only contraction operators and this is also the case considered by Yosida in his first paper. The extension to transition operators occurs in his second paper.

[5] Hille, *loc. cit.*, p. 232, formula (11.7.2).

[6] See the references in footnotes 1 and 2. In the former, consult pages 391–394.

[7] The construction here indicated is an application of a general method used by the author in, for instance, "Sur le problème abstrait de Cauchy," *Compt. rend. Acad. Sci., Paris*, **236**, 1466–1467 (1953). Since all the functions $x_{mn}(\lambda)$ are completely monotone for $\lambda > 0$, the functions $z_{mn}(t)$ will be non-negative, and $Z(t)$ is a positive nul solution. The existence of positive nul solutions for related systems has been proved by W. Feller, *loc. cit.*, using other methods.

AN APPLICATION OF HIGH-SPEED COMPUTING TO FERMAT'S LAST THEOREM

BY D. H. LEHMER, EMMA LEHMER, AND H. S. VANDIVER

UNIVERSITY OF CALIFORNIA AT BERKELEY AND UNIVERSITY OF TEXAS

Communicated November 9, 1953

Introduction.—The statement of Fermat (known as Fermat's Last Theorem), which dates from 1672, that

$$x^n + y^n = z^n, \qquad n > 2, \tag{1}$$

has no non-zero solutions in integers still awaits a proof or disproof. It is known that for a proof it is sufficient to consider the case of $n = l$, an odd prime.

With the assumption that xyz is not divisible by l (known as case (1)), very stringent criteria on (1) have been devised and it was shown by D. H. and Emma Lehmer[1] in 1941 that (1) is impossible for each $l \leqq 253{,}747{,}899$ in this case.

Without the restriction to case (1) the problem appears to be much more difficult and requires the consideration of each prime l individually. In this connection Kummer defined a prime l to be *regular* in case it does not divide any of the first $(l-3)/2$ Bernoulli numbers

$$B_1 = {}^1/_6, \qquad B_2 = {}^1/_{30}, \ldots$$

and gave a proof in 1850 that (1) is impossible for regular primes (Theorem I). Kummer in 1857, and 1874 also, found the eight *irregular* primes less than 164 and devised criteria which he applied to all such primes excepting 101, 103, 131, and 149. This, using his result on regular primes also, enabled him to prove Fermat's Last Theorem for all primes $l < 164$ with the exceptions just mentioned, and the additional exception $l = 157$ when his criteria failed.

During the years 1928–1936 a number of collaborators at the University of Texas under the direction of H. S. Vandiver examined the primes <619 and developed criteria (Theorem II) which proved Fermat's Last Theorem for the 36 primes which were found to be irregular <619 including $l = 157$. At this point the calculations became prohibitively long and laborious for desk calculator work.

It is the object of this paper to show how this program has been carried out for all primes less than 2000 in a few hours using the high-speed calculating machine of the National Bureau of Standards known as the SWAC at the Institute for Numerical Analysis in Los Angeles, as coded by D. H. and Emma Lehmer. As before,

the calculations were in two parts: the determination of irregular primes, and the application of criteria to prove Fermat's Last Theorem for these primes. The first revealed the interesting fact that nearly half the primes <2000 are irregular. For the second part it was necessary to modify the criterion used by Vandiver to make it applicable for high-speed calculation. Some details of this will be discussed in what follows together with the presentation of the results in tabular form. *Besides proving Fermat's Last Theorem for all $l < 2000$, these results have applications to the theory of cyclotomic fields* which will be discussed by Vandiver in another paper.

Determination of the Regular and Irregular Primes < 2000.—The first of Kummer's results (1850) already referred to is specifically as follows:[2]

THEOREM I. *If l is a given regular prime, then*

$$x^l + y^l + z^l = 0 \tag{2}$$

is impossible for rational integers x, y, and z, none zero.

Kummer's[3] second criterion (1857) is not employed in this paper. However, all the criteria for (1) which have been obtained since and which are not subject to the restriction of case (I) have stemmed from it.

