Федеральное государственное автономное
образовательное учреждение высшего образования
Национальный исследовательский университет
«Высшая школа экономики»

Московский институт электроники и математики им. А.Н. Тихонова

Методические рекомендации
по решению конкурсных заданий практического этапа
Московского конкурса межпредметных навыков и знаний
«Интеллектуальный мегаполис. Потенциал» в номинации «ИТ-класс»
по направлению

«Информационная безопасность»

Москва, НИУ ВШЭ

2022 г.

Оглавление

Введение

Материалы практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» предназначены для оценки уровня практической подготовки участников Конкурса.

Задания практического этапа Конкурса разработаны преподавателями образовательных организаций высшего образования, участвующих в проекте «ИТ-класс в московской школе».

Индивидуальный вариант участника формируется автоматически во время проведения практического этапа Конкурса предпрофессиональных умений из базы конкурсных заданий.

Индивидуальный вариант участника включает 15 заданий, базирующихся на содержании элективного курса «Информационная безопасность».

В данном пособии предлагаются теоретические выкладки по проверяемым темам и разбор заданий демонстрационного конкурсного варианта.

Тематическая направленность номеров конкурсных материалов

№ задания	Проверяемые темы	Контролируемые требования к проверяемым умениям
1.	Системы счисления	Умение выполнять переводы чисел в различные системы счисления
2.	Алгебра логики	Умение преобразовывать логические выражения, сопоставлять логические выражения на основе таблиц истинности
3.	Комбинаторика	Умение решать задачи с применением комбинаторных формул
4.	Основы теории информации	Умение рассчитывать количество информации, прибегая к вероятностному подходу
5.	Основы криптографии	Умение выполнять криптографические преобразования
6.	Основы криптоанализа	Умение восстанавливать неизвестные параметры криптографических преобразований
7.	Алгебра в кольцах вычетов	Умения вычислять выражения в кольцах вычетов
8.	Диофантовы уравнения	Умение решать диофантовы уравнения
9.	Китайская теорема об остатках	Умение решать системы линейных сравнений в кольцах вычетов
10.	Квадратичные сравнения в кольцах вычетов	Умение решать квадратичные сравнения в кольцах вычетов
11.	Основы теории информации	Умение рассчитывать количество информации, прибегая к вероятностному подходу
12.	Основы криптографии	Умение выполнять криптографические преобразования

№ задания	Проверяемые темы	Контролируемые требования к проверяемым умениям
13.	Основы криптоанализа	Умение восстанавливать неизвестные параметры криптографических преобразований
14.	Понятие делимости, простых чисел, НОД, НОК	Умение определять простые числа, вычислять НОД и НОК
15.	IP-адресация	Знание и понимание принципов IP-адресации в сети

Теоретические выкладки

О позиционных системах счисления

Система счисления – это знаковая система, в которой числа записываются по определенным правилам с помощью символов некоторого алфавита. Эти символы принято называть цифрами. Все системы счисления делятся на две большие группы: позиционные и непозиционные системы счисления. В позиционных системах количественное значение цифры зависит от ее положения в числе. Основание системы показывает в том числе количество цифр в алфавите системы. Если требуется более 10 цифр (т.е. основание системы больше десяти), прибегают к прочим символам для обозначения. Классически используют заглавные латинские буквы: A, B, C, …

Для перевода десятичного числа в систему с основанием k его и полученные частные необходимо последовательно делить на k до тех пор, пока не останется частное, меньшее или равное $k - 1$. Число в системе счисления с основанием k записывается как последовательность цифр последнего результата деления и остатков от деления в обратном порядке.

Для перевода числа в десятичную систему счисления из системы счисления с основанием k используется следующий принцип:

$$\overline{x_n \dots x_1 x_0}_k = x_n \cdot k^n + \dots + x_1 \cdot k^1 + x_0$$

Об алгебре логики

Приведем тут элементы алфавита языка логики высказываний, знание которых проверяются в конкурсных материалах.

Символы	Значение
¬	Отрицание (инверсия)
∧	Конъюнкция (И)
∨	Дизъюнкция (ИЛИ)
→	Импликация

Этим операциям соответствуют следующие таблицы истинности.

A	¬A
0	1
1	0

A	B	A ∧ B
0	0	0
0	1	0
1	0	0
1	1	1

A	B	A ∨ B
0	0	0
0	1	1
1	0	1
1	1	1

A	B	A → B
0	0	1
0	1	1
1	0	0
1	1	1

Если логическое выражение содержит несколько операций, то их выполнение предписывается в следующем порядке:

1. Отрицание;

2. Конъюнкция;

3. Дизъюнкция;

4. Импликация.

Если указанный порядок необходимо изменить, используются скобки.

Из прочих примечательных инструментов в решении задач по основам алгебры логики используются различные свойства логических операций. Приведем ниже некоторые из них.

Закон не противоречия: логическое высказывание не может одновременно быть истинно и ложно

$$A \wedge \neg A = 0$$

Закон исключения третьего случая: логическое высказывание может быть либо истинно, либо ложно (третьего не дано)

$$A \vee \neg A = 1$$

Закон двойного отрицания: отрицание отрицания логического высказывания есть его утверждение

$$\neg(\neg A) = A$$

Законы идемпотентности: в алгебре логики не допускаются степени и коэффициенты

$$A \vee A = A \qquad A \wedge A = A$$

Законы ассоциативности:

$$A \vee (B \vee C) = (A \vee B) \vee C \qquad A \wedge (B \wedge C) = (A \wedge B) \wedge C$$

Законы дистрибутивности:

$$(A \wedge B) \vee C = (A \vee C) \wedge (B \vee C) \qquad (A \vee B) \wedge C = (A \wedge C) \vee (B \wedge C)$$

