УДК 681.3.06

М.М. Колодницький, к.т.н., доц.
І.І. Самолюк, студ.
Житомирський інженерно-технологічний інститут

БІБЛІОТЕКА АЛГОРИТМІВ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ З ТЕОРІЇ ПОРІВНЯНЬ

Описано бібліотеку алгоритмів для розв'язання порівнянь, наведена її структура. Розглянуто один із алгоритмів бібліотеки – розв'язання порівняння першого степеня. Наведені приклади розв'язання задач за допомогою розроблених алгоритмів.

Бурхливий розвиток комп'ютерно-інформаційних технологій (КІТ) призвів до їх широкого використання в різних фундаментальних науках, зокрема, в математиці та її застосуваннях. Причому, застосування КІТ почали проникати у такі розділи математики, які раніше не мали прикладного значення і розглядалися як суто теоретичні. Так, наприклад, ще недавно теорія чисел вважалася суто теоретичним розділом математики, а багато її задач здавалися надто складними для розв'язку. Пізніше виявилося, що ідеї теорії чисел можуть бути покладеними в основу таких прикладних наук, як теорія захисту інформації, криптографія, теорія кодів, що виправляють помилки, тощо, тобто наук, що є базою КІТ. Таким чином, існує взаємозв'язок та взаємовплив між, здавалося, суто теоретичними розділами математики та суто прикладними комп'ютерними науками та технологіями. Отже, задача дослідження певних теоретичних математичних проблем із використанням сучасних КІТ є, як бачимо, досить актуальною. Особливо цікавим є застосування КІТ з метою вивчення, викладання, дослідження і розв'язання математичних задач.

В даній статті наведено приклад застосування КІТ для розв'язання задач одного з розділів теорії чисел – порівнянь за модулем. Описано бібліотеку алгоритмів для розв'язання порівнянь за модулем (з теорією порівнянь можна ознайомитися, наприклад, в [1, 2]). Ця бібліотека включена до складу прикладної програмної системи "DSR Open Lab 1.0" [3], що призначена для вирішення задач математичного моделювання складних динамічних систем.

На основі вивчення теорії порівнянь були розроблені алгоритми для розв'язання порівнянь з одним невідомим і їх систем, знаходження кореня n-го степеня за простим модулем, визначення індексів чисел за простим модулем тощо. Вони об'єднані в бібліотеку, яка має таку структуру:

1. Розв'язання алгебраїчних порівнянь.
    1. Першого порядку.
    2. Двочленні порівняння.
        1. Квадратичні лишки.
            1. Символ Якобі.
            2. Квадратний корінь.
        2. Лишки n-го степеня.
            1. Корінь n-го степеня.
    3. n-го порядку.
2. Розв'язання систем алгебраїчних порівнянь.
    1. Першого порядку.
    2. n-го порядку.
3. Показникові порівняння.
    1. Знаходження показника, до якого належить число.
    2. Знаходження первісних коренів за простим модулем.
    3. Знаходження індексу числа за простим модулем.
    4. Знаходження числа за заданим індексом за простим модулем.
    5. Побудова таблиці індексів за простим модулем.
        1. Відсортованої в порядку зростання індексів.
        2. Відсортованої в порядку зростання чисел.
    6. Розв'язання показникового порівняння за простим модулем.
4. Функція Ейлера.

Алгоритми в бібліотеці поділені на чотири розділи, кожен із яких відповідає окремому розділу теорії порівнянь. Останній алгоритм обчислення однієї з найважливіших функцій в теорії цілих чисел – функції Ейлера $\varphi(n)$, що визначає кількість чисел взаємно простих зі заданим n і менших за нього. Як видно, в бібліотеці зібрані основні алгоритми для вирішення задач, пов'язаних з теорією порівнянь.

Розроблені алгоритми, в основному, не складні та досить наглядні, оскільки розв'язок відшукується в деякому скінченному кільці класів за модулем m і тому можна за допомогою скінченного числа операцій знайти всі розв'язки задачі, тобто це типова задача для ЕОМ – перебір певного масиву чисел і перевірка виконання деяких умов, наприклад, рівності нулю остачі від ділення. Таким типовим алгоритмом є, наприклад, алгоритм розв'язання порівняння першого порядку виду $ax \equiv b \pmod m$, який наведено на рис. 1. В основу даного алгоритму покладений той факт, що для знаходження розв'язків порівняння достатньо послідовно підставляти в порівняння замість невідомого x число із повної системи лишків (ПСЛ), і перевіряти виконання порівняння. Якщо при деякому x порівняння виконується, то знайдено розв'язок порівняння.

```
Початкові дані:  a, b – коефіцієнти порівняння;
                 m – модуль порівняння.
Результат:       rootsArray – масив розв'язків порівняння.

1. Введення початкових даних: a, b, m.
2. Знаходження найбільшого спільного дільника (a, m) коефіцієнта a і
   модуля m.
3. Перевірка чи має розв'язки порівняння:
   Умова: якщо b ділиться на (a, m) то:
      A = a / (a, m);
      B = b / (a, m);
      M = m / (a, m);
      Цикл ( зміна i від 0 до M – 1 з кроком 1 )
            Умова: якщо A * i % M = B то:
                  Формування масиву розв'язків:
                  Цикл ( зміна j від 0 до (a, m) – 1 з кроком 1 )
                     RootsArray[ j ] = i + j * M;
                  Кінець циклу.
                  Вихід з циклу.
            Кінець умови.
      Кінець циклу.
   Інакше
      Розв'язків немає.
   Кінець умови.
Виведення результату: rootsArray.
```