Consider the cyclotomic algebraic field, designated by K, or $K(\zeta)$, where ζ is a primitive lth root of unity with l as before an odd prime. Let $k_i = \zeta^{ri/2} - \zeta^{-ri/2}$ and $e_i = k_{i+1}/k_i$ with r a primitive root of l. Set

$$E_n(\zeta) = E_n = \prod_{i=0}^{(l-3)/2} e_i^{r^{-2in}}. \tag{3}$$

With these definitions we may state the second criterion which we shall use as follows:

THEOREM II. *Under the following assumption: none of the units E_a (defined in (3)) with $a = a_1, a_2, \ldots, a_s$ (see (4)) is congruent to an lth power of an integer in $K(\zeta)$ modulo $\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal divisor of (p), with p a rational prime $<l^2 - l$ of the form $1 + kl$; (2) is impossible in non-zero rational integers.*

In testing the criteria of Theorems I and II, it is first necessary to determine if l is regular, and if it is not, to determine all the s distinct $a_1, a_2, \ldots, a_s$ in the set $1, 2, 3, \ldots, (l-3)/2$ such that

$$B_{a_1}, B_{a_2}, \ldots, B_{a_s} \tag{4}$$

are each divisible by l.

In order to obtain this information we must examine the first $(l-3)/2$ Bernoulli numbers B_n (modulo l). This is best done by using one of the many congruences expressing Bernoulli numbers modulo l as sums of like powers. Such a formula, which involves the least number of terms, is the following[5]

$$S_a = \sum_{l/6 < s < l/4} s^{2a-1} \equiv (-1)^a(2^{l-2a} - 1)(3^{l-2a} - 2^{l-2a} - 1)B_a/4a, \quad (l > 7, 2a < l-1). \tag{5}$$

The only drawback of this formula is that for some a's the factor

$$f_a = (2^{l-2a} - 1)(3^{l-2a} - 2^{l-2a} - 1)$$

is itself divisible by l, thus leaving the divisibility of B_a in doubt in these cases.

However, if $S_a \not\equiv 0 \pmod{l}$ for all a, then l is regular. The SWAC was programmed to calculate S_a (modulo l) for all $a = 1, 2, \ldots, (l-3)/2$ in succession and to punch out on cards the values of l and a for which $S_a \equiv 0 \pmod{l}$. The SWAC was also instructed to accumulate the sum

$$S = \sum_{a=1}^{\mu} S_a \pmod{l}, \qquad \mu = (l-1)/2,$$

and to test whether $S \equiv 0 \pmod{l}$, as it should be, before proceeding to the next prime l. If S failed to be congruent to zero, the SWAC was instructed to stop; such a contingency did not arise, however, and the operation was completely automatic. The output of this run, consisting of cards with values of l and a punched on them, was then fed back into the machine and the machine was asked to examine the factor f_a (modulo l). If this factor was not divisible by l, then the SWAC was instructed to punch out another card with the values of l and a together with a code word indicating that the prime l was *irregular with index a*. If $f_a \equiv 0 \pmod{l}$, however, the machine was instructed to try another congruence,[5] namely

$$S'_a = \sum_{l/6 < s < l/5} s^{2a-1} + \sum_{l/3 < s < 2l/5} s^{2a-1} \equiv (-1)^a f'_a B_a/4a, \qquad (l > 5, 2a < l-1) \quad (6)$$

containing $[l/10]$ terms; provided the factor

$$f'_a = 6^{l-2a} - 5^{l-2a} - 2^{l-2a} + 1$$

was not divisible by l. Then if S'_a turned out not to be divisible by l, neither was B_a and this particular output of run (I) was merely a false alarm due to the divisibility of f_a by l and was to be disregarded. On the other hand, if $S'_a \equiv 0 \pmod{l}$, then l is irregular with index a and this was recorded on an output card as before. However, if the factor f'_a was divisible by l as well as f_a, then uncertainty prevailed and it was necessary to resort to a much longer formula of $[l/2]$ terms which, however, gives unequivocal results in all cases, namely[5]

$$S''_a = \sum_{r=1}^{\mu} (l-2r)^{2a} \equiv (-1)^{a-1} 2^{2a-1} l B_a \pmod{l^3}. \qquad (7)$$

Although this formula holds modulo l^3, it was sufficient to carry out the calculations modulo l^2. In each case it was tested as a check that $S''_a \equiv 0 \pmod{l}$ and a card was punched every time $S''_a \equiv 0 \pmod{l^2}$.