Законы де Моргана: конъюнкция двойственна дизъюнкции.

$$\neg(A \wedge B) = \neg A \vee \neg B \qquad \neg(A \vee B) = \neg A \wedge \neg B$$

Законы поглощения:

$$A \vee 1 = 1 \qquad A \wedge 1 = A$$
$$A \vee 0 = A \qquad A \wedge 0 = 0$$
$$A \vee (A \wedge B) = A \qquad A \wedge (A \vee B) = A$$

Законы склеивания:

$$(A \wedge B) \vee (\neg A \wedge B) = B \qquad (A \vee B) \wedge (\neg A \vee B) = B$$

О комбинаторике

Число размещений из n по k элементов без возвращения и с учётом порядка равняется

$$A_n^k = n(n-1)\ldots(n-k+1) = \frac{n!}{(n-k)!}$$

Число перестановок из n элементов между собой равняется

$$A_n^n = n(n-1)\ldots 1 = n!$$

Число сочетаний из n по k элементов без возвращения и без учёта порядка равняется

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$$

Число различных наборов из n по k элементов с возвращением и с учётом порядка равняется n^k.

О количестве информации

Существуют разные подходы к определению количества информации. В конкурсных материалах проверяется умение участника искать количество информации по подходу Шеннона.

Формула Шеннона определяет информационную энтропию (количество информации) с учетом вероятностного распределения системы событий:

$$H = -\sum_{i=1}^{n} p\left(x_i\right) \cdot p\left(x_i\right) = \sum_{i=1}^{n} p\left(x_i\right) \cdot \frac{1}{p\left(x_i\right)} \ ,$$

где $a -$ отвечает за единицы измерения (в случае бит $a = 2$);

$p\left(x_i\right) -$ вероятность события x_i из полной системы событий $\left\{x_1, \ ..., x_i, \ ..., \ x_n\right\}$.

В случае одного описанного события, принято прибегать к формуле с удельным количеством:

$$H = -\ p\left(x_i\right) = \frac{1}{p\left(x_i\right)} \ .$$

Если необходимо приводить целое число бит в ответе, то принято округлять всегда вверх. Поступают таким образом, потому что если получается, например, 3,14 бит информации, то получено больше, чем 3 бита.

О криптографических преобразованиях

В криптографии принято выделять два преобразования:

- Подстановки,

- Перестановки.

В случае шифра из класса простых перестановок ключом выступает таблица замен элементов открытого текста (это могут быть не только буквы, но и, например, слоги или слова) на некоторые другие элементы (числа, буквы, картинки и прочие символы).

В случае шифра из класса перестановок для процесса зашифрования нужно выбрать два действия: как разбить открытый текст на элементы и как переставить эти элементы местами.

О методах криптоанализа

Для дешифрования шифртекста (то есть восстановления исходного открытого текста без знания ключа преобразования) существует много разных методов. Наиболее примитивным и универсальным, безусловно, является метод грубой силы (или метод полного перебора), который заключается в том, чтобы перебирать все возможные ключи шифра до тех пор, пока в результате не получится осмысленный открытый текст.

При полном переборе в худшем случае придется перебирать все значения ключей, кроме последнего. Последний вариант проверять уже не потребуется, так как оно заведомо верно (раз не подошли другие).

Существует также метод усеченного перебора, который сохраняет логику предыдущего метода с той разницей, что перебираются не все возможные

ключи, а некоторое усеченное их подмножество.

О простоте и делимости

Простое число – натуральное число, имеющее ровно два различных натуральных делителя – 1 и само себя. Последовательность простых чисел начинается так: 2, 3, 5, 7, 11, 13, 17, 19, …

Существуют разные тесты простоты, например, решето Эратосфена, тест Миллера, вероятностный тест Ферма.

Основная теорема арифметики утверждает, что каждое натуральное число, большее единицы, представимо, причём единственным способом, в виде произведения простых чисел.

Наибольшим общим делителем двух целых чисел A и B называется наибольший из их общих делителей: $\text{НОД}(A, B)$.

Если $\text{НОД}(A, B) = 1$, то числа A и B называются взаимно простыми.

Наименьшее общее кратное двух целых чисел A и B – это наименьшее натуральное число, которое делится на A и B без остатка: $\text{НОК}(A, B)$.

Для нахождения $\text{НОД}(A, B)$ существует множество алгоритмов, мы приведём здесь классический алгоритм Евклида:

Пусть A и B – целые числа, не равные одновременно нулю. Без потери общности положим, $A > B$ (ели числа равны, то задача поиска общего делителя вырождается). Определим последовательность чисел

$$A > B > r_1 > r_2 > \ldots > r_n$$

следующим образом r_k – это остаток от деления предпредыдущего числа на предыдущее, а предпоследнее делится на последнее нацело, то есть:

$A = Bq_0 + r_1,$
$B = r_1 q_1 + r_2,$
$r_1 = r_2 q_2 + r_3,$
...
$r_{n-2} = r_{n-1} q_{n-1} + r_n,$
$r_{n-1} = r_n q_n.$

Тогда $\text{НОД}(A, B) = r_n$ (есть последний ненулевой член этой последовательности).

Об алгебре в кольцах вычетов

Полная система вычетов по модулю m – это набор из m попарно несравнимых по модулю m целых чисел. Будем полагать в качестве полной системы вычетов по модулю m множество наименьшие неотрицательных вычетов, то есть числа:

$$Z_m = \{0,\ 1,\ 2,\ \ldots,\ m - 1\}$$

Для того чтобы в алгебраических операциях система оставалась замкнутой, прибегают к оператору mod: $a\ mod\ m$ – который возвращает неотрицательный остаток от деления на m. Результат операции по модулю всегда целое число между 0 и $m - 1$. Можно сказать, что операция по модулю создает набор чисел, который в модульной арифметике можно понимать как систему наименьших вычетов по модулю m, или Z_m.

