УДК 513.64

С. И. Хашин

КРАТНЫЕ МНОЖИТЕЛИ ПСЕВДОПРОСТЫХ ЧИСЕЛ

Доказываются свойства кратных множителей псевдопростых чисел. Основные результаты работы – теоремы 3,4,5. При практических вычислениях большой интерес могут представлять таблицы 1 и 2.

Ключевые слова: псевдопростые числа, кратные множители.

The properties of the multiple factors of pseudoprime numbers are proved. The main results is theorem 3,4,5. In practical calculations of great interest may be of tables 1 and 2.

Key words: pseudoprime numbers, multiple factors.

1. Введение

Одной из важнейших задач в теории чисел является проверка простоты числа. В настоящее время разработано множество самых разнообразных алгоритмов таких проверок [3,4,5]. Если рассматриваемое число достаточно велико, например, больше 10^{20}, то все эти методы дают лишь вероятностный ответ: число может оказаться гарантировано составным, или «вероятно простым». То есть каждый из этих методов может принять некоторое составное число за простое, но не наоборот. Такие числа называются «псевдопростыми», с различными модификациями. Наиболее простой, популярный, хорошо изученный и довольно эффективный метод основан на малой теореме Ферма.

Определение 1. Составное число n называется псевдопростым по основанию a, если

$$a^{n-1} \equiv 1 \bmod n.$$

Псевдопростые числа по различным основаниям хорошо изучены. Например, имеется полный список [7] всех пседопростых по основанию 2 чисел, меньших 2^{64}, всего 118 968378 чисел. Также можно выписать все числа,

меньшие 2^{32}, псевдопростые одновременно по основаниям 2 и 3. Их оказывается 103:

Таблица 1

1373653	1530787	1987021	2284453	3116107
5173601	6787327	11541307	13694761	15978007
16070429	16879501	25326001	27509653	27664033
28527049	54029741	61832377	66096253	74927161
80375707	101649241	102690677	105919633	106485121
117987841	143168581	154287451	161304001	193949641
206304961	218642029	223625851	247318957	252853921
259765747	275619961	314184487	326695141	390612221
393611653	489994201	540654409	572228929	579606301
581618143	682528687	717653129	745745461	787085857
846961321	871157233	927106561	938376181	960946321
979363153	981484561	1028494429	1157839381	1168256953
1236313501	1463178817	1481626513	1518290707	1521221473
1538012449	1638294661	1854940231	1856689453	1860373241
1909566073	1921309633	1991063449	1995830761	2057835781
2117555641	2217879901	2284660351	2311558021	2323147201
2412172153	2431144801	2626783921	2693739751	2736316301
2781117721	2837917633	3028586471	3056100623	3215031751
3299246833	3344191241	3407772817	3513604657	3697278427
3708905341	3863326897	3867183937	4060942381	4079665633
4117447441	4275011401	4277526901		

С помощью этой таблицы можно осуществить уже не вероятностную, а точную проверку простоты чисел в пределах до 2^{32}.

2. Кратные множители

Несмотря на большое количество исследований, в этой области остается ещё много неисследованных вопросов. Один из них – кратные множители псевдопростых чисел.

Определение 2. Обозначим через ord(a,p) порядок a в мультипликативной группе $\boldsymbol{Z}_p^*$.

Следующее утверждение легко выводится из хорошо известных фактов теории чисел [1,2].

Теорема 1. Пусть p простое, a не делится на p и $b=\mathrm{ord}(a,p)$. Тогда $\mathrm{ord}(a,p^k)$ равно bp^s, $s=0,\ldots,k-1$.

Доказательство. Ядро естественного гомоморфизма мультипликативных групп

$$\varphi: \mathbb{Z}^*_{p^k} \to \mathbb{Z}^*_p$$

имеет порядок p^{k-1}. Отношение порядков $\mathrm{ord}(a,p^k)/\mathrm{ord}(a,p)$ равно порядку некоторой подгруппы в этом ядре, поэтому имеет вид p^s для некоторого s=0,… k–1.

Следующая теорема в немного другой форме доказана в [4].

Теорема 2. Пусть $n=p^kq$ псевдопростое по основанию a. Тогда $p^2, \ldots, p^k$ псевдопросты по основанию a.

Доказательство. Мы имеем: $a^{n-1} \equiv 1 \bmod p^kq$. Поэтому $\mathrm{ord}(a,n)$ является делителем $n-1$ и, следовательно, взаимно просто с n, а значит, и с p. Так как число $\mathrm{ord}(a,p^k)$ является делителем $\mathrm{ord}(a,n)$, то оно также будет взаимно просто с p. Поэтому из предыдущей теоремы следует, что $\mathrm{ord}(a,p^k)=\mathrm{ord}(a,p)$ делитель $p-1$ и $a^{p-1} \equiv 1 \bmod p^k$. Тогда $a^{pk-1} \equiv 1 \bmod p^k$, то есть $p^2, \ldots, p^k$ псевдопросты по основанию a.

