**УДК 004.9**

В. М. Михалевич, Л. О. Майданевич

# ВИКОРИСТАННЯ СИСТЕМИ MAPLE В МАТЕМАТИЧНИХ ЗАДАЧАХ КРИПТОГРАФІЇ. ПОВІДОМЛЕННЯ 1. ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ.

Вінницький національний технічний університет, Вінниця

**Анотація.** На основі аналізу літературних джерел зроблено висновок про актуальність використання середовища системи комп’ютерної математики Maple з метою створення програмного забезпечення для проведення наукових досліджень та створення навчально-методичнх матеріалів з розв’язання типових математичних задач криптографії. Зазначено, що найбільш відомий та поширений криптографічний алгоритм з відкритим ключем RSA базується на низці задач елементарної теорії чисел, що можуть бути розв’язані за допомогою стандартних засобів системи Maple. В цій роботі розглянуто вказані стандартні команди з демонстрацією прийомів їх застосування на спеціально розроблених прикладах. Розглянуто команди для розв’язання задач за такими розділами, як подільність цілих чисел, прості числа; найважливіші функції в теорії чисел: функції виділення цілої та дробової частин числа та мультиплікативні функції; конгруенції та системи конгруенцій першого порядку, квадратичні лишки. Наведено простий та ефективний алгоритм і програма визначення за домогою стандартних команд Maple простих чисел Мерсенна. Вказаний алгоритм базується на необхіднійумові простоти чисел Мерсенна. Продемонстровано роботу авторських навчальних Maple-тренажерів обчислення: за розширеним алгоритмом Евкліда; функції Ейлера; символу Лежандра; символу Якобі. Роботу навчального тренажера з обчисення функції Ейлера продемонстровано під час обчислення відповідного значення для простого числа, складеного числа, що є добутком двох простих, складеного числа, що є натуральним степенем простого числа, а також складених натуральних чисел довільної структури. За допомогою фрагментів програмного коду, що можуть бути покладені в основу розробки навчальних тренажерів продемонстровано визначення повної системи найменших невід'ємних лишків; повної системи абсолютно найменших та зведеної системи лишків за простим та складеним модулями.

**Ключові слова:** математичні задачі криптографії, теорія чисел, Maple, навчальні Maple-тренажери, алгоритм Евкліда, функція Ейлера, конгруенції, квадратичні лишки, символ Якобі**.**

**Abstract.** On the basis of the analysis of literary sources, a conclusion was made about the relevance of using the environment of the Maple computer mathematics system for the purpose of creating software for conducting scientific research and creating educational and methodological materials for solving typical mathematical problems of cryptography. It is noted that the most famous and widespread cryptographic algorithm with a public key RSA is based on a number of problems of elementary number theory that can be solved using standard tools of the Maple system. This work examines the specified standard commands with a demonstration of their application techniques on specially developed examples. The commands for solving problems in such sections as divisibility of whole numbers, prime numbers are considered; the most important functions in number theory: functions for selection of integer and fractional parts of a number and multiplicative functions; congruences and systems of congruences of the first order, quadratic remainders. A simple and effective algorithm and program for determining prime Mersenne numbers based on standard Maple commands is given. This algorithm is based on the necessary condition of simplicity of Mersenne numbers. The work of the author's educational Maple calculation simulators is demonstrated: according to the extended Euclid algorithm; Euler functions; symbol of Legendre; Jacobi symbol. The operation of the Euler function training simulator is demonstrated when calculating the corresponding value for a prime number, a composite number that is the product of two primes, a composite number that is a natural power of a prime number, as well as composite natural numbers of arbitrary structure. With the help of fragments of the program code, which can be used as a basis for the development of training simulators, the determination of the complete system of the smallest integral residues is demonstrated; of the complete system of the absolute smallest and the reduced system of remainders by simple and composite modules.

**Key words:** mathematical problems of cryptography, number theory, Maple, educational Maple simulators, Euclid's algorithm, Euler's function, congruences, quadratic remainders, Jacobi symbol.

**DOI: https://doi.org/10.31649/1999-9941-2024-59-1-105-118.**

## Вступ

Світова наукова спільнота постіно працює в напрямі пошуку, формування та вдосконалення принципово нових технологій навчання, що базуються на використанні інформаційних технологій [1, 2, 3, 4, 5, 6]. Розв’язання математичних задач криптографії, що в значній мірі базуються, зокрема, на задачах елементарної теорії чисел, звичайно передбачають проведення громіздких рутинних обчислень [1, 2, 3, 4, 6]. Такі обчислення можна проводити з використанням багатьох сучасних середовищ. Одним з найкращих представників таких середовищ є системи комп’ютерної математики (СКМ), зокрема, Maple - система, що спрямована на автоматизацію символьних та числових обчислень, аналіз і візуалізацію даних та навчальної інформації [7, 8, 9]. Ця система надає можливість швидко оволодіти основами методів для вирішення математичних задач та широко використовується в академічних та наукових галузях. Пошуки ефективних шляхів та прийомів застосування СКМ Maple під час розв’язання задач теорії чисел, лінійної й абстрактної алгебри, математичного аналізу, теорії ймовірностей та криптографічних перетворень розпочалися декілька десятків років тому [10, 11, 12, 13, 14]. З часом спостерігається посилення інтенсивності подібних пошуків [15, 16, 17, 18].

До суттєвих переваг таких систем можна також віднести простоту їх освоєння, у порівнянні, наприклад, з освоєнням середовища мови Pyton.

**Актуальність**

В той же час, серед численних публікацій, що присвячені описанню доволі ефективних прийомів використання СКМ Maple до розв'язання широкого кола математичних задач, подібних праць, в яких розглядаються задачі елементарної теорії чисел, лінійної алгебри, теорії ймовірностей, що безпосередньо пов'язані із математичними задачами криптографії, залишається недостатньо. До найбільш вдалих та грунтовних праць в цій галузі можна віднести працю [15]. Однак в цій праці увага акцентується на застосуванні стандартних команд СКМ Maple та обмежуються тільки розглядом задач елементарної теорії чисел. Створення навчальних Maple-тренажерів в цій праці не розглядається взагалі. На наш погляд, створення та використання вказаних тренажерів є одним з найефективніших напрямків впровадження СКМ в навчальному процесі здобувачів вищої освіти галузі знань 12 - Інформаційні технології, зокрема, спеціальності 125 - Кібербезпека.

