## 1. Кому что

Ниже пронумерованный список 211 группы и примкнувших к ним. Кого-то, возможно, забыли. Во всех работах, кроме первой, следует выбирать задание со своим номером.

(1) Бондаренко Михаил
(2) Ерохин Станислав
(3) Климовицкий Иосиф
(4) Нетеребский Богдан
(5) Питаль Петр
(6) Пологова Анна
(7) Савенков Кирилл
(8) Смыкалов Владимир
(9) Тыщук Константин
(10) Устинов Никита
(11) Якерсон Мария
(12) Кошкарёв Иван

## 2. Задание №1

Сделайте что-нибудь такое в Maple, в результате чего образуется какая-нибудь картинка, напишите текст в TEX'е, с описанием того, что было сделано, и вставьте в него ту самую картинку.

## 3. Задание №2

Дана функция $f : [-1, 1] \to \mathbb{R}$. Построить систему ортогональных полиномов на отрезке $[-1, 1]$ относительно скалярного произведения с весом $\omega(x)$. Найти частичные суммы ряда Фурье функции $f$ по этой системе полиномов (скажем, для $n \leqslant 10$). Построить графики, показывающие, как функция $f$ приближается частичными суммами ряда Фурье и чезаровскими средними (средними арифметическими частичных сумм ряда Фурье). Написать отчет в TEX'e.

**1.** $f(x) = \begin{cases} x & \text{при } x \in [-1, 0), \\ 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = e^{2x}$;

**2.** $f(x) = \begin{cases} -x & \text{при } x \in [-1, 0), \\ 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = \sin^2(\pi x/2)$;

**3.** $f(x) = \begin{cases} x + 1 & \text{при } x \in [-1, 0), \\ x - 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = e^{-2x}$;

**4.** $f(x) = \begin{cases} 1 - x & \text{при } x \in [-1, 0), \\ x - 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = \cos(\pi x/2)$;

**5.** $f(x) = \begin{cases} -1 & \text{при } x \in [-1, 0), \\ 1 - x & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = \sqrt{x + 1}$;

**6.** $f(x) = \begin{cases} -1 & \text{при } x \in [-1, 0), \\ 1 + x & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = |\sin(\pi x)|$;

**7.** $f(x) = \begin{cases} -x & \text{при } x \in [-1, 0), \\ 1 + x & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = e^x$;

**8.** $f(x) = \begin{cases} x & \text{при } x \in [-1, 0), \\ 1 + x & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = |\ln(x + 1)|$;

**9.** $f(x) = \begin{cases} -x & \text{при } x \in [-1, 0), \\ x - 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = \operatorname{ch} x$;

**10.** $f(x) = \begin{cases} x & \text{при } x \in [-1, 0), \\ x - 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = \cos^2(\pi x)$;

**11.** $f(x) = \begin{cases} x & \text{при } x \in [-1, 0), \\ -x - 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = |\operatorname{sh} x|$.

**12.** $f(x) = \begin{cases} x & \text{при } -x \in [-1, 0), \\ 1 - x & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = e^{-x}$.

**13.** $f(x) = \begin{cases} 1 & \text{при } -x \in [-1, 0), \\ x - 1 & \text{при } x \in [0, 1] \end{cases}$ и $\omega(x) = \ln(x + 2)$.

## 4. Задание №3

Положим $n = 8$. Пусть $\mathcal{H}$ — линейное пространство многочленов степени не выше $n$, в котором задано скалярное произведение из задания №2. Проделайте следующие действия в Maple и напишите отчет о них в TEX'е.

1) Дифференцирование является линейным отображением пространства $\mathcal{H}$ на себя. Запишите матрицу $A$ этого линейного отображения в базисе $w_0$, $w_1$, $\ldots$, $w_n$, построенном в задании №2.

2) Найдите жорданову форму матрицы $A$. Объясните результат, не скупясь на слова и сопутствующие формулы в TEX'е.

3) Вычислите $B = \exp(A/2)$. Полученной матрице соответствует линейный оператор в базисе $w_0$, $w_1$, $\ldots$, $w_n$, его мы обозначим $\mathbf{B}$.

4) Для функции $f$ в задании №2 вычислялось ее приближение $f_n$ суммами Фурье и приближение $g_n$ чезаровскими средними. Найдите многочлены $\mathbf{B}f_n$ и $\mathbf{B}g_n$. Постройте графики функций $f$, $f_n$, $g_n$ (это было сделано в задании №2) и графики функций $h$, $\mathbf{B}f_n$, $\mathbf{B}g_n$, где $h$ — еще одна функция, построение которой явно напрашивается по виду картинки. Результат объясните.

## 5. Задание №4

С помощью метода множителей Лагранжа найдите наибольше и наименьшее значение указанных функций на указанных поверхностях. Если какие-либо из этих значений отсутствуют, то объясните почему. В отчете не забудьте обосновать, что найденые вами значения действительно являются наибольшим и наименьшим.

**1.** Найдите наибольшее и наименьшее значения выражения $ab + bc + ca - abc$ при условии $a^2 + b^2 + c^2 + abc = 4$ и $a,\ b,\ c \geqslant 0$.

**2.** Найдите наибольшее и наименьшее значения выражения $\dfrac{1}{\sqrt{1+a}} + \dfrac{1}{\sqrt{1+b}} + \dfrac{1}{\sqrt{1+c}}$ при условии $abc = 2^9$ и $a,\ b,\ c > 0$.

