К ВОПРОСУ О КОЛИЧЕСТВЕННОМ СОДЕРЖАНИИ ПРОСТЫХ ЧИСЕЛ МЕРСЕННА В НАТУРАЛЬНОМ РЯДУ ЧИСЕЛ

А.В. Баяндин

Среди множества чисел Мерсенна, вида $2^p - 1$, где *p* – простое число, особый интерес представляют простые числа Мерсенна. Назвали эти числа по имени французского монаха и математика Марена Мерсенна, родившегося в 1588 году. Именно Мерсенн вывел формулу простых чисел $2^p - 1$, где *p* –простое число. Многие выдающиеся математики занимались в свое время поиском и доказательством простоты чисел Мерсенна, так Эйлер доказал, что число $2^{31}-1$ – простое. В 1952 году самое большое простое число содержало 157 цифр, в 1985 году – 65050. Таких чисел найдено всего 40 (ноябрь 2003г.). Используя метод распределенных вычислений[1] в августе 2002г. было вычислено 39 простое число Мерсенна: $2^{13466917}-1$, имеющее в десятичной записи 4053946 цифр. В декабре 2003г. этот результат был улучшен и следующее, 40-ое число Мерсенна $2^{20996011} - 1$, имело уже 6320430 цифр[2]. Интерес к таким числам вызван, во-первых, возможностью привлечения разработанного аналитического аппарата теории чисел и, во-вторых, прогрессом в вычислительной технике. Если мы зададимся вопросом, какое же наибольшее простое число известно человечеству - то ответом будет какое-то простое число Мерсенна.

Заметим, что простота числа $2^p - 1$ влечёт простоту p; в противном случае p = xy для x,y > 1 и число $2^p - 1 = 2^{xy} - 1$ не будет простым в виду делимости на 2^x-1 (как, впрочем, и на 2^y-1) [1].

Таких простых чисел в натуральном ряду не так много, то есть эти числа далеко не исчерпывают весь массив простых чисел. Представляет интерес, хотя бы качественно, оценить количественное содержание простых чисел Мерсенна в натуральном ряду чисел.

Подмечено, что все простые числа Мерсенна имеют окончание на цифру 1 и 7. Этот факт наблюдения наглядно представлен в таблице из четырех столбцов [2] в виде записи по порядку следования рассчитанных чисел Мерсенна: $M_n = 2^n - 1$.

Таблица 1

M_{4n-3}		M_{4n-2}		M_{4n-1}		M_{4n}	
M_1	**1**	M_2	**3**	M_3	**7**	M_4	**15**
M_5	**31**	M_6	**63**	M_7	**127**	M_8	**255**
M_9	**511**	M_{10}	**1023**	M_{11}	**2047**	M_{12}	**4095**
M_{13}	**8191**	M_{14}	**16383**	M_{15}	**32767**	M_{16}	**65535**

Действительно числа, попадающие в один и тот же столбец, оканчиваются на одну и ту же цифру. Числа в первом и третьем столбцах имеют окончание 1 и 7 соответственно. Числа четвертого столбца оканчиваются на 5 и, в соответствии с признаком деления на число5, делятся на 5. Также, нетрудно показать, что числа второго и четвертого столбцов делятся на число 3. Это следует из рассмотрения разности двух последовательных чисел с четными номерами M_{2k} и M_{2k+2}:

$$(2^{2k+2} -1) - (2^{2k} - 1) = 2^{2k+2} - 2^{2k} = 3 \cdot 2^{2k} \qquad (1)$$

[1] Метод распределенных вычислений заключается в использовании большого количества персональных компьютеров (от 100тысяч до 250 тысяч единиц) в реальном времени для параллельного вычисления
[2] http://www.izvestia.ru/science/41833_print

И так как число M_{2k} делится на 3, то и M_{2k+2} тоже делится на 3. Следовательно, простые числа Мерсенна необходимо искать только среди тех чисел Мерсенна, которые имеют в окончании цифры 1 и 7. К сожалению, и среди этих чисел редко встречаются простые числа Мерсенна. Так, например, число $M_9 = 511 = 7 \cdot 73$, $M_{11} = 2047 = 23 \cdot 89$, а число $M_{15} = 32767 = 7 \cdot 31 \cdot 151$. То есть, числа Мерсенна, имеющие окончания 1 и 7 и в показателе степени двойки (2^n) как простые (p=11), так и составные (n=9, n=15) числа, могут быть составными числами. Поэтому, вопрос сужения диапазона поиска простых чисел Мерсенна является достаточно актуальным. Другими словами, необходим критерий определения простоты, или необходимые условия простоты, как показателя степени двойки, так и самого числа Мерсенна, ограничивающие перебор чисел.