**Мета та задачі дослідження**

Метою даної статті є розгляд основних прийомів розв'язання з використанням СКМ Maple широкого кола задач теорії чисел, лінійної алгебри, теорії ймовірностей, що мають криптографічні застосування.

Для досягнення поставленої мети вирішувались такі задачі:

- визначити основні розділи та задачі теорії чисел, що мають бути розглянуті в матеріалах досліджень, а також найбільш наочну форму подачу цих матеріалів.
- розробити компактні приклади застосування стандартних команд Maple, що відображують, як математичну сутність відповідних задач, так і особливості синтаксису програмного середовища.
- продемонструвати на окремих характерних прикладах роботу навчальних Maple-тренажерів розв'язування окремих типових задач елементарної теорії чисел.

**Виклад основного матеріалу**

Частина команд для розв'язання задач елементарної теорії чисел знаходяиться в ядрі системи Maple. Такі команди є доступними зразу після запуску цієї системи. Інша частина команд знаходиться в пакеті *numtheory* і стає доступною тільки після підключення. Всі команди цього пакету можна підключити за допомогою командного рядка

```
with(numtheory);
```

[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral_basis, invcfrac, invphi, issqrfree, jacobi, kronecker, lambda, legendre, mcombine, mersenne, migcdex, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, phi, pi, pprimroot, primroot, quadres, rootsunity, safeprime, sigma, sq2factor, sum2sqr, tau, thue];

Якщо в поточному сеансі роботи в середовищі Maple планується використовувати тільки окремі команди пакету, їх можна підключити за допомогою такого командного рядка

```
with(numtheory,divisors,factorset,fermat,jacobi,legendre,phi, pi,sigma);
```

[*divisors*, *factorset*, *fermat*, *jacobi*, *legendre*, $\phi$, $\pi$, $\sigma$]

В той же час, доступ до будь-якої команда цього пакету може бути отриманий за допомогою синтаксису

```
numtheory[phi](35);
```

24,

що може бути зручним, якщо не планується застосовування інших команд пакету і не планується повторного використання цієї команди.

Надалі, звертатися до команд цього пакету будемо саме за таким синтаксисом, щоб підкреслити належність команди до вказаного пакету.

Аналіз форм подачі матеріалів досліджень, подібних до цієї роботи надає можливість припустити, що найбільш наочним є використання таблиць з декількома колонками під час описання широкого кола стандартних команд та однієї колонки - для описання прикладів розв'язування деяких відомих математичних задач з криптографічним застосуванням, також під час демонстрації роботи Maple-тренажерів.

Команди, що будемо описувати, групуватимемо за різними тематичними розділами, безпосереднє пов'язаними з криптографічним алгоритмом з відкритим ключем RSA – найбільш відомим та широкорозповсюдженим в різних додатках для шифрування та цифрового підпису.

Ці розділи визначені на основі низки праць наукового та навчально-методичного характеру [1, 2, 4, 6, 17, 18, 19, 20, 21].

**1.1. Подільність цілих чисел. Прості числа.**

| Команда або оператор | Стисле описання | Приклади застосування* |
|---|---|---|
| `irem(m,n)`<br>`irem(m,n,'q');`<br>`iquo(m,n)` | Якщо *m* і *n* є натуральними числами, тоді *irem* повертає таке ціле число *r* (*iquo* повертає таке ціле число *q*), що *m* = *n***q* + *r*, | `m:=23:n:=4:`<br>`r=irem(m,n,'q');`<br>`m=``(q)*n+``(rhs(%));`<br>*r* = 3 |

| | | |
|---|---|---|
| `%`<br><br>`rhs` | 0≤*r* <*n*;<br>Якщо присутній третій аргумент, йому буде присвоєно значення частки (остачі).<br>Посилання на останнє обчислене значення<br>права частина рівняння | 23 = 4 (5) + (3)<br>`m:=7:n:=16:`<br>`r=irem(m,n,'q');`<br>`m=``(q)*n+``(rhs(%));`<br>*r* = 7<br>7 = 16 (0) + (7)<br>`m:=33:n:=3:`<br>`r=irem(m,n,'q');`<br>`m=``(q)*n+``(rhs(%));`<br>*r* = 0<br>33 = 3 (11) + (0)<br>`m:=23:n:=4:`<br>`iquo(m,n);`<br>5 |
| `isprime(n)`<br><br>`nextprime(n), prevprime(n)`<br><br>`ithprime(n)` | Здійснює перевірку цілого додатного числа на простоту<br>Знаходження найближчого більшого (меншого) простого числа<br>Знаходження простого числа з порядковим номером *n;* | `isprime(7),isprime(15);`<br>*true*, *false*<br>`prevprime(7),nextprime(7);`<br>5, 11<br>`ithprime(7);`<br>17 |
| `ifactor(n)` | Канонічний розклад числа. Канонічним розкладанням натурального числа на прості множники називають таке його розкладання, коли множники записуються в порядку зростання | `n:=728:n=ifactor(n);`<br>$728 = (2)^3 (7) (13)$<br>`n:=101:n=ifactor(n);`<br>101 = (101)<br>`n:=18!:``(18)!=ifactor(n);`<br>$(18)! = (2)^{16} (3)^8 (5)^3 (7)^2 (11) (13) (17)$<br>`n:=3195007177:n=ifactor(n);`<br>3195007177= (58217) (54881) |
| `factorset(n)` | обчислює множину простих дільників числа *n* | `numtheory[factorset](18!);`<br>{2, 3, 5, 7, 11, 13, 17} |
| `divisors(n)` | обчислює множину всіх додатніх<br>дільників числа n: | `numtheory[divisors](128);`<br>`` `+`(%[]); ``<br>{1, 2, 4, 8, 16, 32, 64, 128}<br>255 |
| `igcd`<br>`ilcm` | знаходять найбільший спільний дільник (найменше спільне кратне) двох або більше цілих чисел; | `[[15,35],[5,11],[15,35,45]];`<br>`igcd,map(z->igcd(z[]), %);`<br>`ilcm,map(z->ilcm(z[]), %%);`<br>[[15, 35], [5, 11], [15, 35, 45]]<br>*igcd*, [5, 1, 5]<br>*ilcm*, [105, 55, 315] |
| `igcdex(m,n,'s','t');` | роширений алгоритм Евкліда: обчислює такі цілі числа g, s, t, що, s m + t n= g, g=(m, n); | `m:=11:n:=21:`<br>`igcdex(m,n,'u','v'):`<br>`` (u)*m+``(v)*n=%; ``<br>11 (2) + 21 (-1) = 1 |

НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР
з обчислень за розширеним алгоритмом Евкліда [6]

```
My_Euclid:=proc(a1,b1)
  local aa,bb,ri_1,ri,ri1,qi,xi_1,xi,xi1,yi_1,yi,yi1,i,i_1;
if type(a1,posint) and type(b1,posint) then
 if a1>=b1 then aa:=a1;bb:=b1;ri_1:=a1;ri:=b1
 else
  aa:=b1;bb:=a1;ri_1:=b1;ri:=a1
 end if;
 print(a=ri_1,b=ri);
 qi:=floor(ri_1/ri);
 xi_1:=1;xi:=0;yi_1:=0;yi:=1;
```

```
i_1:=0:
print(''r''[i_1]=ri_1,''x''[i_1]=xi_1,''y''[i_1]=yi_1,[ri_1=xi_1*``(aa)+y
i_1*``(bb)]);
for i while ri1<>0 do
  qi:=floor(ri_1/ri);#print('qi'=qi);
  ri1:=ri_1-qi*ri;
  xi1:=xi_1-qi*xi;
  yi1:=yi_1-qi*yi;

print(''q''[i]=qi,''r''[i]=ri,''x''[i]=xi,''y''[i]=yi,[ri=xi*``(aa)+yi*``
(bb)]);
   ri_1:=ri;ri:=ri1;xi_1:=xi;xi:=xi1;yi_1:=yi;yi:=yi1;
end do
else
 'procname( args )'
end if;
print(gcd=ri_1,xi_1*``(aa)+yi_1*``(bb)=ri_1);
xi_1,yi_1
end proc:
My_Euclid(26, 21):
```

$$a = 26, b = 21$$
$$'r'_0 = 26, 'x'_0 = 1, 'y'_0 = 0, [26 = (26)]$$
$$'q'_1 = 1, 'r'_1 = 21, 'x'_1 = 0, 'y'_1 = 1, [21 = (21)]$$
$$'q'_2 = 4, 'r'_2 = 5, 'x'_2 = 1, 'y'_2 = -1, [5 = (26) - (21)]$$
$$'q'_3 = 5, 'r'_3 = 1, 'x'_3 = -4, 'y'_3 = 5, [1 = -4\ (26) + 5\ (21)]$$
$$gcd = 1, -4\ (26) + 5\ (21) = 1$$
$$-4, 5$$

```
My_Euclid(11,21);
```

$$a = 21, b = 11$$
$$'r'_0 = 21, 'x'_0 = 1, 'y'_0 = 0, [21 = (21)]$$
$$'q'_1 = 1, 'r'_1 = 11, 'x'_1 = 0, 'y'_1 = 1, [11 = (11)]$$
$$'q'_2 = 1, 'r'_2 = 10, 'x'_2 = 1, 'y'_2 = -1, [10 = (21) - (11)]$$
$$'q'_3 = 10, 'r'_3 = 1, 'x'_3 = -1, 'y'_3 = 2, [1 = -(21) + 2\ (11)]$$
$$gcd = 1, -(21) + 2\ (11) = 1$$
$$-1, 2$$

```
My_Euclid(70, 98):
```

$$a = 98, b = 70$$
$$'r'_0 = 98, 'x'_0 = 1, 'y'_0 = 0, [98 = (98)]$$
$$'q'_1 = 1, 'r'_1 = 70, 'x'_1 = 0, 'y'_1 = 1, [70 = (70)]$$
$$'q'_2 = 2, 'r'_2 = 28, 'x'_2 = 1, 'y'_2 = -1, [28 = (98) - (70)]$$
$$'q'_3 = 2, 'r'_3 = 14, 'x'_3 = -2, 'y'_3 = 3, [14 = -2\ (98) + 3\ (70)]$$
$$gcd = 14, -2\ (98) + 3\ (70) = 14$$

ЧИСЛА МЕРСЕННА

Числа Мерсенна мають вигляд $M_n = 2^n - 1$. Числа саме такого виду є найбільшими серед відомих простих чисел. Складемо програму для визначення всіх простих чисел Мерсенна серед першої тисячі натуральних чисел:

```
for n from 1 to 1000 do
  if isprime(2^n-1) then
   print(M[n]=2^n-1);
  end if;
end do;
```

$$M_2 = 3$$
$$M_3 = 7$$

$$M_5 = 31$$
$$M_7 = 127$$
$$M_{13} = 8191$$
$$M_{17} = 131071$$
$$M_{19} = 524287$$
$$M_{31} = 2147483647$$
$$M_{61} = 2305843009213693951$$
$$M_{89} = 618970019642690137449562111$$
$$M_{107} = 162259276829213363391578010288127$$
$$M_{127} = 170141183460469231731687303715884105727$$
$$M_{521} =$$
$$6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559$$
$$6406614545549772963113914808580371219879997166438125740282911150571511$$
$$M_{607} =$$
$$5311379928167670986895882065524686273295931177270319231994441382004035598608522427391625$$
$$0226522928566888932948624650101534657933765270723940951997876658735194383127083539321903$$
$$1728127$$

Легко довести, що числа Мерсенна $M_k = 2^k - 1$, є складеними для будь-яких додатних складених чисел $k$ - парних або непарних. Іншими словами простота числа $k$ є необхідною умовою (проте, недостатньою) простоти числа Мерсенна $M_k = 2^k - 1$. В зв’язку з цим наведений простий алгоритм виявлення засобами СКМ Maple простих чисел Мерсенна серед натуральних чисел певного проміжку легко удосконалити шляхом введення двох додаткових умов. Перша умова – пропускати всі числа Мерсенна, що відповідають парним значенням номера $k$. Друга – для всіх непарних значень $k$ перевіряти спочатку простоту самого числа $k$, і тільки в разі позитивної відповіді переходити до перевірки на простоту відповідного числа Мерсенна. Легко видно, що із зростанням натуральних чисел частота зустрічаємості серед них простих чисел Мерсенна різко знижується. Крім того із зростанням номера числа Мерсенна їх величина також різко зростає, що добре видно із демонстраційного графіка на рис. 1. Наприклад, значно простіше, тобто значно швидше, можна здійснити перевірку на простоту числа $k$=527, ніж здійснити перевірку відповідного числа Мерсенна, десяткове представлення якого містить 159 цифр! Оскільки число $k$=527 є складеним, відпадає необхідність перевірки відповідного числа Мерсена. Наведемо удосконалену програму та приклад її роботи ( $u(k) = \frac{k}{2^k - 1}$ ):

```
for n in [2, 2*k+1 $ k=1..500] do
  if isprime(n) then
   if isprime(2^n-1) then
    print(M[n]=2^n-1,u(n)=evalf(n/(2^n-1)))
   end if
  end if
end do:
```

