Подготовительные задачи Межрегиональной олимпиады школьников по математике и криптографии (по материалам 2008 и 2009 года)

УСЛОВИЯ И РЕШЕНИЯ ЗАДАЧ

Задача 1.

Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Таблица 1

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
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

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей – **р**, четвертой – вновь **м** и $|p-q|=2\,|p-q|\le 100$ т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

мхлщлифцбдюгишсптаивпбьдюолдьуэюыйемхл

Восстановите исходное сообщение и ключевое слово.

Решение задачи 1

Убеждаемся, что шифрованный текст имеет длину 38. Осмысленная фраза имеет тогда длину 19. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв.

в	п	б	ь	д
м	х	л	щ	л
22	27	22	3	25

Если $x_1x_2x_3x_4x_5$ – ключевое слово, то для при первом шифровании использовалось оно само, а при втором – $x_5x_1x_2x_3x_4$. Таким образом, найдены разности: $x_5-x_1=22$, $x_1-x_2=27$, $x_2-x_3=22$, $x_3-x_4=3$, $x_4-x_5=25$. Тогда при известной первой букве x_1 остальные вычисляются по формулам:

$x_5 = x_1 + 22$, $x_4 = x_1 + 14$, $x_3 = x_1 + 17$, $x_2 = x_1 + 6$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: КРЫША. При расшифровании получаем текст:

В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р

Задача 2

Делится ли число $2^{2^{2007}+3^{2008}-2009}-1$ на 1155?

Решение задачи 2

Да, делится. Число вида $2^k - 1$ делится на 3 тогда и только тогда, когда k четно, на 5 – тогда и только тогда, когда k кратно 4, на 7 – тогда и только тогда, когда k кратно 3, а на 11 – тогда и только тогда, когда k кратно 10. Показатель степени $2^{2007} + 3^{2008} - 2009$ делится на 4; он делится на 3, т.к.

$$2^{2007} + 3^{2008} - 2009 = (2^{2007} - 2006) + (3^{2008} - 3) =$$
$$= (2^{2007} - 2 - 2004) + (3^{2008} - 3) = 2 \times (2^{2006} - 1 - 1002) + (3^{2008} - 3),$$

где $2^{2006} - 1 - 1002$ делится на 3. Поэтому в соответствии с первыми тремя критериями N делится на 3, 5 и 7. Числа 3^{2008} и 2^{2007} в десятичной записи оканчиваются на 1 и 8 соответственно, поэтому $2^{2007} + 3^{2008} - 2009$ делится на 10. Таким образом, число $N = 2^{2^{2007}+3^{2008}-2009} - 1$ делится на $3 \times 5 \times 7 \times 11 = 1155$.

Задача 3

На кодовом замке имеется круглый диск с риской. Вокруг диска нанесены числа от 0 до 99 по часовой стрелке. Для управления замком служат две кнопки: “вправо” и “влево”. При нажатии на кнопку “вправо” диск вращается на 43 деления по часовой стрелке, при нажатии на кнопку “влево” – на 20 делений против часовой стрелки. Каждая из этих операций выполняется за 1 секунду. Изначально замок установлен на число 0. Замок открывается при его установке на число 50 – ключ замка.

А. За какое наименьшее время можно открыть замок при данном ключе 50?

Б. Доказать, что замок можно открыть при любом ключе (ключ – число от 1 до 99).

В. За какое наименьшее время можно гарантированно открыть замок при любом ключе?

Решение задачи 3

А. При нажатии u раз на кнопку “вправо” и v раз на кнопку “влево” замок установится на деление с номером $r_{100}(43u - 20v)$, где r_{100} означает остаток от деления на 100. Таким образом, нужно подобрать числа u, v такие, что $r_{100}(43u - 20v)=50$. Далее, понятно, что достаточно подобрать число u, для которого $r_{100}(43u) = 10, 30, 50, 70, 90$, так как после этого замок можно установить на ключ 50, вычитая 20 несколько раз. Будем действовать перебором: 43, 86, 129, 172, 215, 258, 301, 344, 387, 430. Значит 10 вправо, 4 влево, итого *14 секунд*. Как видно из сделанного перебора, меньше чем за 14 секунд не получится.

Б. Продолжим перебор, показывающий, на какие деления можно установить замок только кнопкой “вправо”: 0, 43, 86, 129, 172, 215, 258, 301, 344, 387, 430, 473, 516, 559, 602, 645, 688, 731, 774, 817, 860. Далее кнопкой “влево” можно уменьшать эти числа на 20. Поэтому чтобы можно было открыть замок при любом ключе, достаточно, чтобы среди перечисленных чисел встречались все остатки от деления на 20. Непосредственно видно, что это так. Следовательно, замок можно открыть при любом ключе.

