SQUFOF notes

Daniel Shanks*

Contents

1 Introduction

This algorithm is called SQUFOF, which stands for Square-Form Factorization. It is based upon the theory of real quadratic fields, including the concept of the infrastructure of such fields [Sh1]. The final sentence in [Sh1] alludes to such an algorithm but it was not developed at that time.

In January 1975, I gave a talk [Sh2] entitled "Analysis and Improvement of the Continued Fraction Method of Factorization." The powerful method referred to is that of Brillhart and Morrison which was just about to appear in the Lehmer Jubilee. issue of Math. Comp. [BM]. We abbreviate their algorithm as BRIMOR. Its appearance in that issue was particularly appropriate since it is based upon the much earlier pre-computer method of Lehmer and Powers [4]. In this introduction, I will give.

*Handwritten notes of Shanks' main paper on SQUFOF - never completed - circa 1975-1985. Typed into latex by Stephen McMath [S.M.], March, 2004. Underline for emphasis is in italics. Underline for definitions is in bold. Equation numbers and section numbers match the original. (*) used as symbol for composition of forms while $(\cdot)$ is used for all other multiplication symbols. The rationals are denoted by $\mathbb{Q}$.

1. A brief sketch of BRIMOR,

2. The three salient points in my critique of BRIMOR [Sh2].

3. An account of how the development of SQUFOF was resumed after a six-month delay, because of the pathological response that BRIMOR made when it was used to factor the composite:

$$N_0 = 2^{60} + 2^{30} - 1 \tag{1}$$

This last episode, with its mildly comic aspect, then leads us directly to the algorithm SQUFOF for factoring integers N.

Before I launch into this developmental account of SQUFOF, it seems desirable to list its several characteristics as follows:

A. It is an $O(N^{1/4})$ algorithm.

B. Essentially all numbers in the arithmetic are half-precision, specifically, they are $< 2\sqrt{N}$.

C. It has a very simple, short program.

D. Very little memory is needed.

E. Its theory is based upon that of the period of reduced binary quadratic forms of discriminant $4N$.

After we have SQUFOF before us, it will be appropriate to return to these five characteristics and give them a detailed commentary.

Briefly, this is BRIMOR. N is a large odd number to be factored. Its square-root is expanded in a regular continued fraction:

$$\sqrt{N} = q_0 + \frac{1}{q_1+} \; \frac{1}{q_2+} \; \frac{1}{q_3+} \; ... \tag{2}$$

The q_n are positive integers with

$$q_0 = \lfloor \sqrt{N} \rfloor, \tag{3}$$

and subsequent q_n, together with the associated integers P_n and Q_n, are evaluated by the starting values:

$$Q_0 = 1,\ P_1 = q_0,\ Q_1 = N - q_0^2 \tag{4}$$

and the recurrences

$$q_n = \lfloor \frac{q_0 + P_n}{Q_n} \rfloor, \tag{5}$$

$$\begin{aligned} P_{n+1} &= q_n Q_n - P_n \\ Q_{n+1} &= Q_{n-1} + q_n(P_n - P_{n+1}) \end{aligned} \tag{6}$$

These formulas are well-known, but while we need the same P_n andQ_n in SQUFOF, we record them at once and let them serve both purposes.

Also well-known are A_n and B_n with

$$A_0 = 1,\ B_0 = 0,\ A_1 = q_0,\ B_1 = 1 \tag{7}$$

and the recurrences[1]

$$A_{n+1} = A_n q_n + A_{n-1},\ B_{n+1} = B_n q_n + B_{n-1}. \tag{8}$$

The key relationship for BRIMOR is

$$(-1)^n Q_n = A_n^2 - B_n^2 N \tag{9}$$

The A_n and B_n grow exponentially; we reduce $A_n \pmod N$:

$$\overline{A}_n \equiv A_n \pmod N, \tag{10}$$

ignore the B_n, and have

$$(-1)^n Q_n \equiv \overline{A}_n^2 \pmod N \tag{11}$$

Since

$$P_n, Q_n < 2\sqrt{N}, \qquad \overline{A}_n < N, \tag{12}$$

the former are half-precision numbers while the latter are full-precision.

With a fixed set of trial-divisor primes $p_1 = 2$, $p_2 = 3$, ... p_k, (k dependant on N), BRIMOR factors those Q_n that it can, discards the others, and saves $\overline{A}_n$ for each factored Q_n. The index n is increased until BRIMOR can assemble subsets of these Q_n into products that are perfect squares:

[1]Shanks wrote $B_{n+1} = B_n q_n + q_{n-1}$, but he certainly knew better. [S.M.]

$$\prod_{\text{some n}} (-1)^n Q_n = Q^2 \tag{13}$$

and if

$$A = \prod_{\text{same n}} \overline{A}_n \tag{14}$$

we have

$$N \mid Q^2 - A^2 = (Q - A)(Q + A) \tag{15}$$

If

$$N \nmid (Q - A) \text{ and } N \nmid (Q + A), \tag{16}$$

we call Q^2 a **proper square** and the GCD

$$D = (Q - A, N) \tag{17}$$

is a proper divisor of N. If (16) is not satisfied, Q^2 is an **improper square** and BRIMOR assembles another square and tries again. If the reader wants a fuller account of BRIMOR, then he should read [3].

For that which follows, we single out four features of BRIMOR: two are "peculiar" and two are "disappointing".

It seems peculiar that while most of the arithmetic is half-precision since it involves the P_n and Q_n in (12), that which involves $\overline{A}_n$ is full-precision or multi-precision. Further, these larger numbers $\overline{A}_n$ must also be stored.

Secondly, the condition (16) as to whether a particular Q^2 is proper or not remains completely mysterious here and is only determined (after the fact) by computing D in (17). The authors of BRIMOR [3] are pragmatic. Inasmuch as the whole thing is automatic, it does no harm if the machine finds a few improper squares prior to a proper square. In fact, it alone might even know that it did so. The factor arrives; that is what we want. Still, a mathematician wants to know what is happening. And if one encounters a very long sequence of improper squares, he may even need to know.