The output of run (II) was then a set of cards giving all the irregular primes with their indices of irregularity a_i. These will be found in the first two columns of our table. We shall call the number of indices of irregularity for a given l the *degree of irregularity* of l. The largest degree so far found is three.

For $l < 619$, these results were checked against those found by Vandiver and his collaborators.[6] They were found to agree except that $l = 389$ and $l = 613$ were found to be irregular instead of regular, and the value of $2a = 338$ (or $a = 119$) for $l = 491$, given in the table of the present paper, had not been previously found. Further tests showed the SWAC figures to be correct.

As to the frequency of irregular primes, there are 184 regular and 118 irregular primes less than 2000. The following distribution table may be of interest. We

divide the interval up to 2000 into eight equal parts and let $250k < l < 250(k+1)$, $k = 0, 1, \ldots, 7$.

	$k=0$	1	2	3	4	5	6	7	TOTAL
No. of irregular primes	9	19	20	16	11	14	11	18	118
No. of primes	52	42	37	36	36	35	33	31	302
Percentages, irregular primes	17	45	54	44	31	40	33	58	39

Jensen[7] proved that there exist an infinity of irregular primes of the form $4n + 3$. There is nothing in the table to indicate that there is only a finite number of regular primes. It is well to note this situation, as a number of theorems in the theory of regular cyclotomic fields have been given which do not appear to extend to irregular fields.

If we consider only divisors of the numerators of Bernoulli numbers (in their lowest terms) which are prime to their indices, then a regular prime divides the numerator of no Bernoulli number. An irregular prime divides the numerators of an infinity of Bernoulli numbers.

Treatment of the Irregular Primes.—For this purpose we employ the criterion given in Theorem II. To use this on the SWAC it was necessary to replace the quantity E_a by another simpler quantity in K. For this we need the

LEMMA. *Let t be any integer such that $t^k \not\equiv 1 \pmod{p}$ where p is a prime of the form $p = kl + 1 < l^2 - l$. Define Q_a by*

$$Q_a = t^{-kd/2} \prod_{b=1}^{\mu} (t^{kb}-1)^{b^{l-1-2a}}, \tag{8}$$

where $\mu = (l-1)/2$ and

$$d = 1^{l-2a} + 2^{l-2a} + \ldots + \mu^{l-2a}.$$

Then the unit E_a is congruent to the lth power of an integer in $K(\zeta)$ modulo a prime ideal dividing (p), if, and only if,

$$Q_a^k \equiv 1 \pmod{p}. \tag{9}$$

For proof let

$$R(q) = \zeta^q - \zeta^{-q}; \qquad A = \prod_{i=1}^{\mu} R(r^i)^{r^{-2a(i-1)}}; \qquad B = \prod_{j=0}^{\mu-1} R(r^j)^{r^{-2aj}}. \tag{10}$$

Then

$$E_a(\zeta^2) = A/B. \tag{11}$$

We first note that

$$B^{r^{2a}-1} = E_a(\zeta^2)\rho_1^l. \tag{12}$$

For, we have

$$A^{r^{-2a}} = B\rho_2^l.$$

This follows if we note that $R(r^\mu) = -R(r^0)$ since r is a primitive root of l and $r^\mu \equiv -1 \pmod{l}$, with $(-1) = (-1)^l$. From this we obtain $B^{r^{2a}-1} = (A/B)\rho_2^l$ and with (11) we get (12), where ρ_1 and ρ_2 are numbers in K, whose denominator, if any, can

be put in the form $(\zeta - 1)^h$, with h a positive rational integer. The same statement will hold for $\rho_3, \rho_4, \ldots, \rho_{18}$ in what follows.