В. Нужно найти u, v такие, что $r_{100}(43u - 05v)=k$, где k – ключ. Если $u\geq 20$, то можно уменьшить u на 20 следующим образом: $43u–20v=43(u–20) –20(v–43)$. Следовательно, кнопку “ вправо” имеет смысл жать не более 19 раз. При этом получим все остатки от деления на 20, как видно и из перебора, сделанного в п.2. Затем кнопку “влево” жмем не более 4 раз, так как $5\cdot 20=100$ и за 5 раз диск сделает полный оборот. Таким образом, в выражении $r_{100}(43u – 20v)=k$ числа u, v заключены в пределах $0\leq u\leq 19$, $0\leq v\leq 4$. Итого 19+4=*23 секунд*.

Задача 4 (10-11 класс)

Известно, что число $N = 202718099$ является произведением двух простых чисел p и q, а количество натуральных чисел, меньших N и взаимно простых с N, равно 202687920. Найдите числа p и q.

Решение задачи 4

Сначала заметим, что если $N = pq$, где p и q – простые числа, количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число как $\varphi(N)$). Действительно, всего натуральных чисел, меньших N, имеется $pq-1$ штук. Из них не взаимнопросты с N те числа, которые делятся либо на p, а именно $p, 2p, \ldots, (q-1)p$ (всего $(q-1)$ чисел), либо на q, это числа $q, 2q, \ldots, (p-1)q$ (всего $(p-1)$ чисел). Значит

$$\varphi(N) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1).$$

Поэтому, получаем систему: $\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}; \begin{cases} pq = N \\ p + q = N + 1 - \varphi(N) \end{cases}.$

По теореме Виета получаем, что p и q – решения квадратного уравнения:

$$x^2 - (N + 1 - \varphi(N))x + N = 0.$$

В представленной задаче $N = 202718099$, $\varphi(N) = 202687920$ и квадратное уравнение примет вид: $x^2 - 30180x + 202718099 = 0$. Тогда, корень из дискриминанта квадратного уравнения равен $\sqrt{D} = \sqrt{99960004}$. Для того, чтобы извлечь квадратный корень из этого числа можно заметить, что результат должен быть немного меньше, чем 10000, причем последняя цифра в этом числе должны быть 2 или 8. Тогда претендентами будут следующие числа: 9998, 9992, 9988, 9982… Начинаем последовательно возводить их в квадрат, в результате сразу находим: $9998^2 = 99960004$. Итак:

$$x_1 = \frac{30180 - 9998}{2} = 10091 = p; \quad x_2 = \frac{30180 + 9998}{2} = 20089 = q.$$

Ответ: 10091 и 20089.

Задача 5 (8-9 класс)

Для передачи сообщения на русском языке Крокодил Гена и Чебурашка предпринимают следующие действия. Каждый из них выбирает свою последовательность, состоящую из целых чисел в пределах от 0 до 32 с количеством чисел, равным длине сообщения. Буквы сообщения заменяются числами согласно табл. 2.

Таблица 2

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
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	0

Сначала Гена шифрует сообщение, используя свою последовательность: числовое значение первой буквы сообщения и первое число его последовательности складываются, а полученная сумма заменяется остатком от деления на 33 и переводится обратно в буквенный вид согласно табл. 2. Затем эта процедура повторяется для вторых, третьих и т.д. чисел сообщения и последовательности. Полученный результат: **ЁЛИСУВШОЮЦОМЮВЫЗПЭЪМО** передаётся Чебурашке. Затем Чебурашка шифрует это зашифрованное сообщение с помощью своей последовательности и передает Гене: **ЪЭЛВШРЕЭЭТЖЩЮИГВФБСЦХ.** Гена отнимает от числовых значений букв полученного сообщения числа своей последовательности (к отрицательной разнице прибавляется число 33) и передаёт результат Чебурашке: **ЖЪЫХЙТСЖЫАШШЬЯМЫШЗЬВГ.** Какое сообщение зашифровал Крокодил Гена?

Решение задачи 5

Из условия задачи имеется 3 зашифрованных сообщения:

$$C_1 = M + K_Г = \text{ЁЛИСУВШОЮЦОМЮВЫЗПЭЪМО};$$

$$C_2 = C_1 + K_Ч = M + K_Г + K_Ч = \text{ЪЭЛВШРЕЭЭТЖЩЮИГВФБСЦХ};$$

$$C_3 = C_2 - K_Г = M + K_Ч = \text{ЖЪЫХЙТСЖЫАШШЬЯМЫШЗЬВГ},$$

где M – переданное открытое сообщение, $K_Г$ – последовательность, выбранная Крокодилом Геной; $K_Ч$ – последовательность, выбранная Чебурашкой. Тогда открытый текст можно найти следующим образом: $M = C_1 - C_2 + C_3$.

