) Ответ: $n = 5$, $m = 2$.

Указание. Перепишите уравнение в виде $1 + 2^4 + 2^n = 7^m$. Рассмотрите два случая $n \leqslant 4$ и $n \geqslant 4$. Используйте результат упражнения 4б).

е) Ответ: $n = 5$, $m = 4$. При $n = 1, 2$ решений нет. Пусть $n \geqslant 3$. Тогда $49 + 2^n \equiv 1 \pmod 8$, получаем $m = 2m_1$. Перепишем уравнение в виде $2^n = 3^m - 49 = (3^{m_1} - 7)(3^{m_1} + 7)$. Тогда

$$\begin{cases} 3^{m_1} - 7 = 2^x, \\ 3^{m_1} + 7 = 2^y \end{cases} \quad \Rightarrow \quad 14 = 2^y - 2^x \quad \Rightarrow \quad x = 1,\ y = 4 \quad \Rightarrow \quad m_1 = 2,\ m = 4.$$

Получаем $n = 5$.

ж) Ответ: $n = 4$, $m = 4$. При $n \leqslant 6$ получим решение перебором. Если $n \geqslant 7$, то перепишем уравнение в виде $64(1 + 2^{n-6}) = 3^m - 1$. Из леммы 2 получаем $m = 2^{6-2}t = 16t$, где t — нечётное число. Имеем $3^{16t} - 1 = 81^{4t} - 1 \equiv \equiv 6 - 1 \equiv 5 \pmod{15}$ и по малой теореме Ферма $3^{16t} \equiv 1 \pmod{17}$. Имеем систему сравнений

$$\begin{cases} 2^6 + 2^n \equiv 5 \pmod{15}, \\ 2^6 + 2^n \equiv 0 \pmod{17}. \end{cases}$$

По следствию 2 эта система не имеет решений.

Упражнение 8.

Указание. Пусть $a = 4a_1 + r_1$, $b = 4b_1 + r_2$, $c = 4c_1 + r_3$, где $r_1, r_2, r_3 = = 0, 1, 2, 3$. Имеем

$$2^a + 2^b + 2^c = 2^{r_1}16^{a_1} + 2^{r_2}16^{b_1} + 2^{r_3}16^{c_1} \equiv 2^{r_1} + 2^{r_2} + 2^{r_3} \pmod{15}$$

и

$$2^a + 2^b + 2^c \equiv 2^{r_1}(-1)^{a_1} + 2^{r_2}(-1)^{b_1} + 2^{r_3}(-1)^{c_1} \pmod{17}.$$

В доказательстве леммы 3 показано, что если $r_1 \leqslant r_2 \leqslant r_3$, то сравнение $2^a + 2^b + 2^c \equiv 5 \pmod{15}$ имеет решение в следующих двух случаях:

1) $0 = r_1 < r_2 = r_3 = 1$; 2) $2 = r_1 < r_2 = r_3 = 3$.

Тогда

$$2^a + 2^b + 2^c \equiv 2^{r_1}(-1)^{a_1} + 2^{r_2}(-1)^{b_1} + 2^{r_3}(-1)^{c_1} \in \{\pm 1, \pm 3, \pm 4, \pm 5\} \pmod{17}.$$

В этих случаях сравнение $2^a + 2^b + 2^c \equiv 15 \pmod{17}$ не выполняется.

Упражнение 9.

Отсутствие решений системы 1 следует из отсутствия решений системы 2. Действительно, в любом решении системы 1 какое-то из a_i было бы больше 0, но тогда можно заменить 2^{a_i} на $2^{a_i-1} + 2^{a_i-1}$, получив решение системы 2. Поэтому рассмотрим систему 2.

Пусть $a_i = 8b_i + r_i$, где $r_i = \overline{0, 7}$. Имеем

$$2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} = \\ = 2^{r_1} \cdot 256^{b_1} + 2^{r_2} \cdot 256^{b_2} + 2^{r_3} \cdot 256^{b_3} + 2^{r_4} \cdot 256^{b_4} + 2^{r_5} \cdot 256^{b_5}.$$

Отсюда

$$2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} \equiv 2^{r_1} + 2^{r_2} + 2^{r_3} + 2^{r_4} + 2^{r_5} \pmod{255}$$

и

$$2^{a_1} + 2^{a_2} + 2^{a_3} + 2^{a_4} + 2^{a_5} \equiv 2^{r_1} \cdot (-1)^{b_1} + 2^{r_2} \cdot (-1)^{b_2} + \\ + 2^{r_3} \cdot (-1)^{b_3} + 2^{r_4} \cdot (-1)^{b_4} + 2^{r_5} \cdot (-1)^{b_5} \pmod{257}.$$

Если существует какое-нибудь решение, то очевидно, что существует решение, для которого $r_1 \leqslant r_2 \leqslant r_3 \leqslant r_4 \leqslant r_5$.