Три бинарные операции: сложение, вычитание и умножение – трансформируется в операции в кольце вычетов тривиально. После выполнения операции нужно привести результат в кольцо с помощью оператора mod.

Деление в кольце – более сложная операция. Для ее выполнения необходимо найти мультипликативно обратный элемент кольца. Определим в кольце Z_m элемент x мультипликативно обратным элементом для другого элемента кольца y, если справедливо сравнение:

$$x \cdot y \equiv 1\ mod\ m$$

Если модуль маленький, мультипликативно обратные элементы можно найти устно по определению (перебирая элементы кольца), пока в произведении не получится 1. Сразу упомянем, что перебирать 0 и 1 нет смысла, так как они не могут быть мультипликативно обратными элементами для других элементов кольца, так как умножение на 0 всегда даст 0, умножение на 1 всегда оставит то же число, поэтому 1 мультипликативно обратный элемент только самой себя.

Для больших колец рекомендуется прибегать к расширенному алгоритму Евклида (который рассмотрен в следующем пункте). Предварительно нужно

переформулировать определение, указанное выше, в диофантово уравнение. Итак, следующие записи эквиваленты:

$$x \cdot y \equiv 1 \ mod \ m \qquad\qquad x \cdot y + m \cdot t = 1$$

В результате решения диофантова уравнения относительно переменных x и t (из условия y и m будут известны), найденное наименьшее положительное значение x и будет искомым мультипликативно обратным элементом для y в Z_m.

О диофантовых уравнениях

Линейное диофантово уравнение с двумя неизвестными имеет вид:

$$A \cdot x + B \cdot y = C$$

где A, B, C – заданные целые числа, x и y – неизвестные целые числа. Задача формулируется так: «найти все пары целых x и y, обращающих предложенное выражение в тождество».

При $A = B = 0$ уравнение вырождается. В таком случае при $C = 0$ решений будет бесконечное множество, потому что любые целые x и y подойдут в качестве решения. Если $C \neq 0$ решений нет вовсе, потому что никакие целые x и y не дадут верного равенства.

Критерий разрешимости диофантова уравнения: $C \mid \text{НОД}(A, B)$.

Если уравнение разрешимо, то одно частное решение можно найти с помощью расширенного алгоритма Евклида. Затем по нему записать общее

параметрическое решение.

Алгоритм решения невырожденного диофантова уравнения:

1. Проверить разрешимость по указанному критерию. Если уравнение неразрешимо, ответ – решений в целых числах нет. Дальнейшие шаги применять к разрешимым уравнениям;
2. Сократить уравнение при возможности (если $\text{НОД}(A, B) > 1$, то следует сократить все коэффициенты на $\text{НОД}(A, B)$). В результате получаем:

$$A_1 \cdot x + B_1 \cdot y = C_1$$

3. Расширенный алгоритм Евклида:
   a. Прямой ход алгоритма Евклида – определить последовательность остатков, как было указано в пункте о делимости для чисел A_1, B_1. В разложении остановиться, как только будет получена 1 в качестве остатка;
   b. Выражение остатков – выразить полученные остатки в строках, не применяя вычислений;
   c. Обратных ход алгоритма Евклида – последовательно подставлять остатки и приводить подобные слагаемые, начиная с последнего.
4. Приведение полученных результатов к виду задания. Если после сокращения правая часть диофантова уравнения $C_1 = 1$, то данный шаг можно опустить, так как полученное финальное выражение будет соответствовать виду задания. В противном случае нужно домножить все полученное выражение на C_1, тогда результат примет вид:

$$A_1 \cdot x_0 + B_1 \cdot y_0 = C_1$$

5. Нахождение частного ответа (x_0, y_0) проводится тривиальным сопоставлением полученного выражения с диофантовым уравнением после сокращения. Все несоответствующие знаки должны относиться к частному решению.
6. Параметрическое описание всех решений уравнения записывается так:

$$x = x_0 + B_1 \cdot t,\ \ y = y_0 - A_1 \cdot t,\ \ t \in Z$$

Для контроля знаков рекомендуется проверка:

$$A_1 \cdot x + B_1 \cdot y = A_1 \cdot (x_0 + B_1 \cdot t) + B_1 \cdot (y_0 - A_1 \cdot t) =$$
$$= A_1 \cdot x_0 + A_1 \cdot B_1 \cdot t + B_1 \cdot y_0 - B_1 \cdot A_1 \cdot t = A_1 \cdot x_0 + B_1 \cdot y_0 = C_1$$

О китайской теореме об остатках

Формулировка КТО:

Если натуральные числа $a_1, a_2, \dots, a_n$ попарно взаимно просты, то для любых целых $r_1, r_2, \dots, r_n$ таких, что $0 < r_i < a_i$ при всех $i \in \{1, 2, \dots, n\}$, найдётся число N, которое при делении на a_i даёт остаток r_i при всех $i \in \{1, 2, \dots, n\}$.

Примером задачи на КТО нам послужит следующая:

Маша хочет купить конфет или шоколада. Для этого у нее есть X рублей. Если она купит 11 шоколадок, то у нее останется 7 рублей, если она купить 23 конфеты, у нее останется 3 рубля. Сколько рублей у нее есть?

