



10 класс XXX Межрегиональная олимпиада школьников им.
И.Я. Верченко по математике и криптографии

1 вариант

1. Найдите наибольшее четырёхзначное число, которое в 198 раз больше суммы своих цифр. Решение обоснуйте.

Решение: Обозначим x – искомое число, s – сумма его цифр. Тогда $x = 198 \cdot s$. Следовательно, x делится нацело на 9. По признаку делимости на 9, число s делится на 9. Так как искомое число четырёхзначное, то для s возможны 4 варианта: $s = 9, s = 18, s = 27, s = 36$. Для каждого s , соответственно, находим: $x = 1782, x = 3564, x = 5346, x = 7128$.

Подходящее: $x = 3564$.

Ответ: 3564.

2. На координатной прямой отмечены 5 точек с координатами 2; 25; -5; 8; 9. Найдите координату точки, сумма расстояний от которой до указанных 5 точек минимальна. Ответ обоснуйте.

Решение: Расположим числа в порядке возрастания: -5; 2; 8; 9; 25. Покажем, что выделенное среднее число 8 является искомым. Обозначим $s(y)$ - сумма расстояний от числа y до остальных чисел. Рассмотрим число $y = 8 + x$. Если $x \in (0; 1)$, то сумма расстояний от y до первых четырех чисел увеличится на $2x$, а до последних четырех – уменьшится на $2x$ (по сравнению с числом 8), и при этом до самого числа 8 расстояние равно x , то есть $s(y) = s(8) + x$. Если $x = 1$, то есть $y = 9$, то сумма расстояний от y до всех чисел будет равна $s + 1$. Рассуждая аналогично при $x \in (1; +\infty)$, получим вывод: минимальное значение $s(y)$ достигается при $y = 8$. При отрицательных значениях x рассуждения ничем не отличаются.

Ответ: 8.

3. Ключом шифрсистемы служит таблица 4×4 , в каждую ячейку которой записана одна из цифр 0, 1, 2. При этом должны делиться на 3 сумма цифр в каждой строке, сумма цифр в каждом столбце, а также суммы цифр на каждой из двух диагоналей, отмеченных пунктиром. На рисунке приведен один из возможных вариантов ключа. Сколько существует всего различных ключей?

1	1	2	2
2	1	1	2
0	0	1	2
0	1	2	0

Решение: Указанную в условии таблицу 4×4 , можно построить следующим образом: положим элементы верхнего левого угла размеров 3×3 , произвольным образом, после чего заметим, что все оставшиеся элементы определяются однозначно из линейных (по модулю 3) соотношений для строк и столбцов (при этом элемент в правом нижнем углу будет равен сумме по модулю 3 всех остальных элементов квадрата). Плюс к этому имеем два линейных соотношения для элементов диагоналей. Таким образом, общее число независимого выбора переменных $a_{i,j}, i, j = 1, 2, 3$ равно 7. Следовательно, общее число ключей равно $3^7 = 2187$.

Ответ: 2187.

4. На границе Криптоландии установлена пропускная система, имеющая 17 входов и 17 выходов (входы перед границей, выходы – уже в Криптоландии). Входы и выходы занумерованы независимо друг от друга числами от 1 до 17, причем в неизвестном для посетителей Криптоландии порядке. От каждого входа проложен один «прямой» туннель к одному из выходов, причем от разных входов – к разным выходам. От каждого выхода

проложен один «обратный» туннель ко входу с тем же номером, что у этого выхода. Посетитель сам выбирает один из входов. Войдя в него, он попадает в лифт, в котором есть 2 кнопки: зеленая – «ехать», красная – «выходить». Система работает следующим образом. Посетитель, находясь в лифте около входа, нажимает зеленую кнопку, лифт по прямому туннелю доставляет его к соответствующему выходу. Находясь в лифте около выхода, посетитель может: 1) нажать зеленую кнопку, и тогда лифт по обратному туннелю доставит его ко входу с тем же номером; 2) нажать красную кнопку, и тогда выход откроется, но только если его номер совпадает с номером того входа, через который посетитель вошел первоначально. В противном случае (при несовпадении номеров) посетитель будет удалён за пределы Криптоландии и сможет воспользоваться правом посещения только через год. Алиса решила провести каникулы в Криптоландии. При этом ей стала известна схема прямых туннелей системы пропуска:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
20	11	10	12	18	1	4	7	17	8	5	19	6	3	13	9	16	2	14	15

Здесь верхнее число является номером входа, а стоящее под ним число – номером того выхода, к которому ведет прямой туннель. За какое минимальное число поездок по туннелям Алиса сможет гарантированно попасть в Криптоландию? Ответ обоснуйте.