BRIMOR is a powerful algorithm for factoring large N - say those of about 40 decimals, and if $N = f_1 f_2$ with both factors large, it is the fastest algorithm known at this time. Nonetheless, two principal features are disappointing. Most of the time is spent in trial-and-error division of the Q_n by

the p_i. This does seem rather crude in contrast with the sophistication of the rest of the algorithm. Secondly, much memory is needed to store the large parity matrix $a_{ni} \pmod 2$, which records the parity of the exponent of each $p_i^{a_{ni}}$ that divides each of the factored Q_n. These are needed in assembling the Q_n into squares Q^2. Obviously, space is money, and much space makes it harder for the routine to squeeze onto a time-sharing computer.

These four features of BRIMOR set the stage for my table [Sh2] mentioned above. In [Sh2] we use the *very same* P_n and Q_n that are in BRIMOR but we interpret them as the coefficients of binary quadratic forms, and do not use the language of continued fractions. This change of view makes the theory of real quadratic fields available to us, both the classical theory and modern additions, and this gives us some new insights that do not appear when we confine ourselves to the theory of continued fractions. The two main conclusions that [Sh2] thereby obtained concern the two "peculiar" features given above:

1. The A_n are *not needed at all.* We need not compute them (8), reduce them (10), store them, multiply them (15), or use them in (16). This seems very surprising, since (16) is the heart of BRIMOR, and a Q without an A in (16) looks like a question without an answer. Nonetheless, it is true; the A_n are not needed.

2. We *can predict* a priori whether a given square (14) is proper or not, and if the number of factors on the left of (14) is not too large it is quite feasible to do so.

So the alternative viewpoint in [Sh2] satisfactorily clarifies both of the peculiar features in BRIMOR. In the title of [Sh2] appears the word "Improvement". If we need not compute the A_n, and can bypass the improper squares that fail (17), there is some saving in time, and since the full-precision $\overline{A}_n$ need not be stored, there is also saving in memory. (Of course, other operations are needed to take their place, and these would have to be taken into account.) But the practitioners of BRIMOR said that these savings would be *relatively small* since

(a) Most of the time is taken in factoring the Q_n by the p_i, and

(b) Most of the space is taken by the parity matrix $a_{ni} \pmod 2$, and therefore the proposed, potential savings in time and space would be relatively small.

Thus, my proposed "improvements", based upon an analysis of the two peculiar features of BRIMOR, were frustrated by the two disappointing features of BRIMOR. I had not proposed, in [Sh2], to alter these two latter, and there they stood, like twin dragons, guarding the gate and resistant to progress.

So [Sh2] has not yet been published, the "improvements" it suggested have not been programmed, and some months went by. Now we come to the funny part.

A man, name unknown to me, came up with the following, implausible conjecture: If M_{p_1} and M_{p_2} are successive Mersenne primes, their arithmetic mean is also a prime. While that is true for $\frac{7+31}{2} = 19$, $\frac{31+127}{2} = 79$, etc., Brillhart and friends examined the 19-digit $N_0 = \frac{M_{31}+M_{61}}{2}$, given in (1), and found that it failed a Fermat test since

$$13^{N_0-1} \not\equiv 1 \pmod{N_0}.$$

Therefore, it is composite, but when they tried to factor N_0 by BRIMOR it gave them 114 successive improper squares. The procedure in such a case is to halt execution and begin again with kN_0 for some small multiplier k. No further pathology was encountered and they did factor N_0.

Let us define **practical failure** and **absolute failure**. In a case such as the foregoing, there is no point in continuing execution since there may well be thousands of improper squares still to come, and it is faster to simply restart with kN. When there is such an *excessive* number of improper squares, we say that we have a practical failure. If the period of the continued fraction is very short, say, for such N as $N = M^2 + 1$, there may be no proper square *at all*. We call that an absolute failure, and the remedy is the same: restart with kN. SQUFOF also has such absolute failures but it does not have practical failures.

Brillhart asked me if my [Sh2] could explain why N_0 causes a practical failure and whether, perhaps, it could even be an absolute failure. The answer to the first question is "Yes", that is easy to understand. We have an early Q_n that is exceptionally small (relative to $\sqrt{N}$). Specifically, $Q_2 = 5$, and, as will be seen below, this leads to an immense number of improper squares. In fact, *any*

$$N = M^2 + M - 1 \tag{18}$$

with a very large M will behave the same way; the specific $M = 2^{30}$ is not

the problem. This quadratic has discriminant 5 and that is where $Q_2 = 5$ is coming from. More generally, any

$$N = M^2 + a \quad \text{or} \quad N = M^2 + M + a \tag{19}$$

with M large and the discriminant small will behave the same way. Luckily, most N are not of this type - nonetheless, such numbers are often of specific interest to number-theorists.

Concerning Brillhart's second question, I felt that the answer would be "no" - N_0 does not lead to absolute failure, but to prove this I had only a hand-held HP-65 with its very small memory (100 steps in the program). Obviously, one cannot put the huge BRIMOR on such a machine. But one can put on the simple algorithm in (4)-(6) for computing the Q_n and P_n, and *simply wait* for a Q_n that is a *proper square*. The first such is

$$Q_{162146} = 28185^2 \tag{20}$$

By the criterion alluded to above, which *simplifies greatly* when the square in (13) contains *only one factor*, we know, *at once*, that Q_{162146} is a proper square and that earlier square Q_n that had appeared, including

$$\begin{aligned} Q_{50194} &= 28063^2, \\ Q_{63516} &= 22065^2, \\ Q_{69730} &= 28919^2, \\ Q_{149926} &= 10131^2, \end{aligned} \tag{21}$$

were improper squares. No A_n were computed, but, as stated above, they are not needed. So, from (20), and without the corresponding $\overline{A}_{162146}$, we do factor the N_0 as

$$N_0 = 139001459 \cdot 8294312261 \tag{22}$$

even though the HP-65 only computes with 10-digit numbers. The two factors in (22) are prime and further details are given below after we have SQUFOF before us.

Note the course of events: The twin dragons would not enter the HP-65 since they were too large. In their absence, the elimination of the A_n and the determination of the property of the Q^2, are no longer marginal possibilities. Now they come to the front as essential features of the new algorithm.

Obviously, we must go to longer indices n to find $(-1)^n Q_n$ that are *already* square rather than those of the Q_n in (13) that are *assembled* into

squares. But it might be said (qualitatively) that we can afford to do so, since we merely compute the Q_n and P_n by the very simple (4)-(6) and completely omit all of the complex logistic in BRIMOR. The crucial quantitative questions are these:

(α) What is the *mean* index - difference Δn between successive squares $(-1)^n Q_n$?

(β) What is the probability P that these squares are proper squares?