$$M_2 = 3,\ u(2) = 0.6666666667$$
$$M_3 = 7,\ u(3) = 0.4285714286$$
$$M_5 = 31,\ u(5) = 0.1612903226$$
$$M_7 = 127,\ u(7) = 0.05511811024$$
$$M_{13} = 8191,\ u(13) = 0.001587107801$$
$$M_{17} = 131071,\ u(17) = 0.0001297006966$$
$$M_{19} = 524287,\ u(19) = 0.00003623969315$$
$$M_{31} = 2147483647\ ,\ u(31) = 0.1443549991\ \ 10^{-7}$$
$$M_{61} = 2305843009213693951\ \ ,\ u(61) = 0.2645453301\ \ 10^{-16}$$
$$M_{89} = 618970019642690137449562111\ \ \ ,\ u(89) = 0.1437872549\ \ 10^{-24}$$
$$M_{107} = 162259276829213363391578010288127\ \ \ ,\ u(107) = 0.6594384130\ \ 10^{-30}$$

$M_{127} = 170141183460469231731687303715884105727$ , $u(127) = 0.7464389128\ \ 10^{-36}$

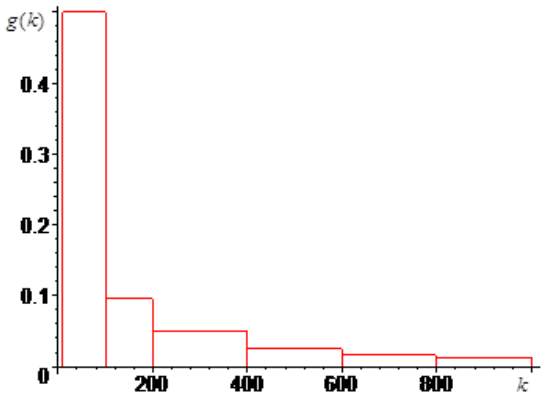


Рисунок 1 – Залежність відношення довжини номера числа Мерсена до довжини його значення $g(k) = \dfrac{length(k)}{length(2^k - 1)}$ (length – кількість цифр в десятковому представлені числа) для різних значень номерів.

**1.2. Найважливіші функції в теорії чисел: функції виділення цілої та дробової частин числа та мультиплікативні функції.**

| | | |
|---|---|---|
| `round(n)`<br><br>`floor(n)`<br><br>`ceil(n)`<br><br>`trunc(n)` –<br><br>`frac(n)` –<br><br>`evalf(x)`<br><br>`map` | округлює число *n* до найближчого цілого;<br>округлює число *n* до найбільшого цілого числа, що менше або дорівнює цьоому числу;<br>округлює число *n* до найменшого цілого числа, що більше або дорівнює цьому числу;<br>округлює дійсне число *n* до найближчого цілого в напрямку до 0. Стандартне математичне позначення: [*n*].<br>знаходить дробову частину числа *n*. Стандартне математичне позначення {*n*}=*n*-[*n*]:<br>подає дійсне число *x* у формі числа з плаваючою точкою або у вигляді числа зі знаками після коми;<br>застосовує процедуру до кожного елемента об’єкта | `L:=evalf([exp(1),3.9,-1.9,Pi,15]);`<br>`` `round(L)`,map(t->round(t),L); ``<br>`` `floor(L)`,map(t->floor(t),L); ``<br>`` `ceil(L)`*`-->`*map(t->ceil(t),L); ``<br>`` `trunc(L)`,map(t->trunc(t),L); ``<br>`` `frac(L)`*`-->`*map(t->frac(t),L); ``<br>$L := [2.718281828, 3.9, -1.9, 3.141592654, 15.]$<br>*round(L)*, [3, 4, -2, 3, 15]<br>*floor(L)*, [2, 3, -2, 3, 15]<br>*ceil(L)* --> [3, 4, -1, 4, 15]<br>*trunc(L)*, [2, 3, -1, 3, 15]<br>*frac(L)* --> [0.718281828, 0.9, -0.9, 0.141592654, 0.] |
| `numtheory[phi](n)` | Функція Ейлера для натурального числа *n*- визначається, як кількість натуральних чисел, що не перевищують *n* і взаємно прості з ним. | `[8,11,21,25];`<br>`map(z->`` `phi`(z)=numtheory[phi](z),%);``<br>[8, 11, 21, 25]<br>$[\phi(8) = 4, \phi(11) = 10, \phi(21) = 12, \phi(25) = 20]$ |
| `tau(n)`<br><br>`sigma(n)` | обчислює кількість додатніх дільників числа *n*:<br>обчислює суму додатніх дільників числа *n*. | `n:=15:numtheory[divisors](n);`<br>`tau(15)=numtheory[tau](15);`<br>`sigma(15)=numtheory[sigma](15);`<br>{1, 3, 5, 15}<br>$\tau(15) = 4$<br>$\sigma(15) = 24$ |

| | | |
|---|---|---|
| **mobius(n)** | Функція Мебіуса для натурального безквадратного числа $n$>1-визначається, як $(-1)^s$, s – кількість простих дільників числа $n$; *mobius*(1)=1, в інших випадках *mobius*($n$)=0. | **[6,70,50];**<br>**map(z->`mobius`(z)=numtheory[mobius](z),%);**<br>[6, 70, 50]<br>[mobius (6) = 1, mobius (70) = -1, mobius (50) = 0] |
| **lambda(n)** | Функція Кармайкла для натурального числа обчислює значення функції Кармайкла, тобто найменшого числа λ(n) , такого, що $n \mid a^{\lambda(n)} - 1$за умови (n,a)=1. | **[5,7,3^3];**<br>**map(z->`lambda`(ifactor(z))=numtheory[lambda](z),%);**<br>**map(z->numtheory[phi](z)-numtheory[lambda](z),%%);**<br>[5, 7, 27]<br>[λ( (5)) = 4, λ( (7)) = 6, λ( $(3)^3$) = 18]<br>[0, 0, 0]<br>**[35,3^3*5*11^2];**<br>**map(z->`lambda`(ifactor(z))=numtheory[lambda](z),%);**<br>**map(z->numtheory[phi](z)-numtheory[lambda](z),%%);**<br>[35, 16335]<br>[λ( (5) (7)) = 12, λ( $(3)^3$ (5) $(11)^2$) = 1980]<br>[12, 5940] |
| **numtheory[pi](n)** | обчислює кількість кількість простих чисел на відрізку від 1 до $n$; | **map(z->numtheory[pi](z), [2,3,10,100]);**<br>[1, 2, 4, 25] |

НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР
з обчислень функції Ейлера [18]

**My_phi(17);**

Число p=17 є простим, отже значення функції Ейлера обчислюємо за формулою

$$\phi(p) = p - 1$$

$$[\phi(17) = (17) - 1] = 16$$

**My_phi(35);**

Задане число є добутком простих чисел

$$35 = (5)\ (7)$$

Отже, для обчислення функції Ейлера використовуємо властивість мультиплікативності цієї функції:

$$[[\phi((5)\ (7)) = \phi(5)\,\phi(7)] = ((5) - 1)\,((7) - 1)] = 24$$

**My_phi(27);**

В канонічній формі задане число має вигляд

$$27 = (3)^3$$

Отже, для обчислення функції Ейлера використовуємо формулу

$$\phi(p^q) = p^{(q-1)}(p-1)$$

$$[\phi((3)^3) = (3)^{(3-(1))}(3-(1))] = 18$$

**My_phi(17*19^2*31);**

В канонічній формі задане число має вигляд

$$190247 = (17)\ (19)^2\ (31)$$

Отже, для обчислення функції Ейлера використовуємо найбільш загальну формулу

$$\phi((17)\ (19)^2\ (31)) = (190247)\left(\prod_{k=1}^{3}\left(1 - \frac{1}{p_k}\right)\right)$$

$$\left[ (190247)\left(\prod_{k=1}^{3}\left(1-\frac{1}{p_k}\right)\right) = (190247)\left(1-\frac{1}{(17)}\right)\left(1-\frac{1}{(19)}\right)\left(1-\frac{1}{(31)}\right)\right] =$$

164160

**1.3. Конгруенції**

| Команда або оператор | Стисле описання | Приклади застосування* |
|---|---|---|
| `a mod b`<br>`modp(a,b)`<br><br>`mods(a,b)` | Здійснює обчислення за модулем цілого числа *b*: повертає найменший додатний лишок;<br>повертає абсолютно найменший лишок; | `19 mod 5;`<br>`modp(19,5);`<br>`mods(19,5);`<br>4<br>4<br>-1 |

```
n:=7:
printf(`повна система найменших невід'ємних лишків за модулем 7: `);
k $ k=0..n-1;
printf(`повна система абсолютно найменших лишків за модулем 7: `);
i:=((-1)^n-1)/2:seq(mods(k,n),k=0..n-1);
printf(`зведена система лишків за модулем 7: `);
select(x->is(igcd(x,n)=1),[k $ k=0..n-1])[]
повна система найменших невід'ємних лишків за модулем 7:
                                  0, 1, 2, 3, 4, 5, 6
повна система абсолютно найменших лишків за модулем 7:
                                  0, 1, 2, 3, -3, -2, -1
зведена система лишків за модулем 7:
                                  1, 2, 3, 4, 5, 6
n:=12:
printf(`повна система найменших невід'ємних лишків за модулем 12: `);
k $ k=0..n-1;
printf(`повна система абсолютно найменших лишків за модулем 12: `);
i:=((-1)^n-1)/2:seq(mods(k,n),k=0..n-1);
printf(`зведена система лишків за модулем 12: `);
select(x->is(igcd(x,n)=1),[k $ k=0..n-1])[];
повна система найменших невід'ємних лишків за модулем 12:
                                  0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
повна система абсолютно найменших лишків за модулем 12:
                                  0, 1, 2, 3, 4, 5, 6, -5, -4, -3, -2, -1
зведена система лишків за модулем 12:
                                  1, 5, 7, 11
```

```
printf(`Перевірка належності двох чисел a, b до одного класу лишків за модулем
11:`);
n:=11:[[3,36],[1,78],[2,14],[-1,11],[-12,12]];
map(z->z*`-->`*is(z[1]-z[2] mod n=0),%);
Перевірка належності двох чисел a, b до одного класу лишків за модулем 11:
                  [[3, 36], [1, 78], [2, 14], [-1, 11], [-12, 12]]
        [[3, 36] --> true, [1, 78] --> true, [2, 14] --> false, [-1, 11] --> false,
                  [-12, 12] --> false ]
```

| | | |
|---|---|---|
| `msolve` | Обчислює розв’язок конгруенції з однією змінною або системи конгруенцій з декілька невідомими за модулем *n;* | `msolve(5*x=29,18);`<br>$\{x=13\}$<br>`msolve(2*x=29,18);`<br>`msolve(3*x=15,18);`<br>$\{x=5\}, \{x=11\}, \{x=17\}$<br>`msolve(14*x^3-6*x+36=0,7);`<br>$\{x=6\}$<br>`msolve({3*x-4*y=5,7*x+y=2},17);`<br>$\{y=4, x=7\}$ |
| `chrem` | обчислює розв’язок лінійної системи конгруенцій з однією змінною і різними попарно | `chrem([6,4],[7,17]);`<br>`chrem([6,4,5],[7,17,6]);`<br>55 |

| | | |
|---|---|---|
| | простими модулями | 293 |
| **legendre** | обчислює символ Лежандра | **legendre(184,347);**<br>1<br>**legendre(3,7);**<br>-1 |

НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР

обчислення символу Лежандра

Символи Лежандра та Якобі використовуються для встановлення числа розв'язків модулярних квадратних рівнянь відповідно за простим та складеним модулем.

Приклад. Дослідити, чи має розв'язки конгруенція $x^2 \equiv 184 \pmod{347}$.

