PROOF OF FERMAT' S GREAT THEOREM FOR ALL PRIME EXPONENTS LESS THAN 5500

1970

SovietRxiv

Abstract

Full Text

UDC 511

MATHEMATICS

V. V. KOBELEV

PROOF OF FERMAT' S GREAT THEOREM FOR ALL PRIME EXPONENTS LESS THAN 5500

(Presented by Academician S. A. Lebedev on 23 VI 1969)

Kummer ([1]) showed that Fermat' s great theorem (FGT) is true for regular prime exponents. In Vandiver' s work ([2]) a criterion is indicated that makes it possible to decide the question of the validity of FGT for irregular prime exponents. According to Vandiver' s criterion ([2]), FGT is true for a given irregular prime L, if for all $Q(a)$

$$Q^k \not\equiv 1(\mathrm{mod}p), \tag{1}$$

where p is any prime number less than $L^2 - L$ and of the form $1 + kL$,

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

t is any integer such that $t^k \not\equiv 1(\mathrm{mod}p)$, $\mu = (L-1)/2$,

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

and $a < \mu$ are the indices of Bernoulli numbers whose numerators are divisible by L. If, for at least one a and all admissible p and t, it turns out that $Q^k \equiv 1(\mathrm{mod}p)$, the question of the validity of FGT for the given L remains open.

Vandiver and collaborators ([2-4]) checked expression (1) on the SWAC computer with an average speed of about 16,000 operations per second ([5]). It turned out that for all irregular primes less than 4002, inequality (1) holds, and thus the validity of FGT was proved for all odd prime numbers $L < 4002$; moreover, the examination of primes in the range from 2500 to 4000 required about 100 hours of SWAC machine time.

The appearance in recent years of more powerful digital computers makes it possible to check the validity of FGT for a larger range of exponents in an acceptable time. Thus, the use of the BESM-6 computer, performing about one million operations per second ([6]), made it possible to verify the results of works ([2-4]) and to examine primes in the range from 4000 to 5500. We note that examining the primes in the range from 2500 to 4000 took only 31 minutes of BESM-6 machine time.

Checking the results of works ([2-4]) revealed a number of errors in them. The prime numbers 1381, 1597, and 1877 turned out to be irregular, and the degree of irregularity of the prime 1663 turned out to be equal to 2. The table of irregularity of primes with the indicated errors was included in the monograph by Borevich and Shafarevich ([7]).

Table 1 presents the results of computations on BESM-6. The first 6 rows of this table fill the gaps and errors of works ([2], [4]). Regular prime numbers are not shown in Table 1.

Table 1

Values of Vandiver' s criterion for irregular prime numbers lying in the range from 4002 to 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

L	$2a$	P	Q^k	L	$2a$	P	Q^k
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	4584
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

Since, as is evident from Table 1, $Q^k \not\equiv 1 \pmod{p}$ for all the irregular L considered, Fermat' s Last Theorem is valid for all odd prime exponents less than 5500. In all cases, for the proof it proved sufficient to use $t = 2$ and the minimal p.

Institute of Precision Mechanics and Computer Engineering
Academy of Sciences of the USSR
Moscow

Received
16 VI 1969

CITED LITERATURE

1. E. E. Kummer, *J. reine u. angew. Math.*, **40**, No. 2, 130 (1850).

2. D. H. Lehmer, E. Lehmer, H. S. Vandiver, *Proc. Nat. Acad. Sci. U.S.A.*, **40**, No. 1, 25 (1954).

3. H. S. Vandiver, *Proc. Nat. Acad. Sci. U.S.A.*, **40**, No. 8, 732 (1954).

4. J. L. Selfridge, C. A. Nicol, H. S. Vandiver, *Proc. Nat. Acad. Sci. U.S.A.*, **41**, No. 11, 970 (1955).

5. H. D. Huskey, R. Thoresen, B. F. Ambrosio, E. C. Yowell, *Proc. IRE*, **41**, No. 10, 1294 (1953).

6. BESM-6, *Basic Technical Data*, 1964.

7. Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Moscow, 1964.

Note: Figure translations are in progress. See original paper for figures.