Для решения такой задачи можно составить систему (при делении x на 11 в

остатке будет 7 рублей, при делении x на 23 – останется 3):

$$\{x \equiv 7\ mod\ 11\ x \equiv 3\ mod\ 23$$

Решение систем сравнений можно проводить разными способами. Мы приведём здесь решение, основанное на КТО. Сразу опишем алгоритм:

1 шаг: модуль решения

$$m = a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

2 шаг: частные модули для всех $i \in \{1, 2, \ldots, n\}$

$$m_i = \frac{m}{a_i}$$

3 шаг: мультипликативно обратные частным модулям для всех $i \in \{1, 2, \ldots, n\}$

$$m_i^{-1}\ mod\ a_i$$

4 шаг: ответ системы

$$x \equiv r_i \cdot m_i \cdot m_i^{-1} + r_2 \cdot m_2 \cdot m_2^{-1} + \ldots + r_n \cdot m_n \cdot m_n^{-1}\ mod\ m$$

О квадратичных сравнениях

Квадратичное сравнение решается по формулам в случае простых модулей и с помощью КТО в случае составного модуля. Тогда нужно декомпозировать сравнение в систему с взаимно простыми модулями, решить сравнения по этим модулям и затем перебрать все возможны решения систем по КТО.

Решение квадратичных сравнений в кольце вычетов простого модуля следует начинать с проверки его разрешимости. Для этого существует критерий Эйлера:

Квадратичное сравнение $x^2 \equiv a \, mod \, p$ разрешимо, если $a^{\frac{p-1}{2}} \, mod \, p \equiv 1$ ($p > 2$).

Для нахождения ответов можно прибегнуть к простому переборе всех элементов кольца (что допустимо, для маленьких модулей), однако в общем случае есть три формулы, которые позволяют, хотя и не всегда, найти решение разрешимого квадратичного сравнения $x^2 \equiv a \, mod \, p$. Эти случаи зависят от модуля.

Если модуль сравнения $p \equiv 3 \, mod \, 4$, то два решения находятся по формуле:

$$x \equiv \pm a^{\frac{p+1}{4}} \, mod \, p$$

Если модуль сравнения $p \equiv 5 \, mod \, 8$, то два решения находятся по более сложным формулам:

- при $a^{\frac{p-1}{4}} \equiv 1 \, mod \, p$ два решения находится по формуле

$$x = \pm a^{\frac{p+3}{8}} \, mod \, p$$

- при $a^{\frac{p-1}{4}} \equiv -1 \, mod \, p$ два решения находится по формуле

$$x = \pm 2a(4a)^{\frac{p-5}{8}} \, mod \, p$$

В данных вариантах не рассматриваются четные модули. Дело в том, что для такого решения модуль квадратичного сравнения должен быть строго простым числом, а как известно, четное простое число единственное – это 2. В данном модуле решения тривиальны, так как в кольце вычетов из двух элементов есть только 0 и 1, и их квадраты совпадают с ними же. Соответственно квадратичные

сравнения по модулю два всегда разрешимы и имеют ровно одно решение.

Теперь остались только те простые числа, которые при делении на 8 дают остаток 1, но именно для таких чисел простой алгоритм решения неизвестен. Поэтому в этих случаях можно прибегнуть к простому перебору для небольших модулей.

Об IP-адресации

IP-адрес четвертой версии протокола состоит из 32 бит, которые принято делить на четыре блока – октета. Маска подсети – это битовая маска для определения по IP-адресу адреса подсети и адреса узла этой подсети. Она формируется так: подряд ставится $32 - n$ единиц, а затем n нулей. Тогда в IP-адресе $32 - n$ первых позиций определят адрес сети (оставшиеся позиции надо заполнить нулями). Адрес сети получается в результате поразрядной конъюнкции к IP адреса узла и маски.

Есть два особых адреса подсети, которые резервируются и не используются на общих основаниях. Это адрес подсети (последние n позиций адреса заменяются нулями) и широковещательный адрес (последние n позиций заменяются единицами). Поэтому, чтобы определить количество доступных адресов для устройств этой подсети, нужно от всех возможных адресов, которые можно записать таким количеством бит, отнять 2 адреса. То есть количество доступных адресов определяется по формуле:

$$2^n - 2.$$

Решение демонстрационного варианта

Рассмотрим решение демонстрационного варианта конкурсных материалов.

Задача 1. Системы счисления

Сколько существует натуральных значений $x \geq 2$, при которых справедливо тождество:

$$101_x = A25_{x-1} ?$$

Здесь нижний индекс указывает на основание системы счисления. A – цифра системы счисления.

A. Одно

B. Два

C. Ни одного

Решение

Переведем правую и левую части предложенного выражения в десятичную систему счисления:

$$101_x = 1 \cdot x^2 + 0 \cdot x + 1$$

$$A25_{x-1} = 10 \cdot (x-1)^2 + 2 \cdot (x-1) + 5$$

Остается решить полученное уравнение:

$$x^2 + 1 = 10x^2 - 18x + 13,$$

$$3x^2 - 6x + 4 = 0,$$

$$D = 36 - 4 \cdot 3 \cdot 4 < 0.$$

Решений нет, значит нет таких значений.

Ответ: C

Задача 2. Алгебра логики

Какая функция из предложенных вариантов тождественна выражению:

$$(a \vee \neg b) \rightarrow c?$$

A. $(a \vee b \vee c)\,(\neg a \vee b \vee c)\,(\neg a \vee \neg b \vee c)$

B. $(a \vee b \vee c)\,(\neg a \vee b \vee c)\,(a \vee \neg b \vee \neg c)$

C. $(a \vee b \vee c)\,(a \vee \neg b \vee c)\,(\neg a \vee b \vee \neg c)$

Решение

Преобразуем логическую формулу, опираясь на свойства логических операций:

$(a \vee \neg b) \rightarrow c = \neg (a \vee \neg b) \vee c = \neg a \wedge b \vee c.$

Преобразуем логическое выражение первого пункта ответов, используя распределительный закон $(a \vee b) \wedge (a \vee c) = a \vee b \wedge c$:

$(a \vee b \vee c)\,(\neg a \vee b \vee c)\,(\neg a \vee \neg b \vee c) = ((b \vee c) \vee a \wedge \neg a)\,(\neg a \vee \neg b \vee c).$

В полученном выражении присутствует слагаемое: $a \wedge \neg a = 0$.