▶ **My_Lej(184,347);**

Число "а" має такий канонічний розклад:

$$184 = (2)^3\ (23)$$

Отже, з використанням мультиплікативності символу Лежандра, отримаємо:

$$\left(\frac{184}{347}\right) = \left(\frac{2}{347}\right)^3 \left(\frac{23}{347}\right)$$

Всі співмножники в парних степенях дорівнюють одиниці, отже:

$$\left(\frac{184}{347}\right) = \left(\frac{2}{347}\right) \left(\frac{23}{347}\right)$$

**My_Lej(2,347);**

$$\left(\frac{2}{347}\right) = (-1)^{\left(\frac{(347)^2-1}{(8)}\right)}$$

$$\left(\frac{2}{347}\right) = -1$$

**My_Lej(23,347);**

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:

для будь-яких простих непарних чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{23}{347}\right) = (-1)^{\left(\frac{((23)-1)\ ((347)-1)}{(4)}\right)} \left(\frac{347}{23}\right)$$

Отже

$$\left(\frac{23}{347}\right) = -\left(\frac{347}{23}\right)$$

**-My_Lej(347,23);**

$$\left(\frac{347}{23}\right) = \left(\frac{347\,['mod'\ (23)]}{(23)}\right)$$

$$-\left(\frac{347}{23}\right) = -\left(\frac{2}{23}\right)$$

**-My_Lej(2,23);**

$$\left(\frac{2}{23}\right) = (-1)^{\left(\frac{(23)^2-1}{(8)}\right)}$$

$$-\left(\frac{2}{23}\right) = -1$$

**``(184/347)=(-1)*(-1);**

$$\left(\frac{184}{347}\right) = 1$$

Відповідь: конгруенція $x^2 \equiv 184 \pmod{347}$ має два розв'язки. ◀

| | | |
|---|---|---|
| **jacobi** | обчислює символ Якобі | **jacobi(1001,9907);**<br>-1 |

НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР

обчислення символу Якобі

Приклад. Дослідити, чи має розв’язки конгруенція $x^2 \equiv 1001 \pmod{9907}$.

```
▶ My_Jac(1001,9907);
```

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:
для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{1001}{9907}\right) = (-1)^{\left(\frac{((1001)-1)\ ((9907)-1)}{(4)}\right)} \left(\frac{9907}{1001}\right)$$

Отже

$$\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right)$$

$$\left(\frac{9907}{1001}\right) = \left(\frac{9907\,['mod'\ (1001)]}{(1001)}\right)$$

$$\left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right)$$

Оскільки число 898 - парне, подамо це число у вигляді

$$898 = 2^t q$$

$$898 = (2)\ (449)$$

$$\left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right) \left(\frac{449}{1001}\right)$$

$$\left(\frac{2}{1001}\right) = (-1)^{\left(\frac{(1001)^2-1}{(8)}\right)}, \quad \left(\frac{2}{1001}\right) = 1$$

$$\left(\frac{898}{1001}\right) = \left(\frac{449}{1001}\right)$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:
для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{449}{1001}\right) = (-1)^{\left(\frac{((449)-1)\ ((1001)-1)}{(4)}\right)} \left(\frac{1001}{449}\right)$$

Отже

$$\left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right)$$

$$\left(\frac{1001}{449}\right) = \left(\frac{1001\,['mod'\ (449)]}{(449)}\right)$$

$$\left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right)$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:
для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{103}{449}\right) = (-1)^{\left(\frac{((103)-1)\ ((449)-1)}{(4)}\right)} \left(\frac{449}{103}\right)$$

Отже

$$\left(\frac{103}{449}\right) = \left(\frac{449}{103}\right)$$

$$\left(\frac{449}{103}\right) = \left(\frac{449\,['mod'\ (103)]}{(103)}\right)$$

$$\left(\frac{449}{103}\right) = \left(\frac{37}{103}\right)$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:
для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{37}{103}\right) = (-1)^{\left(\frac{((37)-1)\ ((103)-1)}{(4)}\right)} \left(\frac{103}{37}\right)$$

Отже

$$\left(\frac{37}{103}\right) = \left(\frac{103}{37}\right)$$

$$\left(\frac{103}{37}\right) = \left(\frac{103\,['mod'\ (37)]}{(37)}\right)$$

$$\left(\frac{103}{37}\right) = \left(\frac{29}{37}\right)$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:
для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{29}{37}\right) = (-1)^{\left(\frac{((29)-1)\ ((37)-1)}{(4)}\right)} \left(\frac{37}{29}\right)$$

Отже

$$\left(\frac{29}{37}\right) = \left(\frac{37}{29}\right)$$

$$\left(\frac{37}{29}\right) = \left(\frac{37\,['mod'\ (29)]}{(29)}\right)$$

$$\left(\frac{37}{29}\right) = \left(\frac{8}{29}\right)$$

Оскільки число 8 - парне, подамо це число у вигляді

$$8 = 2^t\, q$$

$$8 = (2)^3\ (1)$$

$$\left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3 \left(\frac{1}{29}\right)$$

$$\left(\frac{2}{29}\right)^3 = (-1)^{\left(\frac{(29)^2-1}{(8)}\right)}, \left(\frac{2}{29}\right)^3 = -1$$

$$\left(\frac{8}{29}\right) = -\left(\frac{1}{29}\right)$$

$$\left(\frac{1}{29}\right) = 1$$

$$\left(\frac{1001}{9907}\right) = -1$$

Відповідь: не існує розв'язку конгруенції $x^2 \equiv 1001 \pmod{9907}$. ◀

**Висновки**

1. Розглянуто прийоми розв'язання за допомогою стандартних команд системи Maple основних задач елементарної теорії чисел, більшість з яких має безпосереднє відношення до криптографічного алгоритму RSA - одного з найпоширеніших асиметричних криптографічних методів, що використовується для шифрування і цифрового підпису.

2. Продемонстровано роботу авторських Maple-тренажерів, що разом з використанням інших прийомів застосування стандартних команд системи Maple до розв'язання математичних задач криптографічного характеру направлено на покращення ефективності, зокрема, наочності, висвітлення сутності розглянутих методів та ідей, покладених в їх основу.

3. Матеріали статті можуть бути використані здобувачами вищої освіти та викладачами ЗВО під час розв'язання типових математичних задач галузі знань 12 – Інформаційні технологіїі. Особливо корисним представлені матеріали можуть виявитися в процесі вивчення дисципліни «Математичні основи криптографії».

