

$\forall$  В этой задаче нам фактически надо было найти какое-нибудь решение в целых числах одного из уравнений

$$25x - 36y = 1, \quad 25x - 36y = -1$$

или доказать, что таких решений нет.

*Существует стандартная процедура, с помощью которой всегда можно найти решение уравнения  $ax + by = 1$ , если н.о.д.  $(a, b) = 1$ .* Продемонстрируем ее на нашей задаче. Выпишем все шаги алгоритма Евклида (см. обсуждение задачи 2-4 а)) для нахождения н.о.д.  $(36; 25)$ :

$$36 = 25 \cdot 1 + 11; \quad 25 = 11 \cdot 2 + 3; \quad 11 = 3 \cdot 3 + 2; \quad 3 = 2 \cdot 1 + 1.$$

Перепишем эту цепочку равенства так:

$$11 = 36 - 25 \cdot 1; \quad 3 = 25 - 11 \cdot 2; \quad 2 = 11 - 3 \cdot 3; \quad 1 = 3 - 2 \cdot 1.$$

Тогда получим

$$\begin{aligned} 1 &= 3 - (11 - 3 \cdot 3) = 3 \cdot 4 - 11 = (25 - 11 \cdot 2) \cdot 4 - 11 = \\ &= 25 \cdot 4 - 11 \cdot 9 = 25 \cdot 4 - (36 - 25) \cdot 9 = 25 \cdot 13 - 36 \cdot 9. \end{aligned}$$

В результате получается равенство  $25 \cdot 13 - 36 \cdot 9 = 1$ , дающее одно решение  $(13; 9)$  уравнения  $25x - 36y = 1$ .

**Задача 2-7.** *Ответ:* можно.

Проведем какую-нибудь окружность с центром в вершине данного угла. Стороны этого угла высекают на окружности дугу в  $19^\circ$ .

Если последовательно отложить циркулем эту дугу на окружности еще 18 раз, то, поскольку  $19 \times 19 = 361$ , последняя засечка отсечет от первой дуги дугу в  $1^\circ$ . Отложив циркулем эту дугу еще 17 раз, мы разделим дугу в  $19^\circ$  на 19 равных частей. Соединив полученные засечки с вершиной угла, мы разделим данный угол в  $19^\circ$  на 19 равных частей.

$\forall$  Пусть  $m$  и  $n$  – взаимно простые натуральные числа (н.о.д.  $(m, n) = 1$ ) и  $m < n$ . Откладывая на окружности последовательно друг за другом равные дуги, составляющие  $\frac{m}{n}$ -ю часть полной окружности, можно получить за  $n$  шагов все вершины правильного вписанного в окружность  $n$ -угольника (сделав при этом  $m$  полных оборотов). На некотором  $x$ -м шаге мы получим вершину, соседнюю с начальной, – при этом мы сделаем некоторое число  $y$  полных оборотов и еще пройдем  $\frac{1}{n}$ -ю часть окружности, так что  $x \cdot \frac{m}{n} = y + \frac{1}{n}$ . Отсюда получается *геометрический способ решения уравнения*

$$xm - yn = 1$$

*в целых числах.* В нашей задаче  $m = 19$ ,  $n = 360$ ,  $x = 19$ ,  $y = 1$ .

Задача 2-8. *Ответ:* 4 ломаные.

Будем считать какую-нибудь точку деления начальной и занумеруем, начиная с нее, все точки деления по часовой стрелке числами 1, 2, 3, ..., 20.

Ломаные с одинаковыми звеньями будут получаться, если мы будем соединять последовательно каждую точку с  $k$ -й по счету после нее до тех пор, пока не вернемся в исходную точку 1.

При  $k = 1$  получится правильный двадцатиугольник с вершинами в точках 1, 2, 3, ..., 20.

При  $k = 2$  – правильный десятиугольник с вершинами в точках 1, 3, 5, ..., 19.

При  $k = 3$  – самопересекающаяся замкнутая ломаная с 20 вершинами в точках 1, 4, 7, 10, 13, 16, 19, 2, 5, 8, 11, 14, 17, 20, 3, 6, 9, 12, 15, 18.

При  $k = 4$  – правильный пятиугольник.

При  $k = 5$  – квадрат.

При  $k = 6$  – самопересекающаяся замкнутая ломаная с 10 вершинами в точках 1, 7, 13, 19, 5, 11, 17, 3, 9, 15.

При  $k = 7$  – снова 20-звенная ломаная.

При  $k = 8$  – 5-звенная ломаная (пятиконечная звезда).

При  $k = 9$  – снова 20-звенная ломаная.

При  $k = 10$  получается вырожденная 2-звенная ломаная – дважды пройденный отрезок.

При  $k = 11$  получается та же ломаная, что и при  $k = 9$ , так как соединять точки через 10 по часовой стрелке – то же самое, что соединять их через 8 против часовой стрелки.

Точно так же при  $k = 12, 13, 19$  получают соответственно такие же ломаные, что и при  $k = 8, 7, \dots, 1$ .

Таким образом, всего различных 20-звенных ломаных – четыре, они получаются при  $k = 1, 3, 7, 9$ .

∇ При любом  $n$  различных по форме правильных  $n$ -звенных замкнутых ломаных будет столько, сколько существует натуральных

чисел, меньших  $\frac{n}{2}$  и взаимно простых с  $n$ .

Количество натуральных чисел, меньших данного числа  $n$  и взаимно простых с ним, обозначается обычно через  $\varphi(n)$ . Функция  $\varphi(n)$  называется *функцией Эйлера*; если  $p_1, p_2, \dots, p_l$  – все различные простые числа, входящие в разложение числа  $n$  на простые множители, то

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_l}\right).$$

Ответ к обобщению задачи 2-8 можно записать так: число различных

правильных  $n$ -звенных ломаных равно  $\varphi(n)/2$ . В частности, если  $n = 20$ , то  $\varphi(20) = 20 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 8$ , а число ломаных равно  $\varphi(20)/2 = 4$  (см. [88]).

Задача **2-9**. а) *Ответ*: верно.

Разность двух чисел делится на 7 в том и только в том случае, когда равны остатки от деления этих чисел на 7. При делении на 7 существует семь возможных остатков: 0, 1, 2, 3, 4, 5, 6.

Допустим, что нельзя выбрать 15 нужных чисел из 100. Это значит, что не более 14 чисел дают при делении на 7 остаток 0, не более 14 чисел – остаток 1, аналогично – остатки 2, 3, 4, 5, 6. Но тогда всего чисел получается не более чем  $14 \cdot 7 = 98 < 100$ , и наше допущение неверно.

▽ Решение задачи 2-9 а) – типичный пример применения принципа Дирихле: *если в  $n$  клетках сидит  $nk + 1$  зайцев, то хотя бы в одной клетке не меньше  $k + 1$  зайцев* (см. [43]).