Решение: Если для начала движения выбран вход с номером 1, то далее перемещение по циклу 1-20-15-13-6. Для входа с номером 2: 2-11-5-18. Для входа с номером 3: 3-10-8-7-4-12-19-14. Последний цикл 9-17-16. Если бы был известен начальный номер входа, то решение сводилось бы к выбору нужного числа поездок по прямым туннелям из множества чисел $\{5,4,8,3\}$. Но поскольку этот номера неизвестен, то необходимо совершить $\text{НОК}\{5,4,8,3\} = 120$ поездок.

Ответ: 120.

5. Для зашифрования осмысленного слова его буквы заменили числами x_1, x_2, \dots, x_n по таблице. Затем выбирали четные натуральные числа p и q и для каждого числа x_i из соотношений $x_i = y_i + pz_i, z_i = y_i + qx_i$ нашли целые числа y_i и z_i . Потом по формулам $z'_i = r_{32}(z_i), i = 1, \dots, n$ получили числа z'_1, \dots, z'_n (где $r_{32}(a)$ – остаток от деления числа a на 32), которые вновь заменили буквами согласно таблице. В результате получили вот что:

ХСКИЩА. Найдите исходное слово, если известно, что оно начинается на букву **Щ**.

А	Б	В	Г	Д	Е	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

Решение: Рассмотрим произвольную букву открытого и зашифрованного текстов. Для соответствующих им (по таблице) чисел x и z' выполняются равенства $x = y + pz$ и $z = y + qx$, при некотором y, p и q . При этом по условию $z' = r_{32}(z)$. Используя свойство сравнений по модулю целого числа, получим: $x - z' = pz' - qx \pmod{32}$ или $x(1 + q) = z'(1 + p) \pmod{32}$.

Для дальнейшего решения будем пользоваться следующим свойством: если наибольший общий делитель чисел a и n равен 1, то сравнение $x = y \pmod{n}$ равносильно $ax = ay \pmod{n}$. Используя условие задачи для первой буквы открытого и зашифрованного текста, получим равенство $25(1 + q) = 21(1 + p) \pmod{32}$. Заметим, что $21 \cdot 21 = 25 \pmod{32}$. Тогда $25 \cdot 21 \cdot (1 + q) = 21 \cdot 21 \cdot (1 + p) \pmod{32}$, что равносильно равенству $21 \cdot (1 + q) = (1 + p) \pmod{32}$. Значит, $x(1 + q) = 21(1 + p)z' \pmod{32}$. В итоге получаем, что $x = 21z' \pmod{32}$. Остается воспользоваться полученным соотношением для остальных букв. Получится слово **ЩЕТИНА**.

Ответ: ЩЕТИНА.

6. Устройство принимает на вход и выдает на выход наборы из n битов (причем $n \geq 5$). Поданный на вход набор $\mathbf{x} = (x_1, \dots, x_n)$ преобразуется в выходной набор $h(\mathbf{x}) = (x_1 \oplus x_{n-1}, x_2 \oplus x_n, x_2 \oplus x_3, x_3 \oplus x_4, \dots, x_{n-2} \oplus x_{n-1}, x_1 \oplus x_n)$, где \oplus – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$. Подав теперь этот набор $h(\mathbf{x})$ на вход, получим на выходе набор $h(h(\mathbf{x})) = h^{(2)}(\mathbf{x})$, который вновь подадим на вход и получим $h^{(3)}(\mathbf{x})$ и т.д. Докажите, что если все наборы $\mathbf{x}, h(\mathbf{x}), h^{(2)}(\mathbf{x}), \dots, h^{(k)}(\mathbf{x})$ оказались различными, то $k \leq 2^{n-1}$.

Решение: Заметим, что для всех \mathbf{x} вектор $h(\mathbf{x})$ содержит четное число единиц, так как

$$(x_1 \oplus x_{n-1}) \oplus (x_2 \oplus x_n) \oplus (x_2 \oplus x_3) \oplus (x_3 \oplus x_4) \oplus \dots \oplus (x_{n-2} \oplus x_{n-1}) \oplus (x_1 \oplus x_n) = 0.$$

Значит в рассматриваемой последовательности $\mathbf{x}, h(\mathbf{x}), h^{(2)}(\mathbf{x}), \dots, h^{(k)}(\mathbf{x})$ (1) все векторы, начиная со второго, имеют четное количество единиц. Количество всех векторов, имеющих четное количество единиц, равно 2^{n-1} . Поэтому претендентом на самое большое количество различных векторов является последовательность (1), начинающаяся с вектора, содержащего нечетное количество единиц и продолжающаяся всеми векторами с четным количеством единиц. Количество векторов в такой последовательности будет $1 + 2^{n-1}$. Таким образом $k \leq 2^{n-1}$.