Доклады Академии наук СССР
1970. Том 190, № 4

УДК 511

МАТЕМАТИКА

В. В. КОБЕЛЕВ

ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА ДЛЯ ВСЕХ ПРОСТЫХ ПОКАЗАТЕЛЕЙ, МЕНЬШИХ 5500

(*Представлено академиком С. А. Лебедевым 23 VI 1969*)

Куммер ([1]) показал, что великая теорема Ферма (в.т.ф.) справедлива для регулярных простых показателей. В работе Вандайвера ([2]) указан критерий, дающий возможность решать вопрос о справедливости в.т.ф. для иррегулярных простых показателей. По критерию Вандайвера ([2]) в.т.ф. справедлива для заданного иррегулярного простого L, если для всех $Q(a)$

$$Q^k \not\equiv 1 \pmod{p}, \tag{1}$$

где p — любое простое число, меньшее $L^2 - L$ и имеющее вид $1 + kL$,

$$Q = t^{-kd/2} \prod_{j=1}^{\mu} (t^{kj} - 1)^{j^{L-1-2a}}, \tag{2}$$

t — любое целое вида $t^k \not\equiv 1 \pmod{p}$, $\mu = (L - 1)/2$,

$$d = \sum_{j=1}^{\mu} j^{L-2a} \tag{3}$$

и $a < \mu$ — индексы чисел Бернулли, числители которых делятся на L. Если хотя бы для одного a и всех допустимых p и t окажется $Q^k \equiv 1 \pmod{p}$, вопрос о справедливости в.т.ф. для данного L остается открытым.

Вандайвер с сотрудниками ([2–4]) провел проверку выражения (1) на вычислительной машине SWAC со средним быстродействием порядка 16 000 операций в секунду ([5]). Оказалось, что для всех иррегулярных простых чисел, меньших 4002, неравенство (1) выполняется и таким образом справедливость в.т.ф. была доказана для всех нечетных простых чисел $L < 4002$, причем обследование простых чисел в диапазоне от 2500 до 4000 потребовало около 100 час. машинного времени SWAC.

Появление за последние годы более мощных ЦВМ дает возможность проверить справедливость в.т.ф. для большего диапазона показателей за приемлемое время. Так, использование машины БЭСМ-6, выполняющей порядка миллиона операций в секунду ([6]), дало возможность проверить результаты работ ([2–4]) и просмотреть простые числа в диапазоне от 4000 до 5500. Отметим, что просмотр простых чисел в диапазоне от 2500 до 4000 занял всего 31 мин. машинного времени БЭСМ-6.

Проверка результатов работ ([2–4]) выявила в них ряд ошибок. Простые числа 1381, 1597 и 1877 оказались иррегулярными, а степень иррегулярности простого 1663 оказалась равной 2. Таблица иррегулярности простых чисел с указанными ошибками вошла в монографию Боревича и Шафаревича ([7]).

В табл. 1 представлены результаты расчетов на БЭСМ-6. Первые 6 строк этой таблицы выполняют пробелы и ошибки работ ([2, 4]). Регулярные простые числа в табл. 1 не показаны.

Таблица 1

Значения критерия Вандайвера для нерегулярных простых чисел, лежащих в диапазоне от 4002 до 5500

L	$2a$	P	Q^k	L	$2a$	P	Q^k
1381	266	8287	2394	4679	3592	56149	25781
1597	842	6389	1205	4691	3450	37529	24438
1663	1508	6653	2716	4751	3768	95021	30710
1877	1026	15017	3206	4783	252	57397	2027
1933	1320	23197	14917	4793	2636	9587	8063
3631	1104	21787	20749	4813	2620	28879	624
4003	82	24019	23992	4861	4678	29167	9302
4003	142	24019	16308	4889	2924	39113	25494
4003	2610	24019	10633	4903	3106	49031	39929
4021	3228	72379	5044	4909	1462	58909	34697
4027	2332	64433	25116	4943	492	9887	5903
4049	1854	48589	1483	4951	1914	89119	33462
4051	3548	64817	41935	4951	2468	89119	84817
4073	3620	8147	7606	4951	3890	89119	32766
4129	1784	49549	45692	4957	3812	89227	82207
4157	658	24943	20522	4969	1940	59629	47162
4157	2322	24943	17600	4973	4208	69623	68567
4219	4190	168761	148911	5009	1544	90163	30233
4243	2712	101833	68954	5009	4956	90163	36328
4243	4146	101833	65236	5039	594	10079	6342
4259	3580	51109	15188	5077	3092	81233	63245
4259	3726	51109	32808	5081	3016	10163	3634
4261	2068	42611	3207	5099	1378	71387	3659
4339	214	43391	27893	5101	190	112223	69975
4349	2052	8699	2831	5107	4872	30643	21428
4409	636	8819	6641	5119	4086	20477	2624
4409	672	8819	7802	5167	4112	186013	183270
4421	3768	79579	79571	5179	4732	20717	17493
4451	2896	89021	72070	5189	1102	41513	25863
4451	2978	89021	23918	5209	644	93763	4884
4457	444	115883	7480	5209	2928	93763	62346
4493	746	26959	14240	5227	308	397253	183108
4519	848	18077	11229	5231	3466	10463	6828
4523	456	54277	22261	5297	4810	74159	31338
4561	436	27367	1165	5303	4156	10607	3452
4591	2292	128549	85920	5309	158	42473	17346
4591	3596	128549	52979	5351	1948	107021	13365
4637	3618	27823	711	5399	1482	10799	2825
4639	3226	102059	16169	5413	1702	32479	12564
4657	1578	27943	12715	5441	4726	10883	8527
4657	2416	27943	20324	5443	1710	21773	3102
4657	4110	27943	16953	5477	1150	76679	47543
4663	216	74609	56255	5479	1826	120539	19454
4663	4278	74609	30345	5479	4802	120539	59005

Поскольку, как видно из табл. 1, $Q^k \not\equiv 1 \pmod{p}$ для всех рассмотренных иррегулярных L, в.т.ф. справедлива для всех нечетных простых показателей, меньших 5500. Во всех случаях для доказательства оказалось достаточным использовать $t = 2$ и минимальное p.

Институт точной механики и вычислительной техники
Академии наук СССР
Москва

Поступило
16 VI 1969

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] E. E. Kummer, J. reine u. angew. Math., 40, № 2, 130 (1850). [2] D. H. Lehmer, E. Lehmer, H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A., 40, № 1, 25 (1954). [3] H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A., 40, № 8, 732 (1954). [4] J. L. Selfridge, C. A. Nicol, H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A., 41, № 11, 970 (1955). [5] H. D. Huskey, R. Thorensen, B. F. Ambrosio, E. C. Yowell, Proc. IRE, 41, № 10, 1294 (1953). [6] БЭСМ-6, основные технические данные, 1964. [7] З. И. Боревич, И. Р. Шафаревич, Теория чисел, М., 1964.