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

showed [2], each totally positive integer in k could be expressed as the sum of the squares of at most *four* integers in k. Later, Maass [3] made the more remarkable discovery that at most *three* squares would *always* suffice; in fact he arrived at a formula analogous to that of Gauss. Since Maass' formula is the basis of a machine calculation, we avoid irrelevant complexities by making certain further assumptions. First of all μ is to be free from square integral divisors in k except for powers of $(\sqrt{5}+3)/2 = [(\sqrt{5}+1)/2]^2 = \epsilon$. Secondly $a \geq 5b \geq 0$, since if $5b > a > \sqrt{5}b$, we can continually replace μ by μ/ϵ. Then $R(\mu)$, the number of representations of μ as the sum of three squares, is linked to an intrinsically positive quantity H, namely the class number of the bi-quadratic field generated by $\sqrt{5}$ and $\sqrt{-\mu}$, by means of the following formula (which excludes $\mu = 1$, $(5+\sqrt{5})/2$, and 3 where $H = 1$):

$$H = R(\mu)/G. \tag{2}$$

Here $G = 12$ when $(a, b) \not\equiv (1, 3)$, $(1, 5)$, $(2, 4)$, $(5, 1)$, $(5, 7)$, or $(6, 0) \bmod 8$ (actually, when $\eta^2 + \mu \equiv 0 \bmod 4$ is unsolvable for η in k). Otherwise, $G = 120$ except when $(a, b) \equiv (1, 5)$, $(1, 11)$, $(5, 7)$, $(5, 9)$, $(6, 0)$, $(9, 3)$, $(9, 13)$, $(13, 1)$, $(13, 15)$, or $(14, 0) \bmod 16$ (actually, when $\eta^2 + \mu \equiv 0 \bmod 8$ is solvable for η in k); in these cases, $G = 96$.

A tabulation of R and H for 446 selected values of $\mu = [a, b] = (a + b\sqrt{5})/2$ was made on the stored program electronic computer, the IBM 650. The values of a, b were selected with the restrictions

$$100 > a \geq 5b \geq 0,$$

and that μ have (except trivially for powers of ϵ) no square divisors in k; or, in terms of ordinary integral arithmetic, the condition is that d, the g.c.d. of $(\frac{1}{2}[a+b], \frac{1}{2}[a-b])$, be relatively prime to $5(=(\sqrt{5})^2)$, and both d and $(a^2 - 5b^2)/4d^2$ be square free. The machine assembled 446 such couples automatically into the highest four decimal positions of 446 individual ten digit storage locations, in lexicographic order.

The machine next tallied the decompositions $\mu = \xi_1^2 + \xi_2^2 + \xi_3^2$ where $\xi_i = [a_i, b_i]$, $a_i \equiv b_i \bmod 2$. Here the three couples ξ_i were scanned in lexicographic order, with the restriction $0 \leq b_i \leq 7$, while $a_i \geq 0$ and $a' < 100$, (see below). Thus, taking all sign possibilities, with

$$\begin{cases} a' = [a_1^2 + a_2^2 + a_3^2 + 5(b_1^2 + b_2^2 + b_3^2)]/2, \\ b' = \pm a_1b_1 \pm a_2b_2 \pm a_3b_3, \end{cases}$$

the couples a', b' were constructed and compared with the 446 cases stored in the memory. Whenever a matching entry was located the count was augmented and accumulated in the last six decimal positions of the memory word. It might be appropriate to mention that the IBM 650 has a special "table look-up" operation that searches the memory at high speed for the appropriate entry. Without such an instruction the search would have had to be programmed with a considerable loss of running time.

In the final phase the "words" a, b, $R(\mu)$ were unpacked and the congruences were examined automatically to calculate H and to produce the output consisting of one IBM card per value of μ. (See attached table).

