МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
___________О.Г. Локтионова
«___»_______________2016 г.

ЦЕПНЫЕ И ПОДХОДЯЩИЕ ДРОБИ

Методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 511.17

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Цепные и подходящие дроби: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 13 с. Библиогр.: с. 13.

Содержат основные сведения о цепных и подходящих дробях и способах решения сравнений с их помощью. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – изучить понятия цепных и подходящих дробей и научиться решать с помощью них системы сравнений.

2. ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Решить систему сравнения, используя подходящие дроби. Оформить отчет.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Решить систему сравнений под номером, соответствующим варианту задания.
4. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Решение системы сравнений.
4. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Цепная дробь (или **непрерывная дробь**) — это математическое выражение вида

$$[a_0; a_1; a_2; a_3..] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + ..}}}$$

Где a_0 есть целое число и все остальные a_n натуральные числа (то есть положительные целые). Любое вещественное число можно представить в виде цепной дроби (конечной или бесконечной). Число представляется конечной цепной дробью тогда и только тогда, когда оно рационально. Число представляется периодической цепной дробью тогда и только тогда, когда оно является квадратичной иррациональностью.

5.1. Разложение в цепную дробь

Любое вещественное число x может быть представлено (конечной или бесконечной) цепной дробью $[a_0; a_1; a_2; a_3..]$, где

$$a_0 = [x], x_0 = x - a_0$$

$$a_1 = \left[\frac{1}{x_0}\right], x_1 = \frac{1}{x_0} - a_1$$

$$..$$

$$a_n = \left[\frac{1}{x_{n-1}}\right], x_n = \frac{1}{x_{n-1}} - a_n$$

где $[x]$обозначает целую часть числа x.

Для рационального числа x это разложение оборвётся по достижению нулевого x_n для некоторого n. В этом случае x представляется конечной цепной дробью $x = [a_0; a_1; a_2; a_3..]$.

Для иррационального x все величины x_n будут ненулевыми и процесс разложения можно продолжать бесконечно. В этом случае x представляется бесконечной цепной дробью $x = [a_0; a_1; a_2; a_3..]$.

5.2. Подходящие дроби

n-ой подходящей дробью для цепной дроби $x = [a_0; a_1; a_2; a_3..]$, называется конечная цепная дробь $[a_0; a_1; ..; a_n]$, значение которой равно некоторому рациональному числу $\frac{p_n}{q_n}$. Подходящие дроби с чётными номерами образуют возрастающую последовательность, предел которой равен x. Аналогично, подходящие дроби с нечётными номерами образуют убывающую последовательность, предел которой также равен x.

Эйлер вывел рекуррентные формулы для вычисления числителей и знаменателей подходящих дробей:

$$p_{-1} = 1, p_0 = a_0, p_n = a_n p_{n-1} + p_{n-2}$$
$$q_{-1} = 1, q_0 = 1, q_n = a_n q_{n-1} + q_{n-2}$$

Таким образом, величины p_n и q_n представляются значениями континуант:

$$p_n = K_{n+1}(a_0; a_1; ..; a_n)$$
$$q_n = K_n(a_0; a_1; ..; a_n)$$

Последовательности $\{p_n\}$ и $\{q_n\}$ являются возрастающими.

Числители и знаменатели соседних подходящих дробей связаны соотношением:

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1} \qquad (1),$$

которое можно переписать в виде

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1} q_n}.$$

Откуда следует, что

$$\left| x - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{q_{n-1} q_n} < \frac{1}{q_{n-1}^2}.$$

5.3. Приближение вещественных чисел рациональными

Цепные дроби позволяют эффективно находить хорошие рациональные приближения вещественных чисел. А именно, если вещественное число x разложить в цепную дробь, то её подходящие дроби будут удовлетворять неравенству

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Отсюда, в частности, следует:

- подходящая дробь $\frac{p_n}{q_n}$ является наилучшим приближением для x среди всех дробей, знаменатель которых не превосходит q_n;
- мера иррациональности любого иррационального числа не меньше 2.

Примеры.

