Вестник Сыктывкарского университета.
Сер.1. Вып.10. 2009

УДК 511.291

ОХОТА ЗА ЧИСЛАМИ

В.Д. Яковлев, Р.Е. Афонин

В данной статье показана история поиска дружественных чисел со времен древних греков и до наших дней. Также приведены текущие результаты в области поиска циклов общительных чисел и чисел Мерсенна.

Предыстория

Античные математики считали очень важным рассматривать вместе с каждым числом все его делители. Числа, имеющие много делителей, назывались "abundant" (избыточными), а имеющие мало делителей, - "defizient" (недостаточными). При этом в качестве меры использовалось не количество, а сумма собственных делителей, которую сравнивали с самим числом. Так, например, 10 — недостаточное число, а 12 — избыточное число. Встречается и "пограничный" случай, когда сумма собственных делителей равна самому числу. Такие числа древние греки особенно ценили и называли их *совершенными*. Точно неизвестно, когда и где впервые обратили внимание на совершенные числа. Предполагают, что они были известны уже в древнем Вавилоне и древнем Египте.

Первое доказанное утверждение о совершенных числах принадлежит Евклиду (примерно 300 г. до н.э.). В его "Началах" мы находим теорему, устанавливающую способ получения совершенных чисел. На современном языке она звучит так: если число $p = 2^{n+1} - 1$ — простое, то $2^n p$ является совершенным.

Позднее Никомах из Герасы указал первые совершенные числа: 6, 28, 496 и 8128.

Большое внимание в античные времена уделяли и числам 220 и 284, у которых было отмечено следующее удивительное свойство: сумма собственных делителей 220 равна 284 и, наоборот, сумма собственных делителей 284 равна 220. Их назвали дружественными числами. Следы

этих чисел также теряются во тьме веков. Весьма вероятно, что первым обратил на них внимание Пифагор.

Указать какой-нибудь общий способ получения дружественных чисел, дающих пару 220 и 284 и другие, — задача, представляющая значительные трудности и в наши дни. Правда, один способ такого рода указал ещё в IX-м веке Сабит ибн Корра. На современном языке способ получения дружественных чисел звучит так:

Теорема (Сабит). Если все три числа $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ и $r = 9 \cdot 2^{2n-1} - 1$ — простые, то числа $A = 2^n p\, q$ и $B = 2^n r$ – дружественные.

Теорема Сабита даёт дружественные числа при $n = 2, 4, 7$. В настоящее время известно, что этими тремя случаями исчерпываются все значения $n \leq 20000$, при которых указанный способ даёт дружественные числа. С течением времени формулы Сабита были забыты, а его книгу открыли заново лишь в XIX-м веке.

В начале XVII-го века два французских математика — Пьер Ферма в 1636 г. и Ренэ Декарт в 1638 г. — независимо друг от друга и от Сабита получили те же формулы. В ходе своих исследований Ферма и Декарт вывели формулу, дающую сумму делителей числа по его представлению в виде произведения простых чисел, а именно: $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$, если числа a и b взаимно простые.

Здесь через $\sigma(a)$ обозначена сумма всех делителей числа a. При этих обозначениях условие того, что a и b — дружественные числа, можно записать в виде: $\sigma(a) = a + b = \sigma(b)$.

После периода малозначащих работ, последовавшего за работами Ферма и Декарта, существенного продвижения в решении проблемы дружественных чисел добился Леонард Эйлер. С присущей ему основательностью и энергией начал он штурм этой задачи. Прежде всего Эйлер доказал, что по способу Евклида получаются все чётные совершенные числа, а нечетные совершенные числа (если таковые вообще существуют) должны иметь некоторый специальный вид. В своих работах Эйлер излагает пять различных методов для отыскания дружественных чисел, демонстрируя виртуозность в вычислениях и терпение, и дарит изумленным современникам почти 60 новых пар.

Эйлер — признанный всеми авторитет — оставался непревзойденным вплоть до последних десятилетий. Первым побил рекорд Эйлера бельгийский математик Поль Пуле. Его двухтомная монография по теории чисел была издана в 1929 г. в Брюсселе под многозначительным названием “La chasse aux nombres” (“Охота за числами”). Кроме всего прочего, в ней приведены 62 новые пары дружественных чисел.

С наступлением эры ЭВМ возник новый метод, о котором Эйлер не мог и помышлять, — перебирать все числа подряд, пока хватит машинного времени.

