MATHEMATICS OF COMPUTATION, VOLUME 24, NUMBER 110, APRIL, 1970

Integer Sequences Having Prescribed Quadratic Character

By D. H. Lehmer, Emma Lehmer and Daniel Shanks

Abstract. For the odd primes $p_1 = 3, p_2 = 5, \cdots$, we determine integer sequences N_p such that the Legendre symbol $(N/p_i) = \pm 1$ for all $p_i \leqq p$ for a prescribed array of signs ± 1; (i.e., for a prescribed quadratic character). We examine six quadratic characters having special interest and applications. We present tables of these N_p and examine some applications, particularly to questions concerning extreme values for the smallest primitive root (of a prime N), the class number of the quadratic field $R(\sqrt{-N})$, the real Dirichlet L functions, and quadratic character sums.

Introduction. Let $p_1, p_2, \ldots, p_m$ be a set of odd primes and let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ be a sequence with $\varepsilon^2 = 1$. The problem considered here is that of finding an integer N such that

$$(N/p_i) = \varepsilon_i, \qquad (i = 1(1)m), \tag{1}$$

where the symbol is that of Legendre. In other words we are looking for a positive integer N whose quadratic character with respect to each of the given p_i is specified. This is a special case of a more general problem of Kummer in which the ε's are kth roots of unity and the symbols are kth power characters. This problem has infinitely many solutions for every k, cf. Mills [1].

For $k = 2$ the infinitude of solutions follows from the law of quadratic reciprocity, since N lies in an arithmetical progression of difference $4p_i$ for each of the m values of i, and hence there exists an arithmetical progression of difference $4p_1p_2 \ldots p_m$ every term of which is a desired number N. This argument can also be used to obtain the asymptotic density of the N's and even the density of prime values of N, but it fails to give any information about the smallest positive value of N.

The problem of finding the values of N in natural order is solved automatically by the Delay Line Sieve, DLS 127 [2] provided the $p_i \leqq 127$. In what follows we consider six problems of special interest which have applications to other branches of the theory of numbers. In these problems $p_1 = 3$, $p_2 = 5, \ldots, p_i$ is the ith odd prime, the ε's form a simple pattern, and N is usually specified modulo 8.

We present tables of these integer sequences N for the several problems considered, and examine some of their applications, particularly to questions concerning primitive roots, class numbers, Dirichlet L functions, and quadratic character sums. For example, we show that if any algebraic field $R(\sqrt{-\Delta})$ of class number 3 exists besides the known examples, then $\Delta > 1.4 \cdot 10^{12}$.

Received August 22, 1969.

AMS Subject Classifications. Primary 1016, 1060; Secondary 1041, 1064, 1066.

Key Words and Phrases. Quadratic character, sieves, primitive roots, class number, Dirichlet L functions, quadratic character sums, pseudo-squares.

Problem I. Find $N \equiv 1 \pmod 8$ with $\varepsilon_i = 1$ for all odd $p_i \leqq p$ in (1). A solution N_p of this problem is a quadratic residue ($\neq 0$) of all primes $p_i \leqq p$ and hence every odd square satisfies the conditions of the problem. We shall be interested here in solutions which are not perfect squares and which have been called *pseudo-squares.*

Marshall Hall [3] has shown how to use these numbers for a test for primality. Cobham [4] pointed out that the pseudo-squares afford a cheap way of deciding whether a given number is a perfect square or not. Kraitchik [5] listed the least pseudo-square for $p \leqq 47$, and Lehmer [6] and [7] extended this list to $p \leqq 61$, and $p \leqq 79$, respectively. Using the DLS 127 this table was recently extended to $p \leqq 127$. For completeness we give the least pseudo-square for $3 \leqq p \leqq 127$ in Table I.

TABLE I
Table of Pseudo-Squares

p	*Least Solution*	*Least Prime Solution*	*Least Prim. Root*
3	73	73	5
5	241	241	7
7	1009	1009	11
11	$2641 = 19 \cdot 139$	2689	19
13	8089	8089	17
17	$18001 = 47 \cdot 383$	33049	29
19	53881	53881	31
23	87481	87481	29
29	$117049 = 67 \cdot 1747$	483289	31
31	515761	515761	37
37	1083289	1083289	41
41	$3206641 = 643 \cdot 4987$	3818929	53
43	3818929	3818929	53
47	9257329	9257329	53
53	22000801	22000801	59
59,61	48473881	48473881	97
67	175244281	175244281	79
71,73	427733329	427733329	83
79	898716289	898716289	101
83,89,97	$2805544681 = 127 \cdot 859 \cdot 25717$	*Unknown*	
101	$10310263441 = 4007 \cdot 2573063$	*Unknown*	
103	23616331489	23616331489	107
107,109	$85157610409 = 397 \cdot 214502797$	*Unknown*	
113,127	196265095009	196265095009	131

The difficulty of this problem is the necessity of eliminating the perfect squares which, to start with, completely upset the expected asymptotic density of the solutions, which is

$$\Delta_m = \frac{1}{8} \prod_{i=1}^{m} \frac{p_i - 1}{2p_i}. \tag{2}$$

To overcome this difficulty we exploit the capability of the DLS 127 of counting the number of its solutions without actually putting them out. It is clear that the number of unwanted perfect squares $\leqq X$ is exactly the number $\phi(P_m, X^{1/2})$ of numbers prime to $P_m = p_1 p_2 \ldots p_m$ and $\leqq X^{1/2}$. This, in turn, is the number of solutions $x \leqq X^{1/2}$ given by the Sieve of the trivial Diophantine equation $xy = 1$. These two problems were run alternately, using a logarithmic search procedure until the extra nonsquare solution was located and verified.