Далее применим распределительный закон еще раз:

$(b \vee c)\,(\neg a \vee \neg b \vee c) = c \vee b \wedge (\neg a \vee \neg b) = c \vee b \wedge \neg a \vee b \wedge \neg b = c \vee b \wedge \neg a \vee b.$

Получаем тождественное выражение.

Ответ: A

Задача 3. Комбинаторика

Известно, что в качестве пароля используется трёхзначная троичная комбинация $x_1 x_2 x_3$, которая обладает следующим свойством:

$x_1 = (x_2 + x_3) \, mod \, 3$. Сколько паролей в худшем случае придётся перебрать для определения правильного?

Операция T mod P возвращает неотрицательный остаток от деления T на P.

A. 8

B. 12

C. 27

Решение

Задача сводится к определению всех возможных комбинаций, подходящих под описанное условие.

Из трех позиций пароля первая фиксирует значение по двум другим позициям. Она однозначно ими определяется. А вот x_2 и x_3 могут быть любыми допустимыми (т.е. любым значением троичной системы счисления). Получается всех возможных подходящих комбинаций можно рассчитать по формуле выбора *k* элементов из *n* с возвращением:

$$n^k = 3^2 = 9.$$

Всех возможных паролей, подходящих под описанное условие – 9, значит в худшем случае нужно будет перебрать 8 из них.

Ответ: A

Задача 4. Основы теории информации

Дано сообщение: «Одновременно подкинули два одинаковых игральных кубика. На втором выпала грань с чётным значением». Используя формулу Шеннона, определите, сколько бит информации оно несёт?

A. 0

B. 1

C. 2

Решение

Задача сводится к определению вероятности описанного в условии события.

Игральные кубики неотличимы, поэтому речь в задаче идет о такой ситуации: «На игральном кубике выпала четная грань» (про первый – никакой информации, кроме его существования не дано).

Благоприятных событий – три: «выпало 2», «выпало 4» и «выпало 6». Всех возможных событий – шесть. Вероятность описанного события

$$p = \frac{3}{6} = \frac{1}{2}.$$

Даже если учитывать существование второго кубика, раз нам неизвестно ничего о выпавшем значении, вероятность будет рассчитана так

$$p = \frac{3 \cdot 6}{6^2} = \frac{1}{2}.$$

В случае независимых событий действует принцип умножения. На каждое четное значение второго кубика может выпасть любое из шести значений первого кубика – так формируется числитель $3 \cdot 6$. В случае всех возможных событий используется тот же принцип (на любое из 6 значений первого кубика выпало любое из 6 значений второго кубика).

Итак, зная вероятность события, можем рассчитать количество информации:

$$H = \lceil \frac{1}{p} \rceil = \lceil 2 \rceil = 1.$$

Ответ: В

Задача 5. Основы криптографии

Какой шифртекст получится в результате применения перестановки 3-4-1-5-2 к слову ШИФРОВАНИЕ?

A. ОВАНШИИЕФР

B. ФРШОИНИВЕА

C. ФРШОИВАНИЕ

Решение

Шифр перестановки, предложенный в данном задании, относится к классу блочной перестановки по схеме. Предлагается переставить 5 элементов, значит открытый текст надо разбить на блоки по 5 элементов и повторить для каждого из них указанную перестановку.

1 блок

1	2	3	4	5
Ш	И	Ф	Р	О

3	4	1	5	2
Ф	Р	Ш	О	И

2 блок

1	2	3	4	5
В	А	Н	И	Е

3	4	1	5	2
Н	И	В	Е	А

Значит шифртекст по данной задаче: ФРШОИНИВЕА.

Ответ: В

Задача 6. Основы криптоанализа

Известно, что для шифрования слова на русском языке был выбран такой шифр (ключ k неизвестен):

- буквы слова заменены на их порядковые номера в алфавите по схеме

Буква	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
Замена	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	32	33

- затем каждый такой номер n подвергли преобразованию до числа $m = 1 + (n - 1 + k)\, mod\, 33$;

- каждое полученное на предыдущем этапе число m вновь заменили по схеме из первого этапа.

В результате получилось следующее: ЬМШФТЁДСМИ. В ответе укажите

примененный ключ k.

Операция T mod P возвращает неотрицательный остаток от деления T на P.

A. 13
B. 7
C. 4

Решение

Описанный в задании алгоритм соответствует шифру сдвига на k. Для решения удобнее всего перебрать три предложенных в ответе ключа и определить при расшифровке, который из них дает осмысленный открытый текст. Сразу опустим первое и третье действие (они обратны друг другу). Три возможных таблицы замены представлены ниже

Вариант A – сдвиг на 13.

Буква	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
Замена	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

По этой таблице указанный шифртекст расшифровывается, как ПАЛЗЁ… Текст не получается осмысленным.

Вариант B – сдвиг на 7.

Буква	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
Замена	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	А	Б	В	Г	Д	Е	Ё

По этой таблице указанный шифртекст расшифровывается, как ХЁСН… Текст не получается осмысленным.

Вариант C – сдвиг на 4.

Буква	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
Замена	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	А	Б	В	Г

По этой таблице указанный шифртекст расшифровывается, как ШИФРОВАНИЕ.

Ответ: C

Задача 7. Алгебра в кольцах вычетов

Чему равно значение следующего выражения в кольце вычетов $\mathbb{Z}_{23}$:

$$(10 + 7 \cdot 22) / 6 ?$$

A. 7
B. 12
C. 19

Решение

В указанном кольце вычетов справедливо: $22 \equiv -1$, так как

$$-1 \equiv n - 1 \; mod \; n.$$

Тогда числитель преобразуется так: $10 + 7 \cdot 22 \equiv 10 + 7 \cdot (-1) \equiv 3$.