В самом деле, если бы в каждой клетке было не больше  $k$  зайцев, то всего зайцев было бы не больше чем  $nk$ , что противоречит условию.

б) *Ответ*: неверно.

Приведем контрпример: первые сто натуральных чисел от 1 до 100. Среди них 14 чисел: 7, 14, 98, дающих в остатке 0; по 15 чисел, дающих в остатке 1 и 2; по 14 чисел, дающих в остатке 3, 4, 5, 6. Значит, среди них нет 16 чисел, для которых разность любых двух делится на 7.

Задача **2-10**. Всякое целое число либо делится на 3, либо при делении на 3 дает в остатке 1 или 2.

Если число  $n$  делится на 3, то его можно записать в виде  $n = 3k$ , поэтому его квадрат можно записать в виде  $9k^2$ , откуда видно, что он делится на 3.

Если число  $n$  при делении на 3 дает в остатке 1, то его можно записать в виде  $n = 3k + 1$ , тогда для его квадрата получаем:  $n^2 = 3(3k^2 + 2k) + 1$ , откуда видно, что квадрат при делении на 3 также дает в остатке 1.

Если число  $n$  при делении на 3 дает в остатке 2, аналогично получаем:  $n^2 = 3(3k^2 + 4k + 1) + 1$ , т.е. и в этом случае квадрат числа  $n$  дает при делении на 3 остаток 1.

Если ровно одно из двух чисел не делится на 3, то его квадрат при делении на 3 дает, как мы видели, остаток 1, поэтому сумма квадратов этих двух чисел при делении на 3 дает остаток 1; а если ни одно из двух чисел не делится на 3, то их квадраты оба дают

при делении на 3 остатки 1, поэтому сумма их квадратов при делении на 3 даст остаток 2.

Таким образом, сумма квадратов двух целых чисел делится на 3 лишь в случае делимости каждого из них на 3.

∇ Переход от целых чисел к их остаткам от деления на фиксированное число  $m$  – основной прием в задачах на делимость целых чисел. При этом постоянно используется следующее простое правило: *чтобы найти остаток от деления на  $m$  суммы или произведения двух (или нескольких) целых чисел, достаточно проделать те же операции с остатками и найти, какой остаток при делении на  $m$  дает результат.*

Покажем, например, что утверждение задачи 2-10 останется верным, если заменить в ее условии число 3 на число 7. Возведя в квадрат числа от 0 до 6, можно убедиться, что остатки, которые дают квадраты целых чисел при делении на 7, – это только 0, 1, 2 и 4. Поскольку никакие два из этих четырех чисел, кроме пары нулей, в сумме не дают числа, делящегося на 7, сумма квадратов двух целых чисел делится на 7, только если каждое число делится на 7.

*Для знатоков.* Вопрос о том, может ли для данного простого числа  $p$  сумма квадратов двух целых чисел  $x^2 + y^2$  делиться на  $p$ , если ни одно из них не делится на  $p$ , эквивалентен такому: является ли  $(-1)$  квадратичным вычетовом по модулю  $p$ , т.е. существует ли такое  $z$ , что  $1 + z^2$  делится на  $p$ . Ответ (известный еще Эйлеру): это возможно для чисел  $p$  вида  $4k + 1$  ( $p = 5, 13, 17, 29, \dots$ ) и невозможно для  $p = 4k + 3$  ( $p = 3, 7, 11, 19, 23, \dots$ ). Обобщение этого факта, позволяющее для каждого из двух чисел  $q$  и  $p$  быстро решить вопрос, является ли  $q$  квадратичным вычетовом по модулю  $p$ , – *квадратичный закон взаимности Гаусса* (см. [31, 88]).

**Задача 2-11.** Покажем, что ни одно число вида  $9n + 4$ , где  $n$  – натуральное число, не представляется в виде суммы трех кубов; поскольку чисел такого вида бесконечно много, отсюда будет следовать утверждение задачи.

Любое целое число имеет либо вид  $3l$ , либо  $3l + 1$ , либо  $3l - 1$ , где  $l$  – целое число. Поэтому куб любого целого числа имеет соответственно вид либо  $27l^3$ , либо

$$27l^3 \pm 27l^2 + 9l \pm 1 = 9(3l^3 \pm 3l^2 + l) \pm 1,$$

т.е. имеет вид либо  $9m$ , либо  $9m \pm 1$ .

Комбинируя всеми способами эти возможности, мы получим, что сумма кубов трех целых чисел представляется одним из следующих вариантов:  $9n$ ;  $9n \pm 1$ ;  $9n \pm 2$ ;  $9n \pm 3$ , но не может равняться числу вида  $9n + 4$  (и, кстати,  $9n - 4$ ).

В 1909 г. были доказаны следующие гипотезы Э. Варинга (1770 г.): *каждое натуральное число может быть представлено в виде суммы не более 9 кубов натуральных чисел; для каждого натурального  $k$  любое натуральное число представляется как сумма  $w$  или меньше  $k$ -х степеней натуральных чисел, где  $w$  зависит только от  $k$* . Первая гипотеза была доказана А.Виферихом, вторая – Д.Гильбертом (элементарное ее доказательство было получено Ю.В.Линником). Наименьшее значение  $w = w(k)$  неизвестно уже для  $k = 4$  (см. [5, 118]).

Любопытно, что каждое натуральное число  $n$  легко представить в виде суммы пяти кубов целых чисел.

В самом деле,  $n - n^3$  делится на 6 при всех  $n$ . Поэтому  $n = n^3 + 6t$ , где  $t$  целое. Отсюда

$$n = n^3 + (t+1)^3 + (t-1)^3 + (-t)^3 + (-t)^3.$$

**Задача 2-12.** Поскольку каждый ученик мог сидеть не больше чем с 27 учениками, это не могло длиться более 27 месяцев.

Покажем, как учитель мог рассаживать учеников в течение 27 месяцев.

Занумеруем учеников числами от 1 до 28. Поставим числа от 1 до 27 на окружности в вершинах правильного 27-угольника, а число 28 – в центре этой окружности. Соединим отрезком точки 1 и 28. Остальные точки соединим попарно отрезками, перпендикулярными этому отрезку – см. рисунок 10,а. Рассадим учеников так: если два числа соединены отрезком, то соответствующих им школьников сажаем за одну парту.

В следующем месяце соединяем отрезком точки 2 и 28 и через остальные точки проводим перпендикулярные ему отрезки; рассаживаем учеников по этой схеме – рисунок 10,б. Далее берем поочередно отрезки 28-3, 28-4, 28-27 и проводим отрезки, перпендикулярные каждому из них.

