Решения задач по курсу «Дискретные структуры»

Константин Леладзе

2 мая 2019 г.

Задача 99. Решите сравнение $52x \equiv 48 \pmod{404}$. Решение необходимо записать по модулю 404. Для решения задачи нахождения обратного по умножению элемента продемонстрируйте применение алгоритма Евклида. Перебор/угадывание не допускаются.

Решение. Для начала, запишем общий вид уравнения: $ax \equiv b \pmod{m}$. В нашем случае: $a = 52,\ b = 48,\ m = 404$. Найдем $d = \gcd(a, m)$:

$$\begin{aligned} 404/52 &= 7, \text{ остаток } 40; \\ 52/40 &= 1, \text{ остаток } 12; \\ 40/12 &= 3, \text{ остаток } 4; \\ 12/4 &= 3, \text{ остаток } 0; \\ d &= \gcd(52, 404) = 4. \end{aligned}$$

Исходное уравнение упрощается до $ax/d \equiv b/d \pmod{m}/d$, если $d \mid b$. В нашем случае $48/4 = 12$. Получаем: $13x \equiv 12 \pmod{101}$.

$$\begin{aligned} 101 &= 7 \cdot 13 + 10; \\ 13 &= 1 \cdot 10 + 3; \\ 10 &= 3 \cdot 3 + 1; \\ 3 &= 3 \cdot 1 + 0; \\ 1 &= 1 \cdot 1 + 0. \end{aligned}$$

Используя обратный проход (аналог РАЕ):

$$\begin{gathered} 1 = 10 - 3 \cdot \underline{3} = \\ 1 \cdot \underline{10} - 3 \cdot (13 - 1 \cdot \underline{10}) = -3 \cdot 13 + 4 \cdot \underline{10} = \\ -3 \cdot \underline{13} + 4 \cdot (101 - 7 \cdot \underline{13}) = 4 \cdot 101 + -31 \cdot \underline{13} \equiv \\ 70 \cdot \underline{13} \pmod{101}. \end{gathered}$$

Значит, обратный по модулю 101 к 13 элемент - 70.

Имеем $x_0 = 12 * 13^{-1} = 12 * 70 \equiv 32 \pmod{101}$

С учетом того, что исходное уравнение нужно решить по модулю 404:

$x \equiv x_0 + 101 \cdot k \pmod{404},\ k \in 0, 1, \ldots, d - 1.$

$x \equiv 32, 133, 234, 335 \pmod{404}$.

Задача 102. Решите сравнение $71x \equiv 12 \pmod{269}$. Для решения задачи нахождения обратного по умножению элемента продемонстрируйте применение алгоритма Евклида. Перебор/угадывание не допускаются.

Решение. Для начала, запишем общий вид уравнения: $ax \equiv b \pmod{m}$. В нашем случае: $a = 71,\ b = 12,\ m = 269$. Найдем $d = \gcd(a, m)$:

$$\begin{aligned} 269 &= 3 \cdot 71 + 56; \\ 71 &= 1 \cdot 56 + 15; \\ 56 &= 3 \cdot 15 + 11; \\ 15 &= 1 \cdot 11 + 4; \\ 11 &= 2 \cdot 4 + 3; \\ 4 &= 1 \cdot 3 + 1; \\ 3 &= 3 \cdot 1 + 0; \\ 1 &= 1 \cdot 1 + 0; \\ d &= \gcd(71, 269) = 1. \end{aligned}$$

Используя обратный проход (аналог PAE):

$$\begin{gathered}1 = 4 - 1 \cdot \underline{3} = \\ 1 \cdot \underline{4} - 1 \cdot (11 - 2 \cdot \underline{4}) = -11 + 3 \cdot \underline{4} = \\ -1 \cdot \underline{11} + 3 \cdot (15 - 1 \cdot \underline{11}) = 3 \cdot 15 - 4 \cdot \underline{11} = \\ 3 \cdot \underline{15} - 4 \cdot (56 - 3 \cdot \underline{15}) = -4 \cdot 56 + 15 \cdot \underline{15} = \\ -4 \cdot \underline{56} + 15 \cdot (71 - 1 \cdot \underline{56}) = 15 \cdot 71 - 19 \cdot \underline{56} = \\ 15 \cdot \underline{71} - 19 \cdot (269 - 3 \cdot \underline{71}) = -19 \cdot 269 + 72 \cdot \underline{71} \equiv \\ 72 \cdot \underline{71} \pmod{269}.\end{gathered}$$

Значит, обратный по модулю 269 к 71 элемент - 72.
Имеем $x_0 = 12 * 71^{-1} = 12 * 72 \equiv 57 \pmod{269}$
Ответ: $x = 57 + 269k$, где $k \in \mathbb{N}$.

