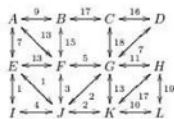


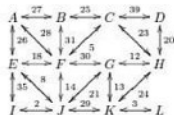
15. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом ($e = 3, m = 33$). Шифрованное сообщение имеет вид (3; 4; 24; 32). Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответствуют числа в диапазоне от 2 до 32 (исключены буквы "ё" и "ъ").
16. Постройте наибольшее паросопряжение для двудольного графа G . Первая доля состоит из вершин $\{a, b, c, d, e, f, g\}$, вторая доля — из вершин $\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta\}$. Ребра заданы следующим списком: $\{(a, \alpha)(a, \beta)(a, \delta)(a, \epsilon)(b, \epsilon)(b, \zeta)(c, \beta)(c, \delta)(c, \epsilon)(d, \gamma)(e, \gamma)(e, \zeta)(e, \eta)(f, \epsilon)(f, \zeta)(g, \epsilon)(g, \eta)\}$.

Вар. 118 (3313)

1. Решить диофантово уравнение $3382x - 4921y = 114$
2. а) Представьте $\sqrt{395}$ в виде периодической цепной дроби; б) вычислите ее с точностью до $\epsilon = 10^{-4}$.
3. Найти наименьшее натуральное число x , удовлетворяющее условиям $x \equiv 4 \pmod{18}$; $x \equiv 18 \pmod{23}$; $x \equiv 12 \pmod{19}$; $x \equiv 25 \pmod{29}$.
4. Найти остаток от деления 53^{2019} на 64.
5. По формуле Лагранжа найти многочлен p не выше 4-ой степени, удовлетворяющий условиям: $p(1) = -2$; $p(4) = -26$; $p(2) = 0$; $p(-1) = -6$; $p(3) = 2$.
6. Найти рациональные корни: $x^4 - 5x^3 - 6x^2 + 7x - 2$
7. Вычислить $17/27$ в кольце вычетов по модулю 58.
8. Найти представление рационального числа $\frac{285}{126}$ непрерывной дробью.
9. Найти остаток от деления многочлена $x^5 + 2x^4 + x^3 + x^2 + 2x$ на $2x^3 + 2x^2 + x + 1$ в кольце $\mathbb{Z}/3\mathbb{Z}[x]$
10. Среди 147 целых чисел, 63 кратно 4, 50 кратно 9, 2 кратно 16, 2 кратно 36, 1 кратно 144. Определить, сколько среди них кратно 4 или 9, но не кратно 16.
11. Все перестановки 7 чисел (1; 2; 3; 4; 5; 6; 7) упорядочены в лексикографическом порядке. Найти перестановку с номером 2695.
12. С помощью алгоритма Хаффмана построить код Шеннона-Фано для текстового сообщения, состоящего из символов "ш", "ъ", "ы", "ю", "э", "з" с частотами соответственно 44, 36, 66, 70, 20, 88.
13. Для заданного на рисунке графа постройте минимальное остовное дерево, применив алгоритм Прима (построение начинать с вершины C). В ответе укажите порядок включения ребер.



14. Для заданного на рисунке графа постройте минимальное остовное дерево, применив алгоритм Краскала. В качестве ответа приведите цвета вершин при каждом добавлении очередного ребра. Начальная раскраска: $A \rightarrow 1, B \rightarrow 2, \dots$. Добавляемое ребро перекрашивает цвет с меньшим номером и цвет с большим номером.



15. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом ($e = 11, m = 34$). Шифрованное сообщение имеет вид (30; 15; 8; 22). Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответствуют числа в диапазоне от 2 до 32 (исключены буквы "ё" и "ъ").
16. Постройте наибольшее паросопряжение для двудольного графа G . Первая доля состоит из вершин $\{a, b, c, d, e, f, g\}$, вторая доля — из вершин $\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta\}$. Ребра заданы следующим списком: $\{(a, \alpha)(a, \beta)(a, \delta)(a, \epsilon)(b, \alpha)(b, \epsilon)(b, \zeta)(c, \alpha)(c, \gamma)(c, \delta)(d, \delta)(e, \alpha)(f, \beta)(f, \gamma)(f, \delta)(f, \zeta)(g, \alpha)(g, \delta)\}$.

