1. H. LAMB, "On the propagation of tremors over the surface of an elastic solid," Roy. Soc. London, *Phil. Trans.*, ser. A, v. 203, 1904.
2. C. L. PEKERIS, "The seismic surface pulse," Nat. Acad. Sci., *Proc.*, v. 41, 1955, p. 469–480.
3. NBS Applied Mathematics Series, 37, *Tables of Functions and of Zeros of Functions*, U. S. Gov. Printing Office, Washington, D. C., 1954. [*MTAC*, v. 10, 1956, Rev. **104**, p. 249–250.]
4. P. DAVIS & P. RABINOWITZ, "Abscissas and weights for Gaussian quadratures of high order," National Bureau of Standards, *Jn. of Research*, v. 56, 1956, p. 35–37. [*MTAC*, v. 11, 1957, Rev. **84**.]

Mersenne Numbers

By Hans Riesel

During 1957 the author of this note had the opportunity of running the Swedish electronic digital computer BESK in order to examine Mersenne numbers. The intention of the author's investigation on the BESK was to check some known results, and to examine some Mersenne numbers not previously examined.

Mersenne numbers are numbers $M_p = 2^p - 1$, where p is a prime. See [1], which contains a more complete list of references. The Mersenne numbers have attained interest in connection with digital computers because there is a simple test to decide whether they are prime or composite. This is Lucas's test [1]. Furthermore the number $2^{p-1}M_p$ is a perfect number, if M_p is a prime, and all known perfect numbers are of this form.

In the beginning of 1957 a program for testing the primeness of the Mersenne numbers on the BESK was worked out by the author. This program, using Lucas's test, works for all $p < 10000$. As a test, this program was run for the following values of p: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, and 2281. The result was that the numbers M_p are prime for these values of p, thus confirming known results.

After these tests, values of $p > 2300$ were to be tested. These values had not been tested before. But since the testing of M_p for one value of p of this order takes several hours on the BESK, a special program for calculating the smallest factor of M_p, if this factor is $< 10 \cdot 2^{20} = 104\ 85760$, was worked out. This special program is based on the following well-known theorem:

All prime factors q of M_p $(p > 2)$ are of the form $q = 2kp + 1$, and of one of the two forms $q = 8l \pm 1$.

The proof of the theorem is quite simple. If q is a factor of M_p, $2^p \equiv 1 \pmod q$. Since p is a prime, since all numbers n for which $2^n = 1 \pmod q$ form a module, and since $2^p \equiv 1 \pmod q$, this module consists of all integral multiples of the prime p. Now $2^{q-1} \equiv 1 \pmod q$ if q is a prime, and hence $q - 1$ is a multiple of p, and in fact an even multiple (since q must be an odd number). This is the first part of the theorem: $q - 1 = 2kp$ $(k = 1, 2, 3, \cdots)$. The second part follows immediately from the theory of quadratic residues. Since $x^2 \equiv 2 \pmod q$ has the solution $x \equiv 2^{(p+1)/2} \pmod q$, we see that 2 is a quadratic residue mod q, hence $q \equiv \pm 1 \pmod 8$.

By the above mentioned special program for small factors of M_p the values of $M_p \pmod q$ for all primes q of the theorem were now calculated. When this residue was $\equiv 0$, the factor q was printed out. When no factor $q < 10 \cdot 2^{20}$ was found, the BESK turned to the next value of p. This program was run for all

Received 8 November 1957.

values of $p < 10000$. The running time on the BESK for one value of p lay between 0 and 2 minutes, depending on the size of the smallest factor. These smallest factors are given below in a table. The known Mersenne primes are also included in the table. Finally, Cole's factor of M_{67}, and Robinson's factors of M_{109} and M_{157}, though greater than $10 \cdot 2^{20}$, have been printed in the table. On checking the values against other sources, a misprint in Archibald's note [2] was detected. This misprint, which concerns the value of the smallest factor of M_{163}, seems to have come from Kraitchik [3], p. 24 and p. 92. As a further check, all factors in our table have been looked up in Lehmer's Prime Tables, except a few, which are too large, and a separate calculation was made, to check that they are of the form $2kp + 1$. Since, however, there are disturbances in digital computers, it is not absolutely sure that all these numbers really are factors of the corresponding Mersenne numbers M_p. Those primes p, for which no factor $< 10 \cdot 2^{20}$ of M_p was found, are, except the known Mersenne primes, omitted in the table.

