MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 126, APRIL 1974, PAGES 625–635

A New Factorization Technique Using Quadratic Forms

By D. H. Lehmer and Emma Lehmer

Abstract. The paper presents a practical method for factoring an arbitrary N by representing N or λN by one of at most three quadratic forms: $\lambda N = x^2 - Dy^2$, $\lambda = 1, -1, 2$, $D = -1, \pm 2, \pm 3, \pm 6$. These three forms appropriate to N, together with inequalities for y, are given for all N prime to 6. Presently available sieving facilities make the method quite effective and economical for numbers N having 20 to 25 digits. Four examples arising from aliquot series are discussed in detail.

It is the purpose of this paper to present and illustrate a new procedure for factoring numbers N of no special form which in the present state of the art is particularly effective for numbers having from 20 to 25 decimal digits. The implementation of the method was the result of three circumstances: (a) a decision to assist Richard Guy and John Selfridge in their survey of aliquot series, i.e., sequences of iterates of the sum of the proper divisors of a number, a source of many numbers N of the above-mentioned magnitude; (b) the elimination of idle time at the Computer Center of the University of California, Berkeley campus, which made direct search for the factors of N prohibitively expensive; and (c) the availability of the Delay Line Sieve, DLS-157 at no cost [5]. It is hoped that those readers who have unlimited access to the virtuosity of an expensive computer system may also find the method of some use although circumstances (a), (b) and (c) may all fail to exist, since the sieving part of the procedure can easily be done inside the system [6], even if at a slower rate than the million per second rate of the off line DLS-157.

The present method is a modification of much older ones depending on the representation of N, or a chosen multiple of N, by a binary quadratic form. Such methods began with Fermat, 1643, [3] who suggested solving

$$N = x^2 - y^2 = (x - y)(x + y) \tag{1}$$

for x and y. One such representation of N with $x < (N + 1)/2$ suffices to factor N, and the nonexistence of a solution is a proof of the primality of N. In recent decades, the Fermat method has been extensively used in the case where N is known to have all its factors of the form $ax + 1$. The method is also a good second step following a disappointing direct search for factors of N below some fairly high limit. The drawback of Fermat's method in the general case is its great average expense, which is $O(N)$. This is to be contrasted with that of the present method which is only $O(\sqrt{N})$.

In 1647, Mersenne [3] noted that N is composite if N is the sum of two squares in two really different ways. Thus, the use of quadratic forms, other than Fermat's degenerate (1), has a long history. Euler, Legendre, Gauss, Chebyshev [3] and a

Received March 30, 1973, revised July 2, 1973.
AMS (MOS) subject classifications (1970). Primary 05B30, 10A25, 10B05, 10C05, 12A50.
Key words and phrases. Factorization, primality, binary quadratic forms, representation.

great many others suggested using forms

$$\lambda N = x^2 - Dy^2 \qquad (D \neq 1) \tag{2}$$

either to factor N or prove N a prime. Again, two really different solutions (x_1, y_1), (x_2, y_2) of (2) result in two incongruent solutions z_1, z_2 of the congruence $z^2 \equiv D \pmod{N}$ so that N and $|z_1 - z_2|$ have a common factor greater than 1 which can be exposed by applying Euclid's algorithm to N and $|x_1y_2 - x_2y_1|$.

The advantage of (2) over (1) is, as we have mentioned, the cost of $O(\sqrt{N})$. In fact, the larger $|D|$, the cheaper the search for y becomes. The big drawback is that, for a given D, (2) may not have a solution at all, even though D is carefully chosen so that the Jacobi symbol $(D/N) = 1$. In fact, the larger D is chosen, the more likely it is that such a disappointment will ensue. When this happens, we must change the D and λ in (2) and try again. The potential cost of successive failures to solve (2) has led many writers to develop other tactics [see Dickson [3], Brillhart and Morrison [1], and Shanks [9] use quadratic forms in different ways]. It is a little surprising that no one seems to have asked: How many failures of (2) need we suffer, before we finally succeed in factoring N? In this paper, we show that the answer is at most two, in the typical case in which N is the product of two primes. The success of the method is due to the utilization of the information generated by each failure.