Простые числа p, для которых $2^p \equiv 2 \bmod p^2$ играют важную роль и в других разделах теории чисел. Например, в книге [1], стр. 252, указано, что «В 1909 г. Виферих доказал, что первый случай теоремы Ферма справедлив для всех тех простых l, для которых $2^{l-1} \neq 1 \bmod l^2$. ... Среди простых чисел $l<6\cdot10^9$ только два числа: 1093 и 3511 удовлетворяют этому сравнению». Чуть дальше отмечается: «Числа 1093 и 3511 в двоичной системе счисления имеют запись

1092 = 0100 0100 0100, 3511 = 110 110 110 110.

В обоих случаях мы видим загадочную закономерность в расположении двоичных знаков. Не имеет ли связи этот феномен с тем, что простые числа l=1093 и l=3511 удовлетворяют сравнению $2^{l-1} \equiv 1 \bmod l^2$?».

Найдем все такие пары (a,p), что $a^{p-1} \equiv 1 \bmod p^2$ для a=2, … , 127 и $p<10^{10}$. Их оказалось 212:

a	**p**	**a**	**p**	**a**	**p**	**a**	**P**
2	1093	25	53471161	62	1291	93	81551
2	3511	25	1645333507	63	36713	94	241
3	11	25	6692367337	63	401771	94	32143
3	1006003	26	71	64	1093	94	463033
4	1093	26	486999673	64	3511	95	2137
4	3511	26	6695256707	65	163	95	15061
5	20771	27	1006003	66	89351671	96	109
5	40487	30	160541	67	268573	96	5437
5	53471161	31	79	68	113	96	8329
5	1645333507	31	6451	68	2741	96	12925267
5	6692367337	31	2806861	69	223	97	2914393
6	66161	32	1093	69	631	98	28627
6	534851	32	3511	69	2503037	98	61001527
6	3152573	33	233	70	142963	100	487
7	491531	33	47441	71	331	100	56598313
8	1093	33	9639595369	75	347	101	1050139
8	3511	35	1613	75	31247	102	7559
9	11	35	3571	76	1109	102	11813
9	1006003	36	66161	76	9241	102	139409857
10	487	36	534851	76	661049	103	24490789
10	56598313	36	3152573	77	32687	104	313
11	71	37	77867	78	151	104	237977
12	2693	38	127	78	181	105	7669
12	123653	39	8039	78	1163	106	79399
13	863	40	307	78	56149	106	672799
13	1747591	40	66431	78	4229335793	107	613181
14	29	41	1025273	79	263	108	3761
14	353	41	138200401	79	3037	108	10271
14	7596952219	43	103	79	1012573	108	1296018233
15	29131	44	229	79	60312841	109	20252173
16	1093	44	5851	80	6343	110	5381
16	3511	45	1283	81	1006003	110	9431
17	46021	45	131759	83	4871	111	131
17	48947	45	157635607	83	13691	112	1037888513

18	37	46	829	83	315746063	114	9181
18	331	48	257	84	163	115	2743780307
18	33923	49	491531	84	653	117	182111
18	1284043	52	461	84	20101	118	3152249
19	43	52	1228488439	85	11779	118	10404887
19	137	53	59	86	68239	119	1741
19	63061489	53	97	86	6232426549	120	653
20	281	54	1949	87	1999	120	2074031
20	46457	55	30109	87	48121	120	124148023
20	9377747	55	7278001	88	2535619637	122	2791
20	122959073	56	647	90	6590291053	123	34849
22	673	56	7079771	91	293	124	22511
22	1595813	57	47699	92	727	125	20771
22	492366587	57	86197	92	383951	125	40487
23	2481757	58	131	92	12026117	125	53471161
23	13703077	58	42250279	92	18768727	125	1645333507
24	25633	59	2777	92	1485161969	125	6692367337
25	20771	60	9566295763	93	509	127	907
25	40487	62	127	93	9221	127	13778951

С помощью дополнительных вычислений, можно проверить, что нет других пар вида $(2,p)$ при $p<758\cdot10^9$, вида $(3,p)$ при $p<681\cdot10^9$ и вида $(5,p)$ при $p<40\cdot10^9$.

Наименьшее число a, при котором не существует указанных пар (a,p) при $p<5\cdot10^9$ это 21. Конечно, вряд ли стоит ожидать, что таких пар нет ни для каких p, скорее всего, это лишь вопрос объема вычислений. Тем не менее, у нас нет и никаких оснований считать, что такие пары существуют для всех a.

С другой стороны, для каждого простого p существует достаточно много подходящих a, правда они равномерно расположены на отрезке $0... p^2$. Это показывает следующая теорема.

Теорема 3. Пусть p простое и a не делится на p. Тогда среди чисел

$$a,\ \ a+p,\ a+2p,\ \ ...,\ a+(p-1)p$$

ровно одно является псевдопростым по модулю p^2.

Доказательство. Рассмотрим многочлен $f(x)=x^p-x \bmod p^2$. Тогда

$$f(x+kp) \equiv f(x) - k\,p \bmod p^2 .$$

Так как $f(x)\equiv 0 \bmod p$, то $f(x) \equiv bp \bmod p^2$ для некоторого b. Поэтому $f(x+bp) \equiv 0 \bmod p^2$. Из этого же следует и единственность такого k.