Определение того, является ли данное число простым или составным, в общем случае не такая уж тривиальная задача. Только в 2002 году было доказано, что она полиноминально разрешима[3]. Тем не менее, предложенный (и строго обоснованный теоретически) детерминированный алгоритм практически непригоден, в виду его большой (хотя и полиномиальной) сложности. Поэтому в криптографии с открытым ключом, где используются простые числа порядка 10300, простоту по-прежнему определяют с помощью эффективного вероятностного алгоритма Миллера - Рабина. Важно отметить, что если практика довольствуется числами, являющимися простыми с вероятностью близкой к 1, то теория такие числа не приемлет: если про число утверждается, что оно простое, это должно быть строго доказано. Эта разница подчёркивается в разделение алгоритмов на вероятностные и детерминированные.

Числа Мерсенна выгодно отличаются от остальных простых чисел наличием эффективного (детерминированного!) критерия их простоты, носящего имя Люка-Лемера:

Число Mp является простым тогда и только тогда, когда оно делит число Lp-1, где числа Lk определяются рекуррентным соотношением:

L1 = 4,

Lk+1 = Lk2 - 2.

Для поиска простых чисел Мерсенна сервер GIMPS раздаёт клиентам простые "экспоненты" p для проверки числа Mp на простоту. Клиент вычисляет последовательность чисел L1, L2, ..., Lp-1 по модулю числа Mp (т.е. вычисляются не сами числа Lk, длина которых растёт экспоненциально; а остатки от деления Lk на Mp, длина которых ограничена p битами). Если последнее число в этой последовательности получается нулевым, то по критерию Люка-Лемера число Mp является простым.

На сегодняшний день достоверно известны только первые 38 простых чисел Мерсенна. Также найдено два больших простых числа Мерсенна, порядковые номера которых пока не установлены.

В настоящее время известен метод, алгоритмы и программы распознавания простоты и факторизации чисел вида [3, 4]:

$$J_n = p_i + 30 \cdot n \qquad (2),$$

где: p_i = (7; 11; 13; 17; 19; 23; 29; 31) – восемь порождающих чисел Джойнт ряда чисел; n = 1, 2, 3… - натуральный ряд чисел.

В связи с изложенным выше, представляет интерес показатель степени двойки (2^p) и само простое число Мерсенна выразить в виде (2). Для этого, сначала, воспользуемся известным методом скрининга – матричным методом анализа простых чисел [5]. В

[3] http://www.cse.iitk.ac.in/news/primality.html , статья индийских математиков Prof. Manindra Agarwal , Nitin Saxena и Neeraj Kayal по обоснованию полиномиального алгоритма нахождения простых чисел на основе китайской теоремы об остатках.

основу этого метода положены свойства простых и составных чисел ≥7, выделяющие их в джойнт (совместный) ряд чисел. Свойства простых и составных из простых сомножителей ≥7 чисел представляют собой признаки деления чисел на число 10 и на 9. Первый признак является окончанием (цифрой в младшем разряде) числа, второй признак является инвариантом или – цифровым корнем (результирующая цифра в последовательной редукции сумм цифр многозначного числа). Совместное использование перечисленных признаков позволяет выделить указанные выше числа в джойнт ряд, составляющий 26,6(6)% всех чисел натурального ряда чисел. Этот подход позволяет выявить закономерность, взаимную зависимость простых и составных из простых сомножителей ≥7 чисел, иначе - Закон обратной связи чисел:

$$\pi(x) + q(x) = [\eta\cdot x] \qquad (3),$$

где - $[\eta\cdot x] = [0{,}26(6)\cdot x]$ – целая часть рационального числа – количество чисел джойнт ряда;
$\eta = 0{,}26(6)$ – структурная постоянная натурального ряда чисел;
$\pi(x)$ – количество простых чисел ≥7 , не превышающих заданное натуральное x;
$q(x)$ – количество составных из простых сомножителей ≥7 чисел не превышающих заданное натуральное x.
Установленный Закон является основой как распределения простых чисел, так и алгоритма и программ распознавания простоты и факторизации чисел [6]. Для более подробного ознакомления с методом, алгоритмами и программами распознавания простоты и факторизации чисел отсылаю любознательных читателей к перечисленным работам автора.

