XXV
Межрегиональная олимпиада школьников по математике и криптографии

Москва 2016

Всего пронумеровано 32 стр.
Подписано к печати 12.02.16
Авт. л.1,5 Усл. печ. л.2,2
Заказ № 236/14 г.
Тираж 350 экз.

Информация о проведении олимпиады

XXV Межрегиональная олимпиада школьников по математике и криптографии проводилась в два тура. Первый тур проводился в дистанционной форме на интернет-сайте www.cryptolymp.ru.

Второй тур проводился в очной форме на базе Академии ФСБ России и во многих городах и ВУЗах России: Москва – ИКСИ, Барнаул – АлтГТУ, Белгород – БГТУ, Владивосток – ДВФУ, Владимир – ВлГУ, Волгоград – ВолГУ, Екатеринбург – УрФУ, Ижевск – УдГУ, Иркутск – ИГУ, Йошкар-Ола – ПГТУ, Казань – КНИТУКАИ, Калининград – БФУ, Кострома – КГТУ, Краснодар – КубГТУ, Красноярск – СибГАУ, СФУ, Курск – ЮЗГУ, Нефтекамск – НФБашГУ, Нижний Новгород – ННГУ, Новосибирск – НГУЭУ, Озерск – ОТИ НИЯУ МИФИ, Омск – ОмГУ, Орел – Академия ФСО России, Оренбург – ОГУ, Пенза – ПГУ, Пермь – ПНИПУ, Пятигорск – ПГЛУ, Ростов-на-Дону – ДГТУ, Рязань – РГРТУ, Самара – СамГУ, Саратов – СГТУ, Санкт-Петербург – ГУАП, Санкт-Петербург – СПбПУ, Севастополь – СевГУ, Ставрополь – СКФУ, Сыктывкар – СГУ, Таганрог – ЮФУ, Тамбов – ТГТУ, Томск – ТГУ, ТУСУР, Тюмень – ТюмГУ, Хабаровск – ДВГУПС, Челябинск – ЧелГУ, Череповец – ЧГУ, Ярославль – ЯрГУ.

Межрегиональная олимпиада школьников по математике и криптографии включена в Перечень олимпиад школьников на 2015/2016 учебный год (2 уровень), что дает право предоставлять льготы победителям и призерам при поступлении в государственные и муниципальные учреждения высшего образования (Приказ Минобрнауки России от 04.04.2014 № 267). Решения о льготах принимаются вузами самостоятельно и должны быть объявлены к 1 июня 2016 года.

Приветствие председателя оргкомитета олимпиады Владимира Николаевича Сачкова участникам XXV Межрегиональной олимпиады школьников по математике и криптографии

Дорогие друзья!

Приветствую участников юбилейной 25 Межрегиональной Олимпиады школьников по математике и криптографии. Криптография (в переводе с греческого языка – тайнопись) – это область научных, прикладных, инженерно-технических исследований и практической деятельности, которая связана с обеспечением информационной безопасности, а также преодолением криптографических средств защиты информации. Изучение достижений современной криптографии невозможно без знания исторических закономерностей развития этой науки. Знание истории криптографии позволяет понять истоки и закономерности развития ее фундаментальных идей, представить в полной мере картину постоянного соперничества разработчиков шифров и дешифровальщиков. Успехи и неудачи криптографов нередко оказывали серьезное влияние на ход войн, революций, внешнюю и внутреннюю политику, проводимую различными государствами.

Криптография ровесница письменности. Эта наука прошла путь от папируса до компьютера и по возрасту старше Египетских пирамид. Она в своем развитии прошла через этапы: «криптография как искусство» и «криптография как ремесло» к этапу «криптография как

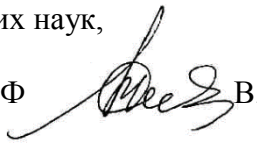
наука». При этом криптография всегда развивались в тесном взаимодействии с математикой. Математический аппарат был и остаётся основным в криптографии. Поэтому не случайно в многовековую историю криптографии вписано много имен видных математиков.

В 2015 году исполнилось 70 лет Великой Победе. Наши криптографы внесли большой вклад в достижение разгрома врага во время Великой Отечественной. В ходе войны советские дешифровальные службы предоставили политическому и военному руководству СССР большое количество важнейшей информации. Эта информация поступала во время всех важнейших сражений и способствовала нашим победам. В частности, коллектив специалистов-криптографов во главе с С.С. Толстым и Б.А. Аронским накануне битвы за Москву предоставил советскому руководству информацию, что Япония нападёт не на СССР, а на США, что позволило перебросить резервы с Дальнего Востока под Москву в самый нужный момент. В то же время шифровальная служба не позволила противнику получить сведения о наших замыслах и действиях.

25 лет в нашей стране проводятся Олимпиады по криптографии и математике. Ваше участие в этих Олимпиадах откроет Вам путь к овладению навыками работы с информацией и методами ее защиты. Это направление человеческой деятельности на данный момент является очень перспективным, как в бизнесе, но самое главное, в обеспечении безопасности нашего государства.

Юные талантливые участники и победители Олимпиад – это источник надежды на то, что пройдет некоторое время, и в ряды отечественных криптографов и математиков вольются свежие силы, которые скажут новое слово в этих важных для нашей страны областях науки и техники. Мы надеемся, что они окажутся достойными продолжателями дела многих поколений отечественных криптографов, которые во время войн и мирных дней героически решали и продолжают самоотверженно решать задачи обеспечения информационной безопасности Родины.