Now also, in a similar way,

$$R(r^k) = -R(r^{k+\mu})$$

if $k = 0, 1, \ldots, \mu - 1$ and

$$R(r^k)^{r-2ak} = R(r^{k+\mu})^{r-2ak}\rho_3^l.$$

Now

$$r^{-2ak} \equiv r^{-2a(\mu+k)} \pmod{l},$$

since $r^{2\mu} \equiv 1 \pmod{l}$, and hence

$$R(r^k)^{r-2ak} = R(r^{k+\mu})^{r-2a(k+\mu)}\rho_4^l.$$

Whence,

$$B^2 = \prod_{h=0}^{l-2} R(r^h)^{r-2ah}\rho_5^l,$$

and since, modulo l; $1, r, r^2, \ldots, r^{l-2}$ are congruent to the integers $1, 2, \ldots, l-1$ in some order

$$B^2 = \prod_{n=1}^{l-1} R(n)^{n-2a}\rho_6^l. \tag{13}$$

We have

$$R(b) = -R(l-b), \qquad R(b)^{b-2a} = R(l-b)^{(l-b)-2a}\rho_7^l;$$

whence, when we replace $(-2a)$ by $(l-1-2a)$ which only changes ρ_7,

$$\prod_{b=1}^{\mu} R(b)^{bl-1-2a} = \prod_{b=1}^{\mu} R(l-b)^{(l-b)l-1-2a}\rho_8^l.$$

Then, since

$$(l-b)^{l-1-2a} \equiv b^{l-1-2a} \pmod{l},$$

(13) gives

$$B^2 = \prod_{b=1}^{\mu} R(b)^{2bl-1-2a}\rho_9^l.$$

Select c so that $2c \equiv 1 \pmod{l}$, then $B^{2c} = B\rho_{10}^l$, and similarly on the right so that

$$B = \prod_{b=1}^{\mu} R(b)^{bl-1-2a}\rho_{11}^l. \tag{14}$$

Now using (12) and raising it to the mth power with $m(r^{2a}-1) \equiv 1 \pmod{l}$, noting that $(l, r^{2a}-1) = 1$, we have from (14)

$$\prod_{b=1}^{\mu} R(b)^{bl-1-2a} = E_a(\zeta^2)^m\rho_{12}^l, \tag{15}$$

or

$$\zeta^{-d} \prod_{b=1}^{\mu} (\zeta^{2b}-1)^{bl-1-2a} = E_a(\zeta^2)^m \rho_{12}^l. \tag{16}$$

Setting $\zeta^{(l+1)/2}$ for ζ in (16) then gives

$$\zeta^{-d/2} \prod_{b=1}^{\mu} (\zeta^{b}-1)^{bl-1-2a} = E_a(\zeta)^m \rho_{13}^l. \tag{17}$$

We easily see, using the methods similar to those employed in obtaining (12) and (13), that

$$E_a(\zeta^r) = (E_a(\zeta))^{r2a} \rho_{14}^l, \tag{18}$$

where r as before is a primitive root of l. Set $r^v \equiv n \pmod{l}$ for any n such that $(n, l) = 1$. Then repeated application of (18) gives

$$E_a(\zeta^{r^v}) = E_a(\zeta)^{r2av} \rho_{15}^l$$

and

$$E_a(\zeta^n) = E_a(\zeta)^{n2a} \rho_{16}^l. \tag{19}$$

Then (17) gives

$$\zeta^{-nd/2} \prod_{b=1}^{\mu} (\zeta^{bn}-1)^{bl-1-2a} = E_a(\zeta)^{n2am} \rho_{17}^l. \tag{20}$$