Следствие 1. Для каждого простого p существует ровно $p-1$ число, псевдопростое по модулю p^2.

3. НОД чисел вида x^n-x

При нахождении пар (a,p), удовлетворяющих соотношению $a^{p-1} \equiv 1 \bmod p^2$ важную роль играет многочлен x^n-x. Согласно малой теореме Ферма, для всех x число x^n-x делится на n, то есть многочлен $(x^n-x)/n$ принимает только целые значения. На самом деле, значения многочлена x^n-x имеют и другие делители, общие для всех x.

Определение 3. Для натурального $n>1$ обозначим через $R(n)$ наибольший общий делитель чисел x^n-x при всех $x \in \mathbb{Z}$

При $n=2$, $x^2-x=x(x-1)$ и $R(2)=2$.

При $n=3$, $x^3-x=x(x-1)(x+1)$ и $R(3)=6$.

При $n=4$, $x^4-x=x(x-1)(x^2+x+1)$ и $R(4)=2$.

Несколько более детальные рассмотрения, показывают, что $R(5)=30$.

Очевидно, что $R(n)$ делится на k тогда и только тогда, когда

$$x^n-x \equiv 0 \bmod k .$$

Кроме того $R(n)$ четно для всех $n>1$.

Теорема 4. $R(n)$ не делится на p^2, где p простое, ни при каком n.

Другими словами, число $R(n)$ не имеет кратных простых множителей ни при каком n.

Доказательство. Так как $p^n-p \equiv p \bmod p^2$, то p^n-p не делится на p^2 и, следовательно, $R(n)$ тоже не делится на p^2.

Теорема 5. $R(n)$ делится на простое p тогда и только тогда, когда n–1 делится на p–1.

Доказательство. Пусть n–1 делится на p–1. Так как для всех ненулевых $a \in \mathbb{Z}_p$ выполнено $a^{p-1} \equiv 1 \bmod p$, то и $a^{n-1} \equiv 1 \bmod p$. Поэтому $x^n \equiv x \bmod p$. для всех $x \in \mathbb{Z}$, то есть $R(n)$ делится на p.

Обратно, пусть $x^n \equiv x \bmod p$. для всех $x \in \mathbb{Z}$. Возьмем a – первообразный корень по модулю p. Тогда $a^k \equiv 1 \bmod p$ тогда и только тогда, когда k делится на p–1. Следовательно, n–1 должно делиться на p–1.

Следствие 2. $R(2k) = 2$.

Доказательство. Если p нечетный простой делитель $R(2k)$, то $2k$–1 должно делиться на p–1, что невозможно.

Следствие 3. $R(n)$ является произведением всех простых p, таких, что n–1 делится на p–1.

Это следствие дает простой и эффективный способ вычисления $R(n)$.

Приведем теперь значения функции $R(n)$ для нечетных $n<100$.

Таблица 3

N	*R*(*n*)	*n*	*R*(*n*)	*n*	*R*(*n*)
3	6	37	6*5*7*13*19*37	71	6*11*71
5	6*5	39	6	73	6*5*7*13*19*37*73
7	6*7	41	6*5*11*41	75	6
9	6*5	43	6*7*43	77	6*5
11	6*11	45	6*5*23	79	6*7*79
13	6*5*7*13	47	6*47	81	6*5*11*17*41
15	6	49	6*5*7*13*17	83	6*83
17	6*5*17	51	6*11	85	6*5*7*13*29*43
19	6*7*19	53	6*5*53	87	6
21	6*5*11	55	6*7*19	89	6*5*23*89
23	6*23	57	6*5*29	91	6*7*11*19*31
25	6*5*7*13	59	6*59	93	6*5*47

27	6	61	6*5*7*11*13*31*61	95	6
29	6*5*29	63	6	97	6*5*7*13*17*97
31	6*7*11*31	65	6*5*17	99	6
33	6*5*17	67	6*7*23*67		
35	6	69	6*5		

Библиографический список

1. *Боревич З.И., Шафаревич И.Р.* Теория чисел. – М. Наука, 1985, 510 с.
2. *Хассе Г.* Лекции по теории чисел. – М. ИЛ, 1953, 520 с.
3. *Crandall R. E.,Pomerance C.* Prime Numbers: a computational perspective, 2nd ed. – Springer, New York, 2005, 597 p.
4. *Jameson G.J.O.* Carmichael numbers and pseudoprimes. – Lancaster Univ. UK, 2010, http://www.maths.lancs.ac.uk/~jameson/carpsp.pdf
5. *Lehmer D.H.* On Fermat's quotient, base two. Math. Comput., 1981, v.36, N153, p.289-290.
6. *Ribenboim P.* My numbers, my friends: popular lectures on number theory. 2nd ed – Springer, NY, 2000, 392 p, ISBN-10: 0387989110.
7. *Washington L.C.* On Fermat's last theorem. Proc. London Math. Soc. –1957. V.7, p.29-62.
8. Tables of pseudoprimes and related data http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html (2013-04-30)