The deviations from the probabilistic estimate (2) caused by the squares is very marked. While odd perfect squares automatically satisfy $N \equiv 1 \pmod 8$ and $\varepsilon_i = 1$, and there are therefore many more solutions of (1) than is indicated by (2), the number of pseudo-square solutions is substantially smaller. For example, for $m = 22$, $p_i \leqq p_m = 83$, there are 168091 solutions of (1) less than $1308943^2 = 1713331777249$. But 161409 of these are squares, and only 6682 pseudo-square solutions occur. The number of solutions predicted by (2) is 12554.

Western and Miller [8] tabulate the least *prime* solution N_p for $p \leqq 53$. By the law of quadratic reciprocity this is equivalent to finding the least prime N_p whose least quadratic nonresidue exceeds p. This insures that every prime $< N_p$ has a quadratic nonresidue less than p and that there exist primes with arbitrarily large least primitive roots. In Table I, the least prime solution N_p and its least primitive root is also listed.

Western and Miller also give a companion table of least negative prime solutions. From our point of view this corresponds to the following problem.

Problem II. Find $N \equiv -1 \pmod 8$ with $\varepsilon_i = (-1/p_i)$ for all $p_i \leqq p$. The negatives $-N_p$ of the solutions of this problem are quadratic residues ($\neq 0$) of all primes $p_i \leqq p$ and hence can be thought of as negative pseudo-squares.

This time there is no direct interference from actual squares and one may expect a more predictable distribution. The following short table is for $p_m = 53$, $m = 15$, $\Delta_m = 1.03829 \cdot 10^{-6}$.

Limit $\cdot 10^{-6}$	*No. of Sol.*	*Exp. No.*	*No. of Sol./Exp. No.*
275	150	286	.524
324	200	336	.595
466	300	484	.620
725	500	753	.664
1297	1000	1347	.742
2720	2500	2824	.885
19617	18560	20368	.911
28925	27950	30033	.931
81324	80654	84438	.955
97900	97463	101649	.959
117000	116780	121480	.961

If Problems I and II are thought of as a single problem, one can conjecture that the density of negative pseudo-squares approaches the expected value as the limit $\to \infty$ and the influence of the perfect squares recedes.

TABLE II
Negative Squares

p	*Least Solution*	*Least Prime Solution*	*Least Prim. Root*
3	23	23	5
5	71	71	7
7	311	311	17
11	479	479	13
13	1559	1559	19
17	5711	5711	19
19	10559	10559	23
23	18191	18191	29
29	31391	31391	31
31	$307271 = 109 \cdot 2819$	366791	43
37,41	366791	366791	43
43	$2155919 = 59 \cdot 36541$	4080359	47
47	2155919	12537719	53
53	2155919	30706079	59
59	$6077111 = 1039 \cdot 5849$	36415991	67
61	6077111	82636319	67
67	$98538359 = 79 \cdot 1247321$	120293879	73
71	120293879	120293879	73
73,79	131486759	131486759	83
83	$508095719 = 367 \cdot 547 \cdot 2531$	2929911599	97
89	$2570169839 = 439 \cdot 5854601$	2929911599	97
97	2570169839	7979490791	109
101, 103	2570169839	33857579279	107
107	2570169839	89206899239	109
109	2570169839	121560956039	113
113,127	328878692999	328878692999	131
131	513928659191	513928659191	139

The least solution of Problem II for each $3 \leqq p \leqq 131$, and the least prime solution, in case the least solution is composite, is given in Table II together, again, with the primitive roots.

The negative squares have the property that the corresponding quadratic imaginary fields $R(\sqrt{-N})$ have exceptionally large class numbers relative to $\sqrt{N}$, and exceptionally large real Dirichlet L functions at argument 1:

$$L(1, \chi) = \sum_{n=1}^{\infty} \left(\frac{-N}{n}\right) \frac{1}{n}. \tag{3}$$

Here, $(-N/n)$ is the Kronecker symbol. A reflection of this property is that for all $-N_p$ listed in Table II with $p > 11$ there exist reduced, binary quadratic forms

$$(A, B, C) = Au^2 + Buv + Cv^2$$

of discriminant $-N_{p_m} = B^2 - 4AC$ for every $A = 1, 2, 3, \ldots$ less than p_{m+1}. For example, for $N_{97} = 7979490791$, we have

TABLE IIa
Negative Squares

p	$h(-N_p)$	$L(1, \chi)$	$h(-N_p)$	$L(1, \chi)$
3			3	1.96520
5			7	2.60987
7			19	3.38472
11			25	3.58858
13			51	4.05786
17			109	4.53127
19			153	4.67767
23			213	4.96137
29			289	5.12442
31	992	5.62213	1121	5.81495
37,41			1121	5.81495
43	2968	6.35035	3997	6.21634
47	2968	6.35035	7457	6.61614
53	2968	6.35035	12017	6.81293
59	5092	6.48918	12719	6.62151
61	5092	6.48918	20299	7.01518
67	21934	6.94169	24503	7.01855
71			24503	7.01855
73,79			25817	7.07318
83	51460	7.17211	128755	7.47286
89	122106	7.56669	128755	7.47286
97	122106	7.56669	219207	7.70933
101, 103	122106	7.56669	456929	7.80137
107	122106	7.56669	761619	8.01103
109	122106	7.56669	883537	7.96118
113,127			1499699	8.21554
131			1870227	8.19583

(1, 1, 1994872698), (2, ±1, 997436349), (3, ±1, 664957566),

(4, ±3, 498718175), (5, ±3, 398974540), (6, ±1, 332478783),

(6, ±5, 332478784), ..., (100, ±53, 19948734).