10. Среди 147 целых чисел, 63 кратно 4, 50 кратно 9, 2 кратно 16, 2 кратно 36, 1 кратно 144. Определить, сколько среди них кратно 4 или 9, но не кратно 16.

Всего 147

63 : 4

2 : 16

1 : 144

50 : 9

2 : 36

? : 4
? : 9

? / 16

$$63 - 2 - 2 - 1 = 58$$

$$58 + 47 + 2 = 107$$

$$50 - 2 - 1 = 47$$

10. Среди 63 целых чисел, 32 кратно 11, 26 кратно 12, 8 кратно 121, 13 кратно 132, 7 кратно 1452. Определить, сколько среди них кратно 11 или 12, но не кратно 132

Всего

$$32 : 11$$

$$26 : 12$$

$$8 : (121)_{11^2}$$

$$13 : 132$$

$$7 : 1452$$

$$(132 \cdot 11)$$

$$121 \cdot 12$$

$$? : 11 \text{ или } ? : 12, \text{ но } \nmid 132$$

$$4 + 6 + (8 - 7) = 11$$

$$\bullet 32 - 8 - 13 - 7 = 4$$

$$\bullet 26 - 13 - 7 = 6$$

11. Все перестановки 7 чисел (1;2;3;4;5;6;7) упорядочены в лексикографическом порядке. Найти перестановку с номером 2695.

$$1) 2695 = 1347 \cdot 2 + 1$$

$$2) 1347 = 449 \cdot 3 + 0$$

$$3) 449 = 112 \cdot 4 + 1$$

$$4) 112 = 22 \cdot 5 + 2$$

$$5) 22 = 3 \cdot 6 + 4$$

$$6) 3 = 0 \cdot 7 + 3$$

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (3, 4, 2, 1, 0, 1) = (4, 6, 3, 2, 1, 7, 5)$$

Проверка

Теорема 1.72. При лексикографическом упорядочении перестановок, номер перестановки (i_1, i_2, \dots, i_n) вычисляется по формуле

$$N = a_1(n-1)! + a_2(n-2)! + \dots + a_{n-1}1!, \quad (1.95)$$

где a_j — количество элементов, меньших i_j и стоящих правее его, причем $0 \leq a_j \leq n-j$.

$$N = 3 \cdot 6! + 4 \cdot 5! + 2 \cdot 4! + 1 \cdot 3! + 1 \cdot 1! =$$

$$= 3 \cdot 720 + 4 \cdot 120 + 2 \cdot 24 + 1 \cdot 6 + 1 \cdot 1 = 2160 + 480 + 48 + 6 + 1 = 2695$$

11. Все перестановки 7 чисел (1;2;3;4;5;6;7) упорядочены в лексикографическом порядке. Какой по счету идет перестановка 5274613?

$$(5, 2, 7, 4, 6, 1, 3) \rightarrow (4, 1, 4, 2, 2, 0) \quad \text{— кол-во}$$

$$N = 4 \cdot (720) + 1 \cdot (120) + 4 \cdot (24) + 2 \cdot (6) + 2 \cdot (2) =$$

$$= 2160 + 480 + 96 + 12 + 4 = 2752$$

$n!$ — кол-во перест.