Желаю участникам Олимпиады удачи и творческих успехов!

Вице-президент Академии криптографии РФ,
доктор физико-математических наук,
профессор,
заслуженный деятель науки РФ  В.Н. Сачков

УСЛОВИЯ И РЕШЕНИЯ ЗАДАЧ

Задача 1 (8-9, 10 классы)

На кодовом замке имеется круглый диск с нанесенными на равноотстоящих интервалах по его периметру числами от 1 до 12. Изначально диск установлен как на Рис. 1. Замок откроется, если диск окажется повернутым на 30^0 относительно своего первоначального положения (Рис. 2). Для изменения положения диска имеется специальный стержень, который можно продеть через два любых диаметрально противоположных числа (например, через 1 и 7 как на Рис. 3), а затем повернуть диск вокруг стержня на 180^0 (в результате диск окажется в положении, изображенном на Рис. 4). Можно ли такими поворотами открыть замок и если да, то каким образом?

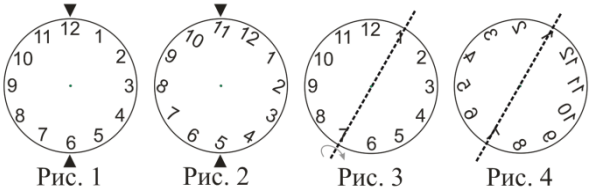


Рис. 1 Рис. 2 Рис. 3 Рис. 4

Решение

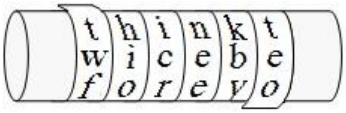
При повороте диска на месте четных чисел вновь оказываются четные, а на месте нечетных – нечетные. Поэтому открыть замок нельзя.

Ответ: Нет.

Комментарий

В представленном решении возможны и более строгие рассуждения. Поворот диска вокруг стержня на 180^0 – это осевая симметрия диска относительно прямой, содержащей стержень. Будем эти осевые симметрии обозначать буквой S. В задаче требуется найти симметрии, композиция которых будут давать поворот на 30^0. Композиция двух осевых симметрий S_1 и S_2 относительно прямых, угол между которыми α, – задают поворот на угол 2α. Обозначая поворот буквой R, можем, таким образом, записать $S_2 \circ S_1 = R_{2\alpha}$. Композицией симметрии и поворота будет вновь симметрия ($S \circ R = S$), а двух поворотов, очевидно, снова поворот ($R \circ R = R$). Видим также, что симметрия меняет начертание цифр на "зеркальное" (см. переход от Рис. 3 к Рис. 4). Значит, чтобы диск оказался в положении, изображенном на Рис. 2, симметрий должно быть четное число. Но каждая пара симметрий – это поворот, а композиция поворотов – это опять же поворот. Следовательно, композиция четного числа симметрий – поворот, причем на угол, кратный 60^0 (т.к. минимальный угол между прямыми – 30^0). Поэтому повернуть диск на 30^0 не получится.

Задача 2 (8-9, 10 классы)



Для шифрования сообщений Катя и Антон использовали шифр Сцитала: на круглую палочку виток к витку без просветов и нахлёстов наматывалась лента. При горизонтальном положении палочки на ленту по всей длине стержня построчно записывался текст сообщения без знаков препинания и пробелов. После этого лента с записанным на ней текстом посылалась адресату. Антон передал Кате ленту, на которой было написано вот что:

К сожалению, Катя свою палочку потеряла, но она видит, что лента исписана полностью, и знает, что при намотке ленты было сделано целое число оборотов. Помогите ей восстановить сообщение.

Решение

“Лента исписана полностью, а при ее намотке было сделано целое число оборотов” - это означает, что текст был, по сути, вписан в ячейки прямоугольной таблицы. Причем таблица оказалась заполненной полностью. В тексте 81 буква. Значит, стоит попробовать вписать зашифрованный текст (по столбцам сверху вниз) в

з	о	в	у	т	е	б	я	н
е	д	л	я	т	о	г	о	ч
т	о	б	у	к	о	р	я	т
ь	л	ю	д	е	й	ч	ь	я
з	л	о	б	а	у	б	и	л
а	д	р	у	г	а	м	о	е
г	о	и	л	ь	ч	т	о	б
и	з	в	е	д	а	т	ь	т
а	й	н	ы	г	р	о	б	а

таблицы размером 3×27, 27×3 и 9×9. Осмысленный текст (при чтении по строкам) получается в последнем случае.

Ответ: Зову тебя не для того, чтоб укорять людей, чья злоба убила друга моего, иль чтоб изведать тайны гроба.

Комментарий

Подобное устройство для ведения секретной переписки использовали еще древние греки в V в. до н.э. во время войны Спарты против Афин. После того как исписанную ленту сматывали с цилиндра, буквы исходного текста оказывались на ней переставленными весьма сложным образом, и прочитать текст становилось затруднительно. Именно поэтому данный шифр (шифр Сцитало) относится к так называемым шифрам перестановки. По-видимому, первому дешифровать сообщения, зашифрованные Сциталой, удалось Аристотелю: он предложил наматывать ленту с сообщением на конус, а затем перемещать ее по его длине, пока не начнут просматриваться участки читаемого текста. Это позволяло определить секретный размер цилиндра.

Задача 3 (11 класс)

Докажите, что существует натуральное число, кратное 2015, десятичная запись которого имеет вид 12351235…1235 (т.е. образована последовательным повторением фрагмента 1235).