Разложим число $\pi = 3{,}14159265..$ в непрерывную дробь и подсчитаем его подходящие дроби:

$$3, {}^{22}/_{7}, {}^{333}/_{106}, {}^{355}/_{113}, {}^{103993}/_{33102}, ..$$

Вторая дробь (${}^{22}/_{7}$) — это известное архимедово приближение. Четвёртая (${}^{355}/_{113}$) была впервые получена в Древнем Китае.

В теории музыки требуется отыскать рациональное приближение для $\log_2 {}^{3}/_{2} \approx 0{,}585$. Третья подходящая дробь: ${}^{7}/_{12}$ соответствует классической октаве из 12 полутонов.

5.4. Свойства и примеры

Любое рациональное число может быть представлено в виде конечной цепной дроби двумя способами, например:

$$\frac{9}{4} = [2; 3; 1] = [2; 4]$$

Теорема Лагранжа. Число представляется в виде бесконечной периодической цепной дроби тогда и только тогда, когда оно является иррациональным решением квадратного уравнения с целыми коэффициентами.

Например:

$$\sqrt{2} = [1; 2{,}2{,}2{,}2{,}..]$$

золотое сечение $\emptyset = [1; 1{,}1{,}1{,}..]$

Для остальных — не квадратичных — алгебраических чисел характер разложений совершенно не известен. До сих пор неизвестно разложение хотя бы одного алгебраического числа степени $N > 2$ в цепную дробь.

Для некоторых трансцендентных чисел можно найти простую закономерность. Например, для основания натурального логарифма:

$$e - 1 = [1; 1; 2; 1; 1; 4; 1; 1; 6; 1; 1; 8; ..; 1; 1; 2n - 2; 1; 1; 2n; ..]$$

для числа

$$tg1 = [1; 1; 1; 3; 1; 5; 1; 7; ..; 1; 2n + 1; 1; 2n + 3; ..]$$

Для числа пи подобной закономерности не выявлено:

$$\pi = [3; 7{,}15{,}1{,}292{,}1{,}1{,}1{,}2{,}1{,}3{,}1{,}14{,}2{,}1{,}1{,}2{,}2{,}2{,}2{,}1{,}84{,}2{,}1{,}1{,}15{,}..]$$

Теорема Гаусса — Кузмина: Почти для всех (кроме множества меры нуль) действительных чисел существует среднее геометрическое коэффициентов соответствующих им цепных дробей, и оно равно одному и тому же числу.

5.5. Приложения цепных дробей

5.5.1. Решение сравнений первой степени

Рассмотрим сравнение $ax \equiv b(mod\ m)$, где $(a,m) = 1, a > 0$ (случай $a < 0$ сводится к данному).

Разложим $\frac{m}{a}$ в непрерывную дробь и обозначим ее подходящие дроби через $\frac{p_k}{q_k}$, $k = 1,2,..,n$.

Тогда, согласно свойству несократимости подходящих дробей, получим $p_k = m, q_k = a.$ Поэтому вместо соотношения

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^k$$

имеем

$$m q_{k-1} - p_{k-1} a = (-1)^k.$$

Отсюда

$$a p_{k-1} = -(-1)^k + m q_{k-1}$$

или (т.к. $q_{k-1} -$ целое число)

$$a p_{k-1} \equiv (-1)^{k-1} (mod\ m).$$

Умножая обе части этого сравнения на $(-1)^{k-1} \cdot b$, получим

$$a((-1)^{k-1} \cdot b \cdot p_{k-1}) \equiv b(mod\ m).$$

Сравнивая это сравнение с исходным, приходим к выводу, что оно имеет решение

$$x \equiv (-1)^{k-1} \cdot b \cdot p_{k-1} (mod\ m),$$

где $p_{k-1} -$ числитель предпоследней дроби в разложении.

Вывод: класс вычетов $x \equiv (-1)^k \cdot p_{k-1} \cdot b(mod\ m)$ является решением исходного сравнения.