Проверьте, что все такие решения сравнения $2^{r_1} + 2^{r_2} + 2^{r_3} + 2^{r_4} + 2^{r_5} \equiv 170 \pmod{255}$ исчерпываются следующими случаями:

$r_1 = r_2 = 0$, $r_3 = 3$, $r_4 = 5$, $r_5 = 7$;
$r_1 = 1$, $r_2 = r_3 = 2$, $r_4 = 5$, $r_5 = 7$;
$r_1 = 1$, $r_2 = 3$, $r_3 = r_4 = 4$, $r_5 = 7$;
$r_1 = 1$, $r_2 = 3$, $r_3 = 5$, $r_4 = r_5 = 6$.

(Для сокращения перебора можно дополнительно использовать модули 3, 5 и 17.) Остаётся проверить, что эти решения не являются решениями сравнения

$$2^{r_1} \cdot (-1)^{b_1} + 2^{r_2} \cdot (-1)^{b_2} + 2^{r_3} \cdot (-1)^{b_3} + 2^{r_4} \cdot (-1)^{b_4} + 2^{r_5} \cdot (-1)^{b_5} \equiv 0 \pmod{257}.$$

Упражнение 10.

а) Ответ: $(b; c; m) \in \{(1; 2; 2), (3; 4; 3)\}$. Если $b = 1$, то мы получаем уравнение $5 + 2^c = 3^m$. Поскольку $3^m \equiv 1, 3 \pmod 8$, уравнение имеет решение только при $c = 2$.

Если $b = 2$, то $c \geqslant 3$ и мы получаем уравнение $7 + 2^c = 3^m$. Аналогично, поскольку $3^m \equiv 1, 3 \pmod 8$, а $7 + 2^c \equiv 7 \pmod 8$, в этом случае нет решений.

Если $b = 3$ или $b = 4$, то мы получим уравнения $11 + 2^c = 3^m$ и $19 + 2^c = 3^m$, которые рассмотрены в задачах 8 и 7.

Пусть теперь $5 \leqslant b < c$. Перепишем наше уравнение в виде

$$2^b(1 + 2^{c-b}) = 3(3^{m-1} - 1).$$

По лемме 2 получаем $m - 1 = 2^{b-2}t = 8d$, где t нечётно. Так как $3(3^{m-1} - 1) = 3(81^{2d} - 1) \equiv 0 \pmod{15}$, правая часть уравнения делится на 15. В то же время левая часть уравнения на 15 не делится, поскольку $1 + 2^{c-b} \equiv 2, 3, 5, 9 \pmod{15}$. Следовательно, при $5 \leqslant b < c$ решений нет.

б) Ответ: $(b; c; m) \in \{(1; 4; 3), (3; 6; 4)\}$. Если $b = 1$, то мы получаем уравнение $11 + 2^c = 3^m$, которое рассмотрено в задаче 8.

Если $b = 2$, то $c \geqslant 3$ и $13 + 2^c = 3^m$. Так как $3^m \equiv 1{,}3 \pmod 8$, а $13 + 2^c \equiv 5 \pmod 8$, в этом случае нет решений.

Если $b = 3$, то $c \geqslant 4$ и $17 + 2^c = 3^m$. Поскольку правая часть уравнения делится на 3, то и левая должна делиться на 3, откуда следует, что $c = 2c_1$ — чётное число. Поскольку $17 + 2^c \equiv 1 \pmod 8$, то $m = 2m_1$. Перепишем наше уравнение в виде $17 = 3^m - 2^c = (3^{m_1} - 2^{c_1})(3^{m_1} + 2^{c_1})$. Тогда $17 = 3^{m_1} + 2^{c_1}$ и $1 = 3^{m_1} - 2^{c_1}$. Отсюда $m_1 = 2$, $c_1 = 3$ и $m = 4$, $c = 6$.