Tabulation of R and H for $\mu = (a + b\sqrt{5})/2$

a	b	R	H	a	b	R	H	a	b	R	H	a	b	R	H
2	0	6	1	33	3	240	2	47	9	144	12	59	1	144	12
4	0	12	1	33	5	288	3	48	2	216	18	59	3	168	14
5	1	24	1	34	0	96	8	48	4	168	14	59	5	96	8
6	0	32	1	34	2	96	8	48	6	144	12	59	7	96	8
7	1	24	2	34	4	120	1	49	1	144	12	59	9	144	12
9	1	24	2	34	6	72	6	49	3	240	2	59	11	144	12
10	2	24	2	35	1	96	8	49	5	288	3	60	2	144	12
11	1	24	2	35	3	144	12	49	7	96	8	60	6	192	16
12	0	48	4	35	7	48	4	49	9	120	10	60	8	192	16
12	2	48	4	36	2	96	8	50	2	144	12	61	1	288	3
13	1	96	1	36	6	96	8	50	6	144	12	61	3	144	12
14	0	96	1	37	1	240	2	50	8	96	8	61	5	144	12
14	2	24	2	37	3	168	14	51	1	144	12	61	7	240	2
15	1	48	4	37	5	96	8	51	3	96	8	61	9	360	3
15	3	48	4	37	7	288	3	51	5	168	14	61	11	96	8
16	2	24	2	38	0	384	4	51	7	144	12	62	0	576	6
17	1	48	4	38	2	96	8	51	9	96	8	62	2	240	20
17	3	120	1	38	4	96	8	52	0	144	12	62	4	216	18
18	2	72	6	38	6	144	12	52	2	144	12	62	6	264	22
19	1	48	4	39	1	72	6	52	6	192	16	62	8	480	5
19	3	48	4	39	3	96	8	52	8	120	10	62	10	192	16
20	2	48	4	39	5	72	6	52	10	192	16	62	12	240	20
21	1	120	1	39	7	96	8	53	1	360	3	63	1	288	24
21	3	48	4	40	2	96	8	53	3	168	14	63	3	192	16
22	0	192	2	40	4	96	8	53	5	144	12	63	7	240	20
22	2	72	6	40	6	144	12	53	7	480	5	64	2	120	10
22	4	72	6	41	1	72	6	53	9	480	5	64	4	168	14
23	1	72	6	41	3	288	3	54	2	120	10	64	6	144	12
24	2	72	6	41	5	120	1	54	4	168	14	64	10	96	8
24	4	48	4	41	7	96	8	54	6	96	8	64	12	168	14
25	1	48	4	42	0	192	16	54	8	384	4	65	1	144	12
25	3	192	2	42	2	168	14	54	10	144	12	65	3	480	4
26	0	96	8	42	4	360	3	55	1	144	12	65	7	192	16
26	2	48	4	42	6	144	12	55	3	192	16	65	9	144	12
26	4	120	1	43	1	120	10	55	7	144	12	65	11	384	4
27	1	120	10	43	3	192	16	55	9	144	12	65	13	240	2
27	3	96	8	43	5	144	12	55	11	96	8	66	0	192	16
27	5	96	8	43	7	144	12	56	2	144	12	66	2	144	12
28	0	96	8	44	0	144	12	56	4	96	8	66	4	360	3
28	2	96	8	44	2	96	8	56	6	120	10	66	6	144	12
29	1	192	2	44	6	96	8	56	10	120	10	66	8	144	12
29	3	48	4	44	8	72	6	57	1	216	18	66	10	192	16
29	5	72	6	45	1	384	4	57	3	576	6	66	12	240	2
30	2	96	8	45	3	96	8	57	5	480	4	67	1	240	20
30	4	96	8	45	7	240	2	57	7	192	16	67	3	192	16
30	6	48	4	46	0	288	3	57	9	192	16	67	5	216	18
31	1	48	4	46	2	120	10	57	11	360	3	67	7	168	14
31	3	72	6	46	4	72	6	58	0	288	24	67	9	312	26
31	5	48	4	46	8	288	3	58	2	144	12	67	11	216	18
32	2	72	6	47	1	96	8	58	4	360	3	67	13	240	20
32	4	120	10	47	3	216	18	58	6	288	24	68	0	288	24
32	6	120	10	47	5	192	16	58	8	192	16	68	2	192	16
33	1	144	12	47	7	120	10	58	10	120	10	68	6	288	24