Aliquot sequences (кратные последовательности)

Кратной последовательностью (aliquot sequence) называется последовательность целых чисел: $n,\ i(n),\ i(i(n)),\ \ldots$, где $i(n) = \sigma(n) - n$ — сумма собственных делителей числа n. В зависимости от поведения все кратные последовательности делят на следующие группы:

1. Последовательности, которые заканчиваются простым числом. Некоторые из таких последовательностей могут сходиться к одному простому числу. Говорят, что такие последовательности образуют семейство последовательностей данного простого числа (prime family).
2. Последовательности, которые входят в цикл. В зависимости от длины циклы делят:
   а) совершенное число (perfect number) — цикл единичной длины
   б) дружественная пара чисел (amicable pair) — цикл из двух чисел
   в) цикл общительных чисел (sociable numbers) — цикл длины больше 2.
3. Последовательности, для которых не известно, заканчиваются они или нет (open-end sequences, OE-sequences).

По гипотезе Каталана третья из вышеперечисленных групп последовательностей пуста, т.е. любая кратная последовательность заканчивается или простым числом, или совершенным числом, или циклом. До сих пор не удалось доказать или опровергнуть это утверждение. Уже в интервале [1,1000] есть пять чисел (276, 552, 564, 660, 966), называемых пятеркой Лемера (Lehmer five), для которых не известно, заканчивается порожденная каждым из них последовательность или нет.

Интервал	Количество OE-sequences	Предел вычисления
[1,1000]	5	$> 10^{157}$
[1,10000]	81	$> 10^{120}$
[1,50000]	442	$> 10^{100}$
$(50000,10^5]$	464	$> 10^{100}$
[1,100000]	906	$> 10^{100}$
(100000,200000]	961	$> 10^{100}$
(200000,300000]	931	$> 10^{80}/> 10^{1000}$
(300000,400000]	876	$> 10^{80}$
(400000,500000]	916	$> 10^{80}$
(500000,600000]	971	$> 10^{80}$
(600000,700000]	958	$> 10^{80}$
(700000,800000]	961	$> 10^{80}$
(800000,900000]	982	$> 10^{80}$
$(900000,10^6]$	985	$> 10^{80}$

Из этой таблицы видно, что только около 1% всех натуральных чисел являются начальными числами открытой последовательности.

Для вычисления кратных последовательностей необходимы быстрые алгоритмы факторизации. В настоящее время наиболее популярными являются следующие:

1. ECM (Elliptic curves method) — факторизация с помощью эллиптических кривых
2. QS (Quadratic sieve) — алгоритм квадратичного решета
3. NFS (Number field sieve) — алгоритм решета числового поля

Ниже приведены некоторые из известных на данный момент 171 цикла, длина которых больше 2.

1. 12496 14288 15472 14536 14264
2. 14316 19116 31704 47616 83328 177792 295488 629072 589786 294896 358336 418904 366556 274924 275444 243760 376736 381028 285778 152990 122410 97946 48976 45946 22976 22744 19916 17716
3. 1264460 1547860 1727636 1305184
4. 2115324 3317740 3649556 2797612
5. 2784580 3265940 3707572 3370604
6. 4938136 5753864 5504056 5423384

7. 7169104 7538660 8292568 7520432
8. 18048976 20100368 18914992 19252208

...

164. 603522492225409264198146583895430075942547 5
603554680606737350549447409891104324057452 5
603586870704718971374954083149006795942547 5
603554680606824940317922004733854324057452 5

165. 391150239292252590375909613374696200110421488
412706950753625424982046686336737421393578512
435451675827984725580928493503563614741333488
412706950753625437407286121400928295713962512

166. 1429728540745639343304676012096852504918147031 1
1464045734255152560735802555313256886436323368 9
1499186629423269768712493378756478308242819031 1
1464045734255153472542398096703640664509052968 9

167. 9076901541921811385428391478566732739553148309 0
9321791554298006204684541639562322426386563691 0
9573288569943390074404654035304330453421456789 0
9321791554298005219762069870998494925019349611 0

168. 181017541347134401796562505110734885245314452710
183453436764234006003455468784446760709757547290
185922111249966914853345771282277471159220833510
183453436764234006002798864819744602767066526490

169. 553844823005460753264102288123635354110397606474428 4
593355153249052011477798973456017657183207506667331 6
635684082008174120791511356952133444956418391790908 4
593355153249052017479288774513988229510323247922371 6

170. 627582618769848520570574836939315116811634898281546 12
636476727110741900878582901916596764893500121897909 88
645496882860874569230306643750596644537433109734474 12
636476727110741900678972467405061673389794583731125 88

171. 1477468340679857073613107326166790072136993663719203 75
1569548520552095711652558920970283632737984689432796 25
1667367408518344883409865637685678915797357130957603 75
1569548520552095711780894271715341666354925800242396 25

Среди известных циклов, длина которых больше 2, 161 цикл имеют длину 4, 1 — длину 5, 5 — длину 6, 2 — длину 8, 1 — длину 9 и 1 — длину 28. Ниже приведены все циклы, длина которых больше 4.