Similarly, for this discriminant, the series (3) begins as the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{100} - \frac{1}{101}$$

with the first hundred terms positive.

We list in Table IIa these class numbers $h(-N_p)$ and these functions $L(1, \chi)$ for both prime and composite N_p. The composite cases (with even class numbers) are on the left, as in Table II. These numbers, which are related by

$$L(1, \chi) = \pi h(-N)/\sqrt{N}, \tag{4}$$

were computed by the method described in [9].

Returning briefly to Problem I, we note that a Table Ia would begin:

p	$h(N)$	$L(1, \chi)$	$h(N)$	$L(1, \chi)$
3			1	1.79464
5			1	2.41835
7			7	3.07844
11	2	3.50737	1	3.48451
13			1	3.96332

We have not completed this table as the functions are much more difficult to compute for large positive discriminants. But two comments are in order. First, while these $L(1, \chi)$ tend to be large, no particular correlation is indicated for the corresponding class numbers. Instead of (4) one has

$$L(1, \chi) = \sum_{n=1}^{\infty} \left(\frac{N}{n}\right) \frac{1}{n} = \frac{\ln(u + v\sqrt{N})h(N)}{\sqrt{N}} \tag{5}$$

where $u^2 - Nv^2 = 1$ is the smallest Pell solution. Usually, $h(N)$ is quite small, and the largeness of $L(1, \chi)$ is reflected, instead, in an exceptionally long period for the regular continued fraction for $\sqrt{N}$. (It is this that makes the computation difficult.) Secondly, while the $L(1, \chi)$ are relatively large, they are not as large as could be expected by a simple probabilistic estimate. This, again, reflects the peculiarities in the distribution of the pseudo-squares discussed above. While the phenomenon is of interest, we will not pursue it here.

The problem which can be thought of as complementary to Problem II is as follows.

Problem III. Find $N \equiv 3 \pmod 8$ with $\varepsilon_i = -(-1/p_i)$ for $p_i \leqq p$. The negatives $-N_p$ of the solutions of this problem are quadratic nonresidues ($\neq 0$) of all the primes $p_i \leqq p$. Such numbers were first considered by Euler in connection with quadratic functions whose values have a high density of primes. In fact, the polynomial

$$x^2 + x + (N + 1)/4 \tag{6}$$

of discriminant $-N$ will not be divisible by 2, or any of the specified primes. Euler hit upon the remarkable $N_{37} = 163$, which led to the well-known polynomial $x^2 + x + 41$. Other polynomials of this sort were proposed by Beeger, Poletti, and others [10]-[11]. See also [14].

Since it was established by Stark [12] that 163 is the largest number N with a class number $h(-N) = 1$, we know that there does not exist another value of N for which the polynomial (6) is a prime for all values of $x < (N + 1)/4$. Nonetheless, further solutions of Problem III beyond $N_{37} = 163$ do provide examples in which the class number $h(-N)$ and L function (3) are apt to be unusually small, while the quadratic polynomial formula (6) possesses an unusually high density of primes. The first two properties are especially obvious when we rewrite (3) in product form:

$$L(1, \chi) = \frac{\pi h(-N)}{\sqrt{N}} = \prod_{p=2}^{\infty} \frac{p}{p - (-N/p)} \tag{7}$$

since we now have $(-N/p) = -1$ for all small p, and that minimizes all of the corresponding factors.

Least solutions N_p and least prime solutions N'_p for $3 \leqq p \leqq 163$ are given in Table III. Table IIIa gives the class numbers and L functions. Table III extends an earlier table to $p = 107$, by Lehmer [13]. Mohan Lal [14] has also computed the $h(-N_p)$ through $p = 107$, and in [14] he, and one of us, discuss some other aspects of this problem.

The decrease of $L(1, \chi)$ with p is, of course, not monotonic. The Legendre symbols beyond $(N \mid p)$ remain unspecified, and if, in these first solutions, these following symbols have an early preponderance of values $(-N \mid p_i) = -1$, as in N_{127}, the $L(1, \chi)$ is especially small. Contrarywise, as in N'_{139}, the $L(1, \chi)$ is "rather poor".

Such small values for $L(1, \chi)$ relate to an investigation of Chowla, Ayoub and Walum [15]. It is known that $h(-q)$ for primes $q \equiv 3 \pmod 4$ can also be obtained from the sums

$$S_1(q) = \sum_{v=1}^{q-1} v\left(\frac{v}{q}\right) = -qh(-q)$$

or from

$$S_2(q) = \sum_{v=1}^{q-1} v^2\left(\frac{v}{q}\right) = -q^2h(-q),$$

and these quadratic character sums are therefore, of necessity, negative. But in [15] it is proven that

$$S_3(q) = \sum_{v=1}^{q-1} v^3\left(\frac{v}{q}\right)$$

will be positive for infinitely many primes q.

To obtain a positive $S_3(q)$ it would suffice if

$$L(1, \chi) < \frac{\zeta(6)}{4\zeta(2)\zeta(3)} = 0.12863, \tag{8}$$

but that is not easy to attain. No entry in Table IIIa is that small, or even close. For all $q = N'_p$ listed, we have $S_3(q) < 0$; e.g., $S_3(163) = -2066677 = -12679 \cdot 163$.