To search for solutions of (2), we use Gauss' method of exclusion, excluding values of y [8]. When a positive y is found for which $\lambda N + Dy^2$ is a perfect square, x is taken to be its positive square root. It is essential to know in each case the range of possible values of y, so that we can be sure when (2) has no solution or, after one solution has appeared, how long we should wait for a second solution. This range depends, of course, on λ, N and D. There are three cases as follows [2], [8].

$$\begin{aligned}
&\text{If } D < 0, && 0 \leqq y < (\lambda/|D|)^{1/2}\sqrt{N}.\\
&\text{If } D > 1 \text{ and } \lambda > 0, && 0 \leqq y < (\lambda(T-1)/2D)^{1/2}\sqrt{N}. \qquad (3)\\
&\text{If } D > 1 \text{ and } \lambda < 0, && (|\lambda|/D)^{1/2}\sqrt{N} \leqq y < (|\lambda|(T+1)/2D)^{1/2}\sqrt{N}.
\end{aligned}$$

Here, (T, U) is the fundamental solution of the Pell equation $T^2 - DU^2 = 1$.

We now proceed to disclose our method. To cover all cases of N, prime to 6, requires only ten examples of (2). These are labeled (A), (B), $\cdots$, (J), as follows:

(A)	$N = x^2 + y^2$	(F)	$-N = x^2 - 3y^2$
(B)	$N = x^2 + 2y^2$	(G)	$N = x^2 + 6y^2$
(C)	$N = x^2 - 2y^2$	(H)	$2N = x^2 + 6y^2$
(D)	$N = x^2 + 3y^2$	(I)	$N = x^2 - 6y^2$
(E)	$N = x^2 - 3y^2$	(J)	$-N = x^2 - 6y^2$

Three of these quadratic forms are chosen according to the following:

THEOREM. *Let $N = pq \equiv n \pmod{24}$ be the product of two primes. From among* (A), (B), $\cdots$, (J), *select the three that correspond to n by the following scheme*

n	1	5	7	11	13	17	19	23
selection	BDI	AHJ	CDG	BFH	ADE	ABC	BDI	CFJ

Then, at least one of the three selected equations has exactly two solutions with y satisfying the inequalities (3). *These two solutions determine p and q.*

Proof. We separate eight cases according to the value of n. All congruences in the proof have modulus 24. Use is made of the "conformal multiplication" identity of Brahmagupta

$$(4) \qquad (\xi_1^2 - D\eta_1^2)(\xi_2^2 - D\eta_2^2) = (\xi_1\xi_2 \pm D\eta_1\eta_2)^2 - D(\xi_1\eta_2 \pm \xi_2\eta_1)^2$$

as well as the following well-known facts about the Legendre symbol

$$\left(\frac{-1}{p}\right) = 1 \quad \text{for } p = 4m + 1,$$

$$\left(\frac{2}{p}\right) = 1 \quad \text{for } p = 8m \pm 1, \qquad \left(\frac{3}{p}\right) = 1 \quad \text{for } p = 12m \pm 1,$$

from which we can conclude that the 10 quadratic partitions given in Table 1 have solutions if and only if p belongs to the corresponding residue classes modulo 24.

TABLE 1

Label	partition	residue classes of p	Label	partition	residue classes of p
(A')	$p = \xi^2 + \eta^2$	1 5 13 17	(F')	$-p = \xi^2 - 3\eta^2$	11 23
(B')	$p = \xi^2 + 2\eta^2$	1 11 17 19	(G')	$p = \xi^2 + 6\eta^2$	1 7
(C')	$p = \xi^2 - 2\eta^2$	1 7 17 23	(H')	$2p = \xi^2 + 6\eta^2$	5 11
(D')	$p = \xi^2 + 3\eta^2$	1 7 13 19	(I')	$p = \xi^2 - 6\eta^2$	1 19
(E')	$p = \xi^2 - 3\eta^2$	1 13	(J')	$-p = \xi^2 - 6\eta^2$	5 23

The details of the proof are given in two cases only; the other six cases are proved in the same way.

