Вестник КРАУНЦ. Физ.-мат. науки. 2020. Т. 30. № 1. С. 79-86. ISSN 2079-6641

DOI: 10.26117/2079-6641-2020-30-1-79-86

ИНФОРМАЦИОННЫЕ И ВЫЧИСЛИТЕЛЬНЫЕ ТЕХНОЛОГИИ

УДК 511

О МЕТОДИКЕ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ТЕОРИИ ЧИСЕЛ

А. П. Горюшкин

Камчатский государственный университет имени Витуса Беринга, 683032, г. Петропавловск-Камчатский, ул. Пограничная , 4

E-mail: as2021@mail. ru

Обсуждаются проблемы, связанные с компьютерным поиском псевдопростых чисел. Предлагаются новые машинные способы быстрого поиска псевдопростых чисел Кармайкла-Черника с использованием пакета символьных математических вычислений Maple.

Ключевые слова: число Кармайкла, число Черника, тест Ферма, алгоритм, псевдопростое число, сравнимость по модулю, конечное кольцо.

INFORMATION AND COMPUTATION TECHNOLOGIES

MSC 03G05

ON THE METHODOLOGY APPLICATION OF MODERN COMPUTING TECHNOLOGIES IN STUDYING THE THEORY OF NUMBERS

A. P. Goryushkin

Kamchatka State University by Vitus Bering, 683032, PetropavlovskKamchatskiy, Pogranichnaya st, 4, Russia

E-mail: as2021@mail. ru

The problems associated with the computer search for pseudo-simple numbers are discussed. New machine methods are proposed to quickly find Carmichael-Chernick numbers using the Maple symbolic mathematical computation package.

Key words: Carmichael number, Fermat's test, algorithm, pseudo-simple number, comparability modulo, end ring

Введение

Информационно-управляющие системы, как правило, нуждаются в защите канала передачи информации. Защитой от несанкционированных проникновений в информационный или управляющий каналы является кодирование сигнала с последующим декодированием. Быстрое кодирование сигнала с практически невозможностью декодирования без наличия декодирующего ключа обычно основано на теоретико-числовых результатах, связанных с применением простых или *псевдопростых чисел*.

Поиски новых простых и псевдопростых чисел возможны только машинным способом. Стоит отметить особую роль пакета математических символьных вычислений *Maple*. Даже первые версии *Maple* позволяли ускорить решение теоретико-числовых задач, числовых эвристических экспериментов в поисках опровержения той или иной гипотезы, делали наглядными многие факты теории чисел (см., например, работы [1] – [5]).

Последние версии пакета *Maple* значительно расширяют возможности применения вычислительной техники для исследования теоретико-числовых задач. Предлагаемая работа показывает новые возможности последнего пакета символьных математических вычислений *Maple* на примере задачи о поиске псевдопростых чисел Кармайкла. Используя закон контрапозиции, запишем малую теорему Ферма в виде: если существует число a такое, что $n > 1$ не делит ни a, ни a^{n-1}, то число n – составное. Это необходимое условие простоты не является достаточным: из сравнимости

$$a^{n-1} \equiv 1 \,(\mathrm{mod}\ n), \qquad (*)$$

для некоторого a, не сравнимого по модулю n ни с единицей, ни с минус единицей, вообще говоря, не следует простота числа n.

Для любого нечетного n

$$(n-1)^{n\,-\,1} \equiv\ 1\ (\mathrm{mod}\ n).$$

Если n – нечетное, и сравнимость $(*)$ выполняется, по крайней мере, для одного числа a из множества $\{2, 3, \ldots, n-2\}$, то n называют *псевдопростым числом* по основанию a. Понятно, что псевдопростое число взаимно просто со своим основанием, и поэтому число кандидатов для такого основания равно $\phi(n)$.

Составное нечетное число, являющееся псевдопростым по любому основанию, называется *числом Кармайкла*. По умолчанию считается, что число Кармайкла составное. Таким образом, n – число Кармайкла, если оно составное и для каждого числа a, взаимно простого с n выполняется сравнимость $(*)$.

Всё это происходит в конечном кольце – кольце классов вычетов по модулю n; после $\phi(n)$ проверок сравнения $(*)$ можно выяснить, является ли число n псевдопростым (если хотя бы одна проверка удалась) или кармайкловым (если удались все проверки).