Итак, воспользуемся указанным выше методом и представим рассчитанные числа Мерсенна из Таблицы 1 в соответствии с окончаниями для простых чисел (3;1;9;7) и инвариантами (1;2;4;5;7;8) в следующем виде:

Таблица 2

End Inv	1	3	7	5	1	3	7	5	1	3	7	5	1	3	7	5	1	3	7	5	1	3
1	1						127						8191						524287			
2																						
3																						
4					31						2047						131071					
5																						
6																						
7			7						511						32767						2097151	
8																						
9																						

Согласно полученным результатам сортировки чисел Мерсенна по свойствам простых чисел (Таблица 2) запишем рекуррентные соотношения для последовательностей чисел каждой строки указанной таблицы:

1) $2^{6k+1} - 1$, первая строка (числа 1; 127; 8191…); Inv = 1, End = 1; 7,
2) $2^{6k+5} - 1$, четвертая строка (числа 31; 2047; …); Inv =4, End = 1; 7,
3) $2^{6k+3} - 1$, седьмая строка (числа 7; 511; …); Inv =7, End = 7; 1.

Вариант 3) для седьмой строки таблицы 2 не интересен нам уже только из-за того, что показатель степени двойки делится на 3. В самом деле: $(6k + 3) / 3 = 2k + 1$. Для вариантов 1) и 2) окончания чисел на 1 и на 7 зависят, соответственно, от четности или нечетности значения k:

-1) и 2) для четного k = 0, 2, 4, …2k, End = 1;
-1) и 2) для нечетного k =1, 3, 5,…2k-1, End = 7.

Далее, рассмотрим представление показателя степени двойки (2^p) в виде выражения

$$J_n = p_i + 30 \cdot n, \qquad (4)$$

где p_i= (7; 11; 13; 17; 19; 23; 29; 31).

Для варианта 1) показатель p = 6k +1, а для варианта 2): p = 6k + 5. Составим таблицы изменения показателей степени двойки в зависимости от множителя ***k***.

а) p = 6k +1

Таблица 3

k	0	1	2	3	4	5	6	7	8	9	10	11
6k+1	**1**	**7**	**13**	**19**	**25**	**31**	**37**	**43**	**49**	**55**	**61**	**67**

б) p = 6k + 5

Таблица 4

k	0	1	2	3	4	5	6	7	8	9	10	11
6k+5	**5**	**11**	**17**	**23**	**29**	**35**	**41**	**47**	**53**	**59**	**65**	**71**

Из таблиц 3 и 4 видно, что для выражений p = 6k + 1 и p = 6k + 5 , исключая числа с окончанием 5, имеет место периодичность при k = 1 +5m; 2 +5m; 3 + 5m; 5 +5m и при k = 1 +5m; 2 + 5m; 3 + 5m; 4 + 5m соответственно. Далее, подставляя значения k в соответствующие выражения p = 6k + 1 и p = 6k + 5, получим интересующие нас представления показателя степени двойки (2^p) в виде формулы (4):

а) 6k + 1 =(7 + 30m; 13 + 30m; 19 +30m; 31 + 30m),
б) 6k +5 = (11 + 30m; 17 + 30m; 23 + 30m; 29 + 30m). (5)

Выше мы показали, что окончание 1 или 7 чисел Мерсенна $2^{6k+1} - 1$ и $2^{6k+5} - 1$ зависит от четности (нечетности) показателя степени двойки. Это же условие для выражений 5а), 5б) представим в виде таблиц:

а) **p = 6k + 1:**

Таблица 5

p	**End** для **$2^p - 1$, m =2t**	**End** для **$2^p - 1$, m =2t - 1**
7 + 30m	**7**	**1**
13 + 30m	**1**	**7**
19 + 30m	**7**	**1**
31 + 30m	**7**	**1**