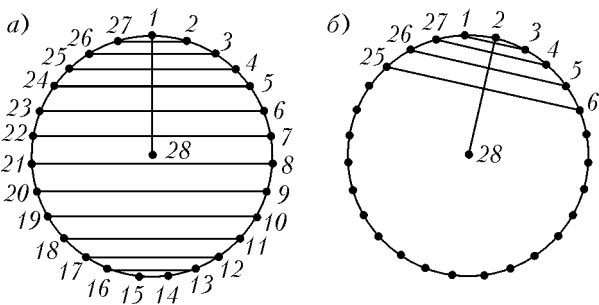


Рис. 10

∇ Заметим, что на рисунке 10,а сумма номеров каждой пары точек круга, соединенных отрезком, равна числу 29, которое дает остаток 2 при делении на 27, а точка 1 соединена с центром точкой 28; эта последняя пара оказывается в особом положении: среди чисел от 1 до 27 невозможно подобрать такую пару к числу 1, кроме него самого, чтобы сумма чисел этой пары давала остаток 2 при делении на 27.

На рисунке 10,б ситуация аналогична: суммы пар номеров соединенных точек дают при делении на 27 остаток 4, а для номера 2 среди чисел от 1 до 27 нет подходящей пары, кроме него самого; этот номер 2 соединен с центром 28.

Эти наблюдения приводят к следующей числовой интерпретации приведенного в задаче 2-12 расписания.

Фиксируем какое-нибудь число  $r$  от 1 до 27. Объединяем в пары те номера от 1 до 27, которые в сумме дают остаток  $r$  при делении на 27. При этом без пары останется только тот номер  $x$ , который в сумме с самим собой дает при делении на 27 остаток  $r$ . Если  $r$  четно, то  $x = r/2$ , а если нечетно, то  $x = (r + 27)/2$ . Этот номер  $x$  мы соединим с номером 28.

Для любого четного числа  $n$  учеников можно аналогичным образом составить расписание на  $n - 1$  месяц. Для этого надо объединять в пары те номера из множества всех целых чисел от 1 до  $n - 1$ , сумма которых дает остаток  $r$  при делении на  $n - 1$ . Если  $r$  четно, то при этом без пары останется номер  $r/2$ , а если нечетно, то номер  $(r + n - 1)/2$ ; этот номер объединим в пару с оставшимся номером  $n$  (см. [34], [124]).

**Задача 2-13.** *Ответ:* например, 48, 49, 50 или 548, 549, 550.

∇ Можно показать, что вообще для любого  $k$  существует  $k$  последовательных натуральных чисел, каждое из которых делится на квадрат целого числа, большего единицы.

Тут уместно воспользоваться так называемой **китайской теоремой об остатках** (см. [88]): *каковы бы ни были натуральные попарно взаимно простые числа  $a_1, a_2, \dots, a_n$  и целые неотрицательные числа  $r_1, r_2, \dots, r_n$  ( $r_1 < a_1, r_2 < a_2, \dots, r_n < a_n$ ), существует такое натуральное число  $m$ , которое при делении на числа  $a_1, a_2, \dots, a_n$  соответственно дает остатки  $r_1, r_2, \dots, r_n$ .*

Пусть  $p_1^2, p_2^2, \dots, p_n^2$  — квадраты  $n$  различных простых чисел. Тогда, по этой теореме, найдется такое целое число  $m$ , которое дает при делении на числа  $p_1^2, p_2^2, \dots, p_n^2$  соответственно остатки  $p_1^2 - 1, p_2^2 - 2, \dots, p_n^2 - n$ . Поэтому  $n$  последовательных чисел  $m + 1, m + 2, \dots, m + n$  будут делиться соответственно на  $p_1^2, p_2^2, \dots, p_n^2$ .

Пример (548, 549, 550), указанный в ответе, подобран именно таким путем: полагаем  $p_1 = 2, p_2 = 3, p_3 = 5$ , находим число  $m$ , которое дает

соответственно остатки 3, 7 и 22 при делении на 4, 9 и 25; годится, например, число  $m = 547$ .

Это число  $m$  можно подобрать таким образом. Ищем его в виде

$$m = a \cdot 9 \cdot 25 + 4 \cdot b \cdot 25 + 4 \cdot 9 \cdot c .$$

Нужно, чтобы число  $a \cdot 9 \cdot 25$  давало остаток 3 при делении на 4, число  $4 \cdot b \cdot 25$  – остаток 7 при делении на 9 и число  $4 \cdot 9 \cdot c$  – остаток 22 при делении на 25. Полагая  $a = -1$ ,  $b = 7$ ,  $c = 2$ , получаем  $m = 547$ .

Задача 2-14. *Ответ:* можно.

На рисунке 11 приведены два примера нужной расстановки. Это можно проверить простым подсчетом.

∇ Числа, выписанные на первом круге на рисунке 11,а по часовой стрелке, – это остатки от деления последовательных степеней  $1, 2, 2^2, 2^3, \dots, 2^{11}$  на число 13, а против часовой стрелки – остатки

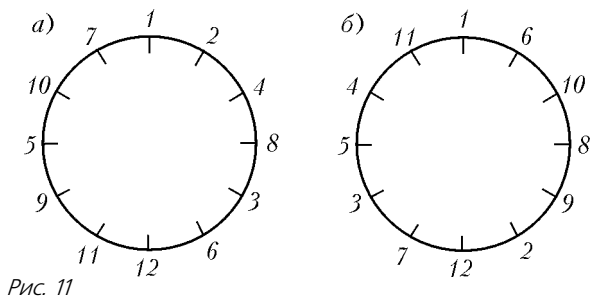


Рис. 11

последовательных степеней  $1, 7, 7^2, 7^3, \dots, 7^{11}$ . Естественно, что для каждых трех соседних чисел  $a, b, c$  (а значит, и для их остатков при делении на 13) число  $b^2 - ac$  делится на 13; если три числа  $a, b, c$  образуют геометрическую прогрессию, то  $b^2 = ac$ .

Точно так же на рисунке 11,б выписаны остатки от деления на 13 последовательных степеней  $1, 6, 6^2, \dots, 6^{11}$  (по часовой стрелке) и  $1, 11, 11^2, \dots, 11^{11}$  (против часовой стрелки).

Числа 2, 6, 11, 7, стоящие на рисунке 11 рядом с 1, – это остатки при делении на 13 чисел  $2, 2^5, 2^7, 2^{11}$ .

Вообще, для любого простого  $p$  существует *первообразный корень* – такое число  $r$ , что его степени  $1, r, r^2, \dots, r^{p-1}$  дают все различные остатки  $1, 2, \dots, p-1$  при делении на  $p$ ; число таких  $r$  равно  $\varphi(p-1)$  – числу взаимно простых с  $p-1$  чисел от 1 до  $p-2$  (см. комментарий к задаче 2-8).