If g is a primitive root of p, then consider the ideal

$$(g^k - \zeta, p) = \mathfrak{p} \tag{21}$$

which divides (p), where $p = 1 + kl$. Let t be a rational integer such that $t^k \not\equiv 1 \pmod{p}$. Set $t \equiv g^n \bmod p$, then $n \not\equiv 0 \pmod{l}$; otherwise, $t^k \equiv 1 \pmod{p}$ when we note that $t^{p-1} \equiv 1 \pmod{p}$. Then $t^k \equiv g^{nk} \pmod{p}$; and using (21) $g^k \equiv \zeta \pmod{\mathfrak{p}}$ gives

$$t^k \equiv \zeta^n \pmod{\mathfrak{p}}. \tag{22}$$

Now from (20) we obtain, using (22),

$$t^{-kd/2} \prod_{b=1}^{\mu} (t^{kb}-1)^{bl-1-2a} \equiv E_a(\zeta)^{n2am} \rho_{18}^l \pmod{\mathfrak{p}} \tag{23}$$

noting that the denominator of ρ_{17}, if any, may be put in the form $(1 - \zeta)^h$, prime to $\mathfrak{p}$. Hence, setting Q_a for the left-hand member, we find

$$Q_a^k \equiv E_a(\zeta)^{n2amk} \pmod{\mathfrak{p}}.$$

Noting that $(n^{2a}m, l) = 1$, we see that $E_a(\zeta)$ is congruent to an lth power in K, modulo $\mathfrak{p}$ if, and only if,

$$Q_a^k \equiv 1 \pmod{p}.$$

This proves the lemma.[8]

Then we may state the

THEOREM III. *Let Q_a be defined as in the lemma and let*

$$B_{a_1}, B_{a_2}, \ldots, B_{a_s} \tag{24}$$

be the only Bernoulli numbers, with indices less than $(l-1)/2$, *which are divisible by* l. *Then if*

$$Q_{a_i}^k \not\equiv 1 \pmod{p}$$

holds for $i = 1, 2, \ldots, s$, *Fermat's Last Theorem holds for the exponent* l.

The above criterion was coded on the SWAC, which was instructed to calculate for each card giving an irregular prime l and its index a, first of all, the least prime p of the form $kl + 1$; it was then programmed to find out whether $2^k \equiv 1 \pmod{p}$ and was prepared to ask the same question about $3^k, \ldots$, etc. if this were the case. However, in all cases tested $2^k \not\equiv 1 \pmod{p}$, so that 2 was used for t in the expression for Q in all cases. After these preliminary calculations, the SWAC proceeded to calculate d. This was done modulo l, then $2^{-kd/2}$ was calculated modulo p and was multiplied by the successive factors in the product; after each multiplication a reduction modulo p was performed by the SWAC. Finally the value of Q_a (modulo p) thus obtained was raised to the kth power (mod p) and compared with unity. Considering the complicated form of the expression for Q_a above, it was rather gratifying to be able to code this whole calculation into the high-speed memory of the SWAC and to be able to perform the test in less than three minutes for our largest prime tested. In all cases the test held for the smallest p tried and the values of p were much smaller than permitted in the Theorem. However, if for some l, p should exceed $l^2 - l$ one can have recourse to a Theorem recently proved by Inkeri[9] to the effect that p can be $< {}^3/_2\,(l^2-l)$ in the statement of Theorems II and III.

Below is a table giving the values of l, $2a$, p, Q_a *and* Q_a^k *for all irregular* l's < 2000. l *is the odd prime exponent in the Fermat relation,* $p = 1 + kl$, Q_a *is the left-hand member of* (23), *and* $2a$ *is twice the index of the Bernoulli numbers defined in* (24) (*that is, for example, if* $l = 647$, *the table gives us the information that the set* (24) *for this value of* l *consists of* B_{118}, B_{121}, *and* B_{277}). *If a prime* <2000 *does not appear in the column for* l, *this indicates that* l *is a regular prime.*

l	$2a$	p	Q_a	Q_a^k	l	$2a$	p	Q_a	Q_a^k
37	32	149	146	81	353	186	4943	1508	3144
59	44	709	137	645	353	300	4943	1088	3660
67	58	269	73	180	379	100	4549	111	4062
101	68	607	514	47	379	174	4549	784	1992
103	24	619	273	389	389	200	9337	1937	8328
131	22	263	91	128	401	382	3209	656	719
149	130	1193	420	178	409	126	1637	609	1506
157	62	1571	1293	102	421	240	4211	3155	2825
157	110	1571	170	1261	433	366	1733	772	496
233	84	467	276	55	461	196	2767	1756	1023
257	164	1543	1371	1258	463	130	5557	1850	5212
263	100	1579	1154	1385	467	94	2803	1742	1536
271	84	1627	951	367	467	194	2803	2051	655
283	20	1699	1388	383	491	292	983	289	949
293	156	587	88	113	491	336	983	213	151
307	88	1229	266	151	491	338	983	17	289
311	292	1867	523	360	523	400	5231	3924	3532
347	280	2083	1561	1711	541	86	9739	5189	7221