Suppose $n = 5$. If $p \equiv 1, 5, 13, 17$, so that $q \equiv 5, 1, 17, 13$; then, by (A'),

$$p = \xi_1^2 + \eta_1^2, \qquad q = \xi_2^2 + \eta_2^2.$$

Hence, (4) shows that $N = x^2 + y^2$ and so (A) has 2 solutions. Next, let

$$p \equiv 7, 11, \quad \text{so that} \quad q \equiv 11, 7.$$

Then, by (G') and (H'),

$$p \quad \text{or} \quad q = \xi_1^2 + 6\eta_1^2, \qquad 2q \quad \text{or} \quad 2p = \xi_2^2 + 6\eta_2^2.$$

Hence, by (4), $2N = x^2 + 6y^2$, so that (H) has 2 solutions. Finally, let $p \equiv 19, 23$ so that $q \equiv 23, 19$. Then, by (I') and (J'),

$$p \quad \text{or} \quad q = \xi_1^2 - 6\eta_1^2, \qquad -q \quad \text{or} \quad -p = \xi_2^2 - 6\eta_2^2.$$

Hence, by (4), $-N = x^2 - 6y^2$ so that J has 2 solutions. This disposes of the case $n = 5$. Next, suppose $n = 23$. If

$$p \equiv 1, 7, 17, 23, \quad \text{so that} \quad q \equiv 23, 17, 7, 1,$$

then, by (C′),

$$p \equiv \xi_1^2 - 2\eta_1^2, \qquad q = \xi_2^2 - 2\eta_2^2.$$

This implies (C) has 2 solutions. Next, if

$$p \equiv 5, 19, \quad \text{so that} \quad q \equiv 19, 5,$$

then, by (I′) and (J′),

$$p \quad \text{or} \quad q = \xi_1^2 - 6\eta_1^2, \qquad -q \quad \text{or} \quad -p = \xi_2^2 - 6\eta_2^2.$$

Hence, (J) has 2 solutions. Finally, let

$$p \equiv 11, 13, \quad \text{so that} \quad q = 13, 11.$$

We can now use (E′) and (F′) to show that (F) has 2 solutions. This completes the case $n = 23$.

In this theorem, we have used the quadratic characters modulo p of $(-1, 2, 3)$. Two other theorems hold in like manner for $(-1, 2, 5)$ and $(-1, 2, 11)$ but not for $(-1, 2, 7)$. The advantages to be expected for these larger values of D are offset by the larger values of T in (3), namely 9 and 10 for $D = 5$ and 11. Also, for 11, we need to use $\lambda = 4$. In either case, the inequalities (3) make the search for y more expensive on the average. In practice, the variable y in Eqs. (A) to (J) is often subject to further restrictions since N is known modulo 24. For example, in Case 1, $N \equiv 1 \pmod{24}$, Eq. (B) becomes

$$1 \equiv x^2 + 2y^2 \pmod{24}.$$

It would be wasteful of machine time not to observe that $y \equiv 0 \pmod 6$. So we should replace (B) by

$$N = x^2 + 72z^2 \quad \text{or} \quad N - 72z^2 = x^2.$$

Again, in Case 2, $N \equiv 5 \pmod{24}$, (H) becomes

$$2N = x^2 + 6(2z + 1)^2 \quad \text{or} \quad 2N - 6 - 24z - 24z^2 = x^2.$$

In each of these examples, we have stated the problem in the form: Find z for which $f(z)$ is a square. This is a standard formulation well suited to machine application and for which a corresponding general program has been written. In our case, $f(z) = a + bz + cz^2$. The theorem now tells us that, for each of the 8 cases of $N \pmod{24}$, there are 3 quadratics each with its own "time coefficient" t, namely

$$(5) \qquad a_1 + b_1z + c_1z^2;\ t_1, \qquad a_2 + b_2z + c_2z^2;\ t_2, \qquad a_3 + b_3z + c_3z^2;\ t_3,$$

such that at least one quadratic has two square values, for z in the range $0 < z < t\sqrt{N}$. Table 2 gives these coefficients.

T is a measure of the maximum possible cost in each of the eight cases of N modulo 24. Since $T \leqq 1$, we can assert that the number of values of y to be excluded is less than $\sqrt{N}$, even in the worst possible case and with the worst possible luck. In each column, the three labels have been arranged in order of increasing cost, i.e., length of run. This does not imply that one should necessarily begin with the top of the column and work down. We have found it expedient to choose that run, long or short, which best fits in with the operator's schedule, and to trust to luck.