We shall see that if N has $1+k$ distinct prime divisors, then

$$\Delta n = 1.77491 \frac{\sqrt[4]{N}}{2^k} \tag{23}$$

is the answer to (α), where the constant is

$$1.77491... = (\log 8)\frac{2+\sqrt{2}}{4}. \tag{24}$$

The answer to (β) is

$$P = \frac{2^k - 1}{2^k} \tag{25}$$

where the *probable* Δn between *proper* squares is

$$\Delta n = 1.77491 \frac{\sqrt[4]{N}}{2^k - 1} \tag{26}$$

This clearly relates to the first characteristic of SQUFOF listed above, namely:

A. It is an $O(N^{1/4}$ algorithm.

This shows that SQUFOF is a practical algorithm; we will return to all five characteristics later.

2 SQUFOF without a list

SQUFOF has many possible variants; the one to be selected depends largely on the size of N and the size of the computer available. For simplicity, I will give the basic algorithm first, and defer the variants, such as "fast return", "fast list-test", "odd discriminant", etc., until later.

The P_n and Q_n generated by (4)-(6) have the invariant

$$N = P_n^2 + Q_{n-1}Q_n \qquad (\text{all } n) \tag{27}$$

Therefore, the quadratic form

$$F_n = (-1)^{n-1}Q_{n-1}x^2 + 2P_nxy + (-1)^nQ_ny^2 \tag{28}$$

has the discriminant $4N$. We abbreviate F_n by writing its coefficients in Gauss's notation with the factor 2 suppressed:

$$F_n = ((-1)^{n-1}Q_{n-1}, P_n, (-1)^nP_n). \tag{29}$$

So we have

$$F_1 = (Q_0, P_1, -Q_1), \quad F_2 = (-Q_1, P_2, Q_2),$$
$$F_3 = (Q_2, P_3, -Q_3), \quad F_4 = (-Q_3, P_4, Q_4), \ \textit{etc.}$$

The F_n constitute the **principal period of reduced forms** of discriminant $4N$, namely, from (4), those generated by

$$F_1 = (1, q_0, q_0^2 - N) \tag{30}$$

These are periodic and for some *even* π, we would have

$$F_\pi = (q_0^2 - N, q_0, 1), \tag{31}$$

the reversal of F_1. Then

$$F_{\pi+1} = (1, q_0, q_0^2 - N) = F_1$$

It is convenient to rename F_π as F_0 and begin the period with F_0, not F_1.

To save space and time, consider the forms strung together in this fashion:

$$
\begin{array}{lll}
-Q_1 & & \\
 & P_1 & \leftarrow F_0 \\
 & 1 & \\
 & P_1 & \leftarrow F_1 \\
-Q_1 & & \\
 & P_2 & \leftarrow F_2 \\
 & Q_2 & \\
 & P_3 & \leftarrow F_3 \\
-Q_3 & & \\
 & . & \\
 & . & \\
 & . & \\
A & B & C
\end{array}
$$

We could store the successive forms in only three registers: A, B, C. Begin with $(-Q_1, P_1, 1)$ in (A, B, C). Compute P_1 and $-Q_1$ for F_1 and store them in B, A, leaving C intact. Compute P_2 and Q_2 for F_2 and store them in B, C, leaving A intact, etc.

We are looking for a square form. This is a form F_n with

$$(-1)^n Q_n = S^2, \tag{32}$$

a perfect square. The index n must be even. The A_n have not been computed and are not needed since, by the *reverse sequence* to be defined presently, F_n leads us to a positive factor of N:

$$0 < f < N, \qquad f|N. \tag{33}$$

The probability that f is a proper factor, that is, that $f > 1$, is given in (25).

In section 4, we define the *list* (in two different variants). Then we will have:

- f is a proper factor,
- S^2 is a proper square,

if S is not in the list. We are deliberately postponing the list for clarity of exposition, and because SQUFOF without the list does have utility, and is an even simpler algorithm.

So suppose

$$F = F_n = (-Q, P, S^2) \tag{34}$$

and consider the form

$$F^{-1/2} = (-S, P, SQ). \tag{35}$$

We explain the notation later. It has the same discriminant but may not be reduced. We reduce it by

$$R_0 = P + S\lfloor \frac{q_0 - P}{S} \rfloor, \tag{36}$$

$$S_{-1} = S, \quad S_0 = \frac{N - R_0^2}{S}, \tag{37}$$

$$G_0 = (-S_{-1}, R_0, S_0). \tag{38}$$

Then G_0 is a reduced form equivalent to $F^{-1/2}$. It generates the reverse sequence:

$$G_m = ((-1)^{m-1} S_{m-1}, R_m, (-1)^m S_m) \tag{39}$$

by exactly the same formulas:

$$s_m = \lfloor \frac{q_0 + R_m}{s_m} \rfloor \tag{5a}$$

$$R_{m+1} = s_m S_m - R_m, \; S_{m+1} = S_{m-1} + s_m(R_m - R_{m+1}). \tag{6a}$$

In the reverse sequence, we are looking for a **symmetry point**, given by the condition

$$R_m = R_{m+1} \tag{40}$$

We then have

$$\begin{array}{ccc} -S_{m-1} & & S_{m-1} \\ R_m & & R_m \\ S_m & \text{or} & -S_m \\ R_m & & R_m \\ -S_{m-1} = -S_{m+1} & & S_{m+1} = S_{m-1} \end{array}$$

The condition (40) will be met for an index m approximately equal to $n/2$ for the n in (34) if n is sufficiently large. The reader need not worry about the vagueness of this

$$m \approx n/2 \tag{41}$$

since we are not using it operationally to find (40). Further, we later have a measure called the *infrastructure distance* for which the length of $S_m - S_0$ is exactly $1/2$ of the length of $Q_n - Q_0$.

By (6a), $R_m = s_m S_m/2$, and the invariant of $N = R_m^2 + S_{m-1}S_m$ gives us

$$N = S_m(S_{m-1} + S_m \frac{s_m^4}{4}) \tag{42}$$

If S_m is odd, it is the asserted factor f. If S_m is even, $S_m/2$ is the asserted factor f. See: no A_n!