Поиск чисел Кармайкла в среде *Maple*

Попробуем найти несколько первых чисел Кармайкла. Вычислим кармайкловые числа из интервала [3, 10 000].

```
> with(numtheory):
> for n from 3 by 2 to 10000 do:
```

k:=0: **for** i **from** 1 **to** $n-1$ **do**
if $igcd(i, n) = 1$ **and** i^{n-1} **mod** $n = 1$ **then** $k := k+1$ **fi od:**
if $k = \phi(n)$ **and** $\phi(n) < n-1$ **then** *print* (n) **fi do**

561

1105

1729

2465

2821

6601

8911

Числа Кармайкла встречаются не часто – оказалось, что таких всего семь чисел из десяти тысяч.

Внесем в алгоритм уточнения, связанные с проверкой простоты и не простоты, и просто проверим конкретное число (например, 41041) на «кармайкловость».

$>$ *with*(*numtheory*):
$> n := 41041$; $k := 0$;
for i **from** 1 **to** $n-1$ **by** 1 **do if** $igcd(i, n) = 1$ **and** $irem(i^{n-1} - 1, n) = 0$
then $k := k+1$
else **fi od**;
if $\phi(n) > k$ **then** n 'составное и не число Кармайкла' **fi**
if $\phi(n) < n-1$ **then** n 'число Кармайкла' **fi**
if $\phi(n) = n-1$ **then** n 'простое' **fi**

41041 *число Кармайкла*

Такая проверка, использует лишь определение псевдопростоты и поэтому выполняет многочисленные лишние вычисления, что существенно замедляет поиск ответа.

Однако еще первой половине прошлого века были найдены сравнительно простые достаточные условия псевдопростоты числа.

Условие Черника

Джон Черник в работе [6] установил, что если для некоторого натурального i все три числа $6i+1$, $12i+1$ и $18i+1$ – простые, то

$$c_i = (6i+1)(12i+1)(18i+1)$$

является числом Кармайкла.

Пусть, например, индекс i пробежит значения от 1 до 100; посмотрим, сколько чисел Кармайкла типа c_i получится.

```
> with(numtheory):
s := 0: for i from 1 to 100 by 1 do
if isprime(6*i+1) and
isprime(12*i+1) and isprime(18*i+1)
then s := s+1; print('c'[i]); print((6*i+1)*(12*i+1)*(18*i+1));
else fi od: s;
```

c_1

1729

c_6

294409

c_{35}

56052361

c_{45}

1189015221

c_{51}

172947529

c_{55}

216821881

c_{56}

228842209

c_{100}

1299963601

8

Таким образом, в интервале [1, 1 300 000 000] содержится всего лишь восемь чисел c_i черниковского типа.

Ускорение поиска чисел вида c_i

Поиск чисел вида c_i можно ускорить в пять раз, увеличив шаг цикла.

Если число i заканчивается цифрой 2 или 7, то число $12i+1$ заканчивается цифрой пять. Если последняя цифра i равна 3 или 8, то число $18i+1$ делится на пять. Наконец, при i с последней цифрой 4 или 9 будет не простым число $6i+1$. Это значит, что для получения чисел Кармайкла c_i вида Черника необходимо выполнение сравнений:

$$i \equiv 0 \pmod 5 \text{ или } i \equiv 1 \pmod 5.$$

Это наблюдение помогает существенно ускорить нахождение чисел Кармайкла такого типа. Найдем для примера количество таких чисел Кармайкла с параметром i от 1 до 100 000 000. Для этого подсчет будем вести с шагом 5 по двум сериям: одну начнем с нуля, а вторую – с единицы.

```
> with(numtheory):
> s := 0; for i from 0 to 100 000 000 by 5 do
if isprime(6*i+1) and
isprime(12*i+1) and isprime(18*i+1))
then s := s+1:
else fi od:
k := 1; for i from 1 to 100 000 000 by 5 do
if isprime(6*i+1)and
isprime(12*i+1)) and isprime(18*i+1))
then k := k+1:
else fi od:
s + k;
```

224906

Пусть индекс i не превышает числа 10^k; тогда число c_i из интервала $(1,\ 10^k)$ индексов для небольших k примерно на два порядка меньше длины интервала.