12. С помощью алгоритма Хаффмана построить код Шеннона-Фэно для текстового сообщения, состоящего из символов "ш", "ъ", "ы", "ю", "ь", "э" с частотами соответственно 44, 36, 66, 70, 20, 88.

$$\frac{88}{88}$$

$$\frac{11}{44}$$

$$\frac{36}{11}$$

$$\frac{20}{10}$$

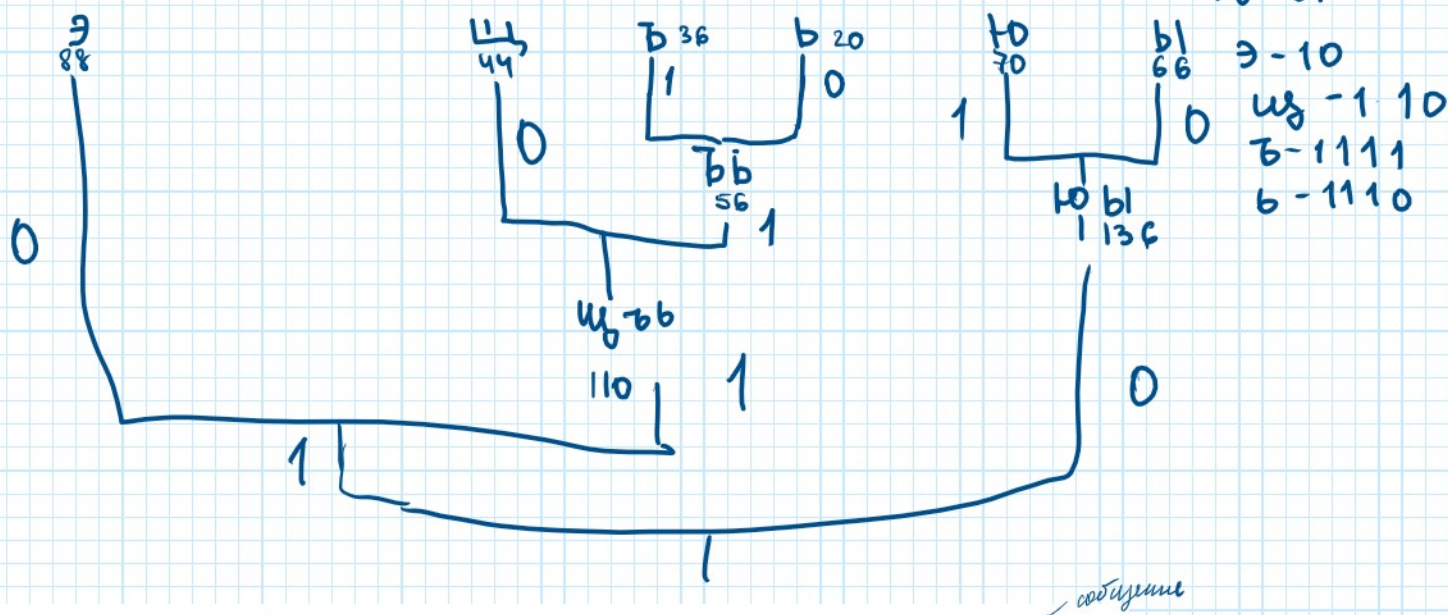
$$\frac{70}{70}$$

$$\frac{66}{66}$$

$$\frac{10}{10}$$

$$\frac{10}{10}$$

$$\frac{3}{3}$$



15. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом ($e = 11, m = 34$). Шифрованное сообщение имеет вид (30; 15; 8; 22). Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответствуют числа в диапазоне от 2 до 32 (исключены буквы "ё" и "ъ").

$$ed \equiv 1 \pmod{\phi(m)}$$

$$34 = 2 \cdot 17$$

$$\phi(m) = 34 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{17}\right) =$$

$$= 16$$

$$11d \equiv 1 \pmod{16}$$

$$11d \equiv 33 \pmod{16}$$

$$d \equiv 3 \pmod{16} \equiv 3$$

$$D = c^d \pmod{m}$$

$$\begin{array}{r} \times 2250 \\ 1125 \\ 3375 \end{array}$$

$$30^3 \pmod{34}$$

$$(p-1)(q-1) = 16$$

$$3375 \pmod{34}$$

$$\begin{array}{r} \times 34 \\ 6 \\ \hline 204 \end{array} \quad \begin{array}{r} \times 34 \\ 7 \\ \hline 238 \end{array}$$

$$D_1 = 30^3 \pmod{34} = (-4)^3 \pmod{34} = -64 \pmod{34} = 4 \pmod{34}$$

$$D_2 = 15^3 \pmod{34} = 9 \pmod{34}$$

$$D_3 = 8^3 \pmod{34} = 64 \cdot 8 \pmod{34} = 240 \pmod{34} = 2 \pmod{34}$$

$$D_4 = 22^3 \pmod{34} = (-12)^3 \pmod{34} = 144 \cdot (-12) \pmod{34} = 8 \cdot (-12) \pmod{34} = -96 \pmod{34} = -28 \pmod{34} = 6 \pmod{34}$$

