Эффективное построение натуральных чисел с большим параметром Фробениуса

Хашин С.И.
Математический факультет Ивановского государственного университета
khash2@gmail.com

8 февраля 2017 г.

1 Символы Лежандра и Якоби

Определение. Пусть p – нечетное простое число. Целое число a называется *квадратичным вычетом по модулю* p, если сравнение $x^2 \equiv a \mod p$ имеет решение. В противном случае будем называть a *квадратичным невычетом по модулю* p.

Среди всех ненулевых вычетов по простому модулю квадратичные вычеты образуют подгруппу индекса 2.

Для простого числа p и целого a определим *символ Лежандра* $\left(\frac{a}{p}\right)$ следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \mod p \\ 1 & a \text{ — квадратичный вычет по молулю } p \\ -1 & a \text{ — квадратичный невычет по молулю } p \end{cases}$$

Свойства символа Лежандра

- Если $a_1 \equiv a \mod p$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.
- Если $(a,p) = 1$, то $\left(\frac{a}{n}\right) = a^{(p-1)/2} \mod p$.
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- Если $(a,p) = 1$, то $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.
- $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Теорема (квадратичный закон взаимности). Пусть p, q – нечетные простые числа. Тогда

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Распространим символ Лежандра на случай составного p. Полученную функцию будем называть *символом Якоби* и обозначать точно также. Пусть n нечетно и имеет следующее разложение на простые множители: $n = p_1^{k_1} \dots p_s^{k_s}$. Тогда для любого целого числа a *символом Якоби* $\left(\frac{a}{n}\right)$ назовем число

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \dots \left(\frac{a}{p_s}\right)^{k_s}.$$

Символ Якоби будем записывать также в виде $J(a/n)$.

Свойства символа Якоби

- Если $a_1 \equiv a \mod n$, то $\left(\frac{a}{n}\right) = \left(\frac{a_1}{n}\right)$.
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- Если $(a,p) = 1$, то $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.
- $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Теорема (обобщенные квадратичный закон взаимности). Пусть p, q – нечетные числа. Тогда

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Ещё раз:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \mod 4 \\ -1, & p \equiv 3 \mod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \mod 8 \\ -1, & p \equiv \pm 3 \mod 8 \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \mod 12 \\ -1, & p \equiv \pm 5 \mod 12 \end{cases} \quad (gcd(6,p) = 1)$$

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1, & p \equiv \pm 1 \mod 5 \\ -1, & p \equiv \pm 2 \mod 5 \end{cases}$$

$$\left(\frac{-7}{p}\right) = \begin{cases} 1, & p \equiv 1, 2, 4 \mod 7 \\ -1, & p \equiv 3, 5, 6 \mod 7 \end{cases}$$

2 Индекс Фробениуса

Определение 2.1. . Пусть n – нечетное натуральное число, не являющееся полным квадратом. Его индексом Фробениуса $Ind_F(n)$ будем называть наименьшее среди чисел $[-1, 2, 3, 4, 5, 6, \dots]$ такое, что символ Якоби $J(c/n) = -1$.

Однако, рассмотрим, например, число $105 = 3 \cdot 5 \cdot 7$.

c	2	3	4	5	6	7	8	9	10	11
$J(c/n)$	1	0	1	0	0	0	1	0	0	-1

То есть при таком определении индекса Фробениуса он окажется равным 11. Поэтому определение индекса лучше несколько изменить.

Определение 2.2. . Пусть n – нечетное натуральное число, не являющееся полным квадратом. Его индексом Фробениуса $Ind_F(n)$ будем называть наименьшее среди чисел $[-1, 2, 3, 4, 5, 6, \dots]$ такое, что символ Якоби $J(c/n) \neq 1$.

Тогда $Ind_F(105)$ будет равен 3.

Из мультипликативности символа Якоби следует, что если индекс $c = Ind_F(n)$ положителен, то он прост.

Приведем таблицу индекса Фробениуса $c = Ind_F(n)$ при малых n:

n	c	n	c	n	c	n	c	n	c	n	c	n	c	n	c	n	c	n	c
3	−1	43	−1	83	−1	123	−1	163	−1	203	−1	243	−1	283	−1	323	−1	363	−1
5	2	45	2	85	2	125	2	165	2	205	2	245	2	285	2	325	2	365	2
7	−1	47	−1	87	−1	127	−1	167	−1	207	−1	247	−1	287	−1	327	−1	367	−1
9	0	49	0	89	3	129	7	169	0	209	3	249	11	289	0	329	3	369	7
11	−1	51	−1	91	−1	131	−1	171	−1	211	−1	251	−1	291	−1	331	−1	371	−1
13	2	53	2	93	2	133	2	173	2	213	2	253	2	293	2	333	2	373	2
15	−1	55	−1	95	−1	135	−1	175	−1	215	−1	255	−1	295	−1	335	−1	375	−1
17	3	57	5	97	5	137	3	177	5	217	5	257	3	297	5	337	5	377	3
19	−1	59	−1	99	−1	139	−1	179	−1	219	−1	259	−1	299	−1	339	−1	379	−1
21	2	61	2	101	2	141	2	181	2	221	2	261	2	301	2	341	2	381	2
23	−1	63	−1	103	−1	143	−1	183	−1	223	−1	263	−1	303	−1	343	−1	383	−1
25	0	65	3	105	11	145	7	185	3	225	0	265	7	305	3	345	13	385	13
27	−1	67	−1	107	−1	147	−1	187	−1	227	−1	267	−1	307	−1	347	−1	387	−1
29	2	69	2	109	2	149	2	189	2	229	2	269	2	309	2	349	2	389	2
31	−1	71	−1	111	−1	151	−1	191	−1	231	−1	271	−1	311	−1	351	−1	391	−1
33	5	73	5	113	3	153	5	193	5	233	3	273	5	313	5	353	3	393	5
35	−1	75	−1	115	−1	155	−1	195	−1	235	−1	275	−1	315	−1	355	−1	395	−1
37	2	77	2	117	2	157	2	197	2	237	2	277	2	317	2	357	2	397	2
39	−1	79	−1	119	−1	159	−1	199	−1	239	−1	279	−1	319	−1	359	−1	399	−1
41	3	81	0	121	0	161	3	201	7	241	7	281	3	321	7	361	0	401	3

Нетрудно выяснить, когда индекс Фробениуса принимает маленькие значения:

Если $n \equiv 3 \mod 4$, то $c = -1$.

Если $n \equiv 5 \mod 8$, то $c = 2$.

Будем считать, что n не делится на 3. Тогда если $n \equiv 17 \mod 24$, то $c = 3$. Если же $n \equiv 1 \mod 24$, то $c \geq 5$.

Будем считать, что n не делится и на 5. Тогда если $n \equiv 73$ или $97 \mod 120$, то $c = 5$. Если же $n \equiv 1$ или $49 \mod 120$, то $c \geq 7$.

2.1 Большие значения индекса

При каких n получаются наибольшие значение c?

n	c	n	c	n	c	n	c
3	−1	8 089	17	1 083 289	41	48 473 881	67
5	2	18 001	19	3 206 641	43	175 244 281	71
17	3	53 881	23	3 818 929	47	872 479 969	73
73	5	87 481	29	9 257 329	53	427 733 329	79
1009	11	117 049	31	22 000 801	59	898 716 289	83
2641	13	515 761	37	56 588 401	61	2805 544 681	101

До 10^{10} числа можно проверить простым перебором. Для больших значений применим более сложный алгоритм.

Выше было отмечено, что $c \geq 5$ будет лишь для $n \equiv 1 \mod 24$.

Предложение 2.3. *Пусть* $c \geq 5$ *и* $x \equiv 1 \mod 4$. *Тогда*

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

Доказательство.

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

□

Пусть N_1, N_2 – произведения нескольких различных простых чисел ≥ 5, например, $N_1 = 5 \cdot 7$, $N_2 = 11 \cdot 17$. Обозначим через X множество вычетов x по модулю N_1 таких, что

$$\left(\frac{c}{24N_2x+1}\right) = 1$$

для всех простых делителей c числа N_1 и через Y множество вычетов y по модулю N_2 таких, что

$$\left(\frac{c}{24N_1y+1}\right) = 1$$

для всех простых делителей c числа N_2. Из доказанного выше предложения следует, что

$$\left(\frac{c}{24N_2x+24N_1y+1}\right) = 1$$

для всех простых делителей c числа $N_1 \cdot N_2$.

Таким образом, возьмем $N_1 = 5 \cdot 11 \cdot 17 \cdot 23 \cdot 31 \cdot 41 \cdot 47 = 1284644185$, $M_1 = 6\,072\,000$, $N_2 = 7 \cdot 13 \cdot 19 \cdot 29 \cdot 37 \cdot 43 = 79774331$, $M_2 = 857\,304$. Тогда

$$7N_{12} < 2^{64} < 8N_{12},$$

где $N_{12} = 4N_1N_2$. Рассмотрим ещё множество $Z = \{0, N_{12}, \ldots, 7N_{12}\}$. Тогда любое число $n < 2^{64}$, для которого

$$J(-1/n) = J(2/n) = \cdots = J(47/n) = 1$$

может быть представлено в виде виде $n = 1 + x_i + y_j + z_k$, где $x_i \in X,\ y_j \in Y,\ z_k \in Z$. При этом $J(p/n)$ при остальных $p = 53, ...$ зависят только от $n \mod p$ и могут быть найдены по таблице.