Решение

Натуральное число делится на 2015 нацело в том и только том случае, когда оно делится на 5 и на 403.

Рассмотрим теперь все числа, десятичная запись которых имеет вид 12351235…1235:

Среди них найдутся два числа, x_m и x_n $(m > n)$, которые имеют одинаковые остатки при делении на 403. Действительно, чисел вида (1) бесконечно много, а различных остатков от деления на 403 всего 403 штуки. Тогда их разность $x_m - x_n$ делится на 403 (см. приложение). Теперь отбросим все нули на конце десятичной записи этой разности. В результате получим число вида (1). И это число, очевидно, по-прежнему делится на 403. Оно делится также и на 5, так как на 5 оканчивается, а значит, делится на 2015.

Задача 4 (8-9, 10 классы)

Для зашифрования осмысленного русского слова используется последовательность натуральных чисел $y_1, y_2, \ldots$, которая формируется так: y_1 выбирается произвольно, а остальные члены последовательности вычисляются по формуле $y_{n+1} = 4y_n + 23, \ n = 1, 2, \ldots$ Зашифрование производилось следующим образом. Первая буква слова заменялась числом согласно таблице и умножалась на y_1. Потом также заменялась вторая буква и умножалась на y_2 и т.д. Затем все произведения были замены остатками от деления на 32. В результате получилось вот что:

8, 16, 24, 13, 22, 10, 9, 16, 0, 28, 24, 29.

А	Б	В	Г	Д	Е Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Какое слово было зашифровано?

Решение

Обозначим через $r_{32}(a)$ остаток от деления числа *a* на 32. Выразим несколько первых членов последовательности $y_2, y_3, \ldots$: через y_1:

$$y_2 = 4y_1 + 23,\ y_3 = 4(4y_1 + 23) + 23 = 16y_1 + 5 \cdot 23,$$

$$y_4 = 64y_1 + 21 \cdot 23.$$

Далее, $r_{32}(y_4) = r_{32}(21 \cdot 23) = 3$, а значит, $r_{32}(y_5) = r_{32}(4y_4 + 23) =$ $= r_{32}(4 \cdot 3 + 23) = 3$. То есть, начиная с четвертого номера, все члены последовательности $r_{32}(y_n)$ равны 3. Пусть $x_1, x_2, \ldots, x_{12}$ – числовые значения букв искомого слова. Чтобы найти x_4 надо решить уравнение $r_{32}(y_4 x_4) = 13$. Заметим, что (см. приложение)

$$r_{32}(y_4 x_4) = 13 \Leftrightarrow r_{32}(3x_4) = 13 \Leftrightarrow r_{32}(11 \cdot 3x_4) = r_{32}(11 \cdot 13) \Leftrightarrow$$

$$r_{32}(x_4) = 15 \Rightarrow x_4 = 15.$$

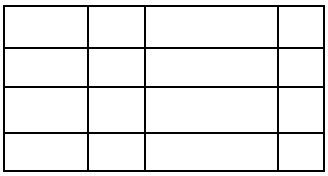
Следовательно, четвертая буква слова – П. Аналогично находятся числовые значения букв $x_5, \ldots, x_{12}$. В итоге, искомое слово принимает вид ***ПТОГРАФИЯ. Ответ легко угадывается.

Ответ: КРИПТОГРАФИЯ.

Комментарий

Представленный в настоящей задаче способ зашифрования относится к так называемым ***шифрам табличного гаммирования***. В самом общем виде они выглядят следующим образом. Пусть – последовательность букв открытого текста и – *ключевая последовательность*, тогда последовательность букв шифрованного текста формируется по правилу

где функция обладает тем свойством, что в ее таблице значений



в каждой строке находятся различные элементы и в каждом столбце находятся различные элементы. Такие таблицы называются *латинскими прямоугольниками*.

В предложенной задаче функция определялась по правилу

,

при этом элементы ключевой последовательности являлись нечетными числами, а буквы открытого текста – элементами множества .

Задача 5 (10, 11 классы)

Для проверки корректности номера пластиковой карты, представляющего собой набор из 16 цифр

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}),$$

вычисляются контрольные суммы A, B и C:

$$A = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} + x_{16},$$

$$B = x_1 + x_3 + x_4 + 3x_5 + x_6 + x_7 + 7x_9 + x_{11} + x_{12} + x_{13} + x_{15},$$

$$C = x_1 + x_2 + x_4 + 7x_5 + x_8 + 3x_9 + x_{10} + x_{14} + x_{16}.$$

Если все три суммы A, B и C делятся нацело на 10, то номер признаётся корректным. Каких корректных номеров больше и насколько: у которых первые 4 цифры 0, 0, 0, 0 или тех, у которых последние 4 цифры 0, 0, 0, 0?