б) **p = 6k + 5:**

Таблица 6

p	**End** для **2^p – 1, m =2t**	**End** для **2^p – 1, m =2t - 1**
11 + 30m	**7**	**1**
17 + 30m	**1**	**7**
23+ 30m	**7**	**1**
29 + 30m	**1**	**7**

Таким образом, мы получили для показателя степени двойки (2^p) чисел Мерсенна (2^p -1) выражения в виде порождающих чисел джойнт ряда [4]. Следовательно, показатели степени двойки (2^p) вида p = 6k + 1 и p = 6k + 5 , представленные в виде чисел джойнт ряда, полностью исчерпывают все простые числа натурального ряда чисел. При этом заметим, что каждая из последовательностей вида 6k + 1 и 6k + 5 количественно содержит в себе по 13, 3(3)% всех чисел натурального ряда чисел. И, как уже упоминали, для чисел Джойнт ряда существует эффективный метод распознавания простоты чисел [3,4,5,6].

Как мы уже убедились, все числа Мерсенна имеют окончание 1 или 7. Теперь нам необходимо представить сами числа Мерсенна $2^{6k+1} – 1$ и $2^{6k+5} – 1$ в виде порождающих чисел джойнт ряда $J_n = p_i + 30 \cdot n$. Для этого воспользуемся свойством счетности чисел джойнт ряда [4, стр. 34]. Сущность этого свойства заключается в следующем: достаточно умножить структурную постоянную на произвольное число джойнт ряда чисел, при этом дробная часть (мантисса) числа указывает на порождающее число, а целая часть - на номер этого числа в последовательности чисел джойнт ряда. Проиллюстрируем это в виде таблицы результатов умножения структурной постоянной на первые 16 членов джойнт ряда:

Таблица 7

p_i	7	11	13	17	19	23	29	31
$[\eta * p_i]$	1	2	3	4	5	6	7	8
$\{\eta * p_i\}$	**.866**	**.933**	**.466**	**.533**	**.066**	**.133**	**.733**	**.266**

Продолжение Таблицы 7

p_i	37	41	43	47	49	53	59	61
$[\eta * p_i]$	9	10	11	12	13	14	15	16
$\{\eta * p_i\}$	**.866**	**.933**	**.466**	**.533**	**.066**	**.133**	**.733**	**.266**

Указанная процедура для чисел Мерсенна $2^{6k+1} - 1$ и $2^{6k+5} - 1$ дает следующие результаты:

а) числа Мерсенна, имеющие окончание 1, дают $J_n = p_i + 30 \cdot n = 31 + 30n$;
б) числа Мерсенна с окончаниями 7 представляются как $J_n = p_i + 30 \cdot n = 7 + 30n$. (6)

Заметим также, что все числа Мерсенна вида $2^p - 1 = J_n = p_i + 30 \cdot n$ располагаются только в четных периодах джойнт ряда чисел. В этом легко убедиться, так как к нечетному числу прибавляется единица и переводит это число в четное $(1 + p)$, а 2^p четно всегда:

$$n = \frac{2^p - 1 - p_i}{30} = 2k \qquad (7)$$

Сейчас, используя данные таблиц 5 и 6 и результаты нахождения порождающих чисел, можно представить все числа Мерсенна, как и показатели степени, в виде порождающих периодических чисел джойнт ряда. В таблицах 8 и 9 показаны представления всех чисел Мерсенна, как и показателей степени двойки, в виде порождающих чисел джойнт ряда в зависимости от четности (нечетности) периода следования у порождающих чисел показателя степени двойки:

Таблица 8

$2^{p_i+30m}-1$ **m=2k**	$2^{7+30m}-1$	$2^{11+30m}-1$	$2^{19+30m}-1$	$2^{23+30m}-1$	$2^{31+30m}-1$	$2^{13+30m}-1$	$2^{17+30m}-1$	$2^{29+30m}-1$
p_i+30n **n=2k**	**7+30n**	**7+30n**	**7+30n**	**7+30n**	**7+30n**	**31+30n**	**31+30n**	**31+30n**