Задача 104. Существует ли k, такое, что 13^k оканчивается на $\ldots 0000169$?

Решение. Да: $k = 500002$. Это можно понять, решив сравнение $13^k \equiv 169 \mod 10^7$. Такое сравнение решается с помощью дискретного логарифмирования, и ответ точно существует, так как $gcd(13, 10) = 1$.

Задача 155. Пусть f, g, h – неубывающие функции из $\mathbb{R}^+$ в $\mathbb{R}^+$. Пусть $n \to \infty$. Верно ли, что если $f(n) = O(g(n))$ и $g(n) = o(h(n))$, то обязательно $f(n) = o(h(n))$? Если верно, то обоснуйте, опираясь исключительно на определения. Если не верно в общем случае, то приведите соответствующий контрпример.

Решение. Вспомним определения o-малого и O-большого:

Пусть $f(x)$ и $g(x)$ — две функции, определенные в $U_\varepsilon(x_0)$ и $\lim_{x \to x_0} g(x) \neq 0$. Тогда говорят, что:
$f = O(g)$, при $x \to x_0$, если $\exists C > 0 : \forall x \in U_\varepsilon(x_0) \Rightarrow |f(x)| \leq C|g(x)|$.
$f = o(g)$, при $x \to x_0$, если $\forall c > 0$, $\exists \delta > 0 : \forall x \in U_\delta(x_0) \Rightarrow |f(x)| < c|g(x)|$.

Теперь, с учетом того, что f, g, h – неубывающие функции и $x_0 = +\infty$:
(1) $\exists C > 0$ и $\exists x_1 \neq +\infty : \forall x > x_1 \Rightarrow |f(x)| \leq C|g(x)|$.
(2) $\forall c > 0 \exists x_2 \neq +\infty : \forall x > x_2 \Rightarrow |g(x)| < c|h(x)|$.
Возьмем в (2) $c = C$. Пусть также $x_3(c) = \max(x_1, x_2(c))$. Тогда выполнено: $\forall x > x_3 : |f(x)| \leq C|g(x)| < C^2|h(x)|$.
Значит $\forall c > 0 \exists x_3(c) \neq +\infty : \forall x > x_3 \Rightarrow |f(x)| < C'|h(x)|$ (тут $C' = C^2$).
Отсюда $f(n) = o(h(n))$.

Задача 202. В чемпионате хоккейной лиги расписание регулярного чемпионата составляется по следующему правилу: не обязательно каждый клуб играет со всеми другими, но среди любых трёх клубов хотя бы два из них должны сыграть матч между собой и никакая пара клубов не играет друг с другом больше одного раза. Всего в лиге играют 26 клубов. Верно ли, что, как бы ни было составлено расписание, найдётся семь клубов, каждые два из которых играли матч друг с другом?

Решение. Рассмотрим неориентированный граф, с вершинами, в которых находятся клубы, и ребрами, которые существуют между двумя вершинами, если клубы, соответствующие этим вершинам, играли.

Среди любых трех клубов найдутся два, которые играли друг с другом, значит в графе не будет независимых множеств на трех и более вершинах.

1. Оценим $R(7, 3)$, используя свойства чисел Рамсея:

$$R(7, 3) \leq R(7, 2) + R(6, 3) = 7 + R(6, 3).$$

2. Оценим $R(6,3)$, используя свойства чисел Рамсея:

$$R(6,3) \leq R(6,2) + R(5,3) - 1 = 6 + R(5,3) - 1 = 5 + R(5,3).$$

Тут также предположили, что $R(5,3)$ — четное. Докажем это далее.

3. Оценим $R(5,3)$, используя свойства чисел Рамсея:

$$R(5,3) \leq R(5,2) + R(4,3) = 5 + R(4,3);$$
$$R(5,3) \leq 5 + R(4,2) + R(3,3) - 1 = 5 + 4 + 6 - 1 = 14;$$
$$R(5,3) \leq 14.$$

4. Приведем пример, который покажет, что $14 \leq R(5,3)$. Для этого, построим два графа на 13 вершинах: без независимых множеств размера 5 и без клик размера 3 соответственно.