Решение

Пусть – остаток от деления на 10, тогда количество корректных номеров есть число решений системы линейных уравнений:

$$\begin{cases} r_{10}(A) = 0, \\ r_{10}(B) = 0, \\ r_{10}(C) = 0. \end{cases}$$

Для удобства расположим слагаемые (из вида A, B и C) в таблице:

x_1		x_3	x_4		x_6	x_7	x_8		x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
x_1		x_3	x_4	$3x_5$	x_6	x_7		$7x_9$		x_{11}	x_{12}	x_{13}		x_{15}	x_{16}
x_1	x_2		x_4	$7x_5$			x_8	$3x_9$	x_{10}				x_{14}		x_{16}

Если первые 4 цифры 0, 0, 0, 0, то таблица примет вид:

	x_6	x_7	x_8		x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
$3x_5$	x_6	x_7		$7x_9$		x_{11}	x_{12}	x_{13}		x_{15}	x_{16}
$7x_5$			x_8	$3x_9$	x_{10}				x_{14}		x_{16}

Но тогда первая строка есть остаток от деления суммы третьей и второй на 10. Вычитая из первой строки вторую и третью, а затем из второй строки третью, получим, что исходная система равносильна системе (см. приложение)

$$\begin{cases} r_{10}(x_{15}) = r_{10}(4x_5 - x_6 - x_7 + x_8 - 4x_9 + x_{10} - x_{11} - x_{12} - x_{13} + x_{14}), \\ r_{10}(x_{16}) = r_{10}(-7x_5 - x_8 - 3x_9 - x_{10} - x_{14}). \end{cases}$$

Количество решений есть количество способов поставить всеми возможными способами на места переменных $x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}$ числа 0,1,2,…,9. Таким образом, число корректных номеров равно 10^{10}.

Если же последние 4 цифры 0, 0, 0, 0, то таблица примет вид:

x_1		x_3	x_4		x_6	x_7	x_8		x_{10}	x_{11}	x_{12}
x_1		x_3	x_4	$3x_5$	x_6	x_7		$7x_9$		x_{11}	x_{12}
x_1	x_2		x_4	$7x_5$			x_8	$3x_9$	x_{10}		

В отличие от первого случая, переменные x_1, x_2, x_3 будут линейно выражаться через $x_4, x_6, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}$. И тогда получим, что число решений системы равно 10^9.

Ответ: в первом случае корректных номеров больше, чем во втором на $10^{10} - 10^9$.

Задача 6 (8-9, 10 классы)

Рис. а

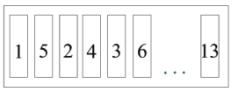


Рис. б

На столе выложены 13 карточек в порядке возрастания их номеров (Рис. а). Карточки разрешается перекладывать *тройками*, а именно: выбираем три любые карточки, например, с номерами $2, 3$ и 5. Затем крайняя левая карточка перемещается на место средней, средняя на место крайней правой, а крайняя правая на место крайней левой. Результат изображен на Рис. б. Можно ли, перекладывая карточки указанным способом, уложить их как на Рис. а, но в порядке убывания номеров (карточка с номером 13 – первая, с номером 1 – последняя)?

Решение

Покажем, что у любых четырех карточек A,B,C,D можно изменить порядок их следования на противоположный (точками сверху будем отмечать те карточки, которые собираемся перекладывать):

$$\dot{A},\dot{B},C,\dot{D}\to D,\dot{A},\dot{C},\dot{B}\to D,\dot{B},\dot{A},\dot{C}\to D,C,B,A.$$

Теперь, перекладывая карточки сразу *четверками*, покажем как переложить 13 карточек в обратном порядке:

$$\dot{1},\dot{2},3,4,5,6,7,8,9,10,11,\dot{12},\dot{13}\to 13,12,\dot{3},\dot{4},5,6,7,8,9,\dot{10},\dot{11},\ 2,1\to$$

$$\to 13,12,11,10,\dot{5},\dot{6},7,\dot{8},\dot{9},4,3,\ 2,1\to 13,12,11,10,9,8,7,6,5,4,3,2,1.$$

Ответ: Можно.

Задача 7 (11 класс)

Рассмотрим множество всех точек плоскости, координаты которых имеют вид $(m+2n, 3m-n)$, где m, n – целые числа. Докажите, что на прямой, проходящей через любые две точки указанного множества, лежит сторона некоторого квадрата, все четыре вершины которого принадлежат этому множеству. Укажите минимальную площадь такого квадрата.

Решение

Для решения поставленной задачи достаточно доказать, что на любой прямой, проходящей через $(0,0)$ и точку вида $(m+2n, 3m-n)$, $m, n \in \mathbf{Z}$ ($\mathbf{Z}$ - множество целых чисел), лежит сторона некоторого квадрата, все вершины которого принадлежат указанному множеству.

Известно, что перпендикулярными к вектору (a,b) являются все вектора вида $k(-b,a), k \in R$ и только они. Применительно к нашей задаче, требуется проверить, что для каждого вектора $(m_1+2n_1, 3m_1-n_1)$, $m_1, n_1 \in \mathbf{Z}$ существует перпендикуляр вида $(m_2+2n_2, 3m_2-n_2)$, $m_2, n_2 \in \mathbf{Z}$. Другими словами надо решить относительно $k, m_2, n_2 \in \mathbf{Z}$ уравнение

$$k(n_1-3m_1, m_1+2n_1) = (m_2+2n_2, 3m_2-n_2).$$

Перепишем полученное уравнение в виде системы

$$\begin{cases} k(n_1-3m_1) = m_2+2n_2, \\ k(m_1+2n_1) = 3m_2-n_2, \end{cases}$$

которую несложно преобразовать в эквивалентную систему

$$\begin{cases} m_2 + 2n_2 = k(n_1 - 3m_1), \\ -7n_2 = k((m_1 + 2n_1) - 3(n_1 - 3m_1)), \end{cases}$$

разрешимость которой очевидна – последовательно выбираем подходящие целые числа k, n_2 и m_2.

