Дано опис основних команд пакету numtheory системи комп'ютерної алгебри Maple. Розглянуто способи розв'язання деяких типових обчислювальних задач елементарної теорії чисел в Maple. Зокрема розглянуті команди для наступних розділів: подільність чисел, арифметичні та мультиплікативні функції, порівняння, символи Якобі та Лежандра, первісні корені та дискретні логарифми

Ключові слова: теорія чисел, Maple, алгоритми, подільність, порівняння, символ Лежандра, первісні корені

Дано описание основных команд пакета numtheory системы компьютерной алгебры Maple. Рассмотрены способы решения некоторых типичных вычислительных задач элементарной теории чисел в Maple. В частности рассмотрены команды для следующих разделов: делимость чисел, арифметические и мультипликативные функции, сравнения, символы Якоби и Лежандра, первообразные корни и дискретные логарифмы

Ключевые слова: теория чисел, Maple, алгоритмы, делимость, сравнения, символ Лежандра, первообразные корни

УДК 510.6

ВИКОРИСТАННЯ СИСТЕМИ КОМП'ЮТЕРНОЇ АЛГЕБРИ MAPLE В ЕЛЕМЕНТАРНІЙ ТЕОРІЇ ЧИСЕЛ

Л. П. Бедратюк
Доктор фізико-математичних наук,
завідувач кафедри*
E-mail: leonid.uk@gmail.com
Г. І. Бедратюк
Старший викладач*
E-mail: bedratyuk@ukr.net
*Кафедра програмної інженерії
Хмельницький національний університет
вул. Інститутська, 11, м. Хмельницький,
Україна, 29016

1. Вступ

Система комп'ютерної алгебри Maple перший реліз якої випущений у 1981 році канадською фірмою Waterloo Maple, Inc., успішно поєднує символьні маніпуляції, обчислювальну математику, потужну графіку та зручну мову програмування. В силу своєї зручності та універсальності система Maple стала незамінним інструментом наукових досліджень для багатьох вчених, інженерів та студентів.

Останнім часом спостерігається активне проникнення систем комп'ютерної алгебри в освітній процес оскільки це дає можливість формування принципово нових технологій навчання [1 – 3].

Практично для кожного розділу математики в Maple розроблено окремий спеціалізований пакет команд. Проте на даний час ці технології, незважаючи на свою ефективність та наочність, в силу різних причин, ще недостатньо поширені в навчальному процесі.

2. Аналіз джерел та постановка проблеми

Метою даної статті є розгляд основних команд спеціалізованого пакету **numtheory**, який розроблений для розв'язання типових задач теорії чисел. Початкові навики роботи в системі комп'ютерної алгебри Maple, детально розглянуто в [4 – 5]. Також, ми будемо дотримуватися стандартної термінології елементарної теорії чисел, див. [6 – 7].

Дана стаття є продовженням статті [8], спрямованих на популяризацію систем комп'ютерної алгебри. Матеріали статті можуть бути використані студентами та викладачами ВНЗ для розв'язання типових задач, які зустрічаються в процесі вивчення дисциплін "Дискретна математика", "Дискретні структури", "Захист інформації", "Безпека програм та даних".

3. Опис пакету numtheory

Дамо короткий опис тієї частини мови програмування системи Maple та стандартних процедур, які необхідні для вирішення типових задач елементарної теорії чисел.

Пакет **numtheory** являє собою великий набір процедур для роботи з цілими та раціональними числами, числами Гауса, многочленами над скінченними полями, мультиплікативними функція та стандартними іменованими числами. У цій статті ми опишемо лише команди для роботи з цілими числами.

Для підключення пакету **numtheory** потрібно в робочому рядку Maple після символу запрошення введення команди > набрати командний рядок такого вигляду:

> with(numtheory):

Розглянемо основні типи команд з цього пакету.

3.1. Подільність чисел. Нагадаємо, що, згідно основної теореми арифметики, для всякого натурального числа n>1 має місце його розклад у вигляді добутку простих чисел:

$$n = p_1^{\alpha 1} \; p_2^{\alpha 2} \; \ldots p_k^{\alpha k}.$$

де p_i – і-те просте число, а α_i – натуральне число. Такий запис називається канонічним розкладом.

Канонічний розклад числа отримується при допомозі команди **ifactor:**

>ifactor(30!);

$226 \cdot 314 \cdot 57 \cdot 74 \cdot 112 \cdot 132 \cdot 17 \cdot 19 \cdot 23\ 29$.