TABLE 2

N modulo 24

	1	5	7	11	13	17	19	23
Label	B	J	G	F	D	A	B	F
a_1	N	α	N-6	γ	N-12	N	N-18	γ
b_1	0	β	-24	δ	-48	0	-72	δ
c_1	-72	24	-24	3	-48	-16	-72	3
t_1	.1179	.1495	.2041	.1298	.1443	.2500	.1179	.1298
Label	D	A	D	H	A	B	D	J
a_2	N	N-4	N-3	2N-6	N-4	N	N-3	α'
b_2	0	-16	-12	-24	-16	0	-12	β'
c_2	-48	-16	-12	-24	-16	-8	-12	24
t_2	.1443	.2500	.2887	.2887	.2500	.3536	.2887	.1495
Label	I	H	C	B	E	C	I	C
a_3	N	2N-6	N+2	N-2	N	N	N+6	N+2
b_3	0	-24	8	-8	0	0	24	8
c_3	24	-24	8	-8	3	8	24	8
t_3	.2887	.2887	.3536	.3536	.4082	.3536	.5773	.3536
T	.5509	.6882	.8464	.7721	.8025	.9572	.9839	.6329

$\alpha = 24g^2 + 24g - N + 6$, $\alpha' = 24g^2 - N$, $\beta = 48g + 24$, $\beta' = 48g$, where $g = 1 + [(N/24)^{1/2}]$, $\gamma = 3h^2 - N$, $\delta = 6h$, where $h = 1 + [(N/3)^{1/2}]$, $T = t_1 + t_2 + t_3$.

We conclude with three typical examples.

Example 1. $N = 1112\ 94469\ 43096\ 92244\ 41331$. This is a factor of the 196th term of the aliquot series 564, 780, 1572, $\cdots$. In this case, $N \equiv 11 \pmod{24}$. Hence, we use (B), (F) and (H). Choosing (H), the corresponding entry in Table 2 gives

$$2N - 6 - 24z - 24z^2 = x^2, \qquad z < .2887\sqrt{N} = 9.631 \cdot 10^{10}.$$

The DLS-157 gave the two solutions

$$z_1 = 10660233669, \qquad z_2 = 21061989605.$$

Thus,

$$2N = 468893980444^2 + 6 \cdot 21320467339^2 = x_1^2 + 6y_1^2$$

and

$$2N = 460371981244^2 + 6\cdot 42123979211^2 = x_2^2 + 6y_2^2.$$

Finally,

$$\mathrm{GCD}(N, x_1y_2 - x_2y_1) = 42492353748443,$$

so that

$$N = 2619164617\cdot 42492353748443.$$

Inspection of the actual factors modulo 24 shows any one of (B), (F) or (H) would have produced the factors of N. The use of (F) would have cost only one half as much as (H).

Example 2. $N = 141\ 50795\ 00009\ 74835\ 27291$. This is a factor of the 116th term of the aliquot series 840, 2040, 4440, $\cdots$. Since $N \equiv 11 \pmod{24}$, we have the same choice (B), (F) or (H) as in Example 1. This time, we choose (F) and find

$$h = 1 + \left[\left(\frac{N+1}{3}\right)^{1/2}\right] = 68679921861,$$

$$\gamma = 3h^2 - N = 401713482672,$$

$$\delta = 6h = 412079531166.$$

The sieve set up is then

$$\gamma + \delta z + 3z^2 = x^2 \quad \text{with} \quad 0 < z < .1298\sqrt{N} = 1.544\cdot 10^{10}.$$

The sieve gave the two solutions

$$z_1 = 2126046669, \qquad x_1 = 29827177847,$$

$$z_2 = 7295140817, \qquad x_2 = 56265757319.$$

Setting

$$y_1 = h + z_1 = 70805968530,$$

$$y_2 = h + z_2 = 75975062678,$$

we have

$$N = 3y_1^2 - x_1^2 = 3y_2^2 - x_2^2.$$

Finally,

$$\mathrm{GCD}(N, x_1y_2 - x_2y_1) = 16490417759.$$

Hence,

$$N = 16490417759\cdot 858122286949.$$

Example 3. $N = 472\ 42657\ 53388\ 82684\ 96419$. This is a factor of the 146th term of the aliquot series 966, 1338, 1350, $\cdots$. Since $N \equiv 19 \pmod{24}$, we have to consider (B), (D) and (I). Failing to obtain solutions for (B) and (D), we finally attempted (I). This gave four solutions of the equation

$$N + 6 + 24z + 24z^2 = x^2, \qquad z \leqq .5773\sqrt{N} = 1.2548\cdot 10^{11};$$

namely,

$$z_1 = 8318338075, \qquad x_1 = 221140976515,$$
$$z_2 = 8685150349, \qquad x_2 = 221479167445,$$
$$z_3 = 12687057797, \qquad x_3 = 226065769163,$$
$$z_4 = 13062176867, \qquad x_4 = 226577908637.$$