В задаче 2-14  $p = 13$ ,  $\varphi(p-1) = \varphi(12) = 4$ , так как имеется 4 числа, 1, 5, 7, 11, взаимно простых с числом 12 и меньших его: все первообразные корни – остатки от деления на 13 чисел  $2, 2^5, 2^7, 2^{11}$  (см. [88]).

Задача 2-15. *Ответ:* неверно. Например, при  $n = 6$  число  $6^3 + 5 \cdot 6 - 1$  равно  $5 \cdot 7^2$ .

▽ Знаток сразу ответил бы на вопрос задачи отрицательно, так как, кроме констант, вообще не существует многочленов  $F(n)$  с целыми коэффициентами, значения которых при всех натуральных  $n$  – простые числа.

В самом деле, если свободный член  $a$  многочлена не равен 0 и  $\pm 1$ , то значения  $F(ka)$  при целых  $k$  делятся на  $a$  и среди них есть составные. Если  $a = \pm 1$ , то можно сначала «сдвинуть» многочлен – заменить  $F(n)$  на  $F(n+h) = G(n)$  так, чтобы свободный член стал не равным  $\pm 1$ .

В задаче 2-15 найти  $n$ , при котором  $F(n) = n^3 + 5n - 1$  – составное число, можно так. Положим  $n = m + 1$ ; у многочлена  $F(m+1) = (m+1)^3 + 5(m+1) - 1$  свободный член равен 5, и поэтому  $F(6)$  делится на 5.

Отметим, что в 1970 году наш отечественный математик Ю.В. Матияевич доказал существование многочлена от 21 переменного с целыми коэффициентами, обладающего таким свойством: множество его положительных значений при целых значениях переменных совпадает с множеством простых чисел (см. [47, 54, 100]).

Задача 2-16. Разложим данное число на множители:

$$\begin{aligned} n^5 - 5n^3 + 4n &= n(n^4 - 5n^2 + 4) = n(n^2 - 1)(n^2 - 4) = \\ &= (n-2)(n-1)n(n+1)(n+2). \end{aligned}$$

В результате получилось произведение пяти последовательных целых чисел.

Одно из таких чисел обязательно делится на 5, одно из трех последовательных чисел делится на 3, а из четырех последовательных чисел одно делится на 4, а другое – на 2. Поэтому произведение делится на 120.

▽ Другое, комбинаторное решение этой задачи можно получить, если заметить, что при  $n \geq 3$  число

$$\frac{(n+2)(n+1)n(n-1)(n-2)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5}$$

есть биномиальный коэффициент  $C_{n+2}^5$  (число 5-элементных подмножеств из  $(n+2)$  элементов), а это число, несомненно, целое.

Вообще, многочлен  $F(x)$  принимает целые значения при всех целых  $x$  тогда и только тогда, когда его можно представить в виде суммы  $F(x) = \sum a_k C_x^k$  с целыми коэффициентами  $a_k$ , где

$$C_x^k = \frac{x(x-1)\dots(x-k+1)}{k!} \quad (\text{см. [104]}).$$



Задача 2-17. а) *Ответ:* да.

Удобно искать такой многочлен в виде

$$p(x) = ax(x-1) + bx + c.$$

Подставляя в это тождество  $x = 0$ ,  $x = 1$  и  $x = 2$ , получаем для определения коэффициентов  $a$ ,  $b$ ,  $c$  удобную «треугольную» систему линейных уравнений

$$\begin{cases} c = 19, \\ b + c = 85, \\ 2a + 2b + c = 1985, \end{cases}$$

из которой находим:  $c = 19$ ,  $b = 66$ ,  $a = 917$  и получаем ответ:

$$p(x) = 917x^2 - 851x + 19.$$

∇ Точно так же удобно искать многочлен степени не выше  $n$ , принимающий в данных  $n + 1$  точках  $c_1, c_2, \dots, c_{n+1}$  данные значения. Записав  $p(x)$  в виде

$$p(x) = b_0 + b_1(x - c_1) + b_2(x - c_1)(x - c_2) + \dots \\ \dots + b_n(x - c_1)(x - c_2)\dots(x - c_n)$$

и подставляя в это тождество  $x = c_1, c_2, \dots, c_{n+1}$ , мы получаем треугольную линейную систему для определения  $m + 1$  неизвестных коэффициентов  $b_0, b_1, \dots, b_n$ .

Указанный метод нахождения многочлена с данными значениями называется *способом интерполяции Ньютона*.

б) *Ответ:* нет, не существует.

Для доказательства воспользуемся следующим утверждением: если дан многочлен

$$p(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n$$

с целыми коэффициентами, то для любых целых чисел  $c$  и  $d$  целое число  $p(c) - p(d)$  делится на число  $c - d$ .

Согласно этому утверждению, число  $p(19) - p(1) = 66$  должно делиться на число  $19 - 1 = 18$ , что неверно, откуда и следует ответ.

Докажем справедливость высказанного утверждения:

$$p(c) - p(d) = (a_0c^n + a_1c^{n-1} + \dots + a_{n-1}c + a_n) - \\ - (a_0d^n + a_1d^{n-1} + \dots + a_{n-1}d + a_n) = \\ = a_0(c^n - d^n) + a_1(c^{n-1} - d^{n-1}) + \dots + a_{n-1}(c - d).$$

Для любого натурального  $k$  справедлива формула

$$c^k - d^k = (c - d)(c^{k-1} + c^{k-2}d + \dots + cd^{k-2} + d^{k-1})$$

(она получается из формулы суммы  $k$  членов геометрической прогрессии с первым членом  $c^{k-1}$  и знаменателем  $d/c$ ). Поэтому каждое слагаемое в полученном равенстве для  $p(c) - p(d)$  делится на  $c - d$ , значит, и вся сумма делится на  $c - d$ .

∇ Аналогично можно показать, что для любого многочлена  $p(x)$  и любого числа  $d$  многочлен  $p(x) - p(d)$  делится на многочлен  $x - d$ , т.е.  $p(x) - p(d) = (x - d)q(x)$ , где  $q(x)$  - некоторый многочлен. Переписав это тождество в виде  $p(x) = (x - d)q(x) + p(d)$ , получаем следующую теорему Безу: *остаток от деления многочлена  $p(x)$  на двучлен  $(x - d)$  равен  $p(d)$ .*

Задача **2-18.** а) *Ответ:*  $(x^2 + x + 1)(x^2 - x + 1)(x^4 - x^2 + 1)$ .