As was indicated, there is no reason for the first solution N'_p to be especially good, in this respect, and we have also examined some subsequent solutions. The best prime q presently known to us has

$$h(-85702502803) = 16259 \quad \text{with } L(1, \chi) = 0.17448.$$

This is a subsequent solution for $p = 107$. The smallest $L(1, \chi)$ presently known to us for negative discriminants is that of a large, composite solution for $p = 149$:

$$N = 84148631888752647283 = 6079 \cdot 30469 \cdot 132137 \cdot 3438209$$

has

$$h(-N) = 496652272 \quad \text{and} \quad L(1, \chi) = 0.17009.$$

TABLE III

$$\left(\frac{N}{p_i}\right) = -\left(\frac{-1}{p_i}\right) \quad \textit{for all} \quad p_i \leqq p, \qquad N = 8x + 3$$

p	*Least Solution* N_p	*Least Prime Solution* N'_p
3	19	19
5,7	43	43
11,13	67	67
17,..,37	163	163
41	$77683 = 131 \cdot 593$	222643
43	77683	1333963
47	1333963	1333963
53,59	2404147	2404147
61	20950603	20950603
67	$36254563 = 127 \cdot 285469$	51599563
71	51599563	51599563
73,79	96295483	96295483
83	$114148483 = 101 \cdot 463 \cdot 2441$	146161723
89	$269497867 = 317 \cdot 419 \cdot 2029$	1408126003
97,101,103	269497867	3341091163
107	$585811843 = 14081 \cdot 41603$	52947440683
109,113	52947440683	52947440683
127	$71837718283 = 281 \cdot 3709 \cdot 68927$	193310265163
131,137	229565917267	229565917267
139	$575528148427 = 149 \cdot 283 \cdot 13648781$	915809911867
149	1271259755683	1271259755683
151,157,163	1432817816347	1432817816347

It is clear that we are a long way from exhibiting even a single example of $S_3(q) > 0$ unless its necessary condition is substantially more generous than the sufficient condition (8).

In fact, however, one has [15]

$$S_3(q) = \frac{q^3\sqrt{q}}{\pi}\left[\frac{3}{2\pi^2} L(3, \chi) - L(1, \chi)\right], \tag{9}$$

where we have corrected an erroneous factor of $\frac{1}{2}$ and where

$$L(3, \chi) = \prod_{p=2}^{\infty} \frac{p^3}{p^3 - (-q/p)}.$$

Now

$$L(3, \chi) > \prod_{p=2}^{\infty} \frac{p^3}{p^3 + 1} = \frac{\zeta(6)}{\zeta(3)} = 0.84634,$$

and this gives the sufficient condition (8). In our cases $L(3, \chi)$ will be slightly larger; e.g., for $q = 163$,

TABLE IIIa

$$\left(\frac{N}{p_i}\right) = -\left(\frac{-1}{p_i}\right) \quad \textit{for all} \quad p_i \leqq p. \qquad N = 8x + 3$$

p	$h(-N_p)$	$L(1, \chi)$	$h(-N'_p)$	$L(1, \chi)$
3			1	0.72073
5,7			1	0.47909
11,13			1	0.38381
17,...,37			1	0.24607
41	22	0.24798	33	0.21971
43	22	0.24798	79	0.21488
47			79	0.21488
53,59			107	0.21680
61			311	0.21346
67	432	0.22540	487	0.21299
71			487	0.21299
73,79			665	0.21290
83	692	0.20348	857	0.22270
89	1044	0.19979	2293	0.19197
97,101,103	1044	0.19979	3523	0.19148
107	1536	0.19937	13909	0.18990
109,113			13909	0.18990
127	15204	0.17821	26713	0.19087
131,137			29351	0.19245
139	44332	0.18358	59801	0.19632
149			66287	0.18470
151,157,163			70877	0.18602

$$L(3, \chi) = \frac{9260\pi^3}{163^2\sqrt{163}} = 0.84643,$$

but for $p \geqq 41$ in Table IIIa we must have

$$L(3, \chi) < \prod_{p=2}^{41} \frac{p^3 - 1}{p^3 + 1}\zeta(3) = 0.84644.$$

Therefore,

$$\frac{3}{2\pi^2} L(3, \chi) < 0.12865,$$

and since this is smaller than any $L(1, \chi)$ shown in Table IIIa, we do confirm that $S_3(q) < 0$ for all of these primes.

In contrast, consider

$$S_4(q) = \sum_{\nu=1}^{q-1} \nu^4 \left(\frac{\nu}{q}\right).$$

Now we have

$$S_4(q) = \frac{q^4\sqrt{q}}{\pi}\left[\frac{3}{\pi^2}L(3,\chi) - L(1,\chi)\right], \tag{10}$$

which may be neatly derived from (9) as follows. For any $n \geqq 0$, we obtain

$$\sum_{v=1}^{q-1} v^n(q-v)^n\left(\frac{v}{q}\right) = 0$$

since

$$((q-v)/q) = -(v/q),$$

and each term $v = a$ cancels that for $v = q - a$.

For $n = 2$ and 1 we obtain

$$S_4(q) - 2qS_3(q) + q^2S_2(q) = 0, \qquad S_2(q) - qS_1(q) = 0,$$

and thus

$$S_4(q) = 2qS_3(q) + q^4h(-q). \tag{11}$$

Combining (11) and (9) now gives (10).

Therefore, a sufficient condition for $S_4(q) > 0$ is

$$L(1,\chi) < \frac{\zeta(6)}{2\zeta(2)\zeta(3)} = 0.25726. \tag{12}$$

This condition is met by all N'_p shown in Table IIIa starting with $N'_{37} = 163$. (In fact, from (11) and the previously indicated value of $S_3(163)$, we have $S_4(163) = [163^2 - 2(12679)]163^2 = 1211 \cdot 163^2$.)