**Список літератури**


[1] В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, В.І. Андреев, В.А. Мухачьов, В.П. Щербина, Ю.Є. Яремчук, *Комп'ютерна криптографія. Лабораторний практикум*. - Київ: НАУ, 2003.

[2] Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук, *Основи криптографічного захисту інформації: підручник*, Вінниця : ВНТУ, 2011. ISBN 978–966–641–430–7.

[3] Р.Н. Квєтний, Є.О. Титарчук, А.А. Гуржій, "Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ECC та RSA", *Інформаційні технології та комп'ютерна інженерія*, № 3, С. 38-43. 2016.

[4] В.А.Лужецький, О. П. Войтович, А. В. Дудатьєв, *Інформаційна безпека : навчальний посібник*, Вінниця : УНІВЕРСУМВінниця, 2009. ISBN 978-966-641-265-53.

[5] В. А. Лужецький, Ю. В. Баришев, "Методи багатоканального керованого хешування для комп'ютерної криптографії", *Інформаційні технології та комп'ютерна інженерія*, № 1, С. 66-72. 2011.

[6] В. М. Михалевич, О. І. Тютюнник, О. Корінний, "Навчальний Maple-тренажер з обчислень за розширеним алгоритмом Евкліда", на *Всеукраїнській науково-методичній конференції «Сучасні науково-методичні проблеми математики у вищій школі»,* 23 – 24 травня 2022 р. , К.: НУХТ, 2022. С. 80-83. https://drive.google.com/file/d/1VlroDm7xDJuf9mjRYoWK2nsRX-cVqaSR/view.

[7] В. А. Лужецький, В. М. Михалевич, О. В. Михалевич, В. А. Каплун, "Щільність заповнення ряду натуральних чисел членами окремої зворотної послідовності другого порядку", *Інформаційні технології та комп'ютерна інженерія*, №1(17) – С. 46-51. 2010.

[8] Ю. В. Добранюк, В. М. Михалевич, А. А. Коломієць, О. М. Козак, "Застосування СКМ Maple для побудови 3D графіків в задачах обчислення об'єму фігур", *Інформаційні технології та комп'ютерна інженерія*№ 2(17). С. 115-123. 2022.

[9] V. M. Mikhalevich, I.V.Abramchuk, "Maximum Accumulated Strain for Linear Two-Link Triangle-Like Deformation Trajectories", *International Applied Mechanics*, No. 57(6). P. 720–73. 2021. doi.org/10.1007/s10778-022-01121-w.

[10] Y. L. Cheung "Learning number theory with a computer algebra system", *International Journal of Mathematical Education in Science and Technology*, 3(27), p. 379-385. 1996. doi:10.1080/0020739960270308.

[11] R. Klima, N.Sigmon, T. Stitzinger, *Applications of abstract algebra with Maple*. CRC Press, Boca Raton, FL. 2000. ISBN 0-8493-8170-3.

[12] A.Baligaand, S. Boztas, "Cryptography in the classroom using Maple". *In W.Yang, S.Chu, Z.Karian, and G. Fitz-Gerald, editors. Proceedings of the Sixth Asian Technology Conference in Mathematics*, 2001. p.343–350.

[13] В. М. Михалевич, "Excel-VBA-Maple програма генерації задач з дисциплін математичного спрямування", *Інформаційні технології та комп'ютерна інженерія*, № 2, С. 74–83. 2005

[14] В. М. Михалевич, І. В. Димніч, О. В. Михалевич, "Захист Maple процедур", *Інформаційні технології та комп'ютерна інженерія*, № 3(10). С. 159-165. 2007.

[15] Л. П. Бедратюк, Г. І. Бедратюк, "Використання системи комп'ютерної алгебри Maple в елементарній теорії чисел", *Восточно-Европейский журнал передовых технологий*, № 6(4), С. 10-13. 2013. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/Vejpte_2013_6%284%29__3

[16] Л. П. Бедратюк, Г. І. Бедратюк, "Використання системи комп'ютерної алгебри Maple в класичних криптосистемах", *Вісник Хмельницького національного університету*, № 231(6), С. 148-153. 2015.

[17] В. М. Михалевич, О. І. Тютюнник, Є. С. Дремлюга, К. В. Медведєва, "Математичні моделі та програмні засоби генерування псевдовипадкових послідовностей для криптографічних застосувань", *L Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії*, 2021, м. Вінниця. − [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/11617/9718.

[18] В. М. Михалевич, Д. Б. Рогачевський, Д. Ю. Желнитський, Б. А. Балух, "Навчальний Maple-тренажер з обчислення функції Ейлера", *LI Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії*, 2022, м. Вінниця. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15034/12681

[19] М. Стасюк, *Елементи математичних основ криптографії : навчальний посібник*, Львів: ЛДУ БЖД, 2021.

[20] О. І. Оглобліна, Т.С. Сушко, Ю.В Шрамко, *Елементи теорії чисел : навч. посіб.*, Суми: Сумський державний університет. 2015.

[21] А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко, *Математичні методи криптології. Навчальний посібник*. 2021. [Електронний ресурс]. Режим доступу: https://duikt.edu.ua/ua/lib/1/category/2132/view/2220.

Стаття надійшла до редакції: 27.02.2024

**References**

[1] V.O. Khoroshko, O.D. Azarov, M.YE. Shelest, V.I. Andreev, V.A. Mukhach′ov, V.P. Shcherbyna, YU.YE. Yarem-chuk, *Komp"yuterna kryptohrafiya. Laboratornyy praktykum*. - Kyyiv: NAU, 2003.

[2] H.M. Hulak, V.A. Mukhachov, V.O. Khoroshko, YU.YE. Yaremchuk, *Osnovy kryptohrafichnoho zakhystu info-rmatsiyi: pidruchnyk*, Vinnytsya : VNTU, 2011. ISBN 978–966–641–430–7.

[3] R.N. Kvyetnyy, YE.O. Tytarchuk, A.A. Hurzhiy, "Metod ta alhorytm obminu klyuchamy sered hrup korystuvachiv na osnovi asymetrychnykh shyfriv ECC ta RSA", *Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya*, № 3, S. 38-43. 2016.

[4] V.A.Luzhetskyy, O. P. Voytovych, A. V. Dudat′yev, *Informatsiyna bezpeka : navchal'nyy posibnyk*, Vinnytsya : UNIVERSUMVinnytsya, 2009. ISBN 978-966-641-265-53.