Рис. 1. Алгоритм розв'язання порівняння першого порядку

Як видно, алгоритм складається з чотирьох основних частин: введення даних, перевірки чи має розв'язки порівняння, циклу, в якому, власне, виконується розв'язання шляхом послідовного перебору чисел із ПСЛ, виведення даних. З іншими алгоритмами із даної бібліотеки можна ознайомитися в посібнику [2].

На рис. 2 наведено приклади розв'язання задач із теорії порівнянь за допомогою описаної бібліотеки.

Розв'язання порівняння першого порядку:

$135x \equiv 555 \pmod{72801435}$.

$x \equiv$ 539274, 5392703, 10246132, 15099561, 19952990, 24806419, 29659848, 34513277, 39366706, 44220135, 49073564, 53926993, 58780422, 63633851, 68487280 (mod 72801435).

Розв'язання порівняння 5-го степеня:

$x^5 - 16x^4 + 11x^3 - 66x^2 + 65x - 50 \equiv 0 \pmod{20420}$.

$x \equiv 458, 666, 1422, 4542, 4750, 5506, 8626, 9590, 12710, 12918, 17002, 17758 \pmod{20420}$.

Розв'язання системи порівнянь:

$19x \equiv 103 \pmod{900}$,

$10x \equiv 511 \pmod{841}$.

$x \equiv 58837 \pmod{756900}$.

Розв'язання показникового порівняння:

$135^{x^4+4x^3+x^2-3x+1} \equiv 7^{x^2-5x+1} \pmod{503}$.

$x \equiv 179, 395 \pmod{502}$.

Таблиця індексів за модулем 17 при первісному корені 3:

Індекс	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Рис. 2. Приклади розв'язання задач за допомогою описаної бібліотеки

Бібліотеки для розв'язання задач, пов'язаних з теорією порівнянь, є не у всіх сучасних математичних комп'ютерних системах. Таких бібліотек, наприклад, не мають відомі обчислювальні програми MathCAD 2000, MATLAB 5.2. За своєю функціональністю розроблена бібліотека не відстає від аналогічних бібліотек Maple V Release 5, Mathematica 4.0. Використовуючи алгоритми описаної бібліотеки, можна розв'язати більшість задач теорії порівнянь. Отже, дана бібліотека буде корисною при вивченні і викладанні теорії чисел, програмування та обчислювальних методів, при розв'язанні відповідних математичних задач, а також проведенні певних наукових робіт.

ЛІТЕРАТУРА:

1. *Завало С.Т.*, *Костарчук В.Н.*, *Хацет Б.И.* Алгебра и теория чисел. – Ч. 2. – Киев: Вища школа, 1980. – 408 с.
2. *Колодницький М.М.* Основи теорії математичного моделювання систем. – Житомир, 2001. – 700 с.
3. *Колодницький М.М.* Програмна система "DSR Open Lab 1.0": сучасний засіб автоматизації математичного моделювання // Вісник ЖІТІ. – 2000. – № 14.

КОЛОДНИЦЬКИЙ Микола Михайлович – кандидат технічних наук, доцент кафедри Житомирського інженерно-технологічного інституту.

Наукові інтереси:

– математичне моделювання технічних систем;

– комп'ютерно-інформаційні технології.

САМОЛЮК Ігор Іванович – студент 4 курсу факультету інформаційно-комп'ютерних технологій Житомирського інженерно-технологічного інституту.

Наукові інтереси:

– комп'ютерно-інформаційні технології.

Подано 21.05.2001

Колодницький М.М., Самолюк І.І. Бібліотека алгоритмів для розв'язання задач з теорії порівнянь

Колодницкий Н.М., Самолюк И.И. Библиотека алгоритмов для решения задач по теории сравнений

Kolodnitsky N.M., Samolyuk I.I. The library of algorithms for solving congruences

УДК 681.3.06

Библиотека алгоритмов для решения задач по теории сравнений / Н.М. Колодницкий, И.И. Самолюк

Описана библиотека алгоритмов для решения сравнений, приведена ее структура. Рассмотрен один из алгоритмов библиотеки – решение сравнения первой степени. Приведены примеры решения задач с помощью разработанных алгоритмов.

УДК 681.3.06

The library of algorithms for solving congruences / N.M. Kolodnitsky, I.I. Samolyuk

In this article the library of algorithms for solving congruences is described, its structure is adduced. One of algorithms of the library is viewed – solving the 1st order congruence. The examples of solving some tasks using developed algorithms are cited.