П И Б Е

Б З К А

4 9 2 6
А Б В Г Д Е Ж З И Й
2 3 4 5 6 7 8 9

15. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом ($e = 5, m = 39$). Шифрованное сообщение имеет вид (28; 11; 32; 2). Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответствуют числа в диапазоне от 2 до 32 (исключены буквы "ё" и "ъ").

$$e = 5 \quad m = 39$$

$$\phi(m) = 39 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{13}\right) = 24$$

$$e = 5 \quad m = 39$$

$$f(m) = 39 \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{3}\right) = 24$$

$$5d = 1 \pmod{24}$$

$$d = 5 \pmod{24} \Rightarrow d = 5$$

$$D = 28^5 \pmod{39} = (-11)^5 \pmod{39} = -20 \pmod{39} = 19$$

$$D = 11^5 \pmod{39} = 11^5 \pmod{39} = 20$$

$$D = 32^5 \pmod{39} = 2$$

$$D = 2^5 \pmod{39} = 32$$

CTAY

A ²	Б ³	В ⁴	Г ⁵	Д ⁶	Е ⁷	Ё ⁸
Ж ⁹	З ¹⁰	И ¹¹	Й ¹²	К ¹³	Л ¹⁴	М ¹⁵
Н ¹⁶	О ¹⁷	П ¹⁸	Р ¹⁹	С ²⁰	Т ²¹	У ²²
Ф ²³	Х ²⁴	Ц ²⁵	Ч ²⁶	Ш ²⁷	Щ ²⁸	Ъ ²⁹
Ы ³⁰	Ь ³¹	Э ³²	Ю ³³	Я ³⁴		

3. Найти наименьшее натуральное число x , удовлетворяющее условиям $x \equiv 4 \pmod{18}$; $x \equiv 18 \pmod{23}$; $x \equiv 12 \pmod{19}$; $x \equiv 25 \pmod{29}$;

НЗ. Найти наим. x :

$$\begin{cases} x \equiv 4 \pmod{18} \\ x \equiv 18 \pmod{23} \\ x \equiv 12 \pmod{19} \\ x \equiv 25 \pmod{29} \end{cases}$$

Китайская-теорема об остатках:

$$1) M_0 = M_1 \cdot M_2 \cdot M_3 \cdot M_4 = 18 \cdot 23 \cdot 19 \cdot 29 = 228114$$

$$M_i = \frac{M_0}{n_i}$$

$$M_1 = \frac{M_0}{18} = 12673$$

$$M_2 = 9918$$

$$M_3 = 12006$$

$$M_4 = 7866$$

$$3) \text{ Решение } = \sum M_i y_i \pmod{M_0} =$$

$$= 12673 \cdot 4 + 9918 \cdot 22 + 12006 \cdot 12 + 7866 \cdot 25 \pmod{228114} =$$

$$= 550822 \pmod{228114} = 94594 \pmod{228114}$$

$$\Rightarrow x = 94594$$

Н4. Найти остаток от деления 53^{2099} на 64.