With $y_i = 2z_i + 1$, we have

$$N = x_i^2 - 6y_i^2 \qquad (i = 1, 2, 3, 4).$$

The GCD$(N, x_1y_i - x_iy_1)$, $i = 2, 3, 4$, give the following factorizations of N:

$$N = 1638023 \cdot 28841266291064453,$$
$$N = 13401284539 \cdot 3525233524921,$$
$$N = 2152127 \cdot 21951612304426397.$$

This redundant information gives

$$N = 1638023 \cdot 2152127 \cdot 13401284539,$$

a product of three primes.

This illustrates that, although our Theorem applies to products of only two primes, the method may well work in other cases. In general, the number of solutions, if any, of Eq. (2), satisfying the inequalities (3), is 2^{k-1}, where k is the number of distinct prime factors of N. The success of run (I) is due to the fact that two of the prime factors of N are congruent to 23 and the other to 19 modulo 24, so that all three are covered by (I′) and (J′). Had all three runs failed to give solutions, we would have concluded that N is a product of three or more primes. Were our project adequately supported, we would normally search directly for prime factors less than the cube root of N before applying the Theorem.

An alternative to this expensive search is the use of additional forms. By splitting the four cases of N modulo 5, it can be shown that the factorization of $N = pqr$ can be achieved by using at most four additional forms. This prospect will be more pleasant with the advent of our new model sieve, the SRS-181, which is faster than the DLS-157 by a factor of 20.

It will be observed that, for $N \not\equiv 1 \pmod{24}$, the three forms specified in our Theorem are not only sufficient but are forced on us. The same fact holds for the 4 additional forms mentioned above in case $N \not\equiv 1$ or $49 \pmod{120}$. [See Appendix.]

Economic considerations of this kind also enter into the problem of testing N for primality. It is very cheap to test whether N is a pseudoprime (i.e., $a^N \equiv a \pmod{N}$); in fact, the cost is only $O(\log N)$. To complete the proof of the primality of a pseudoprime, one must at least partially factor $N - 1$ or $N + 1$ [7]. This could be expensive by direct search. One could alternatively apply the above method to the result of removing the small factors, say <10000, from $N \pm 1$. A cheaper and more direct alternative is to obtain a unique representation of λN by a quadratic form. Any of those specified in Table 2, preferably the one with least t, will suffice. For this application, there may be a still cheaper quadratic form available, such as

$$(6) \qquad 4N = x^2 + 163y^2 \quad \text{if} \quad (N/163) = 1, \qquad y < .15665\sqrt{N}.$$

TABLE 3

n / D	5	7	11	13	17	19	23
-1	1			1	1		
-2			1		1	1	
2		1			1		1
-3		1		1		1	
3			-1	1			-1
-6	2	1	2				
6	-1					1	-1

Example 4. $N = 6\ 17887\ 90759\ 27253\ 99713$. This is a factor of the 187th term of the aliquot series 564, 780, 1572, $\cdots$. Here $(N/163) = 1$. We find by [11] that $N = x^2 + 144 \cdot 163y^2$. The sieve gives

$$x = 16270722841, \qquad y = 122660709$$

as the only solution with $y < 1.6225 \cdot 10^8$. Hence, N must be a prime.

Appendix. The same methods involving determinants D dividing 24 can be applied to the 15 square free divisors of 120. This gives an improved set of binary quadratic forms.

The information in our Theorem can be presented in tabular form by means of Table 3 which is a 7×7 matrix whose nonzero elements are the multipliers λ in (2) that go with the corresponding D and n. We have omitted the column for $n = 1$.

We note that, in each line (i.e., row or column), there are three nonzero elements and that every pair of parallel lines has just one nonzero element in common. This feature is characteristic of the so-called Steiner triple system (7, 3, 1) [10].