Длина цикла	***Номер в списке***	***Цикл***
5	1	12496 14288 15472 14536 14264
6	32	21548919483 23625285957 24825443643 26762383557 25958284443 23816997477
6	38	90632826380 101889891700 127527369100 159713440756 129092518924 106246338676
6	48	1771417411016 1851936384424 2118923133656 2426887897384 2200652585816 2024477041144
6	50	3524434872392 4483305479608 4017343956392 4574630214808 4018261509992 3890837171608
6	53	4773123705616 5826394399664 5574013457296 5454772780208 5363145542992 5091331952624
8	18	1095447416 1259477224 1156962296 1330251784 1221976136 1127671864 1245926216 1213138984
8	20	1276254780 2299401444 3071310364 2303482780 2629903076 2209210588 2223459332 1697298124
9	17	805984760 1268997640 1803863720 2308845400 3059220620 3367978564 2525983930 2301481286 1611969514
28	2	14316 19116 31704 47616 83328 177792 295488 629072 589786 294896 358336 418904 366556 274924 275444 243760 376736 381028 285778 152990 122410 97946 48976 45946 22976 22744 19916 17716

О числах Мерсенна

Числом Мерсенна называется простое число вида $M_p = 2^p - 1$, где p — простое число. Числа Мерсенна получили известность в связи с эффективным критерием простоты Люка – Лемера, благодаря которому простые числа Мерсенна давно удерживают лидерство как самые большие известные простые числа.

Теорема (Люка—Лемер). Пусть n — нечетное число, и последовательность $\{L_m\}$ определена рекуррентным образом:

$$L_0 = 4, \quad L_{m+1} = L_m^2 - 2, \quad 0 \leqslant m < n.$$

Число M_n — простое тогда и только тогда, когда $L_{n-2} \equiv 0 \pmod{n}$

Критерий был первоначально открыт Люка в конце 1890-х гг., а данную краткую форму приобрел около 1930 г. в работах Лемера.

На данный момент самым большим известным простым числом является число Мерсенна $M_{43112609} = 2^{43112609} - 1$, найденное в августе 2008 года в рамках проекта распределённых вычислений GIMPS (Great Internet Mersenne Prime Search). Этот проект был организован в 1995 г. Г. Уолманом, написавшим быструю программу для персонального компьютера и разместившим ее на своем web-сервере. Он организовал также распределенную базу данных, в которой отражался ход поиска. В 1997 г. компанией Entropia, Inc., основанной С. Куровски, была организована система поддержки распределенных вычислений PrimeNet, которая в настоящее время координирует работу нескольких сотен тысяч компьютеров.

Длина $M_{43112609}$ составляет 12978189 десятичных цифр, что позволяет GIMPS претендовать на премию в 100000 долларов США, назначенную сообществом Electronic Frontier Foundation за нахождение простого числа, длина которого превышает 10 миллионов десятичных цифр. Всего известно 46 простых числа Мерсенна, причём порядковые номера с уверенностью установлены только у первых 39.

Ниже приведена таблица со всеми известными числами Мерсенна.

№	p	M_p	Кол-во дес. знаков в M_p	Дата открытия	Исследователь
1	2	3	1	5ый век до н.э.	Древнегреч. математики
2	3	7	1	5ый век до н.э.	Древнегреч. математики
3	5	31	2	3ый век до н.э.	Древнегреч. математики
4	7	127	3	3ый век до н.э.	Древнегреч. математики
5	13	8191	4	1456	неизвестен
6	17	131071	6	1588	Cataldi
7	19	524287	6	1588	Cataldi
8	31	2147483647	10	1772	Euler
9	61	2305843009213693951	19	1883	Pervushin
10	89	618970019...449562111	27	1911	Powers
11	107	162259276...010288127	33	1914	Powers
12	127	170141183...884105727	39	1876	Lucas
13	521	686479766...115057151	157	30 января 1952	Robinson
14	607	531137992...031728127	183	30 января 1952	Robinson
15	1,279	104079321...168729087	386	25 июня 1952	Robinson
16	2,203	147597991...697771007	664	7 октября 1952	Robinson
17	2,281	446087557...132836351	687	9 октября 1952	Robinson
18	3,217	259117086...909315071	969	8 сентября 1957	Riesel
19	4,253	190797007...350484991	1,281	3 ноября 1961	Hurwitz
20	4,423	285542542...608580607	1,332	3 ноября 1961	Hurwitz
21	9,689	478220278...225754111	2,917	11 мая 1963	Gillies
22	9,941	346088282...789463551	2,993	16 мая 1963	Gillies
23	11,213	281411201...696392191	3,376	2 июня 1963	Gillies
24	19,937	431542479...968041471	6,002	4 марта 1971	Tuckerman
25	21,701	448679166...511882751	6,533	30 октября 1978	Noll & Nickel
26	23,209	402874115...779264511	6,987	9 февраля 1979	Noll
27	44,497	854509824...011228671	13,395	8 апреля 1979	Nelson & Slowinski
28	86,243	536927995...433438207	25,962	25 сентября 1982	Slowinski
29	110,503	521928313...465515007	33,265	28 января 1988	Colquitt & Welsh
30	132,049	512740276...730061311	39,751	19 сентября 1983	Slowinski
31	216,091	746093103...815528447	65,050	1 сентября 1985	Slowinski
32	756,839	174135906...544677887	227,832	19 февраля 1992	Slowinski & Gage
33	859,433	129498125...500142591	258,716	4 января 1994	Slowinski & Gage

