УДК 513.64

С. И. Хашин

НАТУРАЛЬНЫЕ ЧИСЛА С БОЛЬШИМ ПАРАМЕТРОМ ФРОБЕНИУСА

Не существует чисел, меньших 2^{60}, псевдопростых по Фробениусу (FPP), с параметром Фробениуса, меньшим 128. В работе доказывается отсутствие FPP-чисел, меньших 2^{60} с любым параметром Фробениуса.

Ключевые слова: псевдопростые числа, кратные множители.

There are no Frobenius pseudoprime numbers (FPP) $<2^{60}$ with the Frobenius parameter < 128. In this paper, we prove the absence of FPP numbers less than 2^{60} with any Frobenius parameter.

Key words: pseudoprime numbers, multiple factors.

Наиболее мощный среди элементарных вероятностных методов проверки чисел на простоту – тест Фробениуса [1, 2, 3, 4].

Определение 1. Нечетное составное число n называется псевдопростым по Фробениусу (Frobenius pseudoprime, FPP), если оно не является полным квадратом и

$$(1 + \sqrt{c})^n \equiv 1 - \sqrt{c} \bmod n,$$

где c — наименьшее нечетное простое число такое, что символ Якоби $J(c/n)$ равен –1. Про такие числа будем говорить, что они принадлежат классу FPP(c).

На сегодняшний день неизвестно ни одного числа, псевдопростого по Фробениусу. Можно предположить, что таких чисел не существует вообще, т. е. тест Фробениуса дает точный критерий простоты числа.

В работах [1, 4] доказано, что не существует FPP-чисел, меньших 2^{60}, при $c < 128$. В связи с этим хотелось бы узнать, насколько большим может оказаться число c.

Определение 2. Для нечетного натурального числа n, не являющегося полным квадратом, назовем параметром Фробениуса и обозначим через $F_c(n)$ наименьшее нечетное число c такое, что символ Якоби $J(c/n)$ равен –1.

Очевидно, число c является простым. Для всех нечетных простых, меньших c, имеем $J(c/n) = +1$ или 0. В частности, n не имеет простых делителей $\le c$.

Сформулируем вопрос несколько по-другому: при каком наименьшем числе n для данного простого нечетного числа c получим $F_c(n) = c$? Для небольших чисел ($\approx 10^9$) ответ можно найти простым перебором. Для больших значений придется искать другой алгоритм.

Таблица 1. $F_c(n)$

c	$F_c(n)$	c	$F_c(n)$	c	$F_c(n)$	c	$F_c(n)$	c	$F_c(n)$	c	$F_c(n)$	c	$F_c(n)$
5	3	43	3	83	5	123	3	163	3	203	5	243	3
7	3	45	3	85	5	125	3	165	3	205	5	245	3
9	–	47	5	87	3	127	3	167	5	207	3	247	3
11	7	49	–	89	3	129	3	169	–	209	3	249	3
13	5	51	3	91	3	131	17	171	3	211	3	251	11
15	3	53	3	93	3	133	5	173	3	213	3	253	5
17	3	55	3	95	5	135	3	175	3	215	5	255	3
19	3	57	3	97	5	137	3	177	3	217	5	257	3
21	3	59	11	99	3	139	3	179	7	219	3	259	3
23	5	61	7	101	3	141	3	181	7	221	3	261	3
25	–	63	3	103	3	143	5	183	3	223	3	263	5
27	3	65	3	105	3	145	5	185	3	225	–	265	5
29	3	67	3	107	5	147	3	187	3	227	5	267	3
31	3	69	3	109	11	149	3	189	3	229	7	269	3
33	3	71	7	111	3	151	3	191	7	231	3	271	3
35	5	73	5	113	3	153	3	193	5	233	3	273	3
37	5	75	3	115	3	155	5	195	3	235	3	275	5
39	3	77	3	117	3	157	5	197	3	237	3	277	5
41	3	79	3	119	7	159	3	199	3	239	7	279	3
–	–	81	–	121	–	161	3	201	3	241	7	281	3

Предложение 1. а) Пусть $c \equiv 1 \bmod 4$ и x,y – нечетные числа. Тогда

$$\left(\frac{c}{4x+y}\right) = \left(\frac{c}{x}\right).$$

б) Пусть $c \equiv 3 \bmod 4$ и x,y – нечетные числа. Тогда

$$\left(\frac{c}{4cx+y}\right) = \left(\frac{c}{y}\right).$$

Доказательство. а)

$$\left(\frac{c}{4x+y}\right) = \left(\frac{4x+y}{c}\right) = \left(\frac{4x}{c}\right) = \left(\frac{x}{c}\right) = \left(\frac{c}{x}\right).$$

б)

$$\left(\frac{c}{4cx+y}\right) = (-1)^{\frac{c-1}{2}\cdot\frac{4cx+y-1}{2}}\left(\frac{4cx+y}{c}\right) = (-1)^{\frac{c-1}{2}\cdot\frac{y-1}{2}}\left(\frac{y}{c}\right) = \left(\frac{c}{y}\right).$$

Пример 1. Пусть $N_1 = 5$, $N_2 = 3$. Обозначим через $X = (3, 7)$ все нечетные вычеты x_i по модулю $2N_1 = 10$ такие, что $J(N_1, N_2x_i) = 1$.

Обозначим через $Y = (5,7)$ все нечетные вычеты y_j по модулю $4N_2 = 12$ такие, что $J(N_2, N_1y_j) = 1$.

Рассмотрим все возможные суммы $4N_2 \cdot x_i + N_1y_j = (1,11,49,59) \bmod 4N_1N_2$. Они составляют все возможные вычеты n по модулю $4N_1N_2$ такие, что $J(3/n) = J(5/n) = 1$.