Команда **divisors(n)** знаходить множину всіх дільників числа n:

>divisors(128);

{1, 2, 4, 8, 16, 32, 64, 128}.

Для знаходження простого числа із порядковим номером і використовується команда **ithprime(i)**, а для перевірки того, чи дане число n є простим, – команда isprime(n):

> isprime(123454321);

false

> ithprime(15);isprime(%);

47

true.

Команди **nextprime(n)** і **prevprime(n)** знаходять відповідно найменше просте число яке перевищує число n і найбільше просте число яке не перевищує:

> nextprime(2013),prevprime(2013);

2017, 2011.

Задача 1. *Знайти всі числа-близнюки серед перших 50 простих чисел.*

Прості числа називаються простими, якщо різниця між ними рівна 2.

Відповідна програма має вигляд:

> BL:={}:for i from 1 to 50 do
if ithprime(i+1) = ithprime(i) + 2 then
BL:=BL union {[ithprime(i),ithprime(i+1)]};
end if;end do: BL;

[3,5],[5,7],[11,13],[17,19],[29,31],[41,43],[59,61], [71,73],[101,103],[107,109],[137,139],

[149,151],[179,181],[191,193],[197,199],[227,229].

Команда **factorset(n)** обчислює множину простих дільників числа n:

> factorset(2013*2014);

{2, 3, 11, 19, 53, 61}.

Задача 2. *Знайти спільні прості дільники чисел 12345678 і 1112131415161718.*

Маємо

> factorset(12345678) intersect factorset (1112131415171718);

{2, 3}.

3.2. НСД та розширений алгоритм Евкліда.

При діленні з остачею числа a на число b остача від ділення знаходиться командою **irem(a,b)** а частка командою **iquo(a,b):**

> irem(13,4),iquo(13,4);

1, 3.

Функції **igcd, ilcm** знаходять найбільший спільний дільник та найменше спільне кратне довільного набору цілих чисел:

> igcd(-10, 6, -8);

2.

> ilcm(-10, 6, -8);

120.

Команда igcdex реалізує розширений алгоритм Евкліда, і для заданих цілих чисел a і b знаходить їхні коефіцієнти Безу, тобто такі цілі числа x і y, для яких виконується рівність $x \cdot a + y \cdot b = d$, де d = (a,b):

> igcdex(2,3,'x','y');x, y;

1

-1, 1.

3.3. Арифметичні функції.

Нагадаємо, що арифметичною функцією називається довільна функція $f:N \to C$. Часто використовуються такі функції:

- **trunc(x)** – округлює число x до найближчого цілого в напрямку до 0. Відповідає стандартному позначенню [x].

> trunc(Pi),trunc(3.9),trunc(-1.9);

3, 3, -1,

- **round** - округлює число до найближчого цілого:

> round(Pi),round(3.9),round(-1.9);

3, 4, -2,

- **frac** – знаходить дробову частину числа, відповідає стандартному позначенню {x}=x-[x]:

> frac(Pi),frac(3.9),frac(-1.9);

π – 3, 0.9, -0.9,

- **floor** – знаходить найбільше ціле число, яке менше або дорівнює даному числу

> floor(Pi),floor(3.9),floor(-1.9);

3, 3, -2,

- **ceil** – знаходить найменше ціле число, яке більше або рівне даному числу

> ceil(Pi),ceil(3.9),ceil(-1.9);

4, 4, -1.

Задача 3. *Знайти показник, з яким число 7 входить в канонічний розклад 50!*

Згідно формули Лежандра, якщо

$n! = p_1^{\alpha 1}\ p_2^{\alpha 2} \ldots p_k^{\alpha k}$,

то показник α_i дорівнює

$$\alpha_i = \sum_{i>0} \left[\frac{n}{p_k^i} \right].$$

Відповідна Maple процедура має вигляд

> P:=proc(n,d) local a,P: a:=round(n/d):P:=a: while a>0 do d:=d*d:a:= round(n/d): P:=P+a end do: return (P) end proc:P(50,7);

8.

Важливі мультиплікативні функції теорії чисел задаються таким чином:

- **tau(n)** обчислює кількість додатніх дільників числа n:

> divisors(128);tau(128);

{1, 2, 4, 8, 16, 32, 64, 128},

8.