	$2a$	p	Q_a	Q_a^k
547	270	5471	1797	3692
547	486	5471	4814	1597
557	222	3343	49	204
577	52	2309	447	1285
587	90	8219	4046	7886
587	92	8219	1960	126
593	22	1187	916	1034
607	592	3643	2811	815
613	522	6131	3872	513
617	20	4937	498	3740
617	174	4937	2952	832
617	338	4937	3569	3592
619	428	2477	1553	794
631	80	6311	1275	2592
631	226	6311	2939	1278
647	236	9059	8095	8931
647	242	9059	3009	7667
647	554	9059	5918	6916
653	48	1307	838	385
659	224	1319	42	445
673	408	2693	2442	2170
673	502	2693	1740	1879
677	628	5417	811	372
683	32	1367	1332	1225
691	12	6911	5642	73
691	200	6911	3360	4497
727	378	2909	1627	812
751	290	4507	3689	1519
757	514	12113	5256	6303
761	260	1523	455	1420
773	732	4639	1332	3942
797	220	4783	1389	2097
809	330	1619	582	353
809	628	1619	1502	737
811	544	8111	3823	6231
821	744	6569	2809	1240
827	102	11579	3683	5688
839	66	10069	4287	4868
877	868	14033	9707	11792
881	162	15859	10672	9493
887	418	5323	3952	4987
929	520	7433	2849	6592
929	820	7433	5250	7415
953	156	1907	1736	636
971	166	5827	1579	1835
1061	474	6367	1932	4808
1091	888	6547	3844	2117
1117	794	6703	2639	60
1129	348	4517	2385	4122
1151	534	6907	4263	3614
1151	784	6907	5747	5121

l	$2a$	p	Q_a	Q_a^k
1151	968	6907	1825	5286
1153	802	25367	18794	18498
1193	262	7159	4936	325
1201	676	7207	5578	114
1217	784	29209	16956	1782
1217	866	29209	3569	21587
1217	1118	29209	6021	13160
1229	784	2459	1408	510
1237	874	19793	5866	18934
1279	518	12791	2027	5662
1283	510	7699	259	6117
1291	206	12911	9593	7683
1291	824	12911	443	85
1297	202	5189	2520	4344
1297	220	5189	1535	4324
1301	176	26021	21535	18702
1307	382	10457	5164	4993
1307	852	10457	1770	9922
1319	304	23743	9120	3063
1327	466	5309	585	3740
1367	234	10937	9041	9634
1409	358	2819	2022	934
1429	996	5717	4436	4539
1439	574	2879	2529	1582
1483	224	14831	14248	2174
1499	94	2999	2747	525
1523	1310	21323	6867	10522
1559	862	3119	337	1285
1609	1356	16091	12146	1078
1613	172	9679	8955	4873
1619	560	12953	3483	9010
1621	980	29179	15527	12268
1637	718	62207	3233	53518
1663	270	6653	520	2691
1669	388	16691	12078	1513
1669	1086	16691	8744	8989
1721	30	34421	12804	14618
1733	810	3467	1656	3406
1733	942	3467	2234	1743
1753	712	7013	1117	4910
1759	1520	31663	13295	29437
1777	1192	7109	5718	6072
1787	1606	10723	3556	7206
1789	848	17891	9604	11296
1789	1442	17891	12106	14937
1811	550	3623	3618	25
1811	698	3623	539	681
1811	1520	3623	2898	290
1831	1274	10987	1860	2735
1847	954	11083	3187	3360
1847	1016	11083	5462	1029