5.5.2. Пример решения сравнения

$$12x \equiv 19(mod 29)$$

$$\frac{29}{12} = 2 + \frac{5}{12} = 2 + \frac{1}{\frac{12}{5}} = 2 + \frac{1}{2 + \frac{2}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{2}}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}$$

Построение подходящей дроби

Номер №	-1	0	1	2	3	4
Член непрерывной дроби			2	2	2	2
Числитель подходящей дроби	0	1	2	5	12	29
Знаменатель подходящей дроби	1	0	1	2	5	12

$$x \equiv (-1)^4 \cdot 12 \cdot 19(mod 29)$$

$$x \equiv 228(mod 29)$$

$$x \equiv 25(mod 29)$$

5.5.3. Другие приложения

- Доказательство иррациональности чисел.
- Определение заведомо трансцендентного числа (теорема Лиувилля).
- Алгоритмы факторизации SQUFOF и CFRAC.
- Характеристика стабильных, ортогональных многочленов.
- Цепные дроби использовались для расчета календарей.

5.6. Историческая справка

Античные математики умели представлять отношения несоизмеримых величин в виде цепочки последовательных подходящих отношений, получая эту цепочку с помощью алгоритма Евклида. По-видимому, именно таким путём Архимед получил приближение $\sqrt{3} \approx \frac{1351}{780}$ — это 12-я подходящая дробь для $\sqrt{3}$ или 1/3 от 4-й подходящей дроби для $\sqrt{27}$.

В V веке индийский математик Ариабхата применял аналогичный «метод измельчения» для решения неопределённых уравнений первой и второй степени. С помощью этой же техники было, вероятно, получено известное приближение для числа π (355/113). В XVI веке Рафаэль Бомбелли извлекал с помощью цепных дробей квадратные корни (см. его алгоритм).

Начало современной теории цепных дробей положил в 1613 году Пьетро Антонио Катальди. Он отметил основное их свойство (положение между подходящими дробями) и ввёл обозначение, напоминающее современное. Позднее его теорию расширил Джон Валлис, который и предложил термин *«непрерывная дробь»*. Эквивалентный термин «*цепная дробь*» появился в конце XVIII века.

Применялись эти дроби в первую очередь для рационального приближения вещественных чисел; например, Христиан Гюйгенс использовал их для проектирования зубчатых колёс своего планетария. Гюйгенс уже знал, что подходящие дроби всегда несократимы и что они представляют наилучшее рациональное приближение.

В XVIII веке теорию цепных дробей в общих чертах завершили Леонард Эйлер и Жозеф Луи Лагранж.

6. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. $9x \equiv 12(\mathrm{mod}21)$
2. $9x \equiv 2(\mathrm{mod}14)$
3. $7x \equiv 10(\mathrm{mod}11)$
4. $5x \equiv 3(\mathrm{mod}6)$
5. $28x \equiv 40(\mathrm{mod}44)$
6. $3x \equiv 4(\mathrm{mod}7)$
7. $5x \equiv 4(\mathrm{mod}11)$
8. $5x \equiv 2(\mathrm{mod}8)$
9. $3x \equiv 1(\mathrm{mod}10)$
10. $3x \equiv 7(\mathrm{mod}31)$
11. $14x \equiv 35(\mathrm{mod}19)$
12. $4x \equiv 3(\mathrm{mod}9)$
13. $3x \equiv 5(\mathrm{mod}11)$
14. $3x \equiv 12(\mathrm{mod}15)$
15. $3x \equiv 1(\mathrm{mod}19)$
16. $7x \equiv 3(\mathrm{mod}7)$
17. $9x \equiv 3(\mathrm{mod}7)$
18. $8x \equiv 2(\mathrm{mod}9)$
19. $3x \equiv 4(\mathrm{mod}19)$
20. $2x \equiv 6(\mathrm{mod}12)$
21. $2x \equiv 10(\mathrm{mod}15)$
22. $24x \equiv 14(\mathrm{mod}26)$
23. $11x \equiv 11(\mathrm{mod}17)$
24. $9x \equiv 3(\mathrm{mod}10)$
25. $3x \equiv 5(\mathrm{mod}11)$
26. $7x \equiv 3(\mathrm{mod}7)$
27. $3x \equiv 9(\mathrm{mod}12)$
28. $5x \equiv 3(\mathrm{mod}9)$
29. $7x \equiv 1(\mathrm{mod}8)$
30. $3x \equiv 5(\mathrm{mod}13)$
31. $12x \equiv 7(\mathrm{mod}13)$
32. $7x \equiv 9(\mathrm{mod}4)$
33. $5x \equiv 1(\mathrm{mod}13)$
34. $4x \equiv 3(\mathrm{mod}7)$
35. $6x \equiv 3(\mathrm{mod}15)$
36. $5x \equiv 20(\mathrm{mod}51)$
37. $11x \equiv 12(\mathrm{mod}41)$
38. $7x \equiv 8(\mathrm{mod}9)$
39. $3x \equiv 9(\mathrm{mod}23)$
40. $3x \equiv -5(\mathrm{mod}37)$
41. $3x \equiv 9(\mathrm{mod}12)$
42. $4x \equiv 20(\mathrm{mod}9)$
43. $5x \equiv 3(\mathrm{mod}17)$
44. $7x \equiv 10(\mathrm{mod}13)$
45. $3x \equiv 8(\mathrm{mod}12)$
46. $7x \equiv 13(\mathrm{mod}17)$
47. $11x \equiv 16(\mathrm{mod}23)$
48. $8x \equiv 4(\mathrm{mod}7)$
49. $97x \equiv 11(\mathrm{mod}41)$
50. $7x \equiv 3(\mathrm{mod}8)$