Now consider an example.

$$N_1 = 13290059,\ q_0 = \lfloor \sqrt{N_1} \rfloor = 3645$$
$$F_0 = (-4034, 3645, 1).$$
$$F = F_{52} = (-5107, 3628, 5^2)$$

is the first square form. So

$$F^{-1/2} = (-5, 3628, 25535),$$

and

$$G_0 = (-5, 3643, 3722).$$

Then,

$$G_{25} = (571, 3119, -6238)$$
$$G_{26} = (-6238, 3119, 571),$$
$$m = 25 \approx \frac{1}{2}52,\ R_{25} = R_{26} = 3119,\ f = 3119,$$

and

$$N_1 = 3119 \cdot 4261.$$

Since the factors are prime, $k = 1$. The first square, Q_{52}, is already proper, and by (25) and (26) we may characterize N_1 as a slightly lucky example.

A digression: N_1 is an appropriate first example since it is given in both [3] and [4]. Further [4], it is a factor of the 55th term of the aliquot series for 276. Since [5, p. 218] aliquot series usually grow fairly rapidly, they produce larger and larger N and require stronger and stronger factorization methods. When Henri Cohen was still a microbiologist in Berkeley, he told me that he had used up much machine-time in computing amicable numbers and in extending [6] the notorious aliquot series for 276. I told him to show it to Lehmer. The recent developments in factorization were first beginning and I know that Lehmer could not resist extending 276 still further. Richard Guy soon organized an international factorization cartel and all of the new methods, including SQUFOF and any earlier [7] CLASNO, were extensively exercised in following this and that aliquot series into the wild blue yonder, [8],[9].

Now consider $N_2 = 42854447$. We have $F_0 = (-4331, 6546, 1)$, $F_{316} = (-6022, 5093, 53^2)$. Absent a list, we do not know if 53^2 is proper, but its reverse sequence gives us $f = 1$ and so we find, after the act, that it is not. All versions of SQUFOF save the last square form and q_0, and so we can return to F_n and continue. We find, close by,

$$F_{332} = (-3382, 6515, 11^2)$$

but its reverse sequence also gives $f = 1$ and so Q_{332} is also improper. Then

$$F_{380} = (-11134, 6401, 13^2),$$
$$F_0 = (-13, 6544, 2347),\ G_{172} = (-2633, 4423, 8846)$$
$$R_{172} = R_{173} = 4423,\ f = 4423,\ and$$
$$N_2 = 4423 \cdot 9689.$$

The reader may recognize these factors as primes and so $k = 1$ again and, by (25), N_2 is a somewhat unlucky example. In the next section, we will return to its improper Q_{316} and Q_{332}.

When I gave my HP-67 SQUFOF to Lenstra his first example was

$$N_3 = 11213 \cdot 19937 = 223553581,$$

and he was surprised to find that $f = 11213$ came back almost at once, (namely, $n = 6$, $m = 2$). He assumed that there must be a trick. In fact, since he had just multiplied the two factors, the multiplier 19937 would still

be in the register called LAST X. If we prefaced SQUFOF with a few steps that examined LAST X, this cofactor 19937, and then f, would have been found at once. However, there was no such preface; N_3 is simply a lucky example.

We will return to luck and to other interesting N after we have developed the theory.

3 The Ambiguous Periods and their Infrastructure

We return to N_2 and determine why Q_{332} and Q_{316} were improper. From $F_{332} = F$ above we have

$$G_0 = (-11, 6537, 11098).$$

Then

$$G_{452} = (-4331, 6546, 1), G_{153} = (1, 6546, -4331),$$

$m = 152$, and $S_{152} = 1 = f$. But G_{153} is merely F_0 read backwards. Now the recursions (4)-(6) or (6a) are *reversible* and may be used for n (or m) either increasing or decreasing. It follows that G_0 is merely F_{153} read backwards and in this G_m sequence, we are merely retracing our steps to the symmetry point $S_{152} = Q_0 = 1$. We verify that in Table I which gives some of the forms in the principal period: those for $n = 0$ through 7, followed by others of interest. The period is $\pi = 886$, and, since $F_{886} = F_0$ is F_1 read backwards, we have a second symmetry point at $n = 443 = 886/2$ where we find $Q_{443} = 4423$.

For $F = F_{332}$, the operation $F^{-1/2}$ jumps backwards "about half-way" to F_{153} and turns around to become G_0. The reader may protest, as in (41) that

$$153/332 \approx 1/2$$

is not very accurate, and so we direct his attention to the infrastructure distances d_n between Q_0 and Q_n that are listed in Table I. Here

$$d_{153} = d_{332}/2 \tag{43}$$

is exact.

Table 1 Principal period F_n for N_2

n		F_n		d_n
0	-4331	6546	1	0.0000000
1	1	6546	-4331	5.2930050
2	-4331	6447	298	7.7298729
3	298	6367	-7771	9.8682646
4	-7771	1404	5261	10.0861182
5	5261	3857	-5318	10.7625349
6	-5318	1461	7657	10.9895336
7	7657	6196	-583	12.7864371
73	3146	5585	-3707	95.7405234
142	-5507	6524	53	182.3677642
153	11098	6537	-11	195.1542013
252	-12731	6521	26	295.8354933
316	-6022	5093	53^2	364.7355284
325	1682	6471	-583	377.5219655
332	-3382	6515	11^2	390.3084026
364	-1279	6525	218	425.2186554
380	-11134	6401	13^2	446.5023708
405	2113	6513	-206	471.3639976
443	5266	4423	-4423	519.0866787
444	-4423	4423	5266	519.9077373
481	5137	6465	-206	566.8093597
506	-7942	6443	13^2	591.6709865
634	-7711	6531	26	742.3378641
886	-4331	6546	1	1038.173357

We define

$$d_n = \log \frac{A_n + B_n\sqrt{N}}{\sqrt{Q_n}} \tag{44}$$

in terms of the A_n and B_n in (7), (8), and we note, from (9), that

$$(-1)^n Q_n = \mathrm{Norm}(A_n + B_n\sqrt{N}). \tag{45}$$

Further, since Q_π is the first occurrence of $(-1)^n Q_n = +1$ after Q_0, we have

$$d_\pi = R = \log \epsilon \tag{46}$$

where ϵ is the fundamental unit of norm $+1$. Thus, the (narrow) regulator R of $\mathbb{Q}(\sqrt{N})$ equals the distance d_π, and d_n is a useful generalization of R. In all versions of SQUFOF here, we *do not* compute A_n or d_n. We use them here merely to illustrate the infrastructure of the quadratic field $\mathbb{Q}(\sqrt{N})$. See my [Sh1] and Lenstra's recent [L].