Таблица 9

$2^{p_i+30m}-1$ **m=2k-1**	$2^{7+30m}-1$	$2^{11+30m}-1$	$2^{19+30m}-1$	$2^{23+30m}-1$	$2^{31+30m}-1$	$2^{13+30m}-1$	$2^{17+30m}-1$	$2^{29+30m}-1$
p_i+30n **n=2k**	**31+30n**	**31+30n**	**31+30n**	**31+30n**	**31+30n**	**7+30n**	**7+30n**	**7+30n**

Чтобы более наглядно представить распределение простых чисел Мерсенна в натуральном ряду чисел необходимо рассмотреть их местоположение в джойнт ряду. В качестве примера покажем расположение простых чисел Мерсенна среди всех простых чисел, расположенных в джойнт ряду:

Простые числа (Джойнт ряд без составных чисел) **Таблица 10**

n	$J_n = p_i + 30 \cdot n$							
0)	7	11	13	17	19	23	29	31
1)	37	41	43	47		53	59	61
2)	67	71	73		79	83	89	
3)	97	101	103	107	109	113		
4)	127	131		137	139		149	151
5)	157		163	167		173	179	181
6)	191	193	197	199			211	
....								
....								
....								
272)								8191
....								
....								
4368)								131071
....								
....								
17476)	524287							
....								
....								
71582788)	2147483647							
....								
....								
76861433640456464)								2305843009213693951
....								
....								
20632333988089671248318736)								618970019642690137449562111
....								

Как видно из таблицы 10 все простые числа Мерсенна имеют порождающие числа 7 и 31, расположены они только в четных периодах n = 2k. Окончания (1 или 7) простых чисел Мерсенна зависят от четности (нечетности) периода m = 2k или m = 2k – 1 в соответствии с таблицами 8 и 9. Представим эти и другие, известные на данный момент времени [7,8], простые числа Мерсенна в «развернутом» виде:

1) $2^2 - 1 = 3 + 30\cdot 0 = 3$

2) $2^3 - 1 = 7 + 30\cdot\mathbf{0} = \mathbf{7}$;
3) $2^5 - 1 = 31 + 30\cdot\mathbf{0} = \mathbf{31}$;
4) $2^7 - 1 = 2^{7+30\cdot 0} - 1 = 7 + 30\cdot\mathbf{4} = \mathbf{127}$;
5) $2^{13} - 1 = 2^{13+30\cdot 0} - 1 = 31 + 30\cdot\mathbf{272} = \mathbf{8191}$;
6) $2^{17} - 1 = 2^{17+30\cdot 0} - 1 = 31 + 30\cdot\mathbf{4368} = \mathbf{131071}$;
7) $2^{19} - 1 = 2^{19+30\cdot 0} - 1 = 7 + 30\cdot\mathbf{17476} = \mathbf{524287}$;
8) $2^{31} - 1 = 2^{31+30\cdot 0} - 1 = 7 + 30\cdot\mathbf{71582788} = \mathbf{2147483647}$;
9) $2^{61} - 1 = 2^{31+30\cdot 1} - 1 = 31 + 30\cdot\mathbf{76861433640456464} = \mathbf{2305843009213693951}$;
10) $2^{89} - 1 = 2^{29+30\cdot 2} - 1 = 31 + 30\cdot\mathbf{20632333988089671248318736} = \mathbf{618970019642690137449562111}$.
11) $2^{107} - 1 = 2^{17+30\cdot 3} - 1 = 7 + 30n = \mathbf{162259276829213363391578010288127}$;
12) $2^{127} - 1 = 2^{7+30\cdot 4} - 1 = 7 + 30n_{12} = \mathbf{170141183460469231731687303715884105727}$;
13) $2^{521} - 1 = 2^{11+30\cdot 17} - 1 = 31 + 30n_{13}$;
14) $2^{607} - 1 = 2^{7+30\cdot 20} - 1 = 7 + 30n_{14}$;
15) $2^{1279} - 1 = 2^{19+30\cdot 42} - 1 = 7 + 30n_{15}$;
16) $2^{2203} - 1 = 2^{13+30\cdot 73} - 1 = 7 + 30n_{16}$;
17) $2^{2281} - 1 = 2^{31+30\cdot 75} - 1 = 31 + 30n_{17}$;
18) $2^{3217} - 1 = 2^{7+30\cdot 107} - 1 = 31 + 30n_{18}$;
19) $2^{4253} - 1 = 2^{23+30\cdot 141} - 1 = 31 + 30n_{18}$;