[5] V. A. Luzhetskyy, YU. V. Baryshev, "Metody bahatokanal′noho kerovanoho kheshuvannya dlya komp″yuternoyi kryptohrafiyi", *Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya*, № 1, S. 66-72. 2011.

[6] V. M. Mykhalevych, O. I. Tyutyunnyk, O. Korinnyy, "Navchal′nyy Maple-trenazher z obchyslen′ za rozshyrenym alhorytmom Evklida", na *Vseukrayins'kiy naukovo-metodychniy konferentsiyi «Suchasni naukovo-metodychni problemy matematyky u vyshchiy shkoli»,* 23 – 24 travnya 2022 r. , K.: NUKHT, 2022. S. 80-83. https://drive.google.com/file/d/1VlroDm7xDJuf9mjRYoWK2nsRX-cVqaSR/view.

[7] V. A. Luzhetskyy, V. M. Mykhalevych, O. V. Mykhalevych, V. A. Kaplun, "Shchil′nist′ zapovnennya ryadu natural′nykh chysel chlenamy okremoyi zvorotnoyi poslidovnosti druhoho poryadku", *Informatsiyni tekhnolohiyi ta komp"yuterna inzheneriya*, №1(17) – S. 46-51. 2010.

[8] YU. V. Dobranyuk, V. M. Mykhalevych, A. A. Kolomiyets, O. M. Kozak, "Zastosuvannya SKM Maple dlya pobudovy 3D hrafikiv v zadachakh obchyslennya ob″yemu fihur", *Informatsiyni tekhnolohiyi ta komp"yuterna inzheneriya*, № 2(17). S. 115-123. 2022.

[9] V. M. Mikhalevich, I.V.Abramchuk, "Maximum Accumulated Strain for Linear Two-Link Triangle-Like Deformation Trajectories", *International Applied Mechanics*, No. 57(6). P. 720–73. 2021. d-oi.org/10.1007/s10778-022-01121-w.

[10] Y. L. Cheung "Learning number theory with a computer algebra system", *International Journal of Mathematical Education in Science and Technology*, 3(27), p. 379-385. 1996. doi:10.1080/0020739960270308.

[11] R. Klima, N.Sigmon, T. Stitzinger, *Applications of abstract algebra with Maple*. CRC Press, Boca Raton, FL. 2000. ISBN 0-8493-8170-3.

[12] A.Baligaand, S. Boztas, "Cryptography in the classroom using Maple". In W.Yang, S.Chu, Z.Karian, and G. Fitz-Gerald, editors. *Proceedings of the Sixth Asian Technology Conference in Mathematics*, 2001. p.343–350. [13]

V. M. Mykhalevych, "Excel-VBA-Maple prohrama heneratsiyi zadach z dystsyplin matematychnoho spryamu-vannya", *Informatsiyni tekhnolohiyi ta komp"yuterna inzheneriya*, № 2, S. 74–83. 2005

[14] V. M. Mykhalevych, I. V. Dymnich, O. V. Mykhalevych, "Zakhyst Maple protsedur", *Informatsiyni tekhnolohiyi ta komp"yuterna inzheneriya*, № 3(10). S. 159-165. 2007.

[15] L. P. Bedratyuk, H. I. Bedratyuk, "Vykorystannya systemy komp″yuternoyi alhebry Maple v elementarniy teoriyi chysel", *Vostochno-Evropeyskyy zhurnal peredovykh tekhnolohyy*, № 6(4), S. 10-13. 2013. [Online]. Available: http://nbuv.gov.ua/UJRN/Vejpte_2013_6%284%29__3

[16] L. P. Bedratyuk, H. I. Bedratyuk, "Vykorystannya systemy komp″yuternoyi alhebry Maple v klasychnykh kryptosystemakh", *Visnyk Khmel'nyts'koho natsional'noho universytetu*, № 231(6), S. 148-153. 2015.

[17] V. M. Mykhalevych, O. I. Tyutyunnyk, YE. S. Dremlyuha, K. V. Medvedyeva, "Matematychni modeli ta pro-hramni zasoby heneruvannya psevdovypadkovykh poslidovnostey dlya kryptohrafichnykh zasto-?uvan′", *L Naukovo-tekhnichna konferentsiya fakul'tetu informatsiynykh tekhnolohiy ta komp'yuternoyi inzheneriyi*, 2021, m. Vinnytsya. − [Online]. Available: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/11617/9718.

[18] V. M. Mykhalevych, D. B. Rohachevs′kyy, D. YU. Zhelnyt·s′kyy, B. A. Balukh, "Navchal′nyy Maple-trenazher z obchyslennya funktsiyi Eylera", LI Naukovo-tekhnichna konferentsiya fakul′tetu informa-tsiynykh tekhnolohiy ta komp'yuternoyi inzheneriyi, 2022, m. Vinnytsya. [Online]. Available: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15034/12681

[19] M. Stasyuk, Elementy matematychnykh osnov kryptohrafiyi : navchal′nyy posibnyk, L′viv: LDU BZHD, 2021.

[20] O. I. Ohloblina, T.S. Sushko, YU.V Shramko, Elementy teoriyi chysel : navch. posib., Sumy: Sums′kyy derzhavnyy universytet. 2015.

[21] A.D. Kozhukhivs′kyy, I.D. Horbenko, H.I. Haydur, O.A. Kozhukhivs′ka, V.V. Marchenko, Matematychni metody kryptolohiyi. Navchal′nyy posibnyk. 2021. [Online]. Available: https://duikt.edu.ua/ua/lib/1/category/2132/view/2220.

**Відомості про авторів**

**Михалевич Володимир Маркусович** – д.т.н., професор, завідувач кафедри вищої математики Вінницького національно-го технічного університету, м. Вінниця

**Майданевич Леонід Олександрович** – к. філос. н., асистент кафедри захисту інформації Вінницького національно-го технічного університету, м. Вінниця

**Mykhalevych Volodymyr** — D.Sc. Professor, head of the Chair for Higher Mathematics, Vinnytsia National Technical University

**Maidanevych Leonid** – Cand. Sc., assistant of the Department of Information Protection, Vinnytsia National Technical University

V. M. Mykhalevych, L. O. Maidanevych

# USE OF THE MAPLE SYSTEM IN MATHEMATICAL PROBLEMS OF CRYPTOGRAPHY. PART 1. ELEMENTARY THEORY OF NUMBERS

Vinnytsia National Technical University, Vinnytsia