Действительно:

$$\begin{aligned} x^8 + x^4 + 1 &= x^8 + 2x^4 + 1 - x^4 = (x^4 + 1)^2 - (x^2)^2 = \\ &= (x^4 + x^2 + 1)(x^4 - x^2 + 1) = \left( (x^2 + 1)^2 - x^2 \right) (x^4 - x^2 + 1) = \\ &= (x^2 + x + 1)(x^2 - x + 1)(x^4 - x^2 + 1). \end{aligned}$$

б) *Ответ:*  $(x^3 - x^2 + 1)(x^2 + x + 1)$ . Действительно:

$$\begin{aligned} x^5 + x + 1 &= (x^5 + x^4 + x^3) - (x^4 + x^3 + x^2) + \\ &+ (x^2 + x + 1) = (x^3 - x^2 + 1)(x^2 + x + 1). \end{aligned}$$

∇ Существуют многочлены любой степени с целыми коэффициентами, которые не разлагаются в произведение многочленов меньшей степени с целыми коэффициентами (например,  $x^n - 2$ ). Они называются неприводимыми (над кольцом целых чисел).

Имеются алгоритмы, позволяющие для любого многочлена указать его разложение на неприводимые множители или показать, что он сам неприводим (см. [85, 117]).

Задача **2-19.** *Ответ:* при  $a = -2$ .

Пусть многочлены  $f(x) = x^4 + ax^2 + 1$  и  $g(x) = x^3 + ax + 1$  имеют общий корень  $x_0$ . Тогда, умножив второй многочлен на  $x$  и вычитая из первого, получим многочлен, имеющий тот же корень, а этот многочлен - просто

$$f(x) - xg(x) = 1 - x.$$

Его единственный корень  $x_0 = 1$ . Многочлены  $f(x)$  и  $g(x)$  имеют этот корень при  $a = -2$ ; чтобы убедиться в этом, достаточно приравнять нулю  $f(1)$  и  $g(1)$  – оба эти числа равны  $a + 2$ .

∇ Для того чтобы многочлены  $f(x)$  и  $g(x)$  имели общий корень  $x_0$ , нужно, чтобы оба они делились на многочлен  $x - x_0$  (теорема Безу, см. задачу 2-17). Найти общий делитель наибольшей степени двух многочленов можно с помощью *алгоритма Евклида* – так же, как и наибольший общий делитель двух чисел. В решении задачи 2-19 мы проделали один шаг этого алгоритма – разделили многочлен  $f(x)$  и  $g(x)$  с остатком, который оказался равным  $1 - x$ .

Если далее разделить  $g(x)$  столбиком на  $(x - 1)$ , то получится остаток  $a + 2$ :

$$g(x) = (x - 1)(x^2 + x + a + 1) + (a + 2).$$

Если  $a = -2$ , то остаток равен 0; если же  $a \neq -2$ , то многочлены не имеют общего делителя степени, большей 0.

**Задача 2-20. а)** Пусть  $k = a^5 + 5b^2$  и  $l = c^2 + 5d^2$  – два каких-нибудь числа из множества  $M$ . Тогда

$$kl = (a^2 + 5b^2)(c^2 + 5d^2) = (ac - 5bd)^2 + 5(ad + bc)^2. \quad (*)$$

Таким образом,  $kl = x^2 + 5y^2$ , где  $x = ac - 5bd$ ,  $y = ad + bc$ , т.е. число  $kl$  принадлежит  $M$ .

б) *Ответ:* существуют. Например,  $84 = 4 \cdot 21 = 6 \cdot 14$ .

Покажем, что все пять вписанных чисел принадлежат множеству  $M$ :

$$4 = 2^2 + 5 \cdot 0^2, \quad 6 = 1^2 + 5 \cdot 1^2, \quad 14 = 3^2 + 5 \cdot 1^2,$$

$$21 = 4^2 + 5 \cdot 1^2, \quad 84 = 2^2 + 5 \cdot 4^2.$$

Для того чтобы показать, что числа 4, 6, 14, 21 – базисные, выпишем все числа из  $M$ , большие 1 и не превышающие 21: 4, 5, 6, 9, 14, 16, 20, 21. Среди них все, кроме 16, 20, – базисные, потому что каждое из них не делится ни на одно из предыдущих.

в) Предположим, напротив, что базисных чисел конечное число:  $b_1, b_2, \dots, b_n$ . Тогда число  $1 + 5(b_1 b_2 \dots b_n)^2$ , очевидно, принадлежащее  $M$ , не делится ни на одно из чисел  $b_1, b_2, \dots, b_n$ , поэтому оно само базисное и не равно ни одному из  $b_1, b_2, \dots, b_n$ , что противоречит предположению.

∇ Обратим внимание на аналогию между множеством  $M$  и множеством всех натуральных чисел.

Так же как всякое натуральное число разлагается в произведение простых чисел, любое число из  $M$  разлагается в произведение базисных

чисел. Однако если натуральное число единственным образом разлагается на простые множители (*основная теорема арифметики*), то, согласно задаче 2-20 б), это неверно для чисел из множества  $M$ .

Для знатоков. Тождество  $(*)$  связано с правилом умножения чисел вида  $x + y\sqrt{-5}$  (см. [48]):

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}.$$

Вопрос о разложении на множители чисел из  $M$  эквивалентен вопросу о разложении на множители в кольце чисел вида  $x + y\sqrt{-5}$ , где  $x$  и  $y$  – целые. Задачи о разложении на множители в кольцах такого типа сыграли важную роль в истории математики. Из этих задач возник новый раздел математики – алгебраическая теория чисел (см. [82]).

Задача **2-21**. *Ответ:* например,  $(7^2, 13^2, 17^2)$ ,  $(17^2, 25^2, 31^2)$ ,  $(31^2, 41^2, 49^2)$ .

Тройка квадратов  $p^2, q^2, r^2$  образует арифметическую прогрессию тогда и только тогда, когда  $p^2 + r^2 = 2q^2$  или

$$(r - q)(r + q) = (q - p)(q + p).$$

Например, для третьей из указанных троек ( $p = 31$ ,  $q = 41$ ,  $r = 49$ ) получаем

$$(49 - 41)(49 + 41) = (41 - 31)(41 + 31) = 720.$$

∇ Вот общие формулы для таких троек (из взаимно простых чисел):

$$p = n^2 + 2nm - m^2, \quad q = m^2 + n^2, \quad r = m^2 + 2mn - n^2,$$

где  $m$  и  $n$  – произвольные взаимно простые числа. Если при каких-нибудь тип числа  $p, q, r$  имеют общий делитель, то мы можем их сократить на него. (Это бывает, когда числа  $m$  и  $n$  оба нечетны; тогда соответствующие числа  $p, q, r$  имеют общий множитель 2. Других общих множителей, как нетрудно показать, быть не может.)

То, что числа такого вида годятся, можно проверить, подставив их в соотношение  $(p - q)(p + q) = (q - r)(q + r)$ .

К этим формулам можно прийти разными путями; мы укажем один из них (см. [122]).