In Table I, besides (43), note

$$d_{316} = 2d_{142}, \qquad d_{506} = 2d_{252}, \qquad R = d_n + d_{\pi - n},$$

e.g., for $n = 252, 380, 405, 443$.

$$d_7 = d_{153} - d_{142}, \quad d_{325} = d_{153} + d_{142}, \quad d_{380} = 2d_{634} - R \tag{47}$$

Finally, what do you make of this:

$$\begin{gathered} d_{73} \approx 2d_{481} - R \quad \text{(not quite equal)}, \\ 3146x^2 + 2 \cdot 5585xy - 3707y^2 = 103^2 \ \textit{for}\ x = y = 1? \end{gathered} \tag{48}$$

We will return to (47) and (48).

The first improper square for N_2 behaves a little differently. For F_{316}, we have

$$G_0 = (-53, 6524, 5507)$$

$$G_{141} = (4331, 6546, -1), \ G_{142} = (-1, 6546, 4331).$$

Here forms are *not* in F_n, since F_n is in the *principle genus* and therefore $((-1)^n Q_n \mid p) = +1$, for $p = 4423$, 9689, and for all n. But $(-1 \mid 4423) = -1$ and G_{141} cannot be an F_n.

If we change the signs of both end-coefficients in Table I, we obtain a *second period of reduced forms* for $\mathbb{Q}(\sqrt{N_2})$. Let us write it as $-F_n$, and then our new G_0 is merely $-F_{142}$ read backwards.

Finally, the proper F_{380} led us to a period of reduced forms that is neither F_n nor $-F_n$. Call it $\overline{F}_n$ and write $\overline{Q}_n$, $\overline{P}_n$, $\overline{r}_n$. Now examine Table II.

Table II Principal period $\overline{F}_n$ for N_2

n		$\overline{F}_n$		$\overline{d}_n$
0	-2633	4423	8846	0.0000000
1	8846	4423	-2633	0.8210586
2	-2633	6109	2102	2.5303631
3	2102	6503	-269	5.3574448
18	-1402	6531	143	28.0969841
93	3718	6543	-361	124.9868675
173	2347	6544	-13	223.2511854
421	8711	6545	-2	519.0866787
422	-2	6545	8711	523.6836397
842	-2633	4423	8846	1038.173357

For the proper F_{380}, we see that G_0 is $\overline{F}_{173}$ read backwards. Since the symmetry points of $\pm F_n$ are ± 1 and ∓ 4423, obviously the present $+8846$ and -2 lie elsewhere. It is also clear that a fourth period $-\overline{F}_n$ will have -8846 and $+2$. The period now, $\overline{\pi} = 842$, is a little different than $\pi = 886$, but $\overline{d}_{\overline{\pi}} = d_\pi = R$ remains the same.

Note that

$$\overline{d}_{173} = d_{380}/2, \tag{49}$$

and, for a later option called "fast return," note that

$$\overline{d}_{18} = (d_{380} - d_{332})/2, \tag{50}$$

so that a

$$G_0 = (-143, 6531, 1402) \tag{51}$$

which we construct later, is very close to the symmetry point -8846 in $-\overline{F}_n$. We return to $\overline{d}_n$ later.

The four periods $\pm F_n$ and $\pm\overline{F}_n$ are called the *ambiguous periods* $\mathcal{A}$ by Gauss, and[2] are those with symmetry points, at which we find two successive forms

[2]I was unable to read the original word. [S.M.]

$$(A,B,C), \quad (C,B,A).$$

Any two forms (A,B,C) and (C,B,A) are *inverses* under Gauss's operation *composition*, cf [7, append 1], and, in any $\mathcal{A}$, if an (A,B,C) is in $\mathcal{A}$ so is its inverse. The name for the $\mathcal{A}$ comes from Latin meaning "facing (or going) both ways." Under composition, the product of any two forms in one $\mathcal{A}$ is a form in the principal period F_n, when it is reduced. In the example above, the form $\mathcal{A}$, including F_n itself, are the four square-roots of F_n. The operation $F^{-1/2}$ in (35), when applied to a square-form F, therefore gives us a G_0 which is the *inverse square-root* of F under composition. It will take us into some $\mathcal{A}$ possibly F itself. We now see that this quadratic-form formulation is much richer than the continued-fraction formulation described above for BRIMOR. In that algorithm, we *never* leave F_n, and, if N is large, we almost never even reach the *second* symmetry point in F_n - that unequal to the $Q_0 = 1$ with which we start. So $Q_0 = 1$ is BRIMOR's only symmetry point, and SQUFOF's method of avoiding the A_n is not possible in BRIMOR.

In SQUFOF, we work only in the $\mathcal{A}$ (unlike CLASNO [7]) where we may encounter any equivalence class). Nonetheless, let us round out our N_2 picture as follows: ¿From Table II, we construct

$$F = -\overline{F}_{93} = (-3718, 6443, 361)$$

which is a square-form *not* in F_n. This is possible since $-\overline{F}_n$, like F_n, is in the principal genus mentioned above. We apply (35) and (38) to F and get

$$H_0 = (-19, 6538, 5737),$$

it being convenient here to write H_0 instead of G_0. Then $H_{878} = H_0$ (at the same distance R) but H_m *never encounters a symmetry point*, since H_m is not an $\mathcal{A}$. In particular, the inverse of H_0, namely

$$H_0^{-1} = (5737, 6538, -19) \text{ and then } H_1^{-1} = (-19, 6534, 8489), \ldots ,$$

are not in H_m. Likewise, $-H_m$ and $-H_m^{-1}$ give distinct, nonambiguous period. So now we have 8 periods of reduced forms:

$$\pm F_n, \ \pm\overline{F}_n, \ \pm H_m, \ \pm\overline{H}_m^{-1}$$

In SQUFOF, we allow *any* odd N with $1+k$ distinct prime divisors for $k>0$. But the theory is simplest if

$$N \equiv -1 \pmod 4 \text{ and } N \text{ square-free}, \tag{52}$$

since our discriminant $4N$ is then a fundamental discriminant, and our periods map directly into the equivalence classes of the real quadratic field $\mathbb{Q}(\sqrt{N})$. In such a field the rational primes fall into three sets p, q and r, according as

$$(4n \,|\, p) = +1, \ (4N \,|\, q) = -1), \quad \text{or} \quad (4N \,|\, r) = 0,$$

when,the Kronecker symbol $(4N \,|\, n)$ gives the well-known

$$L(1,\chi) = \sum_{n=1}^{\infty} (4N \,|\, n)\frac{1}{n} = \frac{kR}{2\sqrt{N}} \tag{53}$$

where k is the narrow class number.