Таким образом, для всякого вектора $(m_1 + 2n_1, 3m_1 - n_1)$, $m_1, n_1 \in \mathbf{Z}$ существует перпендикулярный ему вектор $k(n_1 - 3m_1, m_1 + 2n_1)$ вида $(m_2 + 2n_2, 3m_2 - n_2)$. Нетрудно понять, что вектора $k(m_1 + 2n_1, 3m_1 - n_1)$ и $k(n_1 - 3m_1, m_1 + 2n_1)$ являются сторонами искомого квадрата.

Будем искать квадрат с минимальной площадью. Без ограничения общности можно считать, что вершина A квадрата совпадает с началом координат (0,0). Пусть вершины B и C имеют координаты $B(m_1 + 2n_1, 3m_1 - n_1), C(m_2 + 2n_2, 3m_2 - n_2)$. Координаты четвертой вершины квадрата D совпадают с координатами вектора $\overrightarrow{AD}$, которые находятся из очевидного соотношения

$$\overrightarrow{AD} = \overrightarrow{AB} + \overrightarrow{AC} = (m_1 + m_2 + 2(n_1 + n_2), 3(m_1 + m_2) - (n_1 + n_2)).$$

То есть точка D, разумеется, принадлежит нашему множеству. Данный четырехугольник является квадратом в том и только том случае, когда

$\overrightarrow{AB} \perp \overrightarrow{AC}$ и $\left|\overrightarrow{AB}\right| = \left|\overrightarrow{AC}\right| \Leftrightarrow$

$$\begin{cases} (m_1 + 2n_1)(m_2 + 2n_2) + (3m_1 - n_1)(3m_2 - n_2) = 0, \\ (m_1 + 2n_1)^2 + (3m_1 - n_1)^2 = (m_2 + 2n_2)^2 + (3m_2 - n_2)^2. \end{cases}$$

Решая последнюю систему, находим

$$m_2 = \frac{m_1}{7} - \frac{5n_1}{7}, \quad n_2 = \frac{10m_1}{7} - \frac{n_1}{7}. \qquad (*)$$

Имеется, конечно же, еще одно решение, поскольку точку C можно отразить симметрично относительно прямой AB и получить тот же квадрат, повернутый на 90^0. Это решение рассматривается аналогично.

Мы выразили числа m_2 и n_2 через m_1 и n_1. Однако, целые числа m_1 и n_1 нельзя выбирать совершенно произвольно, так как вычисленные затем по формулам (*) числа m_2 и n_2 должны также быть целыми. Можно в этой связи показать, что число n_1 все же можно выбирать произвольно, но тогда число m_1 должно иметь вид $m_1 = 5n_1 + 7k,$ где k – уже произвольное целое число. Подставив полученное выражение для m_1 в формулу для площади $S = (m_1 + 2n_1)^2 + (3m_1 - n_1)^2$, получим

$$S = 49\left(5n_1^{\,2} + 14n_1k + 10k^2\right).$$

Выражение в скобках принимает только целые положительные значения. Значит, меньше 49 площадь быть

не может. Чтобы убедиться, что значение 49 достижимо, достаточно взять $m_1 = -2, n_1 = 1, m_2 = -1, n_2 = 3.$

Ответ: 49.

Задача 8 (11 класс)

Число городов в Криптоландии равно 4^4. В качестве названий города имеют различные цифровые комбинации вида (a,b,c,d), где a,b,c и d – целые числа из множества {0,1,2,3}. Два города, названия которых отличаются одной цифрой, называются *соседними*. Например, города (3201) и (3001) соседние, а (1111) и (3311) – нет. У каждого города есть флаг определенного цвета, причем флаги соседних городов всегда имеют несовпадающие цвета. Власти объявили конкурс на создание системы флагов для городов, имеющей наименьшее возможное число различных цветов. Найдите это наименьшее число. Ответ обоснуйте.

Решение

Заметим, что среди городов (0000), (1000), (2000) и (3000) любые два являются соседними. Значит, цветов надо минимум четыре. Покажем, что четырех цветов достаточно. Имеющиеся у нас цвета будем называть цвет-0, цвет-1, цвет-2, цвет-3. Флаг города будет окрашен в цвет, номер которого равен остатку от деления на 4 суммы цифр в названии этого города (например, для города (3201) этот остаток равен 2, значит, его флаг будет окрашен в цвет-2). У соседних городов эти остатки всегда различны, так как их названия отличаются *одной* цифрой. Следовательно, 4-х цветов достаточно.

Ответ: 4 цвета.

Комментарий

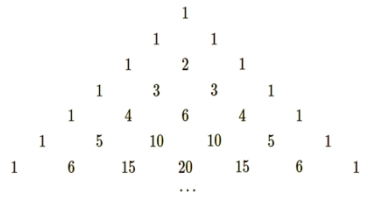
С данной задачей связано одно важное понятие теории графов: *t-раскраска графов*. *Графом* называется множество, состоящее точек (*вершин*) *V* и соединяющих их отрезков (*ребер*) *E*. Говорят, что граф можно раскрасить в цветов, если множество его вершин можно так покрасить, используя цветов, что любые две его вершины, соединенные ребром, будут иметь разные цвета. При этом минимальное число цветов, которым можно раскрасить граф, называется его *хроматическим числом*.

С раскраской графов связан ряд математических проблем, самая известная из которых – *гипотеза о 4-х красках* (решена). Впервые она была сформулирована Францисом Гутри (XIX в.), который пытался раскрасить карту округов Англии в 4 цвета так, что чтобы любые два смежных региона имели разные цвета. В общем виде гипотеза звучит так: *можно ли раскрасить любой плоский граф в 4 цвета?*

Теорема о четырёх красках была доказана в 1976 году англичанами К. Аппелем и В. Хакеном из Иллинойского университета. Это была первая крупная математическая теорема, доказанная с помощью компьютера. Первым шагом доказательства была демонстрация того, что существует определенный набор из 1936 карт, ни одна из которых не может содержать карту меньшего размера, которая опровергала бы теорему. Аппель и Хакен использовали специальную компьютерную программу, чтобы доказать это свойство для каждой из 1936 карт.