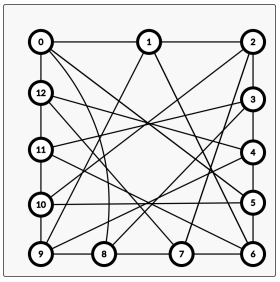

Рис. 1: граф без независимых множеств из пяти вершин.

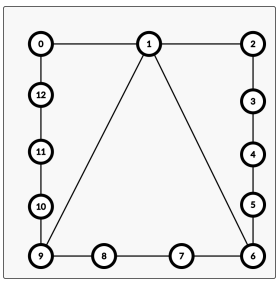

Рис. 2: граф без клик из трех вершин

5. Получается, что

$$R(5,3) = 14;$$
$$R(6,3) \leq 19;$$
$$R(7,3) \leq 26.$$

Значит, в графе на 26 вершинах найдется либо независимое множество размера 3, либо клика размера 7. По условию, независимых множеств размера 3 в графе нет. Значит, среди каких-то семи команд каждые две играли между собой.

Задача 222. Для многочлена $x^4 + x^3 + x^2 + 1$ над полем $\mathbb{Z}_3$ определите, является ли он неприводимым.

Решение. Многочлен четвертой степени неприводим, если он не имеет корней и не делится на многочлен второй степени.

1. Очевидно, корней у данного многочлена нет. Все возможные числа поля 0, -1 и 1 не являются корнями.

2. Предположим, что данный многочлен делится на какой-то многочлен второй степени: $x^4+x^3+x^2+1 = (ax^2+bx+c)\cdot(dx^2+ex+f)$. Выразим коэффициенты:

$$\begin{cases} ad = 1; \\ ae + bd = 1; \\ af + be + cd = 1; \\ bf + ce = 0; \\ cf = 1. \end{cases}$$

Докажем, что данная система не имеет решений для натуральных чисел a, b, c, d, e, f.

Из первого уравнения: $a = \frac{1}{d}$. Подставим в систему:

$$\begin{cases} \frac{e}{d} + bd = 1; \\ \frac{f}{d} + be + cd = 1; \\ bf + ce = 0; \\ cf = 1. \end{cases}$$

Из четвертого уравнения: $c = \frac{1}{f}$. Из третьего: $b = -\frac{ce}{f} = -\frac{e}{f^2}$ Подставим в систему:

$$\begin{cases} \frac{e}{d} - \frac{e}{f^2} = 1; \\ \frac{f}{d} - \frac{e}{f^2} + \frac{d}{f} = 1. \end{cases}$$

Из певрого уравнения: $e = \frac{f^2 d}{f^2 - d}$. Подставим в систему:

$$\frac{f}{d} - \frac{f^4 d^2}{(d^2-d)^2} + \frac{d}{f} = 1.$$

Упростим:

$$(f^2 - df + d^2)(f^2 - d)^2 = f^5 d^3.$$

Это уравнение не имеет решений в натуральных числах.

Значит исходный многочлен неприводим.

Задача 238. На курсе 100 студентов. Известно, что среди них можно выделить 149 различных пар студентов, которые во время семестра давали друг другу списывать на контрольных. Деканат принял решение отчислить после сессии минимально возможное число студентов, но таким образом, чтобы среди оставшихся студентов не осталось ни одной пары списывающих друг у друга. Докажите, что к следующему семестру на курсе останется не менее 26 студентов.

Решение. Возьмем граф G на 100 вершинах (соответствуют студентам). Ребро $e = u, v$ в этом графе будет тогда и только тогда, когда u и v студенты списывали друг у друга. В таком графе 149 ребер (по условию). Рассмотрим граф G', обратный к G. Очевидно: $|E'| = \frac{100\cdot(100-1)}{2} - 149 = 4801$.

Предположим, что к следующему семестру на курсе останется менее 26 студентов. Значит, в графе G нет независимого множества на 26 вершинах. Значит, в графе G' нет клики на 26 вершинах. По теореме Турана: $|E'| \leq \binom{26-1}{2}\cdot 4\cdot 4 = \frac{25\cdot 24\cdot 16}{2} = 4800$ (граф, на котором достигается такая оценка - 25-дольный 4-регулярный на 100 вершинах). Имеем $|E'| < 4801$. Противоречие с условием ($|E'| = 4801$)!