For simplicity, in the discussion that follows, we largely confine ourselves to N that satisfy (52),

Our N_2 satisfies (52) and has the ramified primes:

$$r = 2, 4423, 9689 \ (only),$$

the splitting primes:

$$p = 11, 13, 19, 29, 31, 37, 53, ...$$

and inert primes:

$$q = 3, 5, 7, 17, 23, 41, 43, ...$$

Then

$$\begin{aligned} L(1,\chi) &= 1 - \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{13} + \frac{1}{15} - ... \\ &= \frac{3}{4}\frac{5}{6}\frac{7}{8}\frac{11}{10}\frac{13}{12}\frac{17}{18}\frac{19}{18}... \\ &= 0.63435435... = \frac{hR}{2\sqrt{N_2}}, \end{aligned}$$

and our $R = 1038.173357$ gives $h = 8$. Thus, our 8 periods contain all of the periods of the reduced forms for N_2.

There will be 2^{1+k} $\mathcal{A}$ and therefore 2^{2+k} symmetry points $\pm S$. The factor f given by the reverse sequences G_m will be *improper* at *only four* of these points, namely, at

$$\pm S = \pm 1,\ \pm 2,$$

and we must *design the list* to avoid these four. For all other symmetry points, f is proper, and so the ratio

$$\frac{\text{Proper symmetry points}}{\text{All symmetry points}} = \frac{2^k - 1}{2^k}$$

as in (25).

The Q_n in F_n, and likewise the end-coefficients in any of the periods are divisible by p primes (to any power) but are not divisible by any q primes. If (52) holds, the r primes can divide to the first power only. Thus, in Table I,

$$Q_6 = 13 \cdot 19 \cdot 31,\ Q_{252} = 2 \cdot 13,$$
$$Q_7 = Q_{325} = 11 \cdot 53,\ Q_{142} = 53.$$

A second way in which SQUFOF theory is richer than BRIMOR's is this: The latter regards the $p = 13$ in Q_6 and that in Q_{252} as the *same prime*. Similarly, the $p = 53$ in Q_7, Q_{325} and Q_{142}. But from the point of view of $\mathbb{Q}(\sqrt{N})$, or that of composition, p is a *splitting prime* and there are *two different* prime ideals of norm p. If $p|Q_n$, (27) gives us

$$P_n^2 \equiv N \pmod{p}. \tag{54}$$

We reduce P_n as

$$P_n \equiv \pm a_p \pmod{p} \text{ with } 0 < a_p < \frac{1}{2}p. \tag{55}$$

We can now distinguish between the two different p according as

$$P_n \equiv a_p \text{ or } P_n \equiv -a_p \pmod{p}. \tag{56}$$

Let us adopt the convention that the prime be written as p in the first case in (56), and as $\overline{p}$ in the second case. For example, since

$$1461 \equiv 5 \ \text{ and } \ 6521 \equiv -5 \pmod{13},$$

13 divides Q_6 in Table I while $\overline{13}$ divides Q_{252}. The r primes do not split; there is only one, and we write it r. The factorizations above now become

$$\begin{array}{c} Q_6 = 13 \cdot \overline{19} \cdot 31, \ Q_{252} = 2 \cdot \overline{13} \\ Q_7 = 11 \cdot \overline{53}, \ Q_{325} = 11 \cdot 53, \ Q_{142} = 53. \end{array} \tag{57}$$

BRIMOR makes no distinction between p and $\overline{p}$ and would compute, e.g.,

$$(-Q_7) \cdot (-Q_{325}) = 11^2 \cdot 53^2,$$
$$Q_6 \cdot Q_{252} = 2 \cdot 13^2 \cdot 13 \cdot 31.$$

But the prime ideals 53 and $\overline{53}$, etc., are not equal, and in the composition of forms, which is closely related to ideal multiplication, we have instead, the rules

$$p \cdot p = p^2, \ \overline{p} \cdot \overline{p} = \overline{p}^2, \ \text{but } p \cdot \overline{p} = 1. \tag{58}$$

Similarly, if (52) holds,

$$r \cdot r = 1. \tag{59}$$

Thus, if we compose F_7 and F_{325}, from (57) and prior to any needed reduction, we would obtain the form

$$(-Q, P, 11^2) \tag{60}$$

for some $P \equiv +3$, not -3, $\pmod{11}$. If (60) is reduced, we must have $P = 6515$ and therefore $Q = 3382$. This is, in fact, F_{332}. We may write

$$F_7 * F_{325} = F_{332}, \tag{61}$$

and we note, from (47) and (43), that

$$d_7 + d_{325} = d_{332}. \tag{62}$$

¿From (45) we had

$$-583 = \text{Norm}(A_7 + B_7\sqrt{N}), \ -583 = \text{Norm}(A_{325} + B_{325}\sqrt{N}),$$

$$11^2 = \text{Norm}(A_{332} + B_{332}\sqrt{N}).$$

The cancellation $53 \cdot \overline{53} = 1$ in composition is reflected in the product of principal ideals:

$$(A_7 + B_7\sqrt{N})(A_{325}B_{325}\sqrt{N}) = 53(A_{332} + B_{332}\sqrt{N}). \tag{63}$$

Therefore,

$$\frac{A_7 + B_7\sqrt{N}}{\sqrt{583}} \cdot \frac{A_{325} + B_{325}\sqrt{N}}{\sqrt{583}} = \frac{A_{332} + B_{332}\sqrt{N}}{\sqrt{121}}$$

which, by (44), gives (62).

Let any two principal forms:

$$F_l = (a_l, b_l, c_l), \qquad F_m = (a_m, b_m, c_m),$$

be composed and give a form

$$F = (a, b, c), \tag{64}$$

where c, as in (60), is the product of the p's, $\overline{p}$'s, and r's in c_l and c_m according to the rules (58) and (59). There are three cases. If

$$|c| < \sqrt{N}, \tag{65}$$

there will be a reduced form in the principal period

$$F_n = (a_n, b_n, c_n)$$

with $c_n = c$. In this case, as in (61), we may write

$$F_l * F_m = F_n$$

and have $d_l + d_m = d_n$. All the examples in (43) and (47) are in this case since

$$\sqrt{N} = 6546.33...$$

If

$$2\sqrt{N} < |c| \tag{66}$$

there is *no such* F_n, and when (64) is reduced to, say F_k we have instead

$$r_l + r_m = r_k + \text{a small, computable correction.} \tag{66a}$$

I will show presently how to compute this correction.