Таблица

k	c_i
1	2
2	8
3	27
4	159
5	842
6	5099
7	22937
8	224906

Большое число Кармайкла

Техника позволяет сравнительно быстро находить числа Кармайкла с несколькими сотнями цифр в их десятичной записи. Найдем для примера черниковское число c_i, индекс i которого расположен возле гугола – числа, равного 10^{100}. Сначала уменьшим гугол на миллион, а в программу запишем команду остановки сразу, как только первое Кармайклово число черниковского типа будет найдено.

```
> with(numtheory):
> s:= 0: n:= 10^100 : for i from 1 to n-10^6 by 1 do
if isprime(6*i+1) and
isprime(12*i+1) and isprime(18*i+1)
then s:=s+1; print('c'[i]); a:=(6*i+1)*(12*i+1)*(18*i+1); print(a); print(length(a));break
```

0

Оказалось, что в для индексов i из интервала $[10^{100} - 10^6, 10^{100}]$ нет ни одного числа вида c_i. Увеличим рассматриваемый интервал в десять раз. Заодно укажем индекс этого числа и найдем число цифр в этом, ближайшем к гуголу числе Кармайкла вида Черника.

```
> with(numtheory):
> s := 0: n:= 10^100 : for i from 1 to n -10^7 by 1 do
if isprime(6*i+1) and
isprime(12*i+1) and isprime(18*i+1)
then s:=s+1; print('c'[i]); a:=(6*i+1)*(12*i+1)*(18*i+1); print(a); print(length(a));break
```

c99999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999998631681
12959999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999946799761240000000000000000000000000000000000
00000000000000000000000000000000000000000000000000072794892081301559999
99999999999999999999999999999999999999999999999999999999999999999999999999999
99999966797791158833404382 09

304

В каждой из прогрессий $6i + 1$, $12i + 1$ и $18i + 1$ содержится бесконечно много простых чисел, но, вполне возможно, что с некоторого места эти простые числа для каждой прогрессии будут появляться только в разных местах. Поэтому из теоремы Черника вовсе не следует, что чисел Кармайкла бесконечно много.

Верно и обратное: если окажется, что множество чисел черниковского типа конечно, то это будет означать, что для достаточно большого i, по крайней мере, одно из чисел $6i + 1$, $12i + 1$, $18i + 1$ будет составным.

Функция $C(x)$

Обозначим символом $C(x)$ количество чисел Кармайкла, не превышающих действительного числа x. Например, как было установлено ранее, C(10 000) = 7. Поставим в программу, выдающую последовательно числа Кармайкла, счетчик и вычислим для примера C(1 000 000).

```
> with(numtheory):
> s: = 0:  for n from 3 by 2 to 1 000 000 do:
k:=0: for i from 1 to n − 1 do
if igcd(i, n) = 1 and i^(n−1) mod n = 1 then k := k+1 fi od:
 if k = φ(n) and φ(n) < n − 1 then s:= s + 1: fi do: s
```

43

Итак, C(1 000 000) = 43. Интервал увеличился на два порядка, а значение функции всего лишь на порядок. Функция $C(x)$ растет, но очень медленно.

Заключение

На самом деле установлено, что $\lim\limits_{x\to\infty} C(x) = \infty$ (см., например, [7]), а это значит, что множество чисел Кармайкла бесконечно Конечно или бесконечно множество кармайкловых чисел вида Черника, пока неизвестно.

Список литературы/References

[1] Горюшкин А. П., “Особенности и пути совершенствования информационного обеспечения курса теории чисел”, *Культурно-образовательная среда вуза*, сб. ст. межрегион. науч.-практ. конф. 4–8 февр. 2002 г., Камч. гос. пед. ун-т, Петропавловск-Камч., 2002, 51–59. [Goryushkin A. P., “Osobennosti i puti sovershenstvovaniya informatsionnogo obespecheniya kursa teorii chisel”, *Kul’turno-obrazovatel’naya sreda vuza*, sb. st. mezhregion. nauch.-prakt. konf. 4–8 fevr. 2002 g., Kamch. gos. ped. un-t, Petropavlovsk-Kamch., 2002, 51–59].