l	$2a$	p	Q_a	Q_a^k	l	$2a$	p	Q_a	Q_a^k
1847	1558	11083	1076	1262	1951	1656	42923	19738	13365
1871	1794	14969	8842	6002	1979	148	39581	19694	17972
1879	1260	7517	6650	121	1987	510	7949	7552	3677
1889	242	3779	1574	2231	1993	912	11959	8736	5546
1901	1722	3803	100	2394	1997	772	87869	72402	32194
1933	1058	23197	14251	7103	1997	1888	87869	87154	396
1933	1320	23197	11957	5213					

Irrespective of whether Fermat's Last Theorem is ever proved or disproved, the contents of the table given above constitute a permanent addition to our knowledge of cyclotomic fields, as its use will greatly simplify and facilitate the study of the units and ideals in such a field defined for any $l < 2000$.

[1] *Bull. Am. Math. Soc.*, **47**, 139–142 (1941).

[2] *Jr. für Math.*, **40**, 93–138 (1850); *Jr. Math.*, **16**, 454–498 (1851). An outline of the proof of this Theorem is given in the *Am. Math. Monthly*, **53**, 569–571 (1946). This last paper will be referred to as F.

[3] *Abhandl. Akad. Wiss., Berlin*, 41–74 (1857, 1858). See F, pp. 571–574 (1946). In F there are misprints in two places in the statement of (3). In the relation (17a), p. 568, the summation sign on the right should be a multiplication sign; and the quantity r^{-2in} should be an exponent of $e(\zeta^{r^i})$. Also, in the right-hand member of the equation at the top of p. 572, the addition sign should be a multiplication sign.

[4] *Trans. Am. Math. Soc.*, **31**, 631, 638 (1929). The proof for case (I) was given in *Bull. Am. Math. Soc.*, **40**, 118 (1934). Cf. F, pp. 574–575.

[5] The formula (5) was obtained by Mirimanoff, *Jr. für Math.*, **128**, 45–68 (1905), for the special case where $l - 1$ is divisible by 12, and by Elizabeth T. Stafford and H. S. Vandiver for l general, these PROCEEDINGS, **16**, 143 (1930), relation (9). The relation (6) was proved by Vandiver, *Duke Math. Jr.*, **3**, 570–574 (1937), relation (18). Formula (7) is due to Emma Lehmer, *Ann. Math.*, **39**, 354 (1938), relation (19). In (6) if there is no integral s satisfying the condition given in a summation, then we define the summation as zero.

[6] *Duke Math. Jr.*, **3** (4), 569–584 (1937); *Ibid.*, **5**, 418–427 (1939) and previous references there given.

[7] *Nyt Tidsskrift für Matematik* (Afdeling B), p. 82 (1915) (in Danish). An outline of his proof is given in the "Report on the Theory of Algebraic Numbers, II," *Natl. Research Council Bull. No.* **62**, p. 82 (1928).

[8] If the so-called second factor of the class number of $K(\zeta)$ (cf. F, pp. 567–568) is divisible by l, then at least one of the E_{a_i}, $i = 1, 2, \ldots, s$ is the lth power of a unit in $K(\zeta)$. Cf. *Bull. Am. Math. Soc.*, **35**, 333–335 (1929). The procedure in the proof of our lemma yields various forms of this criterion which appear to be of value for theoretical purposes.

[9] *Ann. Acad. Sci. Fennicae, Series A, Helsinki, I, Mathematica-Physica*, **60**, 18 (1949). Inkeri's theorem referred to here includes another extension of Theorem II aside from the one mentioned.

GEODESIC FLOWS AND UNITARY REPRESENTATIONS

BY F. I. MAUTNER

DEPARTMENT OF MATHEMATICS, THE JOHNS HOPKINS UNIVERSITY

Communicated by Marston Morse, November 9, 1953

Let S be a complete surface of constant negative curvature. It is well known and readily verified that the geodesic flow on S can be described as follows. Let G be the group of all real 2×2 matrices of determinant 1 and Γ the fundamental group of