2.2 Результаты расчетов

Результаты расчетов лежат в текстовом файле

`F:/a/primes/maxFrIindex/maxFrIindex.rar/maxFrIindex.txt`

размером 10 689 292 732 байт. В нём записаны, по одному в строке, в порядке возрастания 458 069 912 чисел с индексом больше 128. Другими словами, это числа, не являющиеся полными квадратами такие, что

$$J(-1/n) = J(2/n) = J(3/n) = \cdots = J(127/n) = +1.$$

Все они не являются псевдопростыми по Фробениусу.

Для чисел, меньших 2^{64} наибольший индекс Фробениуса имеют числа

$$13371308337168834529 = 15671 * 42509111 * 20072209,$$

и

$$10198100582046287689 = 277 * 1091 * 1151 * 29318344777.$$

Их индекс Фробениуса равен 277.

Приведем полный список чисел, меньших 2^{64} с индексом Фробениуса ≥ 241:

n	Разложение	$Ind_F(n)$
10 198 100 582 046 287 689	$277 * 1091 * 1151 * 29318344777$	277
13 371 308 337 168 834 529	$42509111 * 20072209 * 15671$	277
14 556 961 869 213 641 641	$294859 * 49369230273499$	269
8 019 204 661 305 419 761	$85049496359 * 15329 * 6151$	263
9 525 254 728 650 901 321	$269356523164067 * 35363$	257
6 384 991 873 059 836 689	$56634160359229 * 112741$	257
15 559 176 909 429 792 409	15559176909429792409	257
15 841 063 060 186 483 729	15841063060186483729	257
2 327 687 064 124 474 441	$479 * 4859471950155479$	251
4 874 863 023 350 911 369	$3292229887 * 1480717687$	251
7 709 526 364 683 482 161	$2513702759922883 * 3067$	251
8 296 704 369 880 085 329	$224719730759 * 36920231$	251
9 064 125 655 411 231 729	9064125655411231729	251
10 918 467 669 293 400 241	$569 * 360603871 * 53213159$	251
12 144 088 165 752 308 089	$1034549 * 283176937 * 41453$	251
15 092 828 713 838 767 369	$487 * 87168671 * 9221 * 38557$	251
15 161 588 123 783 204 041	15161588123783204041	251
15 615 860 448 589 902 601	$269 * 449 * 20918629 * 6180649$	251
1 773 855 791 877 850 321	$4977618781 * 356366341$	241
4 850 624 987 082 642 769	$599 * 1163 * 4045854797 * 1721$	241
5 799 375 985 159 604 761	$166923876599 * 34742639$	241
6 938 117 179 828 687 609	6938117179828687609	241
10 096 447 955 180 345 641	10096447955180345641	241
10 565 328 852 664 066 849	10565328852664066849	241
10 806 857 647 730 657 041	$108327479152481 * 99761$	241
11 142 142 214 574 728 569	$281 * 39651751653290849$	241
11 257 547 117 859 426 409	$941 * 971 * 12320686866919$	241
11 417 898 363 696 440 641	$1823071748953607 * 6263$	241
11 631 303 398 465 948 521	$540462961687001 * 21521$	241
12 139 477 918 848 888 721	12139477918848888721	241
12 198 313 032 091 127 881	$528089480431 * 23098951$	241
12 780 228 604 848 907 801	$251 * 50917245437645051$	241
13 152 535 378 957 253 449	$1358873373174631 * 9679$	241
13 194 818 078 923 010 209	$1607359980378001 * 8209$	241
13 270 764 547 337 857 921	$463 * 1216294843 * 23565469$	241
13 962 703 804 646 805 289	$313 * 641 * 647 * 564407 * 190577$	241
14 062 107 862 023 021 529	$1470583982389 * 9562261$	241
14 076 396 959 102 325 961	14076396959102325961	241
14 579 447 188 898 695 321	14579447188898695321	241
15 500 304 528 660 177 769	$773 * 20052140399301653$	241
15 563 774 009 731 253 329	$5238710509 * 4597 * 646273$	241
16 051 125 467 279 775 889	$41255129 * 11128681 * 34961$	241
16 539 844 297 164 123 961	$821 * 3421242053 * 5888497$	241
17 730 965 717 070 847 609	17730965717070847609	241
17 895 360 545 240 844 241	17895360545240844241	241
18 160 759 655 635 441 441	$728788153 * 6188011 * 4027$	241
18 229 083 490 490 001 529	18229083490490001529	241

Количество чисел, меньших 2^{64} с данным индексом Фробениуса таково:

Ind_F	Количество
277	2
271	0
269	1
263	1
257	4
251	10
241	29
239	61
233	136
229	306
227	704
223	1 569
211	3 353
199	7 578
197	16 382
193	35 460
191	76 144
181	160 500
179	340 954
173	717 462
167	1 502 782
163	3 133 342
157	6 507 483
151	13 454 113
149	27 707 022
139	56 908 219
137	116 444 144
131	237 733 823