It is reasonable to conjecture that $S_4(q) > 0$ for all subsequent N'_p beyond our table, but probably that would be difficult to prove. Presumably, one should attempt to prove it for all $p > p_0$ (hopefully small), and then continue the table (if necessary) up to this lower bound p_0.

In passing, we note that these character sums may be expressed simply in terms of generalized Euler numbers [16]. For $q \equiv 3 \pmod 8$ we have

$$\begin{aligned} S_3(q) &= q(c_{q,1} - 4q^2c_{q,0})/12 \\ S_4(q) &= q^2(c_{q,1} - 2q^2c_{q,0})/6. \end{aligned} \tag{13}$$

For example, $c_{163,0} = 3$ and $c_{163,1} = 166680$, and we may verify the previously indicated sums.

Problem IV. Find $N \equiv -1 \pmod 8$ as in Problem II, but with $\varepsilon_i = -(-1/p_i)$ as in Problem III. Since the first factor on the right of (7) is now $\frac{2}{1}$ instead of $\frac{2}{3}$ as it was in Problem III, we can expect the values of $h(-N)$ to be about 3 times those of the last problem. It might seem, at first, that these N are of little interest, since we clearly are aiming at small $h(-N)$ and yet we start off immediately in the wrong direction.

But there is another viewpoint. The pre-Kronecker formulation of these problems by Gauss and Dirichlet dealt only with even discriminants. One has the forms

$$Au^2 + 2Buv + Cv^2$$

of *determinant*

$$D = B^2 - AC$$

for *every* nonsquare integer D. The class number is now $h(4D)$, and the Dirichlet series, for negative $D = -N$ is now

$$L_N(1) = \frac{\pi h(-4N)}{\sqrt{4N}} = \sum_{k=0}^{\infty} \left(\frac{-N}{2k+1}\right) \frac{1}{2k+1} = \prod_{p=3}^{\infty} \frac{p}{p - (-N/p)} \tag{14}$$

with Jacobi symbol $(-N/(2k+1))$ and Legendre symbol $(-N/p)$. The quadratic polynomial (6) now becomes

$$x^2 + N, \tag{15}$$

and similar questions arise concerning its density of primes, cf. [17]-[18].

It is known that

$$h(-4N) = h(-N)$$

for our present $N \equiv -1 \pmod 8$, while

$$h(-4N) = 3h(-N)$$

for $N \equiv 3 \pmod 8$. This nullifies the previously mentioned factor of 3, and now, using $L_N(1)$ instead of $L(1, \chi)$, these two residue classes modulo 8 can be compared on an equal basis, not only with each other, but with any residue class modulo 8. This gives us a much richer population to study.

We list the first composite and prime solutions in Table IV, while Table IVa gives the values of $h(-N) = h(-4N)$ and of $L_N(1)$. The smallest $L_N(1)$ presently known to us is

$$L_{569078186623}(1) = 0.25346; \qquad (p = 137).$$

It is smaller than those for any of the N singled out for special mention in the previous problem. These have values

$$L_{71837718283}(1) = 0.26731, \qquad (p = 127)$$

$$L_{85702502803}(1) = 0.26172,$$

and

$$L_{8414863188752647283}(1) = 0.25513.$$

In Problem V below our smallest value is

$$L_{3666575384938}(1) = 0.26064 \qquad (p = 157).$$

Analogous to our remarks concerning $h(-163)$ in the previous problem, we call attention to

$$h(-4 \cdot 7) = 1, \qquad h(-4 \cdot 127) = 5, \qquad h(-4 \cdot 487) = 7$$

in Table IVa. These have been proven [19] to be the largest negative determinants with these class numbers. While the same is probably true of the entry

TABLE IV

$$\left(\frac{N}{p_i}\right) = -\left(\frac{-1}{p_i}\right) \text{ for all } p_i \leqq p, \quad N = 8x + 7$$

p	Least Solution N_p	Least Prime Solution N'_p
3,5	7	7
7	127	127
11	$247 = 13 \cdot 19$	463
13	463	463
17	487	487
19	1423	1423
23	33247	33247
29	$56743 = 179 \cdot 317$	73327
31	$74743 = 41 \cdot 1823$	118903
37,41	118903	118903
43	$348727 = 241 \cdot 1447$	454183
47	348727	773767
53,59,61	773767	773767
67	$2430943 = 227 \cdot 10709$	86976583
71	2430943	125325127
73	2430943	132690343
79	$242675623 = 191 \cdot 263 \cdot 4831$	788667223
83	$393292183 = 5573 \cdot 70571$	788667223
89	393292183	1280222287
97	393292183	2430076903
101	$1656835783 = 739 \cdot 827 \cdot 2711$	10703135983
103	$2713676023 = 17747 \cdot 152909$	10703135983
107	$4352137927 = 64661 \cdot 67307$	10703135983
109	$8133814327 = 643 \cdot 12649789$	10703135983
113,127	8133814327	15605135527
131	$8363603623 = 57047 \cdot 146609$	148202808007
137	8363603623	569078186623
139	$1128864945583 = 4943 \cdot 228376481$	3506439768967
149,151	$3402396344407 = 138727 \cdot 24525841$	3506439768967
157,163	3402396344407	*Unknown*

$$h(-4 \cdot 1423) = 9,$$

that remains unproven [19]. But the proposition is not general. For example,

$$h(-4 \cdot 33247) = 53 \quad \text{with } L_{33247}(1) = 0.45658$$

certainly looks unlikely in view of the size of its $L_N(1)$, and, in fact, we find in Ordman's table [20] that there is a larger example:

$$h(-4 \cdot 39103) = 53 \quad \text{with } L_{39103}(1) = 0.42101.$$

It is instructive to note that this latter determinant already fails on $p = 13$: $(-39103 \mid 13) = +1$.