Пусть  $p^2 + r^2 = 2q^2$ . Разделив все члены этого уравнения на  $q^2$ , получаем  $(p/q)^2 + (r/q)^2 = 2$ . Обозначив  $p/q$  через  $x$ ,  $r/q$  – через  $y$ , получаем уравнение  $x^2 + y^2 = 2$ . Таким образом, задача нахождения чисел  $p, q, r$  сводится к решению уравнения  $x^2 + y^2 = 2$  в рациональных числах  $x, y$ .

Идею решения объясним на геометрическом языке. Решить полученное уравнение – это значит на окружности  $x^2 + y^2 = 2$  найти все точки

с рациональными координатами. Возьмем одну такую точку – скажем,  $(-1; -1)$ . Если провести через эту точку и другую рациональную точку  $(x; y)$  прямую, то ее угловой коэффициент  $t = (y + 1)/(x + 1)$  рационален.

Верно и обратное: любая прямая с рациональным угловым коэффициентом  $t \neq -1$ , проходящая через точку  $(-1; -1)$ , пересекает еще раз окружность  $x^2 + y^2 = 2$  в рациональной точке  $(x; y)$ . Чтобы убедиться в этом, выразим  $y$  из уравнения прямой  $y = t(1 + x) - 1$  и подставим в уравнение окружности:

$$x^2 + (t(1 + x) - 1)^2 = 2,$$

откуда

$$(1 + t^2)x^2 - 2t(1 - t)x + (t^2 - 2t - 1) = 0.$$

Это квадратное уравнение относительно  $x$ , один корень которого,  $x = -1$ , мы знаем.

С помощью теоремы Виета находим второй корень:  $x = \frac{-t^2 + 2t + 1}{t^2 + 1}$ .

Мы нашли одну координату точки  $(x; y)$ . Теперь можно найти и вторую:  $t = \frac{t^2 + 2t - 1}{t^2 + 1}$ .

Положим затем  $t = m/n$ ; тогда из формул для  $x = \frac{p}{q}$  и  $y = \frac{r}{q}$  получаем тройку  $p, q, r$  в таком виде:  $p = -m^2 + 2mn + n^2$ ,  $q = m^2 + n^2$ ,  $r = m^2 + 2mn - n^2$ .

Описанный способ рассуждений годится для отыскания всех рациональных точек на кривой второго порядка (или – что то же самое – всех целых решений уравнений типа  $ax^2 + bxy + cy^2 = dz^2$ ), задаваемой уравнением с целыми коэффициентами, если известна хоть одна такая точка. Для выяснения вопроса о том, существует ли такая точка, также существует эффективный алгоритм (см. [125], [126]).

**Задача 2-22.** *Ответы:* а) семь решений в целых числах:  $(0; 0)$ ,  $(4; 0)$ ,  $(-4; 0)$ ,  $(2; 6)$ ,  $(2; -6)$ ,  $(3; 12)$ ,  $(3; -12)$ ;

б) еще четыре решения в рациональных числах:  $\left(-\frac{1}{2}; \pm \frac{3}{2}\right)$ ,  $\left(-\frac{1}{3}; \pm \frac{4}{3}\right)$ .

▽ Как находить новые решения в рациональных числах по уже имеющимся, можно объяснить на геометрическом языке.

Наше уравнение задает некоторую кривую на координатной плоскости  $Oxy$ .

Пусть мы знаем какие-нибудь две точки этой кривой, координаты

которых  $(x_1; y_1)$  и  $(x_2; y_2)$  – рациональные числа. Прямая, проходящая через эти точки, пересекает кривую в третьей точке, поскольку уравнение кривой имеет третью степень.

Координаты  $x_3, y_3$  этой третьей точки будут рациональными функциями от  $x_1, y_1, x_2, y_2$  с целыми коэффициентами, т.е. тоже рациональными числами.

Таким образом, отправляясь от двух каких-нибудь решений  $(x_1; y_1)$ ,  $(x_2; y_2)$  уравнения в рациональных числах, мы получаем новое решение  $(x_3; y_3)$  в рациональных числах.

Представим теперь результаты соответствующих вычислений.

Прямая, проходящая через данные точки  $(x_1; y_1)$  и  $(x_2; y_2)$ , задается уравнением  $y = t(x - x_1) + y_1$ , где  $t = (y_2 - y_1)/(x_2 - x_1)$ . Подставляя  $y$  в уравнение  $y^2 = 6(x^3 - x)$ , получаем уравнение третьей степени относительно  $x$ , два корня  $x_1, x_2$  которого нам известны (ведь точки лежат на кривой), а третий можно найти по теореме Виета:

$$x_3 = t^2/6 - x_1 - x_2. \quad (1)$$

Аналогично можно найти  $y_3$ :

$$y_3 = t^3/6 + 2y_1 - y_2 - 3tx_1. \quad (1')$$

Можно взять точку  $(x_2; y_2)$ , «совпадающую» с  $(x_1; y_1)$ , – провести в ней касательную к кривой; она будет пересекать кривую еще в одной точке:

$$x_4 = t^2/6 - 2x_1, \quad y_4 = t^3/6. \quad (2)$$

Итак, мы получили формулы, позволяющие находить по известным рациональным решениям уравнения  $y^2 = 6(x^3 - x)$  новые решения.

*Для знатоков.* Естественно задать следующие вопросы. Будем ли мы указанным способом (проводя через известные рациональные точки прямые) получать каждый раз новые рациональные точки? Конечно или бесконечно множество рациональных точек? Каким образом их все можно описать? Сколько среди них целых точек?

Для того чтобы ответить на эти вопросы, целесообразно на кривой третьей степени ввести операцию сложения точек, обладающую свойством ассоциативности. Описать ее удобнее для кривой, заданной уравнением

$$y^2 = x^3 + ax + b. \quad (3)$$

(Любую неособую кривую  $P(x, y) = 0$  третьей степени можно некоторым преобразованием переменных привести к такому виду; при этом если коэффициенты  $P(x, y)$  были целыми, задачу отыскания рациональных точек на кривой  $P(x, y) = 0$  можно свести к аналогичной

задаче для кривой (3) с целыми  $a$  и  $b$ ; для нашей кривой  $y^2 = 6(x^3 - x)$  достаточно заметить переменные  $v = 6x$ ,  $u = 6y$  — она примет вид  $u^2 = v^3 - 36v$ .