Tabulation of R and H for $\mu = (a + b\sqrt{5})/2$—*Continued*

a	b	R	H	a	b	R	H	a	b	R	H	a	b	R	H
68	8	264	22	77	1	672	7	84	2	240	20	91	7	192	16
68	10	192	16	77	3	288	24	84	6	288	24	91	9	240	20
69	1	240	2	77	5	168	14	84	8	168	14	91	11	192	16
69	3	144	12	77	7	480	4	84	10	240	20	91	13	144	12
69	5	240	20	77	9	600	5	84	14	192	16	91	15	216	18
69	7	480	5	77	13	288	24	85	3	288	24	91	17	168	14
69	11	192	16	77	15	672	7	85	7	576	6	92	0	480	40
69	13	144	12	78	0	768	8	85	9	768	8	92	2	336	28
70	2	144	12	78	2	360	30	85	11	144	12	92	6	240	20
70	4	192	16	78	4	240	20	85	13	192	16	92	8	312	26
70	6	192	16	78	6	288	24	85	17	240	2	92	10	192	16
70	8	576	6	78	8	768	8	86	0	672	7	92	14	384	32
70	12	192	16	78	10	312	26	86	2	168	14	92	16	192	16
70	14	240	20	78	12	240	20	86	4	192	16	92	18	384	32
71	1	216	18	78	14	240	20	86	6	192	16	93	1	1056	11
71	3	192	16	79	1	192	16	86	8	384	4	93	3	384	32
71	5	120	10	79	3	264	22	86	10	144	12	93	5	360	30
71	7	144	12	79	5	144	12	86	12	264	22	93	7	720	6
71	9	144	12	79	7	168	14	86	14	144	12	93	9	480	4
71	11	168	14	79	9	168	14	86	16	384	4	93	11	408	34
71	13	144	12	79	11	144	12	87	1	384	32	93	13	288	24
72	2	360	30	79	13	144	12	87	3	288	24	93	15	768	8
72	4	336	28	79	15	144	12	87	5	360	30	93	17	864	9
72	6	192	16	80	2	192	16	87	7	432	36	94	0	480	5
72	10	216	18	80	4	192	16	87	9	288	24	94	2	240	20
72	12	192	16	80	6	336	28	87	11	264	22	94	4	240	20
72	14	216	18	80	12	144	12	87	15	336	28	94	6	264	22
73	3	672	7	80	14	240	20	87	17	264	22	94	8	480	5
73	5	600	5	81	1	144	12	88	2	264	22	94	10	144	12
73	7	192	16	81	3	480	4	88	4	192	16	94	12	216	18
73	9	288	24	81	5	480	5	88	6	336	28	94	14	216	18
73	11	360	3	81	7	216	18	88	10	264	22	94	16	480	5
73	13	576	6	81	11	672	7	88	12	336	28	94	18	240	20
74	0	192	16	81	13	360	3	88	14	288	24	95	1	288	24
74	2	144	12	81	15	192	16	89	1	168	14	95	3	240	20
74	4	240	2	82	0	384	32	89	3	576	6	95	7	288	24
74	6	168	14	82	2	216	18	89	5	360	3	95	9	240	20
74	8	144	12	82	4	480	4	89	7	192	16	95	11	192	16
74	10	144	12	82	6	336	28	89	9	240	20	95	13	240	20
74	12	480	4	82	8	192	16	89	11	480	4	95	17	240	20
74	14	144	12	82	10	312	26	89	13	576	6	95	19	192	16
75	1	192	16	82	12	720	6	89	15	168	14	96	4	216	18
75	3	192	16	82	14	240	20	89	17	168	14	96	6	240	20
75	7	288	24	82	16	240	20	90	2	240	20	96	10	312	26
75	9	192	16	83	1	240	20	90	4	480	4	96	12	240	20
75	11	240	20	83	3	288	24	90	6	288	24	96	14	240	20
75	13	192	16	83	5	240	20	90	8	288	24	96	18	192	16
76	0	144	12	83	7	288	24	90	12	480	4	97	1	288	24
76	2	144	12	83	9	360	30	90	14	336	28	97	3	600	5
76	6	192	16	83	11	168	14	90	16	288	24	97	5	768	8
76	8	192	16	83	13	288	24	91	1	168	14	97	7	336	28
76	10	144	12	83	15	336	28	91	3	240	20	97	9	456	38
76	14	144	12	84	0	192	16	91	5	192	16	97	11	960	10

Tabulation of R and H for $\mu = (a + b\sqrt{5})/2$—*Continued*

a	b	R	H	a	b	R	H	a	b	R	H	a	b	R	H
97	13	600	5	98	6	432	36	98	18	360	30	99	13	288	24
97	15	432	36	98	8	336	28	99	1	192	16	99	15	192	16
97	17	288	24	98	10	336	28	99	3	192	16	99	17	240	20
97	19	360	3	98	12	840	7	99	5	288	24	99	19	288	24
98	2	288	24	98	14	288	24	99	7	264	22				
98	4	840	7	98	16	240	20	99	11	192	16				

The computation was monitored for about the first 200 tally operations to make sure the score-keeping was correct in all possible cases. The tallying was, as before, basically a question of seeing that every permutation and change in sign in the triple (ξ_1, ξ_2, ξ_3) counted as a unit. The total running time was roughly 2.5 hours. One might remark that the human time involved in computing these class numbers H from basic *algebraic* concepts would have to be measured in "life-times," not "man-hours."

The computation was completed 18 April 1958 and was sponsored in part by the National Science Foundation Grant G-4222.

Department of Mathematics
University of Arizona
Tucson, Arizona

1. L. E. Dickson, *History of the Theory of Numbers*, v. III, G. E. Stechert, New York, 1934 (for references in the first paragraph).

2. F. Götzky, "Über eine zahlentheoretische anwendung von modulfunktionen zweier verändlicher," *Mathematische Annalen*, v. 100, 1928, p. 411–437.

3. H. Maass, "Uber die darstellung total positiver zahlen des körpers $R(\sqrt{5})$ als summe von drei quadraten," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universitat*, v. 14, 1941, p. 185–192.

Multiplication Time on The IBM 709

By D. D. Wall

Average multiply time is useful for roughly estimating problem running time for various problems, as well as for roughly comparing different computing machines. Determining average multiply time for the 709 is complicated, however, due to its zero-skipping feature, and requires an investigation of runs of zeros in binary sequences. The particular problem we solve is that of evaluating $R(n, l)$ = total number of runs of length l in all the 2^n words of n bits each, and $S(n, l) = \sum_{x=l}^{n} R(n, x)$ = number of runs of length $\geq l$ in the 2^n words of n bits each. The resulting 709 average multiply time is 193 microseconds fixed point, or 170 microseconds normalized floating point, and the purpose of this note is to derive these two numbers.

We make use of a device which we call "differencing modulo 2," which obtains an $n - 1$ bit number from a given n bit number by writing 1 or 0 according as the successive bits in the given number exhibit a change or no change. For example, each of the (complementary) 8 bit numbers 11010001 and 00101110 gives the same result 0111001 as its 7 bit difference modulo 2.

Received 30 April 1958.