Теперь числитель и знаменатель можно сократить, однако всё-таки не нацело. Придется прибегнуть к поиску мультипликативно обратного элемента в кольце вычетов. Предложим ниже поиск по расширенному алгоритму Евклида.

Пусть $x -$ мультипликативно обратный элемент к 2. По определению $x \cdot 2 \equiv 1 \; mod \; 23$. Это выражение соответствует следующему диофантову уравнению:

$x \cdot 2 + 23 \cdot y = 1.$

1 шаг: прямой ход алгоритма Евклида

$23 = 2 \cdot 11 + 1$

2 шаг: выражение остатков

$1 = 23 - 2 \cdot 11$

3 шаг: обратный ход алгоритма Евклида (вырожден для разложения в одну строку) – сопоставим с заданным уравнением

$-11 \cdot 2 + 23 \cdot 1 = 1,$

$x \cdot 2 + 23 \cdot y = 1.$

Значит, $x = -11$. В кольце вычетов это соответствует $x \equiv 12 \ mod \ 23$.

Теперь выполним деление:

$$\frac{10 + 7 \cdot 22}{6} \equiv \frac{3}{6} \equiv \frac{1}{2} \equiv 1 \cdot 2^{-1} \equiv 1 \cdot 12 = 12 \ mod \ 23$$

Ответ: B

Задача 8. Диофантовы уравнения

Сколько существует целочисленных решений уравнения $13x - 18y = 2$ вида (x, y), у которых x – положительное двузначное число?

A. 5
B. 7
C. 8

Решение

Предложим поиск частного ответа на уравнение по расширенному алгоритму Евклида.

1 шаг: прямой ход алгоритма Евклида

$18 = 13 \cdot 1 + 5$
$13 = 5 \cdot 2 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$

2 шаг: выражение остатков

$5 = 18 - 13$
$3 = 13 - 5 \cdot 2$
$2 = 5 - 3$
$1 = 3 - 2$

3 шаг: обратный ход алгоритма Евклида

$1 = 3 - 2 = 3 - (5 - 3) = 3 \cdot 2 - 5 = (13 - 5 \cdot 2) \cdot 2 - 5 = 13 \cdot 2 - 5 \cdot 5 =$
$= 13 \cdot 2 - 5 \cdot (18 - 13) = 13 \cdot 7 - 18 \cdot 5$

Сопоставим с заданным уравнением

$13 \cdot 7 - 18 \cdot 5 = 1$, домножим на 2, сохраняя 13 и 18.

$13 \cdot 14 - 18 \cdot 10 = 2$
$13 \cdot x - 18 \cdot y = 2.$

Значит, частное решение $x_0 = 14,\ y_0 = 10.$

Все решения описываются выражением:

$$x = 14 + 18 \cdot t,\ \ y = 10 + 13 \cdot t,\ \ t \in Z.$$

Теперь оценим количество решений, подходящих под условие задачи. Для этого нужно решить неравенство: $9 < x < 100$.

$9 < 14 + 18 \cdot t < 100,$
$-5 < 18 \cdot t < 86,$
$-5/18 < t < 43/9 = 4\frac{7}{9},$

Поскольку $t \in Z$, в указанном диапазоне находится 5 целых чисел: 0, 1, 2, 3, 4.

Ответ: A

Задача 9. Китайская теорема об остатках

Решите систему сравнений и найдите наименьшие положительные *x* и *y*. В ответе укажите их сумму.

$$\{x \equiv 2\ mod\ 3\ x \equiv 3\ mod\ 7\ \ y \equiv 4\ mod\ 7\ y \equiv 0\ mod\ 5$$

Операция T mod P возвращает неотрицательный остаток от деления T на P.

A. 37
B. 42
C. 51

Решение

Разобьём систему на две (по переменным):

$\{x \equiv 2 \ mod \ 3 \ x \equiv 3 \ mod \ 7$ $\{y \equiv 0 \ mod \ 5 \ y \equiv 4 \ mod \ 7$

Используя китайскую теорему об остатках, решим эти системы.

1 шаг: модуль решения

$m = 3 \cdot 7 = 21$ $m = 5 \cdot 7 = 35$

2 шаг: частные модули

$m_1 = 21 : 3 = 7$ $m_1 = 35 : 5 = 7$

$m_2 = 21 : 7 = 3$ $m_2 = 35 : 7 = 5$

3 шаг: мультипликативно обратные частным модулям

$m_1^{-1} \ mod \ 3 \equiv 7^{-1} \ mod \ 3 \equiv 1$ $m_1^{-1} \ mod \ 5 \equiv 7^{-1} \ mod \ 5 \equiv \equiv 2^{-1} \ mod \ 5 \equiv 3$

$m_2^{-1} \ mod \ 7 \equiv 3^{-1} \ mod \ 7 \equiv 5$ $m_2^{-1} \ mod \ 7 \equiv 5^{-1} \ mod \ 7 \equiv 3$

4 шаг: ответ системы

$x \equiv 2 \cdot 7 \cdot 1 + 3 \cdot 3 \cdot 5 \ mod \ 21 \equiv \equiv 14 + 45 \ m$ $y \equiv 0 \cdot 7 \cdot 3 + 4 \cdot 5 \cdot 3 \ mod \ 35 \equiv \equiv 0 + 60 \ mod \ 35 \equiv$

Сумма наименьших положительных ответов системы: $17 + 25 = 42$

Ответ: B

Задача 10. Квадратичные сравнения в кольцах вычетов

Сколько решений есть у квадратичного сравнения: $5x^2 \equiv 3 \; mod \; 14$?

Операция T mod P – возвращает неотрицательный остаток от деления T на P.