TABLE 4

n	103	59	37	113	91	47	101	79	89	67	77	109	119	97	107
D	7	11	13	17	19	23	29	31	41	43	53	61	71	73	83
-1			1	1			1		1		1	1		1	
-2		1		1	1				1	1				1	1
2	1			1		1		1	1				1	1	
-3	1		1		1			1		1		1		1	
3		-1	1			-1						1	-1	1	-1
-5	2					2	1		1	2		1			2
5		1			1		1	1	1			1	1		
-6	1	2					2	1			2			1	2
6					1	-1	-1			1	-1		-1	1	
-10	2	1	2		1	2			1		2				
10			2					1	1	2	2		1		2
-15				3	1	3		1			3	1			3
15	3	-1		-3						3	-3	1	-1		
-30		5	3	2		2	5	1		3					
30	-2		-2	2	1		-1						-1		2

TABLE 5

n	λ_1 F_1	t_1	λ_2 F_2	t_2	λ_3 F_3	t_3	τ
1,49	1 (N, 0, -240)	.06455	1 (N, 0, -72)	.11786	1 (N, 0, 120)	.20413	.17451
7,103	-2 (α_2, β_2, 120)	.18713	1 (N-6, -24, -24)	.20413	2 (2N-5,-20,-20)	.31623	.36825
11,59	-1 (α_3, β_3, 3)	.12976	1 (N-10,-40,-40)	.15812	5 (5N-30,-120,-120)	.20413	.25985
13,37	1 (N-12,-48,-48)	.14434	-2 (α_2, β_2, 120)	.18713	2 (2N-10,-40,-40)	.22361	.29381
17,113	2 (2N-30,-120,-120)	.12911	1 (N, 0, -16)	.25000	2 (2N+30, 120, 120)	.28868	.32628
19,91	1 (N-18 , -72, -72)	.11786	1 (N-15, -60, -60)	.12911	1 (N+30, 120, 120)	.20413	.23345
23,47	2 (2N-45,-180,-180)	.10541	3 (3N-60,-240,-240)	.11181	-1 (α_3, β_3, 3)	.12976	.19376
29,101	-1 (α_4, β_4, 120)	.13232	-1 (α_6, β_6, 24)	.14943	1 (N+20, 80, 80)	.22361	.26294
31,79	1 (N-30,-120,-120)	.09129	1 (N+90, 360, 360)	.15812	1 (N-3, -12, -12)	.28868	.24252
41,89	1 (N, 0, -40)	.15812	1 (N, 0, 80)	.22361	1 (N, 0, -8)	.35356	.35832
43,67	1 (N-18,-72,-72)	.11786	3 (3N, 0, -120)	.15812	3 (3N, 0, 15)	.54773	.33385
53,77	-1 (α_6, β_6, 24)	.14943	3 (3N-15, -60, -60)	.22361	2 (2N-10, -40,-40)	.22361	.31714
61,109	1 (N-60,-240,-240)	.06455	1 (N-12, -48, -48)	.14434	1 (N+20, 80, 80)	.22361	.19262
71,119	-1 (α_3, β_3, 3)	.12976	-1 (α_1, β_1, 24)	.14943	1 (N+2, 8, 8)	.35356	.29287
73,97	1 (N, 0, -72)	.11786	1 (N, 0, -48)	.14434	1 (N, 0, 24)	.28868	.26220
83,107	2 (2N-45,-180,-180)	.10541	3 (3N, 0, -240)	.11181	-1 (α_3, β_3, 3)	.12976	.19376

$$g_1 = 1 + \left[\sqrt{\frac{N}{24}}\right] \quad g_3 = 1 + \left[\sqrt{\frac{N}{3}}\right] \quad \alpha_1 = 24g_1^2 - N,\ \beta_1 = 48g_1 \quad \alpha_3 = 3g_3^2 - N,\ \beta_3 = 6g_3$$

$$g_2 = 1 + 2\left[\sqrt{\frac{N}{60}}\right] \quad g_4 = 1 + 2\left[\sqrt{\frac{N}{120}}\right] \quad \alpha_2 = 30g_2^2 - 2N,\ \beta_2 = 120g_2 \quad \alpha_4 = 30g_4^2 - N,\ \beta_4 = 120g_4$$

$$g_6 = 1 + 2\left[\sqrt{\frac{N}{24}}\right] \quad \alpha_6 = 6g_6^2 - N,\ \beta_6 = 24g_6$$

As we have noted, in order to treat the case in which N may be the product of up to three primes, we can introduce the prime 5 and consider the appropriate determinants D which divide 120. In this case, seven forms are required for each $n \equiv N \pmod{120}$ and these are forced when $n \not\equiv 1, 49$.