№	p	M_p	***Кол-во дес. знаков в*** M_p	***Дата открытия***	***Исследователь***
34	1,257,787	412245773...089366527	378,632	3 сентября 1996	Slowinski & Gage
35	1,398,269	814717564...451315711	420,921	13 ноября 1996	GIMPS / Joel Armengaud
36	2,976,221	623340076...729201151	895,932	24 августа 1997	GIMPS / Gordon Spence
37	3,021,377	127411683...024694271	909,526	27 января 1998	GIMPS / Roland Clarkson
38	6,972,593	437075744...924193791	2,098,960	1 июня 1999	GIMPS / Nayan Hajratwala
39	13,466,917	924947738...256259071	4,053,946	14 ноября 2001	GIMPS / Michael Cameron
40?	20,996,011	125976895...855682047	6,320,430	17 ноября 2003	GIMPS / Michael Shafer
41?	24,036,583	299410429...733969407	7,235,733	15 мая 2004	GIMPS / Josh Findley
42?	25,964,951	122164630...577077247	7,816,230	18 февраля 2005	GIMPS / Martin Nowak
43?	30,402,457	315416475...652943871	9,152,052	15 декабря 2005	GIMPS / Curtis Cooper & Steven Boone
44?	32,582,657	124575026...053967871	9,808,358	4 сентября 2006	GIMPS / Curtis Cooper & Steven Boone
45?	37,156,667	202254406...308220927	11,185,272	6 сентября 2008	GIMPS / Hans-Michael Elvenich
46?	43,112,609	316470269...697152511	12,978,189	23 августа 2008	GIMPS / Edson Smith

Неизвестно, существуют ли неоткрытые числа Мерсенна между 39-ым и 46-ым, поэтому нумерация в таблице возможно временная. Интересно отметить, что 29-е число Мерсенна было открыто после 30-го и 31-го, а 46-е известное простое число Мерсенна было найдено на две недели позднее 45-го известного простого числа Мерсенна и оказалось меньше его.

Заключение

Имеют ли данные исследования какие-либо применения, в настоящее время неизвестно. Но вот что сказал по этому поводу Леонард Эйлер в работе "De numeris amicabilibus" ("О дружественных числах"). "Из всех проблем, рассматриваемых в математике, нет таких, которые считались бы в настоящее время более бесплодными и бесполезными, чем проблемы, касающиеся природы чисел и их делителей. В этом отношении нынешние математики сильно отличаются от древних, придававших гораздо большее значение исследованиям такого рода... А именно, они не только считали, что отыскание истины похвально само по себе и достойно человеческого познания, но, кроме того, совершенно справедливо полагали, что при этом замечательным образом развивается изобретательность и перед человеческим разумом раскрываются новые возможности решать сложные задачи. Математика, вероятно, никогда не достигла бы такой высокой степени совершенства, если бы древние не приложили столько усилий для изучения вопросов, которыми сегодня многие пренебрегают из-за их мнимой бесплодности".

Литература

1. **Боро В., Цагир Д., Рольфс Ю., Крафт Х., Янцен Е.** Живые числа. М.: Мир, 1985. 128 с.
2. **Черемушкин А.В.** Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.
3. `http://www.aliquot.de/aliquote.htm`
4. `http://www.mersenne.org`

Summary

Yakovlev V.D., Afonin R.E. The hunting on numbers

In this article the history of search of amicable pairs since times of ancient Greeks and up to now is shown. Also current outcomes of search of aliquot sequences and Mersenne numbers are given.

Сыктывкарский университет *Поступила 05.12.2008*