Ответ: **ТИШЕ ЕДЕШЬ ДАЛЬШЕ БУДЕШЬ**

Задача 6 (10-11 класс)

Известно, что три числа a_1, a_2, a_3 были получены так: сначала выбрали натуральное число A и нашли числа $A_1 = [A]_{16}$, $A_2 = [A/2]_{16}$, $A_3 = [A/4]_{16}$, где $[X]_{16}$ – остаток от деления целой части числа X на 16 (например, $[53/2]_{16} = 10$). Затем было выбрано целое число B такое, что $0 \le B \le 15$. Числа A_1, A_2, A_3 и B записывают в двоичной системе счисления, т.е. представляют каждое из них в виде цепочки из 0 и 1 длины 4, приписывая слева необходимое число нулей. Такие цепочки условимся складывать посимвольно «в столбик» без переносов в следующий разряд согласно правилу: $1+1=0+0=0$ и $0+1=1+0=1$, а саму

операцию посимвольного сложения обозначим как $\oplus$. Например, $3 \oplus 14 = (0011) \oplus (1110) = (1101) = 13$. Положим $a_1 = A_1 \oplus B$, $a_2 = A_2 \oplus B$, $a_3 = A_3 \oplus B$. Найдите все возможные значения числа a_3, если известно, что $a_1 = 4, a_2 = 10$.

Решение задачи 6

Пусть в двоичной системе счисления $A = (x_n, ..., x_0)$. Тогда $A_1 = (x_3, x_2, x_1, x_0)$, $A_2 = (x_4, x_3, x_2, x_1)$, $A_3 = (x_5, x_4, x_3, x_2)$. Следовательно,

$$a_1 \oplus a_2 = (A_1 \oplus B) \oplus (A_2 \oplus B) = A_1 \oplus A_2 = (x_3 \oplus x_4, x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1),$$

$$a_3 \oplus a_2 = (A_3 \oplus B) \oplus (A_2 \oplus B) = A_3 \oplus A_2 = (x_5 \oplus x_4, x_4 \oplus x_3, x_3 \oplus x_2, x_2 \oplus x_1).$$

Итак, если вычислить $a_1 \oplus a_2$, то три младших бита $a_3 \oplus a_2$ будут найдены, а старший бит будет произвольным.

Вычислим значение $a_1 \oplus a_2$:

$$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \end{array}.$$

Тогда возможные значения $(a_2 \oplus a_3)$ имеют вид $(*,1,1,1)$, и $a_3 = a_2 \oplus (a_3 \oplus a_2)$:

$$\begin{array}{cccc} 1 & 0 & 1 & 0 \\ * & 1 & 1 & 1 \\ \hline * & 1 & 0 & 1 \end{array}.$$

Итак, $a_3 = 13$, либо $a_3 = 5$. Можно убедиться в том, что оба варианты верны, если рассмотреть последовательности с параметрами $A = 20$, либо $A = 52$ и $B = 0$.

Ответ: 13 и 5.

Задача 7 (11 класс)

Для зашифрования сообщения на русском языке, записанного без знаков препинания и пробелов, используется последовательность натуральных чисел $x_1, x_2, \ldots$, удовлетворяющая соотношению: $x_k = b \cdot 8^{a(k-1)}$, $k = 1,2,\ldots$ Здесь a и b - фиксированные (но неизвестные) натуральные числа. Зашифрование происходит следующим образом. Первую букву сообщения заменяют числом согласно табл. 3 и складывают с x_1, потом также заменяют вторую букву и

складывают с x_2 и т.д. Затем все суммы заменяют остатками от деления на 31, а остатки заменяют буквами согласно табл. 3.

Таблица 3

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	Ы	Ь,Ъ	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

В результате получился текст

ОЯФПРПЯФБКПЩСЬИЖЬИЯЫСЯЗТХЖУТНАЖБСЁНФВГМНУТУЁШЖФН

Найдите исходное сообщение, представляющее собой отрывок известного стихотворения, если известно, что в нем есть слово **РАВНИНЫ**.

Решение задачи 7

«Двигаем» указанное в условии слово по шифрованному тексту. При правильном расположении после вычитания слова из фрагмента шифрованного текста получим значения, образующие геометрическую прогрессию, от членов которой взяты остатки от деления на 31 (см. табл. 4).

Таблица 4

…	Ф	Б	К	П	Щ	С	Ь	…
	Р	А	В	Н	И	Н	Ы	
…	20	1	10	15	25	17	27	…
…	16	0	2	13	9	13	26	…
…	4	1	8	2	16	4	1	…

Ответ:

МОРОЗНО**РАВНИНЫ**БЕЛЕЮТПОДСНЕГОМЧЕРНЕЕТСЯЛЕСВПЕРЕДИ

b=2, a=2, период равен 5.