- **sigma(n)** обчислює суму додатніх дільників числа n:

> divisors(128);sigma(128);

{1, 2, 4, 8, 16, 32, 64, 128},

255,

- **phi(n)** обчислює функцію Ейлера $\varphi(n)$, тобто кількість додатніх чисел, які не перевищують число n і є взаємно прості з ним:

> phi(128);

64.

- **mobius(n)** обчислює функцію Мебіуса

> mobius(2013);

-1.

- **lambda(n)** обчислює значення функції Кармайкла, тобто найменшого числа $\lambda(n)$, такого, що $n \mid a^{\lambda(n)} - 1$ при (n,a)=1.

Задача 4. *Перевірити співвідношення* $\sum_{d|n} \varphi(d) = n$ *для n=2013.*

Програма на Maple має вигляд

> DD:=divisors(2013);S:=0:for i in DD do S:=S+ +phi(i) end do:is(S=2013);

DD: = (1, 3, 11, 33, 61, 183, 671, 2013},

true.

Задача 5. *Обчислити перші 10 членів послідовності Роланда,*

$\{a_{i+1}-a_i\}$, $a_n=a_{n-1}+(n,a_{n-1})$, $a_1=7$.

Програма на Maple має вигляд

> a:= proc(n) local T: if n=1 then T:=7 else a(n-1)+igcd(n,a(n-1)); end if; end proc:

> seq(R(i+1)-R(i),i=1..10);

1, 1, 1, 5, 3, 1, 1, 1, 1, 11.

Відомо, що всі елементи цієї послідовності, які відмінні від l є простими числами.

3.4. Порівняння

Для обчислення за модулем цілого числа використовується команда

a mod b:

> 15 mod 2, 7^5 mod 11, 1/3 mod 26;

1, 10, 9.

Перевірку того, чи два числа a і b порівняльні за модулем n можна виконати при допомозі логічного оператора **is:**

> is(15=23 mod 3);

false.

Для розв'язання систем лінійних рівнянь за спільним модулем n використовується команда **msolve:**

> msolve({3*x-4*y=1,7*x+y=2},19);

{x = 15, y = 11}.

Систему рівнянь вигляду $x=a_i \bmod b_i$ розв'язують при допомозі команди **chrem([a],[b])**(китайська теорема про остачі):

> chrem([2,3,2],[3,5,7]);

23.

Квадратний корінь із числа a за модулем n (якщо він існує) знаходиться командою **msqrt(a,n):**

> msqrt(3,11),msqrt(3,7);

5, FAIL.

Символ Лежандра $\left(\frac{a}{p}\right)$ обчислює функція **legendre (a, p):**

> legendre(2,5);

-1.

Задача 6. *Перевірити формулу Ейзенштейна для символу Лежандра*

$$\left(\frac{p}{q}\right)=\prod_{n=1}^{\frac{p-1}{2}}\frac{\sin(\frac{2\pi qn}{p})}{\sin(\frac{2\pi q}{p})}.$$

для перших 10 пар сусідніх простих чисел.

Пишемо процедуру на Maple, яка виконує обчислення за формулою Ейзенштейна:

> Lg:=(q,p)-> product(sin(2*Pi*q*n/p)/sin (2*Pi*n/p), n=1..(p-1)/2);

Порівнюємо результат обчислень за цією формулою із стандартною процедурою:

> f:=0:for i from 1 to 10 do if Lg(ithprime(i), ithprime(i+1))=

legendre(ithprime(i),ithprime(i+1))

then f:=f+1 end if; end do; is(f=10);

true.

Символ Якобі обчислює функція **jacobi(a, b)**:

> jacobi(3,10);

1.

Символи Лежандра та Якобі використовуються для встановлення числа розв'язків модулярних квадратних рівнянь.

Задача 7. *Скільки розв'язків має рівняння* $3x^2+4x+5=0$ *за модулями 7, 9,12,15,17?*

Домножимо рівняння на 3. Отримаємо

$9x^2+12x+15=(3x+2)^2+11=0=(3x+2)\text{^}2=-11.$

Знаходимо символи Якобі

> jacobi(-11,7),jacobi(-11,9),jacobi(-11,12),jacobi (- 11,15),jacobi(-11,17);

-1, 1, 1, 1, -1.

Отже, рівняння має розв'язки за модулями 9, 12, 15, а за модулями 7, 17 розв'язків немає.