When this table had been calculated, the BESK examined the omitted values of p with Lucas's test. This was done for all values of p between 2300 and 3300. Since the available running time for testing Mersenne numbers on the BESK was limited, every value of p was tested only once. The final remainder, see [1], was printed out in hexadecimal form. On September 8th, 1957, a run indicated that the number M_{3217} is prime. This result was repeated on September 12th. All other numbers tested turned out to be composite; however, this result could be false, since the running time is very long. The testing of M_{3217} took about $5^h\ 30^m$ on the BESK, for one run.

A table of the smallest factor of $2^p - 1$, p prime follows. Primes $2^p - 1$ are indicated by a dash.

Ormangsgatan 67C
Stockholm-Vallingby, Sweden

1. R. M. Robinson, "Mersenne and Fermat numbers," Amer. Math. Soc., *Proc.*, v. 5, p. 842–846.
2. R. C. Archibald, "Mersenne's numbers," *Scripta Mathematica*, v. 3, 1935, p. 112–119.
3. M. Kraitchik, *Recherches sur la Theorie des Nombres*, Gauthier-Villars, Paris, 1952.

Table of Factors of $2^p - 1$: $\frac{p}{\text{factor}}$

2	3	5	7	11	13
—	—	—	—	23	—
17	19	23	29	31	37
—	—	47	233	—	223
41	43	47	53	59	61
13367	431	2351	6361	1 79951	—
67	71	73	79	83	89
1937 07721	2 28479	439	2687	167	—
97	107	109	113	127	131
11447	—	7459 88807	3391	—	263
151	157	163	167	173	179
18121	8521 33201	1 50287	23 49023	7 30753	359

Table of Factors of $2^p - 1$: $\frac{p}{\text{factor}}$—*Continued*

181	191	197	211	223	229
43441	383	7487	15193	18287	15 04073
233	239	251	263	277	281
1399	479	503	23671	11 21297	80929
283	311	317	337	353	359
9623	53 44847	9511	18199	9 31921	719
367	383	397	419	431	443
12479	14 40847	2383	839	863	887
449	461	463	487	491	499
12 56303	2767	11113	4871	983	20959
521	547	557	571	577	587
—	5471	3343	5711	3463	5 54129
593	601	607	617	619	641
1 04369	3607	—	59233	1 10183	35897
643	659	683	701	719	743
31 89281	1319	1367	7 96337	1439	1487
757	761	773	811	827	829
98 15263	4567	68 64241	3 26023	66161	72953
839	857	859	863	877	881
26849	6857	72 15601	82 58911	35081	26431
883	907	911	929	937	941
8831	11 70031	1823	13007	28111	7529
953	967	977	1009	1013	1019
3 43081	23209	8 67577	34 54817	6079	2039
1021	1031	1033	1039	1049	1051
40841	2063	1 96271	50 80711	33569	35 75503
1091	1093	1097	1103	1117	1129
87281	43721	9 80719	2207	53617	33871
1153	1181	1187	1193	1201	1213
2 67497	47 42897	2 56393	1 21687	57649	3 27511
1223	1229	1231	1249	1279	1303
2447	36871	5 31793	97423	—	104 44849
1321	1327	1361	1367	1381	1423
7927	27 30967	8167	10937	8287	16 99063
1433	1439	1447	1451	1453	1459
20063	2879	57881	2903	8719	14591
1481	1489	1499	1511	1523	1531
71089	71473	2999	3023	25 22089	88799
1543	1559	1583	1607	1609	1663
1 01839	3119	3167	28927	23 94193	16631
1667	1693	1697	1709	1721	1723
13337	10159	12 35417	3 79399	1 75543	17231