Доказательство этого факта заняло сотни страниц. Изначально представленное доказательство гипотезы не было принято всеми математиками, поскольку его невозможно было проверить вручную. В дальнейшем оно получило более широкое признание, хотя у некоторых долгое время оставались сомнения. Чтобы развеять оставшиеся сомнения, в 1997 году Робертсон, Сандерс, Сеймур и Томас опубликовали более простое доказательство, использующее аналогичные идеи, но по-прежнему проделанное с помощью компьютера. Кроме того, в 2005 году доказательство было проделано Д. Гонтиром с использованием специализированного программного обеспечения.

Задача 9 (8-9, 10, 11 классы)

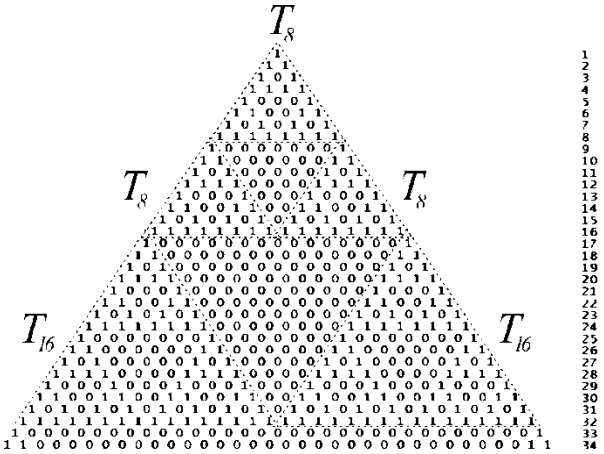


Треугольником Паскаля называют бесконечную треугольную таблицу чисел, у которой на вершине и по бокам стоят единицы, а каждое число внутри равно сумме двух стоящих над ним чисел. Так, например, третья строка треугольника (1,2,1) содержит два нечетных числа и одно четное. Сколько четных чисел содержится: а) в строке с номером 256? б) в строке с номером 200?

Решение

Будем заменять в треугольнике нечетные числа единицами, а четные нулями. При этом каждое число внутри по-прежнему остается равным сумме стоящих над

ним чисел, если принять, что 0+0=1+1=0, 1+0=0+1=1. Рассмотрим структуру треугольника подробнее. Треугольник, сформированный первыми восемью строками, обозначим T_8. В строке 9 всего две единицы (по бокам), остальные – нули. С этой строки и вниз далее идет



формирование двух треугольников T_8, которые «встречаются друг с другом» в строке 16. Начиная со строки 17 и ниже, образовываются два треугольника T_{16}, которые, в свою очередь, «встречаются» в строке 32. Со строки 33 и ниже формируются два треугольника T_{32} и т.д. Таким образом, строки, чей номер представляет собой степень двойки, состоят только из единиц. Поэтому в строке 256 четных чисел нет.

Обратимся теперь к строке 200. Понятно, что после строки 128 (степень двойки), идет формирование «с нуля» двух одинаковых треугольников. Строки с номером 72 в

этих новых треугольниках как раз и содержатся в строке 200 исходного (большого) треугольника, т.к. 200=128+72. Значит единиц в строке 200 вдвое больше, чем единиц в строке с номером 72. В свою очередь единиц в строке 72 вдвое больше, чем в строке 8. Количество же единиц в строке 8 можно подсчитать непосредственно – их 8 штук. Значит в строке 200 их 32, остальные 168 – нули.

Ответ: а) 0, б) 168.

Задача 10 (8-9 класс)

Докажите, что для каждого натурального $n \geq 5$ квадрат можно разрезать на n прямоугольников (не обязательно одинаковых), у каждого из которых одна сторона вдвое больше другой. Резать разрешается по линиям, параллельным сторонам исходного квадрата.

Решение

Если квадрат уже разрезан на k прямоугольников с отношением сторон 2:1, то его можно разрезать и на k+3 таких прямоугольников. Действительно, для этого достаточно один из этих k прямоугольников разрезать на четыре прямоугольника, у каждого из которых стороны также относятся как 2:1 (Рис. I). Таким образом, для завершения доказательства остается показать, что квадрат можно разрезать на n=5, 6 и 7 прямоугольников указанного вида. Соответствующие линии разреза приведены на Рис.II–IV. Для удобства сторона квадрата принята равной 24.

Рис.I

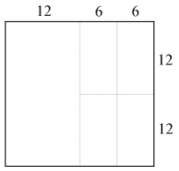


Рис.II. $n = 5$.

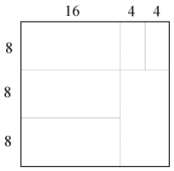


Рис.III. $n = 6$.

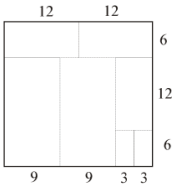


Рис.IV. $n = 7$.