$$\varphi(64) = \varphi(2^6) = \frac{64-1}{2} = 32$$

$$\varphi(32) = \varphi(2^5) = 16$$

$$53^{32k+r} \equiv 53^r \pmod{64}$$

$$53^{2099} \equiv 53^{31} \pmod{64} \equiv (-3)^{31} \pmod{64} \equiv -27 \pmod{64} \equiv 37$$

$$2) M_i y_i \equiv a \pmod{n_i}$$

$$12673 y_1 \equiv 4 \pmod{18} \quad (1)$$

$$9918 y_2 \equiv 18 \pmod{23} \quad (2)$$

$$12006 y_3 \equiv 12 \pmod{19} \quad (3)$$

$$7866 y_4 \equiv 25 \pmod{29} \quad (4)$$

$$(1) 12673 y_1 \equiv 4 \pmod{18}$$

$$18 \cdot 704 y_1 + 1 y_1 \equiv 4 \pmod{18}$$

$$y_1 \equiv 4 \pmod{18} \Rightarrow y_1 = 4$$

$$(2) 12006 y_2 \equiv 12 \pmod{19}$$

$$19 \cdot 631 y_2 + 12 y_2 \equiv 12 \pmod{19}$$

$$12 y_2 \equiv 12 \pmod{19}$$

$$12 y_2 \equiv 12 \pmod{19} \Rightarrow y_2 = 1$$

$$12 y_2 \equiv 12 \pmod{19} \Rightarrow y_2 = 1$$

$$-2 y_2 \equiv 12 \pmod{19}$$

$$-y_2 \equiv 6 \pmod{19}$$

$$y_2 \equiv 13 \pmod{19}$$

$$y_2 = 13$$

$$(2) 9918 y_2 \equiv 18 \pmod{23}$$

$$23 \cdot 431 y_2 + 5 y_2 \equiv 18 \pmod{23}$$

$$5 y_2 \equiv 18 \pmod{23}$$

$$5 y_2 \equiv 18 + 23 \cdot 2 \pmod{23}$$

$$5 y_2 \equiv 110 \pmod{23}$$

$$y_2 \equiv 22 \pmod{23}$$

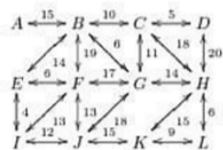
$$y_2 = 22$$

$$(4) 7866 y_4 \equiv 25 \pmod{29}$$

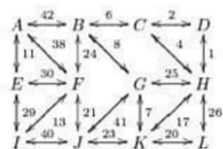
$$y_4 = 16$$

$$\frac{13}{81} \cdot \frac{1}{91}$$

10. Среди 63 целых чисел, 32 кратно 11, 26 кратно 12, 8 кратно 121, 13 кратно 132, 7 кратно 1452. Определить, сколько среди них кратно 11 или 12, но не кратно 132.
11. Все перестановки 7 чисел $(1; 2; 3; 4; 5; 6; 7)$ упорядочены в лексикографическом порядке. Какой по счету идет перестановка 5274613?
12. С помощью алгоритма Хаффмана построить код Шеннона-Фэно для текстового сообщения, состоящего из символов "ш", "ь", "ы", "ю", "ъ", "э" с частотами соответственно 40, 86, 42, 87, 52, 76.
13. Для заданного на рисунке графа постройте минимальное остовное дерево, применив алгоритм Прима (построение начинать с вершины L). В ответе укажите порядок включения ребер.



14. Для заданного на рисунке графа постройте минимальное остовное дерево, применив алгоритм Краскала. В качестве ответа приведите цвета вершин при каждом добавлении очередного ребра. Начальная раскраска: $A = 1, B = 2, \dots$. Добавляемое ребро перекрашивает цвет с меньшим номером в цвет с большим номером.



15. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом $(e = 5, m = 39)$. Шифрованное сообщение имеет вид $(28; 11; 32; 2)$. Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответствуют числа в диапазоне от 2 до 32 (исключены буквы "ё" и "ъ").
16. Постройте наибольшее паросочетание для двудольного графа G . Первая доля состоит из вершин $\{a, b, c, d, e, f, g\}$, вторая доля — из вершин $\{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta\}$. Ребра заданы следующим списком: $\{(a, \delta)(b, \varepsilon)(c, \gamma)(c, \delta)(d, \alpha)(d, \eta)(e, \varepsilon)(f, \beta)(f, \delta)(g, \zeta)(g, \gamma)\}$.