Table of Factors of $2^p - 1$: $\frac{p}{\text{factor}}$—*Continued*

1741	1777	1789	1801	1811	1823
10 02817	10663	39359	28817	3623	1 20319
1847	1861	1871	1877	1879	1913
33247	10 23551	14969	15017	6 05039	63 01423
1931	1973	1987	1993	1997	1999
3863	1 22327	67559	11959	3 95407	18 07097
2003	2011	2017	2039	2063	2069
4007	21 71881	93 38711	4079	4127	3 26903
2081	2083	2111	2113	2131	2141
2 66369	72 69671	3 41983	22 31329	32 73217	3 89663
2179	2203	2207	2213	2251	2281
2 48407	—	1 23593	53113	4 00679	—
2297	2333	2339	2351	2389	2393
57 65471	3 12623	4679	4703	71671	33503
2399	2411	2417	2447	2459	2531
4799	19289	14503	81 63193	4919	7 89673
2539	2543	2549	2591	2593	2609
25391	5087	43 63889	7 66937	15559	36527
2617	2621	2657	2663	2677	2687
78511	15727	37199	63913	3 64073	1 98839
2689	2699	2707	2711	2741	2753
71 58199	5399	1 73249	5 85577	82231	47 95727
2767	2819	2837	2843	2857	2897
6 25343	5639	22697	1 42151	36 79817	17383
2903	2909	2939	2953	2963	2999
5807	1 10543	5879	88591	5927	6 71777
3001	3011	3023	3037	3041	3119
32 17073	20 23393	6047	18223	24329	24953
3121	3137	3163	3181	3217	3221
11 23561	20 01407	4 55473	19087	—	6 44201
3257	3299	3319	3323	3329	3347
97711	6599	33191	23 12809	26633	26777
3359	3361	3391	3433	3457	3491
6719	5 57927	2 98409	44 42303	20743	6983
3499	3511	3517	3527	3529	3533
35 82977	35111	5 62721	63487	1 05871	1 90783
3539	3541	3557	3571	3581	3593
7079	7 64857	4 26841	64279	21487	21559
3623	3659	3701	3719	3733	3767
7247	41 05399	1 11031	43 51231	13 14017	30137
3779	3793	3797	3803	3823	3851
7559	60689	91129	7607	89 68759	7703

Table of Factors of $2^p - 1 : \frac{p}{\text{factor}}$—*Continued*

3853	3863	3907	3911	3917	3923
33 90641	7727	5 31353	7823	4 07369	2 19689
3931	3967	3989	4001	4013	4019
26 18047	63473	1 91473	24007	1 20391	8039
4057	4073	4099	4127	4129	4153
97369	56 69617	73783	74287	15 85537	91367
4211	4217	4229	4243	4271	4273
8423	21 84407	3 29863	1 01833	8543	25639
4289	4297	4373	4391	4441	4447
34313	8 93777	61223	8783	26647	71153
4457	4483	4513	4517	4549	4561
16 31263	58 54799	1 35391	27103	1 36471	72977
4597	4603	4639	4649	4657	4691
27583	6 26009	1 94839	5 95073	11 45623	5 72303
4723	4759	4787	4793	4801	4813
29 09369	1 14217	1 14889	67103	28807	28879
4861	4871	4903	4919	4933	4943
29167	9743	49031	9839	29599	9887
4957	4967	4993	4999	5003	5011
1 48711	3 27823	79889	2 09959	10007	80177
5021	5039	5051	5087	5101	5107
40169	10079	10103	40697	81 10591	51071
5167	5171	5179	5189	5197	5227
65 31089	10343	2 48593	1 55671	31183	11 29033
5231	5233	5237	5261	5279	5297
10463	9 94271	40 22017	42089	10559	44 49481
5303	5347	5393	5399	5413	5417
10607	3 10127	32359	10799	53 26393	4 33361
5431	5437	5441	5449	5483	5501
54311	20 87809	36 56353	25 17439	8 88247	6 93127
5519	5521	5531	5557	5563	5623
6 62281	88337	9 40271	33343	5 34049	11 35847
5639	5683	5711	5717	5743	5779
11279	8 75183	11423	34303	5 43217	9 24641
5791	5801	5807	5843	5849	5861
9 26561	34807	1 39369	7 12847	41 05999	46889
5903	5939	6011	6029	6067	6101
11807	6 17657	2 88529	84407	2 06279	79 06897
6113	6131	6143	6163	6173	6197
25 30783	12263	8 84593	5 91649	37039	2 97457
6199	6203	6263	6277	6287	6311
61991	1 48873	12527	37663	50 29601	36 47759