If

$$\sqrt{N} < |c| < 2\sqrt{N}, \tag{67}$$

we have a *no-man's land*: there may be such an F_n, or there may not be such an F_n. If there is, then $r_l + r_m = r_n$, as before. As an example, let $F_l = F - m = F_{481}$ in Table I. Then

$$6546.33 < c = 103^2 < 13092.66.$$

If there were a reduced form:

$$F_n = (a, b, 10609) \tag{67a}$$

it would be at $d_n = 2(566.8093597) - R = 95.4453620$. *There is no such reduced form.* When reduced, we obtain F_{73} instead very close to this distance. See (48).

Let us contrast two cases involving F_6 that are *not* shown in Table I. By (57),

$$F_6 * F_{252} = (-Q, P, 2 \cdot \overline{19} \cdot 31)$$

with $P \equiv -2 \pmod{19}$, $\equiv +4 \pmod{31}$. Since $2 \cdot 19 \cdot 31 = 1178 < \sqrt{N}$, (65) holds and we *predict* that

$$F_n = (-4031, 6173, 1878)$$

will be in the principal period at $d_n = d_6 + d_{252}$. In fact, one finds $F_{260} = F_n$ at this distance. Now try

$$F_6 * F_{506} = (-Q, P, \overline{13} \cdot \overline{19} \cdot 31) \tag{68}$$

with $P \equiv -5 \pmod{13}$, $\equiv -2 \pmod{19}$, $\equiv +4 \pmod{31}$. Here $c = 7657 = Q_6$, but with 13 replaced by $\overline{13}$. Now, (67) holds, and there may, or may not be a principal form (68) at $d_n = d_6 + d_{506}$. This time,

$$F_6 * F_{506} = F_n = (-3694, 3817, 7657)$$

is found for $n = 514$ at this distance.

We note, in passing, that we will deduce (23) from the probability distribution that (64) will appear as a reduced from F_n, with $(-1)^n Q_n = c$, at the distance $d_n = d_l + d_m$. This probability is 1 if (65) holds, 0 if (66) holds, and decreases monotonically from 1 to 0 if (67) holds. A priori, our last $c = 7657$ was more likely to appear than was the $c = 103^2$ above. (Nonetheless, one easily notes the much larger $|c| = 12731$, etc., in Table I.)

¿From Table I, the reader can now make many predictions. Thus: At what distance d_n will one find

$$(-1)^n Q_n = -11^3 \quad \text{or} \quad \overline{13} \cdot \overline{109} \quad \text{or} \quad -2 \cdot 11 \cdot 149?$$

Or, again, although $F_7 2$ is not shown in Table I, predict $d_7 2 = 94.4729093$. (Hint: Use (6) to determine whether 11 or $\overline{11}$ and 13 or $\overline{13}$ divides Q_{72}.)

Let us now contrast these predictions with the continued fraction theory in BRIMOR. There are a few N, such as $N = M^2+1$, where the pattern of the Q_n is obvious. There are a few others [11], [12], such as $N = S_k = (2^k+3)^2-8$, where the pattern is complicated, but still discernable. But for most large N, the Q_n appear to be almost random and completely unpredictable. Similarly, it is very mysterious in BRIMOR whether a Q^2 is proper or not. All this occurs if one does not distinguish p and $\overline{p}$.

But with this distinction, we see that there is a great deal of predictable inner structure within the principal period. It also occurs in the other periods and is called the **infrastructure** in [Sh1]. We will use it to design the **list**, and later the **fast return** for SQUFOF.

Since the infrastructure is still relatively new, it should be informative and interesting to briefly mention four background topics.

1. Lagrange (long before Gauss) gave a complete theory of the reduction and equivalence of binary quadratic forms. But he regarded $Ax^2 + Bxy + Cy^2$ and $Ax^2 - Bxy + Cy^2$ as equivalent since they represent the same numbers. In contrast, Gauss called them improperly equivalent, not properly equivalent (unless they are ambiguous). This distinction between proper and improper equivalences seems almost trifling, or pedantic, when one first reads it in, say Dickson's book [13]. Yet, it is all-important. Without this distinction, the class number comes out wrong, composition collapses, the class group disappears, and so do equations like (53). The distinction between p and $\overline{p}$ above is very

closely related, and we see, again, that without it the whole structure largely collapses.

2. In my original talk [Sh1], I defined the distance by

$$d_n = \log(A_n + B_n\sqrt{N}) \tag{69}$$

instead of (44), and used a "ramification factor" and a "reduction factor" to correct, when needed, such relations as those in (47) and (66a). Since $A_n + B_n\sqrt{N}$ grows exponentially with n, while $\sqrt{N}$ is bounded, the difference between (69) and (44) is relatively small when n is large; e.g. in Table I we would have $d_{443} = 523.28...$ instead of $519.09....$ The definition (69) is workable, but that in (44) is simpler and more elegant. For something we call "distance", we would like the distance to the midpoint, such as d_{443} above, to equal $R/2$. But it does not with (69). So, shortly after [Sh1], I changed the definition to that in (44) but I did not publish it.

Lenstra, independently therefore, made essentially the same change [L]. (Originally, he differed by a factor of 2.) Simultaneously, he considerably simplified the treatment that I had given [Sh1] for the reduction factor. He gives (in our notation)

$$d_n - d_{n-1} = \frac{1}{2}\log\mid\frac{\sqrt{N}+P_n}{\sqrt{N}-P_n}\mid \tag{70}$$

whether F_n is *reduced or not.* That (70) is consistent with (44) follows from the identities

$$\frac{A_n + B_n\sqrt{N}}{\sqrt{Q_n}} = \frac{A_{n-1} + B_{n-1}\sqrt{N}}{\sqrt{Q_{n-}}}\cdot\frac{\sqrt{N}+P_n}{\sqrt{Q_nQ_{n-1}}},$$

and

$$\frac{(\sqrt{N}+P_n)^2}{Q_nQ_{n-1}} = \frac{\sqrt{N}+P_n}{\sqrt{N}-P_n}.$$

We illustrate (70) with two examples. We gave a hint above to be used in computing d_{72}. But (70) gives us

$$d_{72} = d_{73} - \frac{1}{2}\log\frac{\sqrt{N}+5585}{\sqrt{N}-5585}$$

at once. Next, return to (48), (66a) and (67a). By composition, the latter is

$$F_{481} * F_{481} = (3146, 8731, 10609) \tag{71}$$

and is not reduced. We reduce it by, first, $(10609, -8731, 3146)$ and then F_{73} in Table I. Then, one verifies that

$$2d_{481} - R + \frac{1}{2}\log\mid\frac{\sqrt{N}-8731}{\sqrt{N}+8731}\mid + \frac{1}{2}\log\frac{\sqrt{N}+5585}{\sqrt{N}-5585} = d_{73}.$$