Рассмотрим две точки  $A, B$  кривой (3), найдем третью точку пересечения прямой  $AB$  с этой кривой. Обозначим через  $A \oplus B$  точку, симметричную ей относительно оси  $Ox$  (рис.12). Тогда для любых трех точек  $A, B$  и  $C$  кривой имеет место соотношение

$$(A \oplus B) \oplus C = A \oplus (B \oplus C).$$

Это свойство ассоциативности имеет интересную геометрическую интерпретацию. Если на плоскости проведены две тройки прямых так, что прямые из разных троек пересекаются в 9 точках, то кривая третьей степени, содержащая 8 из этих точек, должна содержать и девятую. Если добавить к кривой бесконечно удаленную точку  $Z$ , то множество всех ее точек с операцией  $\oplus$  образует коммутативную группу (свойство  $A \oplus B = B \oplus A$  очевидно). Точка  $Z$  играет в этой группе роль нуля; точкой  $\ominus A$ , противоположной точке  $A$ , считается точка, симметричная точке  $A$  относительно оси  $Ox$ . Условие принадлежности трех точек  $A, B, C$  одной прямой имеет вид  $A \oplus B = \ominus C$  или  $A \oplus B \oplus C = Z$ .

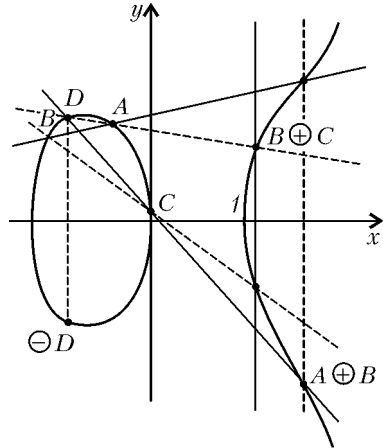
Рациональные точки на кривой (3) с целыми  $a, b$  также образуют группу относительно операции  $\oplus$ . Для нашей кривой  $y^2 = 6(x^3 - x)$  сложение точек задается формулами (1), (1'), (2), а именно

$$(x_1; y_1) \oplus (x_2; y_2) = (x_3; -y_3);$$

$$(x_1; y_1) \oplus (x_1; y_1) = 2(x_1; y_1) = (x_4; y_4).$$

Все указанные в ответе точки легко получить из трех точек:  $E(1; 0)$ ,  $F(-1; 0)$ ,  $G(2; 6)$ . При этом  $E \oplus F$  имеет координаты  $(0; 0)$ ,  $E \oplus G = (3; 12)$ ,  $F \oplus G = (-1/3; 4/3)$ ,  $E \oplus F \oplus G = (-1/2; -2/3)$ ,  $G \oplus G = 2G = (25/24; -35/48)$ ,  $2G \oplus F = (-1/49; 120/49)$ ,  $2G \oplus E = (49; 840)$  и т.д. (Заметим, что  $2E = 2F = 2(E \oplus F) = Z$ .)

Найти полностью группу рациональных точек для конкретной кривой (3) — очень трудная задача. Известно, что это — группа с



$$\ominus D = (A \oplus B) \oplus C = A \oplus (B \oplus C)$$

Рис. 12

конечным числом образующих (*теорема Морделла*), но непросто найти в конкретном случае даже количество ее образующих бесконечного порядка (т.е. количество независимых точек  $A$  кривой, для которых  $nA \neq Z$  ни при каком  $n$ ). (См. [122]).

Целые точки, как видно из нашего примера, могут появляться среди рациональных достаточно неожиданно. Однако, согласно *теореме Туэ*, на неособой кривой степени 3 (или больше) их всегда лишь конечное число.

Еще одна «теорема конечности» явилась недавней математической сенсацией: в 1983 г. появилось доказательство (молодого математика Фалтинга) **гипотезы Морделла**: на неособой кривой  $P(x, y) = 0$  рода больше 1 (кривая предполагается неособой и на бесконечности) может быть лишь конечное число рациональных точек (здесь  $P(x, y)$  – неприводимый многочлен с целыми коэффициентами).

Род кривой  $P(x, y)$  – сравнительно легко вычисляемая целочисленная характеристика, связанная со степенью  $n$  многочлена  $P(x, y)$ . К кривым рода 0 относятся окружности и другие кривые второго порядка, рода 1 – неособые кривые третьей степени. Что же касается неособых кривых  $P(x, y) = 0$  степени  $n \geq 4$ , то их род, как правило, не меньше двух, и поэтому они могут содержать лишь конечное число рациональных точек. В частности, это относится к кривой Ферма  $x^n + y^n = 1$  при  $n \geq 4$ . (Подробнее см. [125].)

### Задачи для самостоятельного решения

**2-23.** Имеются контейнеры двух видов: по 130 кг и по 160 кг. Нужно полностью загрузить ими грузовик грузоподъемностью 3 тонны. Можно ли это сделать?

**2-24.** По окружности радиуса 40 см катится колесо радиуса 18 см. В колесо вбит гвоздь, который, ударяясь об окружность, оставляет на ней отметки.

а) Сколько всего таких отметок оставит гвоздь на окружности?

б) Сколько раз прокатится колесо по всей окружности, прежде чем гвоздь попадет в уже отмеченную ранее точку?

**2-25.** На кольцевой дороге проводилась эстафета мотоциклистов. Старт и финиш находились в одном и том же месте. Длина кольцевой дороги 330 км, а длина каждого этапа – 75 км (движение по дороге – одностороннее). Сколько было пунктов, в которых передавалась эстафета, и каково расстояние между соседними пунктами?



**2-26.** Про некоторую фигуру на плоскости известно, что при повороте вокруг точки  $O$  на угол  $48^\circ$  она переходит в себя. Можно ли утверждать, что она переходит в себя при повороте вокруг точки  $O$  на угол: а)  $90^\circ$ ; б)  $72^\circ$ ?

**2-27.** Фигура на плоскости переходит в себя при повороте вокруг точки  $O$  на угол  $19^\circ$ . Докажите, что она переходит в себя при повороте на угол  $86^\circ$ .

**2-28.** Найдите наибольший общий делитель чисел:

а)  $2^{63} - 1$  и  $2^{91} - 1$ ; б)  $2^{19} + 1$  и  $2^{86} + 1$ .

**2-29.** От параллелограмма с острым углом  $60^\circ$  и сторонами  $a > b$  ( $a$  и  $b$  – целые числа) прямой, проходящей через вершину, отрезают равносторонний треугольник. С оставшейся трапецией проделывают ту же операцию – получается параллелограмм, из него – трапеция и так далее, пока не получится ромб, а) Какова будет сторона ромба, если  $a = 1986$ ,  $b = 1800$ ? б) Найдите какие-нибудь  $a$  и  $b$ , чтобы при таком разрезании параллелограмма получились треугольники восьми разных размеров.

**2-30.** Прямоугольник разбит на клетки  $1 \times 1$  см. Внутри каждой клетки написано число. Известно, что сумма всех чисел в каждой горизонтальной строчке равна 1, а в каждом вертикальном столбике равна 2. Может ли площадь прямоугольника равняться  $1986 \text{ см}^2$ ?

**2-31.** Верно ли, что:

а) из 100 целых чисел всегда можно выбрать два таких, что их сумма делится на 7;

б) из 5 целых чисел всегда можно выбрать два таких, разность квадратов которых делится на 7?