Пример 2. Пусть $N_1 = 5\cdot13\cdot17\cdot29\cdot37\cdot41 = 48\,612\,265$, $N_2 = 3\cdot7\cdot11\cdot19\cdot23\cdot31\cdot43 = 134\,562\,351$. Обозначим через X все нечетные вычеты x_i по модулю $2N_1$ такие, что

$$\left(\frac{5}{N_2x}\right) = \left(\frac{13}{N_2x}\right) = \left(\frac{17}{N_2x}\right) = \left(\frac{29}{N_2x}\right) = \left(\frac{37}{N_2x}\right) = \left(\frac{41}{N_2x}\right) = 1.$$

Обозначим через Y все нечетные вычеты y_j по модулю $4N_2$ такие, что

$$\left(\frac{3}{N_1 x}\right) = \left(\frac{7}{N_1 x}\right) = \left(\frac{11}{N_1 x}\right) = \left(\frac{19}{N_1 x}\right) = \left(\frac{23}{N_1 x}\right) = \left(\frac{31}{N_1 x}\right) = \left(\frac{43}{N_1 x}\right) = 1.$$

Тогда всевозможные суммы $4N_2 \cdot x_i + N_1 y_j \bmod 4N_1N_2$ составляют все возможные вычеты n по модулю $4N_1N_2$ такие, что $J(3/n) = J(5/n) = \ldots = J(43/n) = 1$.

Более детально, $N_1 = 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37 \cdot 41 = 48\,612\,265$, $N_2 = 3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 31 \cdot 43 = 134\,562\,351$ и $N_{12} = 4N_1N_2$. Тогда каждый нечётный вычет n по модулю N_{12} может быть единственным образом представлен в виде:

$$n = y_i \cdot N_1 + x_i \cdot (4N_2) + kN_{12}$$

где $x_j \in X$, $y_i \in Y$ и k – целое неотрицательное.

Так как $45\ N_1N_2 > 2^{60}$, то для перебора чисел меньших 2^{60} будет достаточно брать $k \leq 45$, то есть всего 46 значений. При этом количество пар (x_j, y_i) будет около 450 млрд. Это, конечно, большое число, но вполне подъемное для современных, даже персональных компьютеров (несколько дней работы).

Найдем все такие $n < 2^{60}$, точнее говоря, $n < 45\ N_1N_2 \approx 1.02 \cdot 2^{60}$. Для всех них оказалось, что $F_c(n)$ не превышает 257. Вот список чисел $n < R$, для которых $F_c(n) \geq 239$:

```
257  1116971853972029831=1721*869521*746416591
257   682237826125094149=36047443*18926108743
257    24976302418603981=24976302418603981
251  1024042985038958771=57367*17850732739013
251   453954035543431861=304373*1491439896257
251   154149168067800611=421*366150042916391
251    64138805744679371=262740781*244114391
241  1026219868955993351=1243523*825252021037
241   999495089664227939=7215601*138518619539
241   794589470364458999=839*2437*19583*19844771
241   695681268077667119=3413*203832777051763
241   590562913970779429=21433*35759*770544707
241   530036595989136011=20161*26290193739851
241   341890388250402059=1999*171030709479941
241   236544798837871499=236544798837871499
241   189483189883094579=571*331844465644649
241    59471645416610171=2699*22034696338129
239  1157422019106907319=1157422019106907319
239  1073453847303031619=773*1388685442824103
239  1044220207258355111=170299*1283591*4776979
239  1034939251005361321=673223*34763*44222029
239  1012160911903194769=12737399*79463704631
239   868116409360316399=868116409360316399
239   781158046093912369=781158046093912369
239   741164938828874171=741164938828874171
239   724567276754267231=281*331*2609*10193*292933
239   712624335095093521=28099*25361199156379
239   636437033373755821=563107651*1130222671
239   600640889133973091=22331531*26896538761
239   595920634874656979=1511863*394163118533
```

```
239   52639673384245 4219=34367*15316924195957
239   43737251173080 3659=974286749*448915591
239   42341493135980 7911=241*1756908428878871
239   32238391626415 0571=322383916264150571
239   18594811907584 2899=7057*26349457145507
239    37136361651508019=37136361651508019
239    32378801299267331=329776151*98184181
239    17199376594892579=269*357437*178879643.
```

Всего же чисел, меньших 45 N_1N_2, для которых параметр Фробениуса $\min_c$ превышает 127, оказалось 119 027 246. Их можно все проверить напрямую, среди них нет ни одного числа, псевдопростого по Фробениусу. Таким образом, рассматривая числа до 2^{60}, можно ограничиться только теми, у которых $\min_c < 128$. Следовательно, мы имеем только 30 допустимых значений *c*:

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,
71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127.

Учитывая, что в работе [4] доказано, что не существует чисел, меньших 2^{60}, псевдопростых по Фробениусу, для которых $\min_c < 128$, отсутствие FPP, меньших 2^{60}, доказано полностью.

Библиографический список

1. *Хашин С. И.* Кратные множители псевдопростых чисел // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2013. Вып. 2. С. 102—107.
2. *Хашин С. И., Хашина Ю. А.* Свойства чисел, псевдопростых по Фробениусу // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2014. Вып. 2. С. 104—108.
3. *Crandall R. E., Pomerance C.* Prime Numbers: a Computational Perspective. 2nd ed. New York, etc. : Springer, 2005. 597 p.
4. *Khashin S. I.* Counterexamples for Frobenius primality test. // arxiv.org/abs/ 1307.7920. 2013. URL: http://arxiv.org (дата обращения: 10.01.2015).
5. *Ribenboim P.* My Numbers, My Friends: Popular Lectures on Number Theory. 2nd ed. New York, etc. : Springer, 2000. 392 p.