TABLE IVa

$$\left(\frac{N}{p_i}\right) = -\left(\frac{-1}{p_i}\right) \text{ for all } p_i \leqq p, \quad N = 8x + 7$$

p	$h(-4N_p)$	$L_{N_p}(1)$	$h(-4N'_p)$	$L_{N'_p}(1)$
3,5			1	0.59371
7			5	0.69693
11	6	0.59968	7	0.51101
13			7	0.51101
17			7	0.49826
19			9	0.37477
23			53	0.45658
29	60	0.39565	73	0.42346
31	66	0.37921	83	0.37810
37,41			83	0.37810
43	136	0.36176	157	0.36594
47	136	0.36176	185	0.33036
53,59,61			185	0.33036
67	312	0.31433	1927	0.32456
71	312	0.31433	2295	0.32202
73	312	0.31433	2273	0.30996
79	3064	0.30896	5313	0.29718
83	3718	0.29449	5313	0.29718
89	3718	0.29449	7173	0.31490
97	3718	0.29449	9529	0.30364
101	8096	0.31243	18545	0.28157
103	9826	0.29629	18545	0.28157
107	12384	0.29487	18545	0.28157
109	16602	0.28916	18545	0.28157
113,127	16602	0.28916	22635	0.28462
131	16760	0.28787	66011	0.26934
137	16760	0.28787	121725	0.25346
139	182424	0.26970	344909	0.28933
149,151	323392	0.27540	344909	0.28933
157,163	323392	0.27540	*Unknown*	*Unknown*

Class Number 3 and a Brief Return to Problem III. The question whether

$$h(-4 \cdot 1423) = 9$$

exhibits the largest determinant having class number 9 is essentially equivalent to that whether

$$h(-907) = 3$$

exhibits the largest discriminant having class number 3. The primes $p = 8x + 7$ having $h(-p) = 3$ or 9 are completely known [19]:

$$h(-p) = 3 \quad \text{for } p = 23, 31;$$

$$h(-p) = 9 \quad \text{for } p = 199, 367, 823, 1087, 1423;$$

and if we join these sets, respectively, with all $p = 8x + 3$ having $h(-p) = 3$, we would obtain the complete set of discriminants with $h(-p) = 3$, or the complete set of determinants with $h(-4p) = 9$.

The known $p = 8x + 3$ with this class number are [19]:

$$p = 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907$$

to which we may add

$$p^5 = 243$$

if we do not insist that the discriminant be square-free. There are no other $h(-p) = 3$ for $p \leqq 166807$ by the tables of Ordman [20] and Newman [21].

Any $P = 8x + 3 > 1467 = 3^2 \cdot 163$ having $h(-P) = 3$ must have

$$L(1, \chi) < 0.24607.$$

By a systematic calculation, we find that there are only eight $p = 8x + 3 < 318028$ with an $L(1, \chi)$ that small, and they have these class numbers:

p	$h(-p)$	p	$h(-p)$
90787	23	210907	35
166147	29	222643	33
191563	33	253507	39
205627	35	296587	41

Since any further example P must therefore exceed $318028 = 4 \cdot 43^3$, the argument in [19, esp. p. 153, 162], based upon composition of forms, may now be applied as follows. If $(-P \mid q) = +1$, there is a form $F = (q, b, c)$ of discriminant $-P$. Then

TABLE V

$$\left(\frac{N}{p_i}\right) = -\left(\frac{-2}{p_i}\right) \text{ for all } p_i \leqq p, \quad N = 8x + 5$$

p	*Least Solution* N_p	*Least Prime Solution* N'_p
3	5	5
5,...,23	29	29
29,...,47	23669	23669
53	1508789	1508789
59	5025869	5025869
61,67	$7841261 = 227 \cdot 34543$	9636461
71	9636461	9636461
73	$18127229 = 491 \cdot 36919$	37989701
79,83	$31839341 = 101 \cdot 239 \cdot 1319$	37989701
89,97	37989701	37989701
101,103,107	240511301	240511301
109	$23739440141 = 241 \cdot 367 \cdot 268403$	41868418349
113	$44913466781 = 13339 \cdot 3367079$	90664613309
127,131,137	$60664576541 = 149 \cdot 407144809$	123464393861
139,149,151	123464393861	123464393861
157,...,181	1833287692469	1833287692469

$F^3 = F^{h(-P)}$ represents q^3 and equals the principal form. Therefore,

$$q^3 = u^2 + uv + (P+1)v^2/4 \quad \text{or} \quad 4q^3 = (2u+v)^2 + Pv^2.$$

Since this is impossible for $4q^3 < P$, we must have

$$(-P/q) = -1$$

for every $q \leqq 43$. By Tables III and IIIa we therefore have $P > N'_{43} = 1333963$. But, one also has

$$4 \cdot 67^3 < N'_{43}, \qquad 4 \cdot 163^3 < N'_{67},$$

and

$$4 \cdot 7079^3 < N'_{163},$$

so repetition of the argument shows that

$$P \geqq N'_{7079} > N'_{163} = 1432817816347,$$

and

$$(-P/q) = -1$$

for all $q \leqq 7079$, are both necessary. Such a P must also have

$$L(1, \chi) < 3\pi/\sqrt{N'_{163}} = 0.0000079,$$

and therefore either 907 and 1423 are the last examples of $h(-p) = 3$ and $h(-4p) = 9$, or any counterexample would (easily) satisfy $S_3(P) > 0$. We must admit that we would be pleased with either contingency.

