10. Числовые алгоритмы, преобразование Фурье

1. В протоколе RSA выбраны $p = 17$, $q = 23$, $N = 391$, $e = 3$. Выберите ключ d и зашифруйте сообщение 41. Затем расшифруйте полученное сообщение и убедитесь, что получится исходное 41.

2. Пусть в протоколе RSA открытый ключ (N, e), $e = 3$. Покажите, что если злоумышленник узнаёт закрытый ключ d, то он может легко найти разложение N на множители.

3. Докажите, что в шифре Шамира в итоге у B в действительности оказывается то сообщение, которое A планировал передать.

4. Докажите, что в шифре Эль-Гамаля в итоге у B в действительности оказывается то сообщение, которое A планировал передать.

5. Докажите, что в алгоритме шифрования Рабина B в итоге сможет найти исходное передаваемое сообщение среди $(\pm apm_q \pm bqm_p)$.

6. Докажите формулу обращения: $(M_n(\omega))^{-1} = \dfrac{1}{n} M_n(\omega^{-1})$. Вычислите также матрицу $(M_n(\omega))^4$.

7. Найдите произведение многочленов $A(x) = x^3 + 3x + 2$ и $B(x) = 3x^3 + 3x^2 + 2$ с помощью алгоритма быстрого преобразования Фурье. Для этого найдите рекурсивно дискретное преобразование Фурье двух массивов $A = (0, 0, 0, 0, 1, 0, 3, 2)$ и $B = (0, 0, 0, 0, 3, 3, 0, 2)$, затем вычислите ДПФ массива C и восстановите коэффициенты многочлена-произведения, используя обратное преобразование.

8 (Доп). Многочлен $A(x) = \sum\limits_{i=0}^{n-1} a_i x^i$ задан последовательностью коэффициентов. Пусть последовательность $\{y_k\}_{k=0}^{n-1}$ — его ДПФ, т. е. $y_k = A\left(e^{\frac{2\pi k}{n} i}\right)$. Предложите алгоритм, вычисляющий $\sum\limits_{k=0}^{n-1} (\mathrm{Re}\ y_k + \mathrm{Im}\ y_k)$ и требующий $o(n^2)$ арифметических операций.