Пусть теперь $4 \leqslant b < c$. Перепишем наше уравнение в виде

$$2^b(1 + 2^{c-b}) = 9(3^{m-2} - 1).$$

По лемме 2 получаем $m - 2 = 2^{b-2}t = 4d$, где t нечётно. Так как $9(3^{m-2} - 1) = 9(81^d - 1) \equiv 0 \pmod{15}$, правая часть уравнения делится на 15. В то же время левая часть уравнения на 15 не делится, поскольку $1+2^{c-b} \equiv 2, 3, 5, 9 \pmod{15}$. Следовательно, при $4 \leqslant b < c$ решений нет.

в) Ответ: $(b; c; m) \in \{(1; 3; 3)\}$.

Если $b=1$, то мы получаем уравнение $19+2^c=3^m$, которое рассмотрено в задаче 7.

Если $b=2$, $b=4$ или $b=6$, то мы получаем уравнения $21+2^c=3^m$, $33+2^c=3^m$ и $81+2^c=3^m$. Эти уравнения не имеют решений, поскольку их правая часть делится на 3, а левая не делится.

Если $b=3$, то $c \geqslant 4$ и $25+2^c=3^m$. Так как $25+2^c \equiv 1 \pmod 8$, то $m=2m_1$. Перепишем наше уравнение в виде $2^c=3^m-25=(3^{m_1}-5)(3^{m_1}+5)$. Тогда

$$\begin{cases} 3^{m_1}-5=2^x, \\ 3^{m_1}+5=2^y \end{cases} \Rightarrow \quad 10=2^y-2^x.$$

Это уравнение не имеет решений в целых неотрицательных числах.

Если $b=5$, то $c \geqslant 6$ и мы получим уравнение $49+2^c=3^m$. Из упражнения 7е) следует, что оно имеет решение только при $c=5$. Противоречие.

Пусть теперь $7 \leqslant b < c$. Перепишем наше уравнение в виде

$$2^4(1+2^{b-4}+2^{c-4})=3^m-1.$$

Поскольку $1+2^{b-4}+2^{c-4}$ — нечётное число, по лемме 2 получаем $m = 2^{4-2}t=4t$, где t нечётно. Положим $t=2s+1$.

Далее, $3^m-1=81^t-1 \equiv 5 \pmod{15}$, откуда $2^4+2^b+2^c \equiv 5 \pmod{15}$. Как следует из доказательства леммы 3, это возможно, только если $b \equiv c \equiv 1 \pmod 4$, т. е. $b=4b_1+1$, $c=4c_1+1$. Имеем

$$16+2\cdot 2^{4b_1}+2\cdot 2^{4c_1}=81^{2s+1}-1=80\cdot(81^{2s}+81^{2s-1}+81+1),$$

тогда

$$1+2\cdot 16^{b_1-1}+2\cdot 2^{c_1-1}=5\cdot(81^{2s}+81^{2s-1}+81+1).$$

Заметим, что $1+2\cdot 16^{b_1-1}+2\cdot 2^{c_1-1} \equiv 1 \pmod{16}$. С другой стороны $5\cdot(81^{2s}+81^{2s-1}+81+1) \equiv 5\cdot(1^{2s}+1^{2s-1}+1+1)1 \equiv 5(2s+1) \pmod{16}$, поэтому $10s+5 \equiv 1 \pmod{16}$, т. е. $s \equiv 6 \pmod 8$. Положим $s=8s_1+6$. Тогда $17+2\cdot 16^{b_1}+2\cdot 16^{c_1}=81^{16s_1+13}$. Поскольку

$$17+2\cdot 16^{b_1}+2\cdot 16^{c_1} \equiv 2\cdot(-1)^{b_1}+2\cdot(-1)^{c_1} \pmod{17}$$

и

$$81^{16s_1+13} \equiv 3^{4(16s_1+13)} \equiv 3^4\cdot 3^{16(4s_1+3)} \equiv 81 \equiv -4 \pmod{17},$$

получаем, что b_1 и c_1 — нечётные числа. Положим $b_1=2b_2+1$, $c_1=2c_2+1$. Тогда имеем $17+32\cdot 16^{2b_2}+32\cdot 16^{2c_2}=3^{64s_1+52}$ или $17+32\cdot 256^{b_2}+32\cdot 256^{c_2} = 3^{64s_1+52}$.