Table 4, the counterpart of Table 3, gives the multipliers λ by means of a 15×15 matrix.

Again, we note that in each line of this matrix there are seven nonzero elements and each pair of parallel lines has just three elements in common. This gives us one of the (15, 7, 3) Steiner systems [10], with the additional feature that, out of the seven elements in each column, three can be chosen in just seven different ways so that the product of the three chosen determinants is a square. Any one of these sets of three determinants with their multipliers λ constitute a triple of forms (2) that could be substituted for the triple suggested by our Theorem for a given n. Table 5 gives for each n (mod 120) the most efficient triple of polynomials F_1, F_2, F_3. Instead of using the total T of maximum time factors,

$$T = t_1 + t_2 + t_3$$

(representing the worst possible luck), as a measure of goodness, we have adopted the more sophisticated "expected time factor"

$$\tau = t_1 + \tfrac{1}{2}t_2 + \tfrac{1}{4}t_3 \qquad (t_1 \leqq t_2 \leqq t_3)$$

as a measure of efficiency of a triple of forms, resulting in a considerable improvement. In fact, of the 32 values, all but $n = 71, 73, 97$ and 119 are improved by the consideration of determinants modulo 120.

In the general case, in which N may be the product of t distinct primes, one chooses $2^t - 1$ determinants $D \not\equiv 1$ dividing $M_t = 2p_2p_3 \cdots p_t$ where the p's are distinct odd primes. N must be considered modulo $4M_t$. The $2^{t+1} - 1$ by $2^{t+1} - 1$ matrix of λ's corresponding to Tables 3 and 4 will have $2^t - 1$ nonzero elements in each line, and every pair of parallel lines will have $2^{t-1} - 1$ elements in common. This gives a Steiner system $(2^{t+1} - 1, 2^t - 1, 2^{t-1} - 1)$.

Although the structure of this general system is independent of the choice of the p's, it behooves us, for practical reasons, to limit not only t, but also the size of p_t, in order that all the determinants dividing M_t have small class numbers.

Our best thanks are due to Richard Guy, John Selfridge, and Daniel Shanks for valuable suggestions and corrections in the manuscript.

Mathematics Department
University of California
Berkeley, California 94720

1. J. D. Brillhart & M. A. Morrison, "The factorization of F_7," *Bull. Amer. Math. Soc.*, v. 77, 1971, p. 264. MR **42** #3012.

2. P. L. Chebyshev, "Sur les formes quadratiques," *J. Math.* (1), v. 16, 1851, pp. 257–282.

3. L. E. Dickson, *History of the Theory of Numbers.* Vol. 1, Washington, 1919, Chap. 14.

4. R. K. Guy & J. L. Selfridge, "Interim report on aliquot series, *Conf. Numerical Mathematics, Winnipeg 1971*, pp. 557–580.

5. D. H. Lehmer, "An announcement concerning the Delay Line Sieve DLS127," *Math. Comp.*, v. 20, 1966, pp. 645–646.

6. D. H. LEHMER, "The sieve problem for all-purpose computers," *Math. Tables and Other Aids to Computation*, v. 7, 1953, pp. 6–14. MR 14, 691.

7. D. H. LEHMER, *Computer Technology Applied to the Theory of Numbers*, Studies in Number Theory, Math. Assoc. Amer. (distributed by Prentice-Hall, Englewood Cliffs, N.J.), 1969, pp. 117–151. MR 40 #84.

8. G. B. MATHEWS, *Theory of Numbers*, Cambridge, 1892; reprint, New York, 1961, pp. 261–270.

9. D. SHANKS, *Class Number, A Theory of Factorization and Genera*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R.I., 1970, pp. 415–440.

10. J. A. TODD, "A combinatorial problem," *J. Mathematical Phys.*, v. 11, 1932, pp. 321–333.

11. EMMA LEHMER, "On the quartic character of quadratic units," *J. Reine Agnew. Math.* (To appear.)