**2-32.** Пусть длины всех трех сторон прямоугольного треугольника – целые числа. Могут ли длины обоих катетов быть нечетными?

**2-33.** Найдите три таких простых числа, чтобы их сумма была в 5 раз меньше их произведения.

**2-34.** Найдите все такие простые числа  $p$ , что число

а)  $p^2 + 13$ ; б)  $p^2 + 14$

– простое.

**2-35.** Докажите, что следующие числа составные:

а)  $2^{3^{1987}} + 1$ ; б)  $2^{3^{1987}} - 1$ .

**2-36.** Найдите все пары целых чисел, удовлетворяющие уравнению:

а)  $x^2 = y^2 + 2y + 13$ ; б)  $x^2 - 3xy + 2y^2 = 3$ .

**2-37.** Докажите, что следующие уравнения не имеют решений в целых числах:

а)  $y^2 = 5x^2 + 6$ ; б)  $2^x - 1 = y^2$  ( $x > 1$ ).

**2-38.** Докажите, что если сумма нескольких целых чисел делится на 6, то и сумма их кубов делится на 6.

**2-39.** Докажите, что при любых целых  $n$  и  $m$  число  $m^5n - mn^5$  делится на 30.

**2-40.** Докажите, что если число  $a - 1$  делится на  $k^m$ , то число  $a^k - 1$  делится на  $k^{m+1}$  ( $a, k, m$  – натуральные числа).

**2-41.** Найдите три последние цифры суммы

$$1^{100} + 2^{100} + 3^{100} + 4^{100} + \dots + 999998^{100} + 999999^{100}.$$

**2-42.** Найдите какие-нибудь четыре последовательных натуральных числа, каждое из которых делится на квадрат целого числа, большего единицы.

**2-43.** Напишите шесть чисел 1, 2, 3, 4, 5, 6 по окружности в таком порядке, чтобы для любых трех чисел  $a, b, c$ , стоящих подряд, число  $b^2 - ac$  делилось на 7.

**2-44.** Укажите такое  $n$ , при котором число  $n^4 + (1+n)^4$  – составное.

**2-45.** Докажите, что при всех натуральных  $n > 1$  число

а)  $n^4 + 4$ ; б)  $n^5 + n^4 + 1$

– составное.

**2-46.** Разложите многочлен  $x^9 + x^4 - x - 1$  на 5 множителей с целыми коэффициентами.

**2-47.** Докажите, что многочлен  $(x+1)^{2n} - x^{2n} - 2x - 1$  делится на многочлен  $x(x+1)(2x+1)$ .

**2-48.** При каких значениях  $a$  и  $b$  многочлен  $x^n - ax^{n-1} + bx - 1$  делится на  $(x-1)^2$ ?

**2-49.** Известно, что многочлен  $f(x)$  при делении на  $x-1$  дает остаток 3, а при делении на  $x-2$  – остаток 5. Какой остаток дает этот многочлен при делении на  $(x-1)(x-2)$ ?

**2-50.** Докажите, что если у многочлена  $f(x)$  с целыми коэффициентами значения  $f(0)$  и  $f(1)$  нечетны, то у него нет целых корней.

**2-51.** Докажите, что если  $f(x)$  – многочлен с целыми коэффициентами и  $|f(3)| = |f(7)| = 1$ , то этот многочлен не имеет целых корней.

**2-52.** Пусть  $f(x)$  – многочлен седьмой степени с целыми коэффициентами. Докажите, что если его значения при пяти различных целых значениях  $x$  по модулю равны 1, то многочлен

нельзя разложить в произведение двух многочленов ненулевой степени с целыми коэффициентами.

**2-53.** Существует ли такое натуральное  $n$ , что число  $3^n + 1$  делится на:

а)  $5^{1000}$ ; б)  $10^{1000}$  ?

**2-54.** Имеется много карточек, на каждой из которых написано одно из чисел 2, 3, 5, 7. Можно ли выложить в ряд

а) 15; б) 16

карточек так, чтобы ни одно из произведений нескольких подряд идущих чисел не было полным квадратом?

в) Какое наибольшее количество карточек, на которых написано одно из первых  $n$  простых чисел, можно выложить в ряд так, чтобы выполнялось это условие?

**2-55.** Во всех целочисленных точках  $(x; y)$  координатной плоскости  $Oxy$  растут деревья. Какой наибольшей ширины дорогу можно провести в этом лесу, не задевая деревьев, если ее края должны быть прямыми, параллельными прямой

а)  $3y = 5x$ ; б)  $ax = by$ ,

где  $a$  и  $b$  – заданные натуральные числа? (Толщиной стволов пренебрегаем.)

**2-56.** а) Найдите четыре тройки  $(x; y; z)$  взаимно простых чисел, удовлетворяющие уравнению  $x^2 + 2y^2 = z^2$ .

б) Докажите, что существует бесконечно много таких троек.

**2-57.** Натуральное число  $n \geq 7$  обладает тем свойством, что все натуральные числа, меньшие  $n$  и взаимно простые с ним, образуют арифметическую прогрессию. Докажите, что число  $n$  – или степень двойки, или простое.

**2-58.** а) Найдите двузначное число, если известно, что две последние цифры его квадрата совпадают с этим числом.

б) Докажите, что для всякого  $n$  существует  $n$ -значное число, совпадающее с последними  $n$  цифрами своего квадрата ( $n$ -значное число может начинаться с нуля).

**2-59.** а) Найдите десять троек  $(x; y; z)$  натуральных чисел, удовлетворяющих уравнению  $x^2 + y^2 + z^2 = 3xyz$ .

б) Докажите, что существует бесконечно много таких троек.

**2-60.** Докажите, что число  $(\sqrt{3} - \sqrt{2})^{1987}$  можно представить в виде  $a\sqrt{3} - b\sqrt{2}$ , где  $a$  и  $b$  – такие целые числа, что  $3a^2 - 2b^2 = 1$ .

**2-61.** Рассмотрим множество  $M$  натуральных чисел, представимых в виде  $x^2 + xy + y^2$ , где  $x$  и  $y$  – некоторые целые числа.

а) Докажите, что произведение двух чисел из  $M$  также принадлежит  $M$ .

б) Назовем *базисным* число из  $M$ , большее 1, которое не делится ни на одно из чисел множества  $M$ , кроме себя. Существует ли число из  $M$ , которое можно двумя разными способами представить в виде произведения базисных?

**2-62.** Найдите пять троек натуральных чисел  $(x; y; z)$ , удовлетворяющих уравнению  $x!y! = z!$  ( $n! = 1 \cdot 2 \cdot \dots \cdot n$  – произведение всех натуральных чисел от 1 до  $n$ ).