A. 1
B. 2
C. 4

Решение

Решим полученное квадратичное сравнение. Для этого нужно сделать два действия – избавиться от коэффициента перед переменной, решить квадратичного сравнение (в данном пособии будет приведено решение с помощью китайской теореме об остатках).

Первое действие. Для этого необходимо найти мультипликативно обратный элемент для 5 в кольце Z_{14}. Используем для этого расширенный алгоритм Евклида.

Пусть $x -$ мультипликативно обратный элемент к 5. По определению $x \cdot 5 \equiv 1 \; mod \; 14$. Это выражение соответствует следующему диофантову уравнению:

$x \cdot 5 + 14 \cdot y = 1.$

1 шаг: прямой ход алгоритма Евклида

$14 = 5 \cdot 2 + 4$
$5 = 4 \cdot 1 + 1$

2 шаг: выражение остатков

$4 = 14 - 5 \cdot 2$
$1 = 5 - 4$

3 шаг: обратный ход алгоритма Евклида

$1 = 5 - 4 = 5 - (14 - 5 \cdot 2) = 5 \cdot 3 - 14$

Сопоставим с заданным уравнением

$3 \cdot 5 + 14 \cdot (-1) = 1$
$x \cdot 5 + 14 \cdot y = 1.$

Значит, $x = 3$. Теперь выполним деление:

$$5x^2 \equiv 3 \ mod \ 14,$$
$$5 \cdot 3 \cdot x^2 \equiv 3 \cdot 3 \ mod \ 14,$$
$$x^2 \equiv 9 \ mod \ 14,$$

Второе действие. Проверять на разрешимость полученное квадратичное сравнение нет смысла. Во-первых, в предложенных вариантах решений нет такого ответа, что подразумевает, что хотя бы один ответ точно будет. Во-вторых, в правой части сравнения стоит 9, что является полным квадратом, то есть два решения (3 и -3) тривиально находятся сразу. Тем не менее опишем ниже полное решение для любого возможного случая.

Прибегнем к декомпозиции полученного квадратичного сравнения в систему сравнений с простыми модулями. Модуль 14 раскладывается в произведение 2 и 7. Значит наше квадратичное сравнение соответствует системе:

$$\{x^2 \equiv 9 \ mod \ 2 \ x^2 \equiv 9 \ mod \ 7$$

Приведём полученные сравнения в соответствии с модулями на строках:

$$\{x^2 \equiv 1 \ mod \ 2 \ x^2 \equiv 2 \ mod \ 7$$

Первое сравнение имеет один ответ. Второе квадратичное сравнение имеет либо два ответа, либо ни одного. Проверим его разрешимость с помощью критерия Эйлера:

$$2^{\frac{7-1}{2}} \ mod \ 7 \equiv 2^3 \ mod \ 7 \equiv 8 \ mod \ 7 \equiv 1$$

Согласно критерию Эйлера, можно сделать вывод, что 2 является квадратичным вычетом в кольце из 7 элементов.

Так как $p = 7 \equiv 3 \ mod \ 4$, решение найдем по формуле

$$x \equiv \pm 2^{\frac{7+1}{4}} \ mod \ 7 \equiv \pm 2^2 \ mod \ 7 \equiv \pm 4 \ mod \ 7$$

Теперь у нас есть следующая система:

$$\{x \equiv 1 \ mod \ 2 \ [x \equiv 3 \ mod \ 7 \ x \equiv 4 \ mod \ 7$$

И решения найдутся после решения двух систем:

$\{x \equiv 1 \ mod \ 2 \ x \equiv 3 \ mod \ 7$ $\{x \equiv 1 \ mod \ 2 \ x \equiv 4 \ mod \ 7$

В результате получаем два решения 3 и 11 в кольце Z_{14}.

Ответ: В

Задача 11. Основы теории информации

Дано сообщение: «Подкинули три игральных кубика. На одном выпала грань с чётным значением, на двух других выпали грани одинаковой чётности». Используя формулу Шеннона, определите, сколько бит информации оно несёт? В ответе укажите целое число бит.

Решение

Задача сводится к определению вероятности описанного в условии события.

Речь в задаче идет о такой ситуации: «Подкинули три игральных кубика. На одном выпала грань с чётным значением, на двух других выпали грани одинаковой чётности». Игральные кубики неотличимы, поэтому речь в задаче идет не о «первом, втором и третьем» кубиках.

Заранее заметим, что любой кубик может выпасть на четную (или нечетную) грань с вероятностью 1/2.

Решение, может быть оформлено двумя способами, с расчетом вероятности по свойствам или с использованием определения вероятности через перебор всех исходов в поиске благоприятных. Приведём два решения.

1 способ. Возможны случаи:

- все три кубика выпали на четные грани. Так как эти исходы не зависят друг от друга, общую вероятность рассчитываем через умножение:

$$p_1 = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}.$$

- один из трех кубиков (любой) выпал четным, два других – на нечетные грани: первый из описанных можно выбрать тремя способами (любой и трех кубиков), два других (неотличимых кубика) выпадут на нечетные грани с вероятностью $1/2 \cdot 1/2 = 1/4$. Общая вероятность описанного случая:

$$p_2 = 3 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}.$$

Вероятность описанного в задаче события (считаем теперь через сложение, так как могло произойти ИЛИ один описанный случай, ИЛИ второй)

$$p = \frac{1}{8} + \frac{3}{8} = \frac{1}{2}.$$

2 способ. Перебор четности (см. таблицу).

один	**другой**	**третий**	**Исход подходит по условию задачи**
0	0	0	ДА
0	0	1	
0	1	0	
0	1	1	ДА
1	0	0	
1	0	1	ДА
1	1	0	ДА
1	1	1	

Пусть 0 – четная грань, 1 – нечетная грань.