Table of Factors of $2^p - 1$: $\frac{p}{\text{factor}}$*—Continued*

6317	6323	6343	6353	6367	6373
6 94871	12647	90 45119	38119	63671	38239
6389	6397	6421	6449	6473	6481
1 91671	19 44689	56 89007	51593	27 96337	6 22177
6491	6521	6529	6551	6553	6563
12983	48 90751	7 31249	13103	14 54767	13127
6569	6607	6637	6673	6691	6703
66 21553	80 34113	52 03409	67 66423	3 21169	4 42399
6719	6737	6781	6803	6841	6871
12 90049	7 41071	1 08497	2 17697	41047	2 88583
6883	6899	6917	6947	6949	6959
18 85943	13799	55337	1 80623	68 79511	55673
6967	6977	6983	6997	7039	7043
10 72919	41863	13967	21 69071	12 52943	14087
7057	7079	7103	7129	7151	7193
6 21017	14159	14207	18 67799	14303	54 09137
7207	7211	7297	7411	7417	7459
1 72969	14423	18 68033	10 22719	1 18673	1 34263
7487	7529	7537	7561	7573	7589
1 79689	1 05407	7 23553	5 89759	45439	2 88383
7591	7639	7643	7673	7681	7687
18 97751	5 50009	15287	1 84153	39 94121	4 45847
7691	7741	7759	7789	7823	7841
15383	89 64079	1 39663	8 72369	15647	23 67983
7853	7873	7883	7901	7919	8011
47119	11 80951	15767	47407	63353	80111
8017	8059	8101	8111	8161	8167
1 28273	70 43567	7 12889	16223	67 08343	31 36129
8171	8179	8219	8221	8231	8237
8 00759	43 18513	19 88999	9 20753	2 14007	10 54337
8243	8269	8273	8293	8317	8353
16487	7 27673	10 42399	1 99033	3 82583	50119
8377	8387	8419	8423	8429	8431
50263	92 76023	4 88303	3 53767	67433	8 09377
8461	8467	8501	8513	8597	8599
14 04527	2 03209	6 80081	2 72417	4 81433	85991
8629	8663	8669	8693	8699	8713
2 58871	17327	26 18039	2 60791	4 17553	16 03193
8719	8731	8737	8741	8761	8783
28 77271	25 14529	6 81487	69929	1 92743	2 28359
8803	8807	8821	8839	8867	8929
28 34567	2 28983	4 05767	65 23183	70937	1 96439
8951	8963	9001	9007	9029	9059
17903	6 63263	15 12169	90071	7 22321	18119

Table of Factors of $2^p - 1$: $\dfrac{p}{\text{factor}}$*—Continued*

9109	9127	9137	9157	9173	9181
49 55297	1 46033	10 05071	30 76753	4 95343	13 77151
9221	9283	9311	9323	9337	9341
7 19239	59 41121	14 15273	8 95009	26 14361	74729
9343	9371	9391	9397	9403	9419
1 49489	18743	93911	2 25529	25 76423	18839
9421	9431	9461	9479	9491	9497
85 73111	6 79033	75689	18959	5 31497	5 31833
9511	9521	9539	9601	9613	9619
95111	3 61799	19079	22 85039	57679	6 15617
9791	9811	9829	9833	9851	9859
19583	77 70313	7 07689	45 62513	78809	11 04209
9883	9949	9973			
1 58129	80 98487	2 99191			

A Computation of Some Bi-Quadratic Class Numbers

By Harvey Cohn

A fascinating chapter in computational number theory began when Lagrange showed that every positive integer is representable as the sum of at most *four* perfect squares [1]. Clearly three would not suffice in every case, as $7 = 2^2 + 1^2 + 1^2 + 1^2$ would be an exception; nevertheless, the problem of expressing some positive integer n as the sum of at most *three* squares soon achieved a very special role. For, Gauss showed that $r(n)$, the number of such representations, is connected in a very simple way with the much studied (intrinsically positive) class number, h, of the field generated by $\sqrt{-n}$. Specifically for n square-free (and $n \neq 1, 3$ where $h = 1$),

$$r(n) = gh \tag{1}$$

where $g = 12$ for $n \equiv 1, 2, 5, 6$ and $g = 24$ for $n \equiv 3 \pmod 8$. Thus we could conclude the existence of at least one such representation for the indicated n. Gauss and later, Kronecker, reversed the direction of these equations by making large scale tabulations of h from $r(n)$, although, unfortunately, no location for Kronecker's alleged tabulation (for odd n up to 10,000) seems to exist in the literature. In tallying the representation $n = x_1^2 + x_2^2 + x_3^2$ it might be noted that one must count each ordered triple (x_1, x_2, x_3) of positive, negative, or zero integers as a separate unit, so that as much as $2^3 \cdot 3! = 48$ could be contributed to $r(n)$ when such a decomposition into squares is expressed as triples.

In more recent times, the representation theory was extended to integers in the field k generated by $\sqrt{5}$, i.e., to the quantities $\mu = (a + b\sqrt{5})/2$ where a and b are of the same parity. Here we seek to represent, necessarily, only those integers μ which are positive together with their conjugate (i.e., totally positive). Thus, e.g., $a > |b\sqrt{5}| \geq 0$. The special surd $\sqrt{5}$ must be used because then, as Götzky

Received 8 January 1958.