TABLE Va

$$\left(\frac{N}{p_i}\right) = -\left(\frac{-2}{p_i}\right) \text{ for all } p_i \leqq p, \quad N = 8x + 5$$

p	$h(-8N_p)$	$L_{2N_p}(1)$	$h(-8N'_p)$	$L_{2N'_p}(1)$
3			2	0.99346
5,...,23			2	0.41251
29,...,47			46	0.33210
53			406	0.36713
59			718	0.35573
61,67	832	0.33002	950	0.33991
71			950	0.33991
73	1148	0.29949	1698	0.30599
79,83	1648	0.32440	1698	0.30599
89,97			1698	0.30599
101,103,107			3990	0.28577
109	39880	0.28749	53510	0.29047
113	59012	0.30928	77970	0.28762
127,131,137	65300	0.29448	89478	0.28285
139,149,151			89478	0.28285
157,...,181			317722	0.26064

Our next problem is associated with some of the fields having class number 2.

Problem V. Find $N \equiv 5 \pmod 8$ with $\varepsilon_i = -(-2/p_i)$ for all $p_i \leqq p$. This implies that $-2N$ is a quadratic nonresidue of all odd primes $\leqq p$. The solutions are given in Tables V and Va, as before, and note, that in this case, $L_{2N}(1)$ and $L(1, \chi)$ are identical. The first two entries have $h(-8N') = 2$. Recently, Peter Weinberger [22] proved that $h(-8N')$ exceeds 2 for all $N' > 29$. We also note that, for all p,

$$h(-8N') \equiv 2 \pmod 4.$$

This follows from the fact that the only ambiguous form besides the principal form is

$$(2, 0, N'),$$

and this form is not in the principal genus since 2 is a quadratic nonresidue of N'. Therefore, the class number is a multiple of 2, but not of 4.

Relative to Table IV, Table V is quite short since many of its least solutions are valid for a whole string of p_i, e.g., 123464393861 is valid for six p_i, and then 1833287692469 is valid for six more. We do not know if this phenomenon is of significance, or merely a fluke. A number of these N'_p—those for $p = 5, 29, 101$, and 157—have exceptionally small values of $L_{2N'_p}(1)$ for determinants of their size.

We round out our choice of quadratic characters by returning to positive discriminants and examining the problem that complements Problem I and extends Problem III into the positive range.

Problem VI. Find $N \equiv 5 \pmod 8$ with $\varepsilon_i = -1$, for all $p_i \leqq p$. The least prime residue of N will therefore exceed p. The least solutions are given in Table VI. Those for $p = 43 - 53$ were given earlier by N. Beeger and E. Karst [23]. As with Problem I, we have not completed a Table VIa and merely show its beginning:

p	$h(N_p)$	$L(1, \chi)$	$h(N'_p)$	$L(1, \chi)$
3			1	0.43041
5			1	0.54002
7, 11			1	0.39091
13			1	0.33144
17	2	0.29106	1	0.26009
19, 23			1	0.26045
29	4	0.25762	1	0.29195
31, 37, 41			5	0.26510

In Table VI we have included 3D values of $L(1, \chi)$ for each N. These approximations were obtained by a program called SPEEDY that computes the partial products of (7) for $p < 132000$. It evaluates the needed Jacobi symbols by the Reciprocity Law, and requires only a few seconds on an IBM 7094 for each discriminant. While it is very difficult to bound the error of these partial products with a bound that is both realistic and mathematically sound, we know by comparison with many examples where $L(1, \chi)$ is known exactly that usually these SPEEDY approximations are correct to 1 part in 1000. The very low value of $L(1, \chi)$ for $N'_{131} = 49107823133$ is of

TABLE VI

$$\left(\frac{N}{p_i}\right) = -1 \text{ for all } p_i \leqq p, \qquad N = 8x + 5$$

p	N_p	$L(1, \chi)$	N'_p	$L(1, \chi)$
3	5		5	0.430
5	53		53	0.540
7, 11	173		173	0.391
13	293		293	0.331
17	437 = 19·23	0.291	2477	0.260
19, 23	9173		9173	0.260
29	24653 = 89·277	0.258	61613	0.292
31–41	74093		74093	0.265
43	170957		170957	0.246
47	214037 = 193·1109	0.250	360293	0.224
53	214037 = 193·1109	0.250	679733	0.223
59	214037 = 193·1109	0.250	2004917	0.205
61	2004917		2004917	0.205
67	44401013 = 157·282809	0.212	69009533	0.209
71	94948157 = 317·299521	0.226	138473837	0.233
73	154554077 = 97·1593341	0.223	237536213	0.224
79	154554077 = 97·1593341	0.223	324266477	0.227
83	163520117 = 2027·80671	0.214	324266477	0.227
89, 97	163520117 = 2027·80671	0.214	1728061733	0.194
101, 103	261153653 = 8191·31883	0.190	1728061733	0.194
107–113	1728061733		1728061733	0.194
127	9447241877		9447241877	0.181
131	19553206613 = 14221·1374953	0.177	49107823133	0.169(5)
137, 139	49107823133		49107823133	0.169(5)
149–163	385995595277 = 191·10711·188677	0.174	*Unknown*	*Unknown*

special interest. It is exceptionally small for a discriminant of this size, and appears to be even smaller than the 0.17009 value mentioned in Problem III.