20) $2^{4423} - 1 = 2^{13 + 30\cdot 147} - 1 = 7 + 30n_{20}$;
21) $2^{9689} - 1 = 2^{29 + 30\cdot 322} - 1 = 31 + 30n_{21}$;
22) $2^{9941} - 1 = 2^{11 + 30\cdot 331} - 1 = 31 + 30n_{22}$;
23) $2^{11213} - 1 = 2^{23 + 30\cdot 373} - 1 = 31 + 30n_{23}$;
24) $2^{19937} - 1 = 2^{17 + 30\cdot 664} - 1 = 31 + 30n_{24}$;
25) $2^{21701} - 1 = 2^{11 + 30\cdot 723} - 1 = 31 + 30n_{25}$;
26) $2^{23209} - 1 = 2^{19 + 30\cdot 773} - 1 = 31 + 30n_{26}$;
27) $2^{44497} - 1 = 2^{7 + 30\cdot 1483} - 1 = 31 + 30n_{27}$;
28) $2^{86243} - 1 = 2^{23 + 30\cdot 2874} - 1 = 7 + 30n_{28}$;
29) $2^{110503} - 1 = 2^{13 + 30\cdot 3683} - 1 = 7 + 30n_{29}$;
30) $2^{132049} - 1 = 2^{19 + 30\cdot 4401} - 1 = 31 + 30n_{30}$;
31) $2^{216091} - 1 = 2^{31 + 30\cdot 7202} - 1 = 7 + 30n_{31}$;
32) $2^{756839} - 1 = 2^{29 + 30\cdot 25227} - 1 = 7 + 30n_{32}$;
33) $2^{859433} - 1 = 2^{23 + 30\cdot 28647} - 1 = 31 + 30n_{33}$;
34) $2^{1257787} - 1 = 2^{7 + 30\cdot 41926} - 1 = 7 + 30n_{34}$;
35) $2^{1398269} - 1 = 2^{29 + 30\cdot 46608} - 1 = 31 + 30n_{35}$;
36) $2^{2976221} - 1 = 2^{11 + 30\cdot 99207} - 1 = 31 + 30n_{36}$;
37) $2^{3021377} - 1 = 2^{17 + 30\cdot 100712} - 1 = 31 + 30n_{37}$;
38) $2^{6972593} - 1 = 2^{23 + 30\cdot 232419} - 1 = 31 + 30n_{38}$;
39) $2^{13466917} - 1 = 2^{7 + 30\times 448897} - 1 = 31 + 30n_{39}$[4];
40) $2^{20996011} - 1 = 2^{31 + 30\times 699866} - 1 = 7 + 30n_{40}$[5].

Из всех известных сорока простых чисел Мерсенна только первое $2^2 - 1 = 3$ имеет окончание 3, шестнадцать чисел имеет окончание 7 и двадцать три – 1.
Аналогичным образом формируются все остальные простые числа Мерсенна. Так, найденные недавно 39 и 40 простые числа Мерсенна можно представить следующим образом:
39-ое простое число Мерсенна $2^{13466917} - 1 = 2^{7 + 30\times 448897} - 1 = 31 + 30n_{39}$;
40-ое простое число Мерсенна $2^{20996011} - 1 = 2^{31 + 30\times 699866} - 1 = 7 + 30n_{40}$.
Следовательно, даже не зная числа Мерсенна в «развернутом» виде, можно сказать, что 39-ое простое число Мерсенна имеет в окончании 1, 40-ое - 7. Периоды повторения равны, соответственно:

$$\mathbf{n}_{39} = \frac{2^{7+30\times 448897} - 32}{30}, \quad \mathbf{n}_{40} = \frac{2^{31+30\times 699866} - 8}{30} \qquad (8).$$

Периоды повторения, как в показателе степени двойки, так и самого числа Мерсенна, выраженного числами джойнт ряда, имеют самостоятельный интерес. Поэтому, остановимся на выяснении данного вопроса по существу.