Применим модуль 257.

Поскольку

$$17 + 32 \cdot 256^{b_2} + 32 \cdot 256^{c_2} \equiv 17 + 32 \cdot (-1)^{b_2} + 32 \cdot (-1)^{c_2} \pmod{257},$$

левая часть уравнения при делении на 257 даёт остатки $17, 81, 210$.

Пусть $s_1 = 2s_2 + r$, где $r = 0, 1$. Тогда получаем

$$3^{64s_1+52} = 3^{52} \cdot (3^{64})^{s_1} = 3^{52} \cdot (3^{64})^{2s_2+r} = \\ = 3^{52} \cdot (3^{64})^{r} \cdot (3^{128})^{s_2} \equiv 162 \cdot 241^{r} \cdot (-1)^{s_2} \pmod{257}.$$

Следовательно, правая часть уравнения при делении на 257 может давать остатки 22, 95, 162 и 235. Противоречие, т. е. при $7 \leqslant b < c$ нет решений.

г) Ответ: $(b; c; m) \in \{(4; 5; 4)\}$.

Если $b = 1$, $b = 2$ или $b = 3$, то мы получаем уравнения $35 + 2^c = 3^m$, $37 + 2^c = 3^m$, $41 + 2^c = 3^m$, которые не имеют решений (см. упражнение 6).

Если $b = 4$, то $49 + 2^c = 3^m$. Из упражнения 7е) следует, что оно имеет решение только при $c = 5$.

Если $b = 5$, то $c \geqslant 6$ и $65 + 2^c = 3^m$. Из упражнения 7ж) следует, что оно имеет решение только при $c = 4$. Противоречие.

Пусть теперь $6 \leqslant b < c$. Перепишем наше уравнение в виде

$$2^5(1 + 2^{b-5} + 2^{c-5}) = 3^m - 1.$$

По лемме 2 получаем $m = 2^{5-2}t = 8t$, где t — нечётное число, положим $t = 2s + 1$. Имеем $33 + 2^b + 2^c = 3^{16s+8}$, тогда $3^{16s+8} \equiv 81^{4s+2} \equiv 6 \pmod{15}$ и $3^{16s+8} \equiv 3^8 \cdot 3^{16s} \equiv 81^2 \equiv -1 \pmod{17}$. Получаем систему сравнений

$$\begin{cases} 2^5 + 2^b + 2^c \equiv 5 & \pmod{15}, \\ 2^5 + 2^b + 2^c \equiv -2 \equiv 15 & \pmod{17}. \end{cases}$$

Из упражнения 8 следует, что эта система не имеет решений. Следовательно, при $6 \leqslant b < c$ решений нет.

Упражнение 11.

Если $a_1 \geqslant 10$, то перепишем наше уравнение в виде

$$2^{a_1}(1 + 2^{a_2-a_1} + 2^{a_3-a_1} + 2^{a_4-a_1} + 2^{a_5-a_1}) = 3^m - 1.$$

Поскольку в скобках стоит нечётное число, из леммы 2 получаем, что $m = 2^{a_1-2}q = 256 \cdot d$.

Поскольку для любого натурального k выполняется $3^{16k} \equiv 171^k \equiv 171 \pmod{255}$, получаем, что $3^m = 3^{256d} \equiv 171 \pmod{255}$. Используя малую теорему Ферма, получим $3^m = 3^{256d} \equiv 1 \pmod{257}$. Но тогда мы приходим к системе сравнений

$$\begin{cases} 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}=3^m-1\equiv 170 \pmod{255}, \\ 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}=3^m-1\equiv 0 \pmod{257}. \end{cases}$$

Как следует из упражнения 8, эта система не имеет решений, ч. т. д.

Упражнение 12.

В качестве одного из решений можно взять следующее: $a_1=0$, $a_2=8$, $a_3=2$, $a_4=10$, $a_5=4$, $a_6=12$, $a_7=6$, $a_8=14$.