Самі розв'язки можна знайти при допомозі команди msolve:

> msolve(3*x^2+4*x+5,9);msolve(3*x^2+4*x+5,12); msolve(3*x^2+4*x+5,15);

{x = 7},

{x = 1}, {x = 7},

{x = 7}, {x = 10}.

Якщо нам потрібно знати кратності коренів рівняння то для цього використовується команда **Roots:**

> Roots(x^3-x) mod 6;

[[0,1], [1,1], [2,1], [3,1], [4,1], [5,1]].

В квадратних дужках на першому місці знаходиться корінь, а на другому – його кратність.

3.5. Первісні корені та дискретні логарифми.

Порядком числа a за модулем n, (a,n)=1, називається найменше число r, таке, що $a^r=1 \bmod n$. Порядок числа шукає команда **order:**

> order(7,12),order(2013,nextprime(2013));

2, 168.

Перевірка

> 7^order(7,12) mod 12;

1.

Число a називається первісним коренем за модулем n, якщо його порядок за модулем n дорівнює знайченню функції Ейлера $\varphi(n)$. Найменший первісний корінь за даним модулем знаходить команда **primroot:**

> primroot(41);

6.

Перевірка

> order(6,41),phi(41);

40, 40.

Первісні корені за модулем n існують лише тоді, коли множина ненульових елементів в кільці Z_n утворює циклічну групу. У цьому випадку кожен ненульовий елемент $x \in Z_n$ подається як степінь породжуючого елемента a цієї групи. Цей степінь називається дискретним логарифмом (або індексом) числа x за модулем n і основою a і позначається $\log_a x$. Дискретний логарифм знаходить команда mlog(x,a,n):

> mlog(9,4,11);

3.

> 4^3 mod 11;

9.

Задача 8. *Перевірити явну формулу [9] для обчислення дискретного лагарифма*

$$\log_a x=\sum_{i=1}^{p-2}\frac{x^i}{1-a^i} \bmod p.$$

для x=9, a=6, p=41.

Процедура на Maple

> Dlog:=(x,a,p)->add(x^i/(1-a^(i)),i=1..p-2) mod p;

$$\mathrm{Dlog} := (x,a,p) \to \mathrm{add}\left(\frac{x^i}{1-a^i}, i = 1..p-2\right) \bmod p.$$

Знаходимо

> Dlog(9,6,41), mlog(9,6,41);

30, 30.

4. Висновки

В статті дано опис опис команд пакету **numtheory** системи комп'ютерної алгебри **Maple**. Розглянуто способи розв'язання деяких типових задач елементарної теорії чисел в **Maple**.

Використовуючи розглянуті команди пакету **Maple** можна ілюструвати розв'язання задач на заняттях із курсу дискретної математики, дискретних структур, теорії чисел.

Література

1. Черняк, А. А. Синтез классической и компьютерной математики в обучении [Текст] /А. А. Черняк, Ю. А. Доманова, Т. Н. Ранько // Информатизация образования. –2005. – № 1. –С. 36–45.
2. Samkova, L. Calculus of one and more variables with Maple [Текст] / L. Samková // International Journal of Mathematical Education in Science and Technology. –2012. – V. 43. –№2.–P.230-244.
3. Adym, E. The use of computers in mathematics education: A paradigm shift from "computer assisted instruction" towards "student rogramming" [Текст] /E.Adym // The Turkish Online Journal of Educational Technology. –2005. – 4(2).– P.27–34.
4. Дьяконов, В. П. Maple 9.5/10 в математике, физике и образовании [Текст] / В. П. Дьяконов. – М.: С.Пресс, 2000. – 453 с.
5. Васильев, А. Н. Maple 8. Самоучитель Текст] / А. Н. Васильєв. –М.: Диалектика, 2003.— 352 с.
6. Виноградов, И. М. Основы терии чисел [Текст] / И. М. Виноградов. –М.:Наука, 1981. –180 с.
7. Song, Y. Number Theory for Computing, Springer [Текст] / Y. Song. –Springer, –2002. – 453 p.
8. Бедратюк, Л. П. Системи комп'ютерної алгебри в теорії графів [Текст] / Л.П. Бедратюк, Г.І. Бедратюк // Східно-Європейський журнал передових технологій. – 2012. – № 6/4 (60). - С. 43-46.
9. Zhe-Xian Wan, A shorter proof for an explicit formula for discrete logarithms in finite fields [Текст] / W. Zhe-Xian // Discrete Mathematics. –2008. –Vol.308(21). – P. 4914–4915.