Задача 11 (11 класс)

Чтобы снять деньги с карточки, Алиса в банкомате вводит пин-код (ПК) x_1, x_2, x_3, x_4 – набор из 4-х целых чисел ($0 \le x_i \le 9, i = 1,2,3,4$). Банкомат зашифровывает введенный ПК по следующему правилу: он случайным образом выбирает целое число x_5 такое, что $10 \le x_5 \le 15$, а затем формирует зашифрованный пин-код (ЗПК) y_1, y_2, y_3, y_4, y_5 по формулам:

$$y_1 = f\left(r_{16}(x_1 + 3 \cdot y_0)\right), y_2 = f\left(r_{16}(x_2 + 3 \cdot y_1)\right),$$
$$y_3 = f\left(r_{16}(x_3 + 3 \cdot y_2)\right), y_4 = f\left(r_{16}(x_4 + 3 \cdot y_3)\right),$$
$$y_5 = f\left(r_{16}(x_5 + 3 \cdot y_4)\right),$$

где $y_0 = 2$, $r_{16}(x)$ – остаток от деления числа x на 16, а f – некоторое правило, по которому одно целое число от 0 до 15 заменяется на другое (возможно, то же самое) целое число от 0 до 15, причем разные числа заменяются разными. После этого ЗПК отправляется на сервер, где он расшифровывается (т.е. по присланным числам y_1, y_2, y_3, y_4, y_5 вычисляются x_1, x_2, x_3, x_4 и x_5), и,

если x_5 не удовлетворяет неравенству $10 \le x_5 \le 15,$ то сервер выдает сообщение об ошибке. Известно, что для ПК Алисы был сформирован следующий ЗПК: 13,13,1,11,7. Известно также, что хакеры пытались отсылать на сервер (напрямую, минуя банкомат) в качестве y_1, y_2, y_3, y_4, y_5 комбинации чисел вида $0,0,0,a,b.$ Результаты их попыток приведены в таблице (знак "+" – сервер не выдал сообщение об ошибке, знак "-" – выдал). Какой ПК у Алисы?

a \ b	1	2	3	11	12	13
1	-	+	-	-	-	+
2	-	+	+	-	-	-
3	+	-	+	-	+	-
4	+	-	-	-	+	-
5	-	-	-	+	-	+
6	-	-	-	+	-	+
7	-	+	+	-	-	-
8	-	+	+	-	+	-
9	+	-	-	-	+	-
10	+	-	-	+	-	+

Решение

Для формирования величины x_5, которая будет проверяться на предмет того, принадлежит ли она множеству $\Omega_1 = \{10,11,12,13,14,15\}$, будут задействованы только последние два числа: a, b. Тогда процедура проверки будет выглядеть следующим образом:

$$x_5 = r_{16}(f^{-1}(b) - 3a) \stackrel{?}{\in} \Omega_1.$$

Нетрудно догадаться по виду данной в условии таблицы, что структура каждого столбца с номером b таблицы с точки зрения возникающих ошибок x_5 будет следующей:

+	+	-	-	-	-	+	+	-	-	-	+	+	-	-	-
a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}

$$a_j = r_{16}(a_1 + j),\ j = \overline{1,16}.$$

Вариант рассуждений а).

Выделяем случаи, когда $x_5 \in \Omega_1$ (помечены в таблице темным, далее по тексту условно обозначим $\Omega_1 + c$ - множество элементов Ω_1, к каждому из которых прибавлено число c и от получившихся значений взят остаток от деления на 16):

- при a_1 имеем

$$r_{16}(f^{-1}(b) - 3a_1) \in \Omega_1 = \{10,11,12,13,14,15\};$$

- при $a_2 = a_1 + 1$ имеем

$$r_{16}(f^{-1}(b) - 3a_1) \in \Omega_1 + 3 = \Omega_2 = \{13,14,15,0,1,2\};$$

- при $a_7 = a_1 + 6$ имеем

$$r_{16}(f^{-1}(b) - 3a_1) \in \Omega_1 + 2 = \Omega_7 = \{12,13,14,15,0,1\};$$

- при $a_8 = a_1 + 7$ имеем

$$r_{16}(f^{-1}(b) - 3a_1) \in \Omega_1 + 5 = \Omega_8 = \{15,0,1,2,3,4\};$$

- при $a_{12} = a_1 + 11$ имеем

$$r_{16}(f^{-1}(b) - 3a_1) \in \Omega_1 + 1 = \Omega_{12} = \{11,12,13,14,15,0\};$$

- при $a_{13} = a_1 + 12$ имеем

$$r_{16}(f^{-1}(b) - 3a_1) \in \Omega_1 + 4 = \Omega_{13} = \{14,15,0,1,2,3\}.$$

Нетрудно заметить, что $\Omega_1 \cap \Omega_8 = \{15\}$, то есть

$$r_{16}(f^{-1}(b)-3a_1)=15.$$

Вариант рассуждений б).

Ответим на вопрос, при каких значениях $x_5=r_{16}(f^{-1}(b)-3\cdot a)$ возможна ситуация, что при проверке $x_5\in\Omega_1$ при a_1 будет “+”, при $a_2=a_1+1$ будет “+”, а при $a_3=a_2+1,\ a_4=a_3+1,\ a_5=a_4+1,\ a_6=a_5+1$ будет “-”. Исходя из приведенной ниже таблицы, нетрудно заметить, что только при $x_5=r_{16}(f^{-1}(b)-3a_1)=15.$

$-3\cdot a=$	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
	-	-	-	-	-	-	-	-	-	-	+	+	+	+	+	+
$x_5=$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	a_6			a_5			a_4			a_3			a_2			a_1

Общий вывод из рассуждений а) или б):

Если в таблице ошибок для x_5 при заданном b есть структура вида

+	+	-	-	-	-
a_1	a_2	a_3	a_4	a_5	a_6

то $r_{16}(f^{-1}(b)-3a_1)=15$, то есть $f^{-1}(b)=r_{16}(3a_1-1)$. Это является удобным критерием для определения обратных значений функции .