Имеем

$$2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}+2^{a_6}+2^{a_7}+2^{a_8}=(2^0+2^8)(1+4+16+64)=257\cdot 85.$$

Следовательно, выполнено

$$\begin{cases} 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}+2^{a_6}+2^{a_7}+2^{a_8}\equiv 170 \pmod{255}, \\ 2^{a_1}+2^{a_2}+2^{a_3}+2^{a_4}+2^{a_5}+2^{a_6}+2^{a_7}+2^{a_8}\equiv 0 \pmod{257}. \end{cases}$$

Комментарии к задачам 9–13

9. По всей видимости, решений при $m>1$ и $q>7$ не существует, но доказательство этого факта авторам неизвестно.

10. Как мы обсуждали в § 2, уравнение имеет конечное число решений. Нетрудно найти пару $(n; m)=(5; 3)$, являющуюся решением. Вероятно, других решений нет, но доказательство этого факта авторам неизвестно.

11. Задача является обобщением упражнения 3. Общее решение авторам неизвестно.

12. Задача обобщает идею задачи 3. Общее решение авторам неизвестно.

13. Ответ: $n\in\{1, 2, 5\}$. Это задача с историей. В своё время Э. Б. Винберг задал этот вопрос Ж.-П. Серру. Через несколько дней Серр прислал решение, основанное на p-адическом анализе. Решение задачи двумя способами, принадлежащее Н. Н. Осипову, опубликовано в [6]. Одно из решений, использующее теорию уравнений Пелля, доступно школьникам.

Благодарности

Авторы благодарят членов редколлегии «Математического просвещения» за ценные замечания.

Список литературы

[1] *Винберг Э. Б.* Малая теорема Ферма и её обобщения // Математическое просвещение. Сер. 3. Вып. 12. М.: МЦНМО, 2008. С. 43–53.

[2] *Гиндикин С. Г.* Малая теорема Ферма // Квант. 1972. № 10. С. 2–9.

[3] Задачник Кванта. 1978. № 6. М509 а); 1983. № 3. М792 а), б).

[4] *Кожевников П. А., Сендеров В. А.* Степени n и n-е степени // Квант. 2012. № 1. С. 9–12.

[5] Математическое просвещение. Сер. 3. Вып. 16. М.: МЦНМО, 2012. С. 231, задача 11.

[6] Математическое просвещение. Сер. 3. Вып. 17. М.: МЦНМО, 2013. С. 203–207.

[7] *Сендеров В. А., Спивак А. В.* Малая теорема Ферма // Квант. 2000. № 1. С. 9–16, 37; № 3. С. 11–17; № 4. С. 15–18.

[8] *Сендеров В. А., Френкин Б. Р.* Гипотеза Каталана // Квант. 2007. № 4. С. 8–10.

[9] *Серпинский В.* 250 задач по элементарной теории чисел. М.: Просвещение, 1968. Задачи 154, 155, 207.

[10] *Спивак А. В.* Арифметика-2 // Библиотечка Квант. Вып. 109. М.: Бюро Квантум, 2008. С. 90, упр. 64.

[11] *Фёдоров Р. М., Канель-Белов А. Я., Ковальджи А. К., Ященко И. В.* Московские математические олимпиады 1993–2005 г. М.: МЦНМО, 2006.

[12] *Ферма П.* Исследования по теории чисел и диофантову анализу. М.: Наука, 1992.

[13] *Shorey T. N., Tijdeman R.* Exponential diophantine equations. Cambridge: Cambridge University Press, 2008. (Cambridge Tracts in Math.; V. 87).

[14] *Stewart C. L.* On the representation of an integer in two different bases // J. Reine Angew. Math. 1980. V. 319. P. 63–72.

[15] `http://en.wikipedia.org/wiki/Subspace_theorem`.

[16] `http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=GDZPPN002197707`.

[17] `http://mathoverflow.net/questions/143263/letting-sm-be-the-digit-sum-of-m-then-lim-n-to-inftys3n-infty`.

[18] `http://mathoverflow.net/questions/161960/looking-for-a-reference-to-a-classical-formula-for-the-sum-of-the-base-b-digit`.

[19] `http://mathoverflow.net/questions/179782/optimal-lower-bounds-for-the-sum-of-digits-in-base-b`.

[20] `http://mathoverflow.net/questions/38971/sums-of-digits-of-powers-of-integers`.

В. М. Журавлёв, ОАО «Туполев», Москва

`zhuravlevvm@mail.ru`

П. И. Самовол, Университет им. Бен-Гуриона, проект Эйлера (Беэр-Шева, Израиль)

`pet12@012.net.il`