Во-первых, четность или нечетность периодов повторения порождающих чисел (показателя степени двойки) и их значение формируют окончания чисел Мерсенна (см. таблицы 8 и 9). Рассмотрим два произвольных числа Мерсенна с четными и нечетными периодами повторения:

1) $2^{7 + 30\times 2} - 1$ и $2^{7 + 30\times 4} - 1$ при $m = 2k$, ($m_1 = 2$, $m_2 = 4$), составим отношение

[4] Для 39-ого простого числа Мерсенна не определен его порядковый номер в ряду чисел Мерсенна
[5] Для 40-ого простого числа Мерсенна – аналогично.

$$\frac{2^{7+30\times4}}{2^{7+30\times2}} = 2^{60} = 1{,}152921504606846976\times10^{18} \qquad (9)$$

2) $2^{7+30\times1} - 1$ и $2^{7+30\times3} - 1$ при $m = 2k - 1$, (m_1=1, m_2=3), и также составим соотношение

$$\frac{2^{7+30\times3}}{2^{7+30\times1}} = 2^{60} = 1{,}152921504606846976\times10^{18} \qquad (10)$$

Необходимо заметить, что константа 2^{60} определяет периодичность изменения значений чисел Мерсенна. Представим это положение для чисел Мерсенна в виде таблиц:

Таблица 11

$2^{p_i + 60k}$ **k = m/2**	$2^7 2^{60k}$-1	$2^{11} 2^{60k}$-1	$2^{19} 2^{60k}$-1	$2^{23} 2^{60k}$-1	$2^{31} 2^{60k}$-1	$2^{13} 2^{60k}$-1	$2^{17} 2^{60k}$-1	$2^{29} 2^{60k}$-1
p_i + 60t **t = n/2**	**7+60t**	**7+60t**	**7+60t**	**7+60t**	**7+60t**	**31+60t**	**31+60t**	**31+60t**

Таблица 12

$2^{p_i + 60k - 30}$ **k =(m+1)/2**	$2^{-23} 2^{60k}$-1	$2^{-19} 2^{60k}$-1	$2^{-11} 2^{60k}$-1	$2^{-7} 2^{60k}$-1	$2^{1} 2^{60k}$-1	$2^{-17} 2^{60k}$-1	$2^{-13} 2^{60k}$-1	$2^{-1} 2^{60k}$-1
p_i + 60t **t = n/2**	**31+60t**	**31+60t**	**31+60t**	**31+60t**	**31+60t**	**7+60t**	**7+60t**	**7+60t**

Примечание: k = 0;1;2;3;4…….для Таблицы11 и k = 1;2;3;4…….. для Таблицы 12;
t = 0;1;2;3;4….. для обеих таблиц.

Рассмотрим формирование периода повторения порождающих чисел 7 и 31 джойнт ряда, соответствующих числам Мерсенна. Соответствующие вычисления сведем в Таблицу 13 и 14:

7 + 30n Таблица 13

m	0	0	0	0	0	1	1	1
n	**4**	68	**17476**	279620	**71582788**	293203100740	4691249611844	19215358410114116

Таблица 13а

m	2	2	2	2	2	3	3	3
n	4,919e18	7,870e19	2,014e22	3,223e23	8,252e25	3,380e29	**5,408e30**	2,215e34

31 +30n Таблица 14

m	0	0	0	1	1	1	1	1
n	**272**	**4368**	17895696	4581298448	73300775184	18764998447376	300239975158032	**76861433640456464**

Выделенные жирным шрифтом цифры в таблицах 13, 13а и 14 подчеркивают периоды ***n*** чисел 7 + 30n и 31 + 30n, соответствующие простым числам Мерсенна. Легко заметить, что с возрастанием значения периода ***n*** отношение соседних периодов стремится к значению:

$$\lim_{n\to\infty}\frac{n_i}{n_{i-2}}=\frac{8,252e+25}{7,158e+7}\approx 1,152\times 10^{18}\to\frac{2^{7+30\times 3}}{2^{7+30\times 1}}=2^{60}=1,152921504606846976\times 10^{18} \qquad (11)$$

Представим значения периодов следования чисел Мерсенна посредством рекурсии степени двойки:

1) End = 7 для 7 + 30n,

***n*: 0; 2^2;** $2^2(2^4+1)$; **$2^2(2^4(2^4(2^4+1)+1)+1)$; $2^2(2^4(2^4(2^4(2^4(2^4(2^4+1)+1)+1)+1)+1)+1)$;……….**

(0; 4; $4\times(16+1)$; **$4\times(16(16(16+1)+1)+1)$; …………………………………………)**

2) End = 1 для 31 + 30n,

***n*: 0; $2^4(2^4+1)$; $2^4(2^4(2^4+1)+1)$;** $2^4(2^4(2^4(2^4(2^4(2^4+1)+1)+1)+1)+1)$;…….

(**0; $16\times(16+1)$; $16\times(16(16+1)+1)$;……………………………………………………).**

Таким образом, в последовательности периодов повторения чисел джойнт ряда, соответствующих числам Мерсенна, наблюдается закономерность формирования значений периодов. Закономерность представляет собой бесконечное повторение операций сложения исходного числа (2^4) с единицей и последующего умножение на исходное (2^4). Для случая 1), дополнительно, производится умножение на множитель 2^2.

Выделенным жирным шрифтом обозначены номера периодов чисел джойнт ряда для простых чисел Мерсенна.

Таким образом, необходимыми условиями существования простых чисел Мерсенна вида $2^p - 1$ является:

а) принадлежность этих чисел к числам джойнт ряда;

б) четность периодов следования n = 2k простых чисел Мерсенна в джойнт ряду;

в) зависимость окончаний чисел Мерсенна (1 или 7) от четности или нечетности периодов повторения (m = 2k или m = 2k – 1) порождающих чисел в показателе степени двойки (2^{p+30m} -1);

г) представление чисел Мерсенна только двумя порождающими числами 7 + 30n и 31 + 30n.

Достаточными условиями простоты чисел Мерсенна является алгоритм распознавания простоты чисел джойнт ряда [4].

Теперь можно ответить на основной вопрос, поставленный в заглавии данной статьи. Зная количественное содержание чисел джойнт ряда в натуральном ряду чисел, а именно 26,6(6)%, можно определить количественные границы содержания простых чисел в натуральном ряду чисел.

Так как, простые числа Мерсенна имеют только четные периоды n = 2k, то этих чисел меньше, чем $\frac{26,6(6)}{2}=13,3(3)$ %. Простые числа Мерсенна выражаются только двумя порождающими числами 7 и 31 из восьми порождающих чисел джойнт ряда. Поэтому, их количество меньше, чем $\frac{2}{8}\times 13,3(3)$ % = 3,3(3)% от всех чисел натурального ряда чисел.

Примечания

1. Сайт: http://www.distributed.org.ru/?gimps-max
2. Ю.В. Королев, О.М. Мамедов**. Числа Мерсенна**. «КВАНТ», № 10, 1986, стр.24
3. А.В. Баяндин. **К распределению простых чисел в натуральном ряду чисел**. Новосибирск, «НАУКА», 1999, СИФ РАН,-40.
4. А.В. Баяндин. **Методологический принцип обратной связи в естествознании.** Новосибирск, Институт теплофизики СО РАН, 2003, -100.
5. А.В. Баяндин. **Матричный метод анализа натурального ряда чисел.** Тезисы докладов V Международной конференции «Алгебра и теория чисел: современные проблемы и приложения», Тула, 2003, стр. 33.
6. А.В. Баяндин. **Закон обратной связи чисел: простые числа и разложение чисел на множители.** Тезисы докладов V Международной конференции «Алгебра и теория чисел: современные проблемы и приложения», Тула, 2003, стр. 31.
7. В.И. Нечаев. Элементы криптографии. Основы теории защиты информации. М. «Высшая школа»,1999г.
8. Сайт: http://primes.utm.edu/largest.html.

Институт философии и права
СО РАН, г. Новосибирск

Bajandin A.V. To a question on the quantitative maintenance of prime numbers Mersenn in a natural line of numbers.

In the given work the analysis of prime numbers Mersenn on their accessory to numbers Joint lines will be carried out Necessary conditions of primes of numbers Mersenn are proved, there is a quality standard of borders of the quantitative maintenance of numbers Mersenn in a natural line of numbers.