Переберём все возможные случаи, отдельно выделяя подходящие.

Из восьми вариантов подходят под условие 4, а всего возможных исходов 8, значит вероятность описанных событий

$$p = \frac{4}{8} = \frac{1}{2}.$$

Итак, зная вероятность события, можем рассчитать количество информации:

$$H = \lceil \frac{1}{p} \rceil = \lceil 2 \rceil = 1.$$

Ответ: 1

Задача 12. Основы криптографии

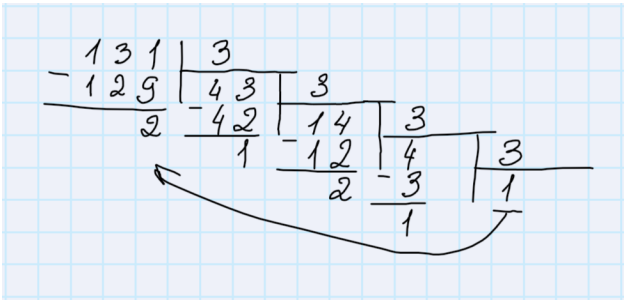
Зашифруйте число 131, проведя следующие манипуляции:

- Перевод в троичную систему счисления;
- Перестановка: 2-5-4-1-3.

Решение

Выполним шаги алгоритма, описанного в условии задачи.

Переведем число 131 в троичную систему счисления:



$$131_{10} \rightarrow 11212_3$$

Выполним перестановку полученных цифр.

1	2	3	4	5
1	1	2	1	2

2	5	4	1	3
1	2	1	1	2

Значит, шифртекст по данной задаче: 12112.

Ответ: 12112

Задача 13. Основы криптоанализа

Известно, что используется криптосистема RSA, однако секреты были выбраны слабые. В результате опубликован открытый ключ $e = 17$ и модуль $m = 77$. В ответе укажите значение закрытого ключа системы d.

Решение

Вообще задача взлома криптосистемы RSA – сложная математическая задача факторизации. Но если секреты выбраны слабыми, то факторизация будет тривиальной. В данном задании $m = 77 = 7 \cdot 11$. Значит далее остается посчитать закрытый ключ по алгоритму.

Задачу свели к поиску мультипликативно обратного элемента к $e = 17$ в кольце из $\varphi(m) = (p - 1) \cdot (q - 1) = 6 \cdot 10 = 60$, то есть $d \equiv 17^{-1} \, mod \, 60$. Прибегнем к диофантову уравнению

$$17 \cdot d + 60 \cdot y = 1$$

1 шаг: прямой ход алгоритма Евклида

$$60 = 17 \cdot 3 + 9$$
$$17 = 9 \cdot 1 + 8$$
$$9 = 8 \cdot 1 + 1$$

2 шаг: выражение остатков

$9 = 60 - 17 \cdot 3$
$8 = 17 - 9$
$1 = 9 - 8$

3 шаг: обратный ход алгоритма Евклида

$$1 = 9 - 8 = 9 - (17 - 9) = 9 \cdot 2 - 17 = (60 - 17 \cdot 3) \cdot 2 - 17 = 60 \cdot 2 - 17 \cdot 7$$

Сопоставим с заданным уравнением

$17 \cdot (-7) + 60 \cdot 2 = 1$
$17 \cdot d + 60 \cdot y = 1$

Значит, $d \equiv -7 \; mod \; 60 \equiv 53 \; mod \; 60$.

Ответ: 53

Задача 14. Понятие делимости, простых чисел, НОД, НОК

В ответе укажите наибольший общий делитель чисел 1890 и 5712.

Решение

Выполним алгоритм Евклида:

$5712 = 1890 \cdot 3 + 42$
$1890 = 42 \cdot 45$

Другим вариантом решения может стать факторизация предложенных чисел и составление из их общих простых делителей наибольшего. Факторизация возможна, благодаря специально подобранным числам, на которых очевидна кратность маленьким простым: 2, 3 и 5. Итак

$5712 = 2^4 \cdot 357 = 2^4 \cdot 3 \cdot 119 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 17$
$1890 = 2 \cdot 945 = 2 \cdot 3^3 \cdot 35 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7$

Общие делители для этих чисел – 2, 3, 7. Значит,

$$\text{НОД}(5712,\ 1890) = 2{\cdot}3{\cdot}7 = 42.$$

Ответ: 42

Задача 15. IP-адресация

В ответе укажите количество хостов, на которые рассчитана подсеть с маской 255.255.248.0.

Решение

Рассмотри двоичное представление маски:

255.255.248.0 11111111.11111111.11111000.00000000

В ней 11 нулей в конце. Значит, количество устройств, которые можно связать этой подсетью:

$$2^{11} - 2 = 2\,046.$$

Ответ: 2046

Список литературы

1. Информатика. 10 класс. Базовый и углубленный уровни: учебник: в 2 ч. Ч. 1. ФГОС / К. Ю. Поляков, Е. А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2018. – 352 с.: ил.
2. Информатика. 10 класс. Базовый и углубленный уровни: учебник: в 2 ч. Ч. 2. ФГОС / К. Ю. Поляков, Е. А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2018. – 352 с.: ил.
3. Гашков С.Б. Системы счисления и их применение. – М.: МЦНМО, 2004. — 52 с.
4. Златопольский Д.М. Занимательная информатика. – М.: Бином. Лаборатория знаний, 2011. – 424 с.
5. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2018. — 473 с. — (Высшее образование). — ISBN 978-5-534-01530-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/413075 (дата обращения: 27.03.2020).
6. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учебное пособие для магистратуры / О. М. Замятина. — Москва : Издательство Юрайт, 2019. — 159 с. — (Университеты России). — ISBN 978-5-534-00335-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433938 (дата обращения: 27.03.2020).