1. Кому что

Ниже пронумерованный список 211 группы. Везде нужно выбирать задание со своим номером.

(1) Басок Михаил
(2) Васильев Иоанн
(3) Галашин Павел
(4) Золотов Владимир
(5) Лавренов Андрей
(6) Ненашев Глеб
(7) Русских Марианна
(8) Сидоров Андрей
(9) Соколов Вячеслав

2. Задание №1

Для данного дифференциального уравнения построить пикаровские приближения, стартовав с нескольких разных функций, например, с тождественного нуля, с тождественной единицы и с икса. Построить графики приближений, а также график точного решения. Написать отчет в TEX'е. Отчет должен содержать фрагменты Вашей программы с пояснениями и полученную картинку.

1. $y' + \dfrac{x}{1-x^2}y = x\sqrt{y}$, $y(0) = 1$;

2. $y' - 2xy = 2x^3y^2$, $y(0) = 1/2$;

3. $xy' + y = y^2 \ln x$, $y(1) = 1$;

4. $xy' + y = xy^2$, $y(0) = 0$;

5. $xy' - y = y^2/x^2$, $y(1) = 1$;

6. $x^2y' + (xy - 2)^2 = 0$, $y(1) = 2$;

7. $x^2y' = x^2y^2 + xy + 1$, $y(1) = 1$;

8. $xy' = x^2y^2 - y + 1$, $y(1) = 1$;

9. $xy' = y^2 - 3y + 4x^2 + 2$, $y(1) = 1$;

10. $y' + y^2 = -\dfrac{1}{4x^2}$, $y(1) = 1$.

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 $\omega(x) = |\ln(x + 1)|$;

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

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

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

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

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

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

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

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

4. Задание №3

Реализовать в Maple предложенный алгоритм (с добавлением шифрования RSA, кроме задания 9). Изготовить презентацию, рассказывающую как устроен алгоритм шифрования RSA (кроме задания 9) и алгоритм, который Вам достался. В презентации, в частности, должен быть приведен пример реализации Вашего алгоритма(ов).

1. Разделяете секрет, созданный RSA, на 8 участников так, что любые 5 могут его увидеть. Секрет разделяется по схеме Карнина–Грини–Хеллмана (Karnin, Greene, Hellman).

Описание алгоритма можно найти тут: `http://ru.wikipedia.org/`.

2. Разделяете секрет, созданный RSA, на 10 участников так, что любые 8 могут его увидеть. Секрет разделяется по схеме Миньотта (Mignotte).

Описание алгоритма можно найти тут: `http://ru.wikipedia.org/`, но более внятно написано тут: `http://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_remainder_theorem`.

3. Разделяете секрет, созданный RSA, на 10 участников так, что любые 6 могут его увидеть. Секрет разделяется по схеме Асмута–Блума (Asmuth, Bloom).

Описание алгоритма можно найти тут: `http://ru.wikipedia.org/`, но более внятно написано тут: `http://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_remainder_theorem`.

4. Разделяете секрет, созданный RSA, на 7 участников так, что любые 5 могут его увидеть. Секрет разделяется по схеме Блэкли (Blakley), она же векторная схема разделения секрета.

Описание алгоритма можно найти тут: `http://ru.wikipedia.org/`.

5. Модификация алгоритма RSA для слепой подписи.

Описание алгоритма: `http://en.wikipedia.org/wiki/Blind_signature` раздел Blind RSA signatures. В русской википедии на первый взгляд написана какая-то ерунда.

6. Разделеняете секрет, созданный RSA, на 10 участников так, что любые 7 могут его увидеть. Секрет разделяется по схеме Шамира (Shamir), она же схема интерполяционных многочленов Лагранжа.

Схема обсуждалась на занятии, но описание алгоритма можно найти и тут: `http://ru.wikipedia.org/`.

7. Модификация алгоритма RSA для цифровой подписи несколькими участниками. Пример на 5 подписывающих.

Описание алгоритма можно найти тут: `http://www.math.spbu.ru/user/aih/students/CM2011/Algorithms.pdf`.

8. Модификация алгоритма RSA передачи пароля для участия в конференции. Пример на 5 участников.

Описание алгоритма можно найти тут: `http://www.math.spbu.ru/user/aih/students/CM2011/Algorithms.pdf`.

9. Три способа бросания жребия по телефону. Один из них обсуждался на занятии.

Описания всех алгоритмов можно найти тут: `http://www.math.spbu.ru/user/aih/students/CM2011/Algorithms.pdf`.