Рассмотрим столбец из данной в условии таблицы с $b=11$. Из-за закономерностей в образовании “+” не трудно догадаться, что подходящей под критерий структурой будет

+	+	-	-	-	-
15	0	1	2	3	4

Поэтому $a_1 = 15$ и $f^{-1}(11) = r_{16}(3 \cdot 15 - 1) = 12$, что позволяет найти x_4:

$$x_4 = r_{16}(f^{-1}(11) - 3 \cdot 1) = r_{16}(12 - 3) = 9.$$

Рассмотрим столбец из данной в условии таблицы с $b = 1$. Не трудно заметить, что подходящей под критерий структурой будет

+	+	-	-	-	-
3	4	5	6	7	8

Поэтому $a_1 = 3$ и $f^{-1}(1) = r_{16}(3 \cdot 3 - 1) = 8$, что позволяет найти x_3:

$$x_3 = r_{16}(f^{-1}(1) - 3 \cdot 13) = r_{16}(8 - 7) = 1.$$

Рассмотрим столбец из данной в условии таблицы с $b = 13$. Из-за закономерностей в образовании "-" не трудно догадаться, что подходящей структурой будет

+	+	-	-	-	-
10	11	12	13	14	15

Поэтому $a_1 = 10$ и $f^{-1}(13) = r_{16}(3 \cdot 10 - 1) = 13$, что позволяет найти x_1, x_2:

$$x_1 = r_{16}(f^{-1}(13) - 3 \cdot 2) = r_{16}(13 - 6) = 7;$$

$$x_2 = r_{16}(f^{-1}(13) - 3 \cdot 13) = r_{16}(13 - 7) = 6.$$

Ответ: ПК Алисы 7,6,1,9.

Комментарий

Ситуация, описанная в задаче, описывает вполне реальный сценарий действий нарушителя, располагающего

возможностью перехвата зашифрованных данных в сети от отправителя, передачи на их основе сфабрикованных данных получателю и получения ответных от него пакетов. Такие ответы практически всегда будут содержать информацию о невозможности корректно расшифровать полученные данные из-за внесенных изменений со стороны противника, что может быть использовано в процедуре дешифрования.

Такой сценарий становится вполне реальной угрозой, когда клиент осуществляет безопасное соединение с сервером (по протоколу TLS от англ. Transport Layer Security, набирая в браузере https://) для осуществления оплаты предоставляемых им услуг, например при покупке авиабилета через веб-сайт. Возможность определения ПК Алисы в задаче по ответам от сервера иллюстрирует то, что в случае передачи в зашифрованном виде, например, реквизитов банковской карточки (а не просто ПК) нарушитель также может получить и эти реквизиты, включая так называемый CCV-код подтверждения (или ему подобный). Этой информации будет вполне достаточно, чтобы пользоваться денежными средствами клиента, располагаемыми на счете, к которому данная карточка привязана. Также нарушитель может создать и дубликат карточки клиента – затраты на это не будут превосходить несколько десятков тысяч рублей.

Возможность проведения данной атаки в частности обуславливается выбором самого способа шифрования данных, определяемого формулой: $y_i = f\left(r_{16}(x_i + 3 \cdot y_i)\right)$,

$i=\overline{1,4}$, y_0 - фиксированное и известное значение. Этот способ фактически в точности представляет собой один из широко используемых в сети Интернет вариант шифрования данных (при использовании блочной шифрсистемы f), называемый режимом сцепления блоков CBC (от англ. Cipher Block Chaining). Данный режим обладает рядом недостатков, которые в частности и позволили провести ряд атак на протоколы семейства TLS, IPsec (протокол защиты сетевого уровня), S/MIME (протокол защищенной почты). На настоящее время постепенно предпочтение отдается более защищенным режимам, которые относятся к классу так называемых режимов аутентичного шифрования, позволяющих одновременно как зашифровывать данные, так и обеспечивать их целостность.

ПРИЛОЖЕНИЕ
(свойства остатков)

Определение. *Разделить целое число на ненулевое целое число с остатком означает найти такие целые числа , что выполнено равенство:*

и при этом

При этом число называют остатком от деления числа на и обозначают , а число называют неполным частным.

Пример. Остаток от деления 7 на 3 равен 1, поскольку

В то же время остаток от деления –2 на 3 так же равен 1:

Теорема. *Любое целое число можно разделить с остатком на число при этом остаток и неполное частное определены однозначно.*

Утверждение. *Справедливы следующие свойства:*

1.
2.
3. делится на .

С задачами прошедших олимпиад по математике и криптографии и их решениями можно ознакомиться:

- на сайте www.cryptolymp.ru в разделе «Подготовка к олимпиаде» и «Архив задач»;
- на сайте Академии ФСБ России по адресу www.academy.fsb.ru (раздел для абитуриентов);
- в учебно-методическом журнале "Математика", Издательский дом «Первое сентября» (ежегодно в одном из апрельских выпусков, www.1september.ru);
- в книге «Введение в криптографию» (М.:МЦНМО, 2012);
- в книге «Олимпиады по криптографии и математике для школьников» (М.: МЦНМО, 2013).
- также можно получить доступ к системе дистанционного обучения для подготовки к олимпиаде на сайте: http://www.v-olymp.ru