51. $21x \equiv 5 \pmod{35}$
52. $3x \equiv 4 \pmod{7}$
53. $6x \equiv 2 \pmod{9}$
54. $7x \equiv 19 \pmod{3}$
55. $17x \equiv 89 \pmod{4}$
56. $5x \equiv 3 \pmod{11}$
57. $7x \equiv 10 \pmod{13}$
58. $5x \equiv 7 \pmod{11}$
59. $9x \equiv 12 \pmod{21}$
60. $9x \equiv 2 \pmod{14}$
61. $12x \equiv 7 \pmod{13}$
62. $6x \equiv 9 \pmod{15}$
63. $3x \equiv 5 \pmod{14}$
64. $16x \equiv 4 \pmod{14}$
65. $19x \equiv 5 \pmod{7}$
66. $5x \equiv 1 \pmod{11}$
67. $8x \equiv 2 \pmod{7}$
68. $7x \equiv 10 \pmod{11}$
69. $7x \equiv 9 \pmod{15}$
70. $13x \equiv 3 \pmod{11}$
71. $2x \equiv 14 \pmod{15}$
72. $5x \equiv 2 \pmod{3}$
73. $2x \equiv 7 \pmod{15}$
74. $9x \equiv 22 \pmod{23}$
75. $15x \equiv 2 \pmod{19}$
76. $9x \equiv 12 \pmod{17}$
77. $4x \equiv 6 \pmod{22}$
78. $2x \equiv 8 \pmod{11}$
79. $3x \equiv 3 \pmod{21}$
80. $17x \equiv 9 \pmod{39}$

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Разложение числа в цепную дробь.
2. Подходящие дроби.
3. Приближение вещественных чисел.
4. Применения цепных и подходящих дробей.
5. Теорема Лагранжа.
6. Условия разрешимости сравнения.
7. Решение сравнений первой степени с помощью подходящих дробей.

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. В. И. Арнольд Цепные дроби. — М.: МЦНМО, 2000. — Т. 14. — 40 с. — (Библиотека «Математическое просвещение»).
2. Н. М. Бескин Цепные дроби // Квант. — 1970. — Т. 1. — С. 16—26.
3. Н. М. Бескин Бесконечные цепные дроби // Квант. — 1970. — Т. 8. — С. 10—20.
4. С. Н. Гладковский Анализ условно-периодических цепных дробей, ч. 1. — Незлобная: 2009. — 138 с.
5. С. В. Сизый Лекции по теории чисел. — Екатеринбург: Уральский государственный университет им. А. М. Горького, 1999.