Задача 318. Сколько перестановок на множестве $\{1, 2, \ldots, n\}$ представимы в виде композиции чётного количества транспозиций?

Решение. Итак, всего на n элементах существует $n!$ перестановок. Докажем, что количество четных перестановок равно количеству нечетных. Рассмотрим четную перестановку π. Заметим, что перестановка $\psi = (1,2)\circ\pi$ – нечетна. При этом, для перестановки $\theta = (1,2)\circ\psi$ будет выполнено $\theta = \pi$, так как композиция – ассоциативная операция и дважды примененная перестановка не меняет исходной. Значит, функция $f(\pi) = (1,2)\circ\pi$ – биекция из множества четных перестановок в множество нечетных. Отсюда, получим, что число четных перестановок равно числу нечетных, значит всего четных перестановок на множестве $\{1, 2, \ldots, n\}$ равно $n!/2$.

Задача 322. Пусть n — произвольное натуральное число. Пусть $S_1, \ldots, S_{n^{2017}}$ — произвольные n-элементные множества. Докажите, что при всех достаточно больших значениях n можно покрасить элементы в красный и синий цвета, так, чтобы в каждом из множеств S_i нашёлся хотя бы один красный и хотя бы один синий элемент.

Решение. Рассмотрим случайную раскраску. Каждый элемент сделаем красным с вероятностью $1/2$ и синим с вероятностью $1/2$. Событие H_i соответствует наличию в S_i двух цветов. Наше условие: $H_1 \cap H_2 \cap \cdots \cap H_{n^{2017}}$.

$$P(H_1 \cap H_2 \cap \cdots \cap H_{n^{2017}}) = 1 - P(\overline{H_1 \cap H_2 \cap \cdots \cap S_{n^{2017}}}) =$$

$$1 - P(\overline{H_1} \cup \overline{H_2} \cup \cdots \cup \overline{H_{n^{2017}}}) \geq 1 - \sum_{i=1}^{n^{2017}} P(\overline{H_i}).$$

$\overline{H_i}$ соответствует одноцветности множества S_i.

$$P(\overline{H_i}) = 2 \cdot (1/2)^n = 2^{(1-n)}.$$

Получим $P(H_1 \cap H_2 \cap \cdots \cap H_{n^{2017}}) \geq 1 - \sum\limits_{i=1}^{n^{2017}} 2^{1-n}$. При достаточно больших n выражение положительно, значит требуемая раскраска возможна.

Задача 335. Сформулируйте теорему Эрдёша—Ко—Радо.

Решение. При данных натуральных k и n, т.ч. $k \leq \frac{n}{2}$, число ребер в 1-пересекающемся k-однородном гиперграфе на n вершинах не превосходит $\binom{n-1}{k-1}$.

Задача 326. Пусть Докажите экспоненциальную нижнюю асимптотическую оценку чисел Рамсея вида $R(s,s) > c^s$ для любой удобной Вам константы $c > 1$.

Решение. Из известного факта: $R(n,m) > R(n-1,m) + R(n,m-1)$, следует: $R(n,m) \geq (n+m)!/(n!m!)$. Это утверждение тривиально проверяется по индукции. Воспользуемся формулой Стирлинга: $R(s,s) \geq (2s)!/((s)!)^2 \geq \frac{\sqrt{2\pi\cdot 2s}\cdot(2s/e)^{2s}}{(\sqrt{2s\pi}\cdot(s/e)^s)^2} \geq \frac{1}{\pi\sqrt{s}} \cdot 4^s > 2^s$. Что и требовалось.

Задача 327. Вычислите в $\mathbb{Z}_7$ значение выражения

$$\left(2017^{-1} + 2018^{-1}\right)^{2018} \cdot 2018.$$

Ответ должен принадлежать множеству $\{0, 1, 2, 3, 4, 5, 6\}$.

Решение.