These Table VI integers N have a pleasing property when considered as negative determinants. All negative determinants $-N$ have ratios

$$h(-4N)/\sqrt{N}$$

that are asymptotically bounded as $N \to \infty$ by

$$AN^{-\varepsilon} < h(-4N)/\sqrt{N} < AN^{+\varepsilon}$$

for any positive ε [24]. Our present N satisfy

$$(-N/p_i) = -(-1/p_i) \qquad (p_i \leqq p)$$

and therefore have

$$L_N(1) = C(p) \prod_{q>p} \frac{q}{q - (-N/q)}$$

where the coefficient

$$C(p) = \frac{3}{3-1} \cdot \frac{5}{5+1} \cdot \frac{7}{7-1} \cdot \frac{11}{11-1} \cdot \ldots \cdot \frac{p}{p+(-1/p)}$$

converges to $\pi/2$ as $p \to \infty$, cf. Euler, Landau [25]. These N, therefore, have class numbers $h(-4N)$ approximately equal to $\sqrt{N}$ by (14). But the convergence is, of course, quite slow:

$$h(-4N_{131}) = 145644 = 1.042\sqrt{N_{131}},$$

$$h(-4N'_{131}) = 224546 = 1.013\sqrt{N'_{131}},$$

$$h(-4N_{149}) = 592288 = 0.953\sqrt{N_{149}}.$$

There are obviously many similar problems that one can propose and solve with the Delay Line Sieve [2]. The DLS 127 is available to anyone with a suitable problem without charge. We are pleased to acknowledge the assistance of Richard Serafin in computing most of the class numbers.

University of California
Berkeley, California 94720

1180 Miller Avenue
Berkeley, California 94708

Applied Mathematics Laboratory
Naval Ship R&D Center
Washington, D.C. 20007

1. W. H. MILLS, "Characters with preassigned values," *Canad. J. Math.*, v. 15, 1962, pp. 169–171. MR **28** #71.
2. D. H. LEHMER, "An announcement concerning the Delay Line Sieve DLS-127," *Math. Comp.*, v. 20, 1966, pp. 645–646.
3. MARSHALL HALL, "Quadratic residues in factorization," *Bull. Amer. Math. Soc.*, v. 39, 1933, pp. 758–763.
4. ALLAN COBHAM, *The Recognition Problem for the Set of Perfect Squares*, IBM Research Paper, R.C. 1704, April 26, 1966.
5. M. KRAITCHIK, *Recherches sur la Théorie des Nombres*. Vol. 1, Paris, 1924, pp. 41–46.
6. D. H. LEHMER, "The mechanical combination of linear forms," *Amer. Math. Monthly*, v. 35, 1928, pp. 114–121.
7. D. H. LEHMER, "A sieve problem on "pseudo-squares"," *MTAC*, v. 8, 1954, pp. 241–242. MR **16**, 113.
8. A. E. WESTERN & J. C. P. MILLER, *Indices and Primitive Roots*, Royal Soc. Math. Tables, v. 9, Cambridge Univ. Press, New York, 1968, p. xv.
9. DANIEL SHANKS, "Class number, a theory of factorization, and genera." (To appear.)
10. N. G. W. H. BEEGER, "Report on some calculations of prime numbers," *Nieuw. Arch. Wiskde.* v. 20, 1939, pp. 48–50. MR **1**, 65.
11. LUIGI POLETTI, "Atlante di centomila numeri primi di ordine quadratico entro cinque miliardi," UMT 62, *MTAC*, v. 2, 1947, p. 354.
12. H. M. STARK, "A complete determination of the complex quadratic fields of class-number one," *Michigan Math. J.*, v. 14, 1967, pp. 1–27. MR **36** #5102.
13. D. H. LEHMER, "On the function $X^2 + X + A$," *Sphinx*, v. 6, 1936, pp. 212–214; v. 7, 1937, p. 40; v. 9, 1939, pp. 83–85.
14. MOHAN LAL & DANIEL SHANKS, "Class numbers and a high density of primes." (To appear.)
15. R. AYOUB, S. CHOWLA & H. WALUM, "On sums involving quadratic characters," *J. London Math. Soc.*, v. 42, 1967, pp. 152–154. MR **34** #4224.
16. DANIEL SHANKS, "Generalized Euler and class numbers," *Math. Comp.*, v. 21, 1967, pp. 689–694. MR **36** #6343.
17. DANIEL SHANKS, "On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$," *Math. Comp.*, v. 14, 1960, pp. 320–332. MR **22** #10960.
18. DANIEL SHANKS, "Supplementary data and remarks concerning a Hardy-Littlewood conjecture," *Math. Comp.*, v. 17, 1963, pp. 188–193. MR **28** #3013.

19. DANIEL SHANKS, "On Gauss's class number problems," *Math. Comp.*, v. 23, 1969, pp. 151–163.
20. EDWARD T. ORDMAN, "Tables of class numbers for negative prime discriminants," UMT 29, *Math. Comp.*, v. 23, 1969, p. 458.
21. MORRIS NEWMAN, "Table of the class number $h(-p)$ for p prime, $p \equiv 3 \pmod 4$, $101987 \leqq p \leqq 166807$," UMT 50, *Math. Comp.*, v. 23, 1969, p. 683.
22. PETER WEINBERGER, *Dissertation*, University of California, Berkeley, Calif., June, 1969.
23. EDGAR KARST, "The congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and quadratic forms with high density of primes," *Elem. Math.*, v. 22, 1967, pp. 85–88. MR **35** #6612.
24. C. L. SIEGEL, "Uber die Classenzahl quadratischer Zahlkorper," *Acta Arith.*, v. 1, 1935, pp. 83–86.
25. E. LANDAU, *Handbuch der Lehre von der Verteilung der Primzahlen*. Bände 2, Chelsea, New York, 1953, §186, "Euler's Reihen," pp. 673–676. MR **16,** 904.