**3.** Найдите наибольшее и наименьшее значения выражения $\dfrac{1}{(x+y)^2} + \dfrac{1}{(y+z)^2} + \dfrac{1}{(z+x)^2}$ при условии $xy + yz + zx = 1$ и $x,\ y,\ z \geqslant 0$.

**4.** Найдите наибольшее и наименьшее значения выражения $xy + yz + zt + tx + zx + yt$ при условии $x^2 + y^2 + z^2 + t^2 = 1$.

**5.** Найдите наибольшее и наименьшее значения выражения $x^2 + y^2 + z^2 + 10xyz$ при условии $x + y + z = 1$ и $x,\ y,\ z \geqslant 0$.

**6.** Найдите наибольшее и наименьшее значения выражения $xy + yz + zx - x^3 - y^3 - z^3$ при условии $x^2 + y^2 + z^2 = 1$.

**7.** Найдите наибольшее и наименьшее значения выражения $x + y + z$ при условии $xy + xz + yz + xyz = 1$ и $x,\ y,\ z \geqslant 0$.

**8.** Найдите наибольшее и наименьшее значения выражения $\dfrac{1}{(1+a)^2} + \dfrac{1}{(1+b)^2} + \dfrac{1}{(1+c)^2} + \dfrac{1}{(1+d)^2}$ при условии $abcd = 1$ и $a,\ b,\ c,\ d > 0$.

**9.** Найдите наибольшее и наименьшее значения выражения $a^3 + b^3 + c^3 + 4abc$ при условии $a + b + c = 1$ и $0 \leqslant a, b, c \leqslant \frac{1}{2}$.

**10.** Найдите наибольшее и наименьшее значения выражения $xy^2 + yz^2 + zx^2 - \dfrac{xy + yz + zx}{3}$ при условии $x + y + z = 1$ и $x,\ y,\ z \geqslant 0$.

**11.** Найдите наибольшее и наименьшее значения выражения $x + y + z - xyz$ при условии $x^2 + y^2 + z^2 = 2$.

**12.** Найдите наибольшее и наименьшее значения выражения $ab + bc + cd + da + ac + bd - 4abcd$ при условии $a^2 + b^2 + c^2 + d^2 \leqslant 1$.

**13.** Найдите наибольшее и наименьшее значения выражения $a^3 + b^3 + c^3 + 5abc$ при условии $a + b + c = 1$ и $a,\ b,\ c \geqslant 0$.

## 6. Задание №5

Сделать презентацию в TEX'е, рассказывающую о протоколе (или схеме), который выпал на соответствующий номер. В презентации, в частности, должен быть представлен пример с конкретными числами (и этот пример должен быть отличным от приведенного в источнике знаний). Он должен быть сконструирован в прилагающемся Maple-файле. Причем в этом файле часть данных должна выбираться случайным образом (например, в виде цикла, генерирующего случайные числа до тех пор, пока они не будут удовлетворять нужным ограничениям).

Все ссылки даны на книгу *Mollin R.* RSA and public-key cryptography. CRC Press, 2003.

**1.** Протокол идентификации Шнорра (стр. 129) [Schnorr Identification Protocol].

**2.** Протокол идентификации Окамото (стр. 131) [Okamoto Identification Protocol].

**3.** Схема подписи Эль-Гамаля (стр. 136) [ElGamal Signature Scheme].

**4.** Схема подписи Шнорра (стр. 138) [Schnorr Signature Scheme]. Вместо криптографической хеш-функциии можете использовать тождественное отображение или, скажем, возведение в квадрат.

**5.** Алгоритм цифровой подписи (стр. 139) [Digital Signature Algorithm]. Числа следует взять поменьше. Вместо криптографической хеш-функциии можете использовать дописывание нулей до нужной длины.

**6.** Разделение секрета: схема Шамира (стр. 154) [Shamir's Threshold Scheme].

**7.** Разделение секрета: схема Асмута–Блума (стр. 156) [Asmuth–Bloom Threshold Scheme].

**8.** Разделение секрета: схема Блейкли (стр. 157) [Blakely's Secret Sharing Vector Scheme].

**9.** Схема Жиро генерации совместного ключа (стр. 162) [Girault's Self-Certifying Key Agreement Scheme]. Полагаем, что $I_A$ и $I_B$ — это просто имена участников переконвертированные в остатки по модулю $n$.

**10.** Схема обмена ключами EKE. Алгоритм Диффи–Хеллмана (стр. 170) [Encrypted Key Exchange (EKE) — Diffie–Hellman Implemented]. Полагаем, что на шаге 1 Боб не проверяет, что сообщение сгененрировано Алисой, и таким образом подробность с идентификационной строкой $I_A$ опускаем. Под алгоритмом шифрования $E_k$ с симметричным ключом $k$ здесь будем понимать какую-нибудь простенькую операцию шифрования, скажем, умножение на $k \bmod p$.

**11.** Протокол идентификации Фейга–Фиата–Шамира (стр. 34) [Feige–Fiat–Shamir Identification Protocol].

**12.** Алгоритм шифрования Мэсси–Омуры (стр. 71) [Massey-Omura Cryptosystem].

**13.** Алгоритм шифрования Эль-Гамаля (стр. 67) [The ElGamal Cryptosystem].