Найдем обратный элемент к 2017 в $\mathbb{Z}_7$:

$$2017 = 288 \cdot 7 + 1; 1 = 2017 - 288 \cdot 7; 2017^{-1} \equiv 1 \pmod 7.$$

Найдем обратный элемент к 2018 в $\mathbb{Z}_7$:

$$2018 = 288 \cdot 7 + 2$$
$$1 = 7 - 2 \cdot 3 \equiv 7 + (2016 - 2018) \cdot 3$$
$$2018^{-1} \equiv 4 \pmod 7$$

Теперь:

$$(1+4)^{2018} = 5^{2 \cdot 1009} = 25^{1009} \equiv 4^{16 \cdot 63 + 1} \equiv 4 \cdot (4^{16})^{63} \equiv$$
$$4 \cdot 4^{63} = 4 \cdot 4^{31 \cdot 2 + 1} \equiv 2 \cdot 2^{31} =$$
$$2^{32} = 4^{16} \equiv 2^8 = 4^4 = 16^2 \equiv 2^2 \equiv 4 \pmod 7$$

Наконец: $4 \cdot 2018 = 8072 \equiv 1 \pmod 7$.

Задача 332. Зачеркнув лишнее, укажите верную идею доказательства теоремы Фишера: «Для доказательства того, что объектов в некоторой совокупности «немного»/«достаточно много», строим биекцию/инъекцию/сюръекцию множества этих объектов в линейное пространство, так, чтобы векторы, сопоставленные объектам, оказывались линейно зависимыми/независимыми.»

Решение. Для доказательства того, что объектов в некоторой совокупности «немного»/ ~~«достаточно много»~~, строим ~~биекцию~~/инъекцию/~~сюръекцию~~ множества этих объектов в линейное пространство, так, чтобы векторы, сопоставленные объектам, оказывались линейно ~~зависимыми~~/независимыми.

Задача 335. Сформулируйте теорему Эрдёша—Ко—Радо.

Решение. При данных натуральных k и n, т.ч. $k \leq \frac{n}{2}$, число ребер в 1-пересекающемся k-однородном гиперграфе на n вершинах не превосходит $\binom{n-1}{k-1}$.

Задача 336. Подмножества $X_1, \ldots, X_n$ и $Y_1, \ldots, Y_n$ некоторого N-элементного множества таковы, что X_i пересекается с Y_j по пяти элементам при $i = j$ и по четырём элементам иначе. Докажите, что $n \leq N$.

Решение. Обзовем данное нам N-элементное множество множеством A с элементами a_i. Рассмотрим две матрицы размера $n \cdot n$:

$$M_1 : M_{1i,j} = I(a_j \in X_i);$$
$$M_2 : M_{2i,j} = I(a_j \in Y_i).$$

Эти матрицы являются матрицами смежности двудольных графов G_1 и G_2 с долями размера n. В левой доли G_1 и G_2 - элементы a_j, а в правой - множества X_i и Y_i соответственно.

Тогда, как известно, при перемножении матриц смежности двудольного графа – получим матрицу $M = M_1 \cdot M_2$, т.ч. $M_{i,j} = \{$кол-во общих элементов X_i и Y_j $\}$. По условию: $M_{i,j} = 4 + I(i = j)$. Данная квадратная матрица, очевидно, имеет ранг равный ее размеру n.

С другой стороны: $n = rk(M) = rk(M_1 \cdot M_2) \leq \min(rk(M_1), rk(M_2))$. В свою очередь, очевидно, что $rk(M_1) \leq \min(n, N)$ и $rk(M_2) \leq \min(n, N)$.

Таким образом, получим $n \leq N$.

Задача 337.

1. Какое наибольшее количество рёбер, согласно теореме Турана, может быть в графе на 2018 вершинах, не содержащем четырёхвершинных клик? Можно дать ответ в виде формулы.

2. Найдите точное значение числа Заранкевича $Z_{1,b}(m, bm)$ для произвольных натуральных b и m.

3. Что можно сказать про почти все двудольные графы с равномощными долями: доля таких графов, не содержащих $K_{2,2}$, константная // почти все такие двудольные графы не содержат $K_{2,2}$ в качестве подграфа // почти все такие двудольные графы содержат $K_{2,2}$ в качестве подграфа.

Решение.

1. Будем действовать по теореме Турана. Разделим граф на три части, внутри которых не будет ребер: по $672, 673, 673$ вершин соответственно. Посчитаем наибольшее возможное кол-во ребер в таком графе: $672 \cdot 673 \cdot 2 + 673 \cdot 673 = 1357441$.
2. $m \cdot (b-1)$.
3. Правильный ответ: почти все такие двудольные графы содержат$K_{2,2}$ в качестве подграфа. Это следует из нижней оценки числа Заранкевича.