[2] Горюшкин А. П. , Горюшкин В. А., *Элементы абстрактной и компьютерной алгебры*, изд. 2-е, исправленное и дополненное, КамГУ им. им. Витуса Беринга, Петропавловск-Камч., 2011, 518 с. [Goryushkin A. P. , Goryushkin V. A., *Elementy abstraktnoy i komp’yuternoy algebry*, izd. 2-ye, ispravlennoye i dopolnennoye, KamGU im. im. Vitusa Beringa, Petropavlovsk-Kamch., 2011, 518 pp.]

[3] Горюшкин А. П., “Машинное решение задач дискретной математики”, *Вестник КРАУНЦ. Физико-математические науки*, 2011, № 2(3), 58–68. [Goryushkin A. P., “Mashinnoye resheniye zadach diskretnoy matematiki”, *Vestnik KRAUNTS. Fiziko-matematicheskiye nauki*, 2011, № 2(3), 58–68].

[4] Горюшкин А. П., “Исследование дискретных объектов компьютерными средствами”, *Теория и практика современных гуманитарных и естественных наук*, Материалы ежегодной науч.-практ. конф. 8-11 февр. 2012 г.. Т. 2, КамГУ им. Витуса Беринга, Петропавловск-Камч., 2012, 185–187. [Goryushkin A. P., “Issledovaniye diskretnykh ob"yektov komp’yuternymi sredstvami”, *Teoriya i praktika sovremennykh gumanitarnykh i yestestvennykh nauk*, Materialy yezhegodnoy nauch.-prakt. konf. 8-11 fevr. 2012 g.. V. 2, KamGU im. Vitusa Beringa, Petropavlovsk-Kamch., 2012, 185–187].

[5] Горюшкин А. П., *Теория чисел в Maple*, Palmarium Academic Publishing, Саарбрюккен, 2017, 156 с. [Goryushkin A. P., *Teoriya chisel v Maple*, Palmarium Academic Publishing, Saarbryukken, 2017, 156 pp.]

[6] Chernick J., “On Fermat’s simple theorem”, *Bull. Amer. Math. Soc.*, 1939, № 45, 269-274.

[7] Alford W. R., Granville A., Pomeranse C., “There are infinitely many Carmichael numbers”, *Annals Math.*, 1994, № 140, 703-722.

Список литературы (ГОСТ)

[1] Горюшкин А. П. Особенности и пути совершенствования информационного обеспечения курса теории чисел // Культурно-образовательная среда вуза : сб. ст. межрегион. науч.-практ. конф. 4–8 февр. 2002 г. / Камч. гос. пед. ун-т. - Петропавловск-Камч., 2002. – С. 51–59.

[2] Горюшкин А. П. , Горюшкин В. А. Элементы абстрактной и компьютерной алгебры, изд. 2-е, исправленное и дополненное // КамГУ им. им. Витуса Беринга. – Петропавловск-Камч. : 2011. – 518 с.

[3] Горюшкин А. П. Машинное решение задач дискретной математики // Вестник КРАУНЦ. Физико-математические науки. 2011. №2 (3). С. 58–68.

[4] Горюшкин А. П. Исследование дискретных объектов компьютерными средствами / Теория и практика современных гуманитарных и естественных наук. Вып. 2: Материалы ежегодной науч.-практ. конф. Петропавловск-Камч., 8-11 февр. 2012 г. / КамГУ им. Витуса Беринга. С. 185–187.

[5] Горюшкин А. П. Теория чисел в Maple. Саарбрюккен: Palmarium Academic Publishing, 2017. 156 с.

[6] Chernick J. On Fermat's simple theorem // Bull. Amer. Math. Soc. 1939. no. 45. pp. 269-274.

[7] Alford W.R., Granville A., Pomeranse C. There are infinitely many Carmichael numbers // Annals Math.1994. no. 140. pp. 703-722.

Для цитирования: Горюшкин А. П. О методике применения современных вычислительных технологий при изучении теории числе // *Вестник КРАУНЦ. Физ.-мат. науки*. 2020. Т. 30. № 1. С. 79-86. DOI: 10.26117/2079-6641-2020-30-1-79-86

For citation: Goryushkin A. P. On the methodology application of modern computing technologies in studying the theory of numbers, *Vestnik KRAUNC. Fiz.-mat. nauki.* 2020, **30**: 1, 79-86. DOI: 10.26117/2079-6641-2020-30-1-79-86

Поступила в редакцию / Original article submitted: 12.02.2020