Задача 344. Перечислите все попарно неизоморфные связные простые графы на шести вершинах, в которых ровно три блока.

Решение. Разобьем графы на группы, для простоты и алгоритмичности перебора:

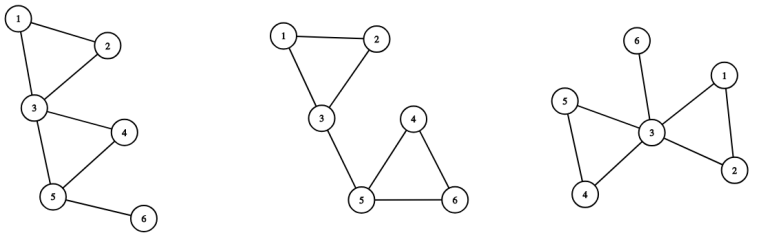

Рис. 3: Два треугольника и ребро.

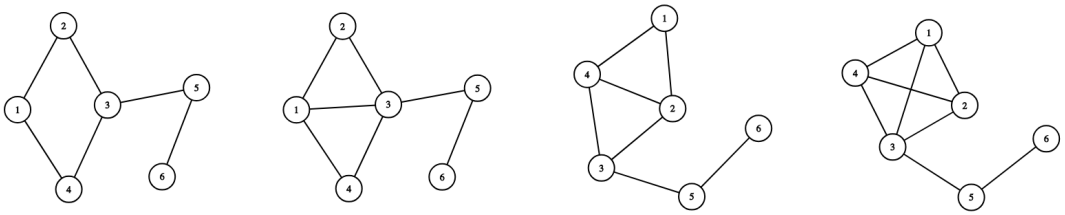

Рис. 4: Квадрат и два последовательных ребра.

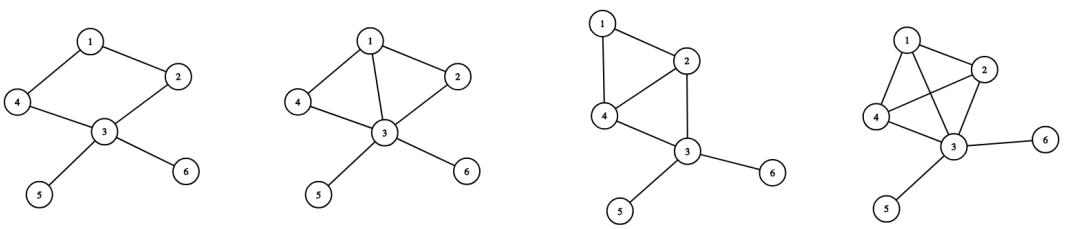

Рис. 5: Квадрат и два инцидентных ребра.

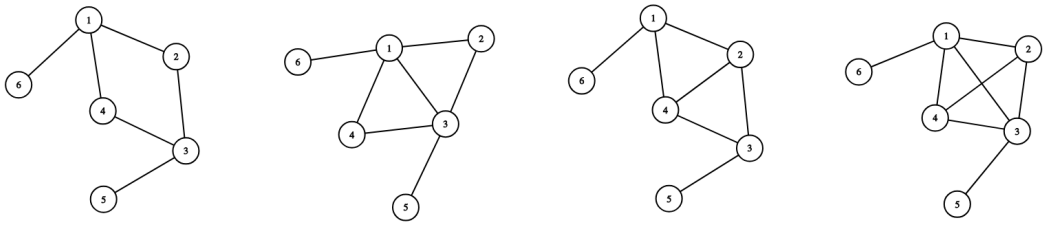

Рис. 6: Квадрат и два диаметрально противоположных ребра.

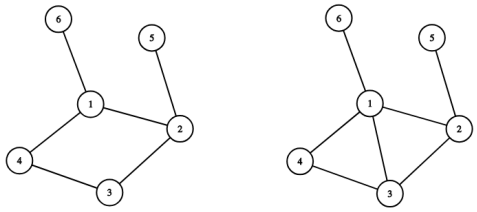

Рис. 7: Квадрат и два ребра.

Таким образом, искомых графов всего семнадцать.