The fact that $2d_{481} - R$ differs from d_{73} by only 0.295... is reflected in the fact that 10609 is represented by F_{73} with the smallest variables $x = y = 1$ in (48).

3. With some exceptions, such as the aforementioned $N = M^2 + 1$ or $N = S_k$, the regular continued fractions for most large $\sqrt{N}$ with large periods π tend to approximately obey the known probabilistic laws, cf. [14]. These are the laws of Khintchine, Gauss - Kuzmin, and Lévy. In our notation, the latter approximation can be written as

$$\log(A_n + B_n\sqrt{N}) \approx \frac{\pi^2}{12\log 2}n$$

and therefore, for large n,

$$d_n \approx \frac{\pi^2}{12\log 2}n \tag{72}$$

Thus, the approximation

$$153/332 \approx \frac{1}{2}$$

that we mentioned prior to (43), and its error, is a reflection of the approximation, and error, in (72). For large n, we will usually find that (72) is roughly correct. For example, our N_2 has eight periods: 2

with $\pi = 886$, 2 with $\pi = 842$, and 4 with $\pi = 878$. The average is 871, and we do find that

$$871 \cdot \frac{\pi^2}{12 \log 2} = 1033.5 \approx R = 1038.2.$$

We may call the distance in (70) the **length** of the form F_n. Some forms are "long" and some are "short". The mean length is

$$1.18657... = \frac{\pi^2}{12 \log 2}$$

by (72). If Q_{n-1} or Q_n is very small relative to $\sqrt{N}$, then F_n must be long.

4. The key operation in SQUFOF is (35), wherein we compute an (inverse) square-root of F_n. This is trivially accomplished since S^2 is a perfect square. Gauss proved that *any* form F in the principal genus has a square-root f such that

$$f * f \quad (\text{under composition and reduction}) \ = F.$$

His constructive proof gives a remarkable algorithm for computing f. (This is simplified in my algorithm GATESR [12]. But GATESR is of no use to us here since it requires the complete factorization of N, and, if we knew that, we obviously would not need SQUFOF.)

But the S^2 in (34) is the **value** of a form (28) with $x = 0$ and $y = 1$. If, for any F_n in (28), its value is a square for certain valued of x and y, then one can easily construct an equivalent form (probably not reduced) that is a square-form (34). For example, in our much-mentioned F_{73} in (48), $x = y = 1$ gives $S^2 = 103^2$, and F_{73} is equivalent to (71). Then

$$F^{-\frac{1}{2}} \rightarrow G_0 = (-103, 6465, 10274) \tag{73}$$

is $-\overline{F}_{32}$ read backwards. $\overline{F}_{32}$ is not shown in Table II but would be at $\overline{d}_{32} = 47.7226810 = d_{481} - \frac{1}{2}R$. So, (73) would factor N_2 very quickly.

This variation on SQUFOF was suggested by R. de Vogelaine when I first spoke on SQUFOF in [15]. He calls it the "fat" SQUFOF. One

tries small pairs (x, y) in F_n to see if it has a small square value. I know of no one who has actually tried it, or who analyzed its relative efficiency. For N_2, it appears to be of value, since F_{73} is encountered long before the first *explicit* proper square-form F_{380}. Of course, one would want to know that (71) is also proper. In the next section, we turn to construction of the list.

His paper is a long one, and, for brevity, we refer the reader to Lenstra's [L] for a more thorough, theoretical treatment of the infrastructure.

4 The Lists (Two Types)

We have two versions of the list: the first we call the Queue, or the Necessary and Sufficient List; the second is the Sufficient List, or the Cheap list. First lists first!

In the foregoing analysis of N_2 we saw that the improper square-forms F_{316} and F_{332} arose from $F_{142}^2 = F_{316}$ and $F_{153}^2 = F_{332}$ and appear at the distances

$$d_{316} = 2d_{142} \quad \text{and} \quad d_{332} = 2d_{153}.$$

Here, F_{142}^2 and F_{153}^2 are already reduced and these squares can be predicted to occur in F_n as soon as we encounter $Q_{142} = 53$ and $Q_{153} = 11$. We generalize this.

In (32) above, we had the test:

$$Q_{2l} = S^2 \ ?$$

for every l. We now add to the test:

$$Q_n < L = 2\sqrt{2\sqrt{N}} \ ? \tag{74}$$

for every n. If (74) does not hold (the usual case when N is large) we continue. If Q_n is *odd* and (74) holds we make the further test:

$$Q_n < \frac{1}{2}L \ ? \tag{75}$$

If Q_n is even and (74) holds, or if Q_n is odd and (75) holds, then (66) *does not hold* and F_n^2 *may* appear as an improper square-form. If, in addition, (65) holds, then F_n^2 will appear as an improper square-form.

The queue algorithm is this: If Q_n is even, and (74) holds, put the pair

$$Q_n/2, \qquad P_n \pmod{Q_n/2} \geq 0 \tag{76}$$

into the queue. If Q_n is odd, and (75) holds, put the pair

$$Q_n, \qquad P_n \pmod{Q_n} \geq 0 \tag{77}$$

into the queue. If we call N a full-precision number, the numbers in (76)-(77) are quarter-precision and we can pack either pair into one half-precision number. For example, in my SQUFOF program for an HP-41C, $N < 10^{20}$, the word-length is 10^{10}, and either pair packs into one word as follows.

Return to N_2 in Table I. We have $L = 228.85$. At $n = 142, 153$, and 252 we place numbers into the queue as follows

n	queue
142	53.00005
153	11.00003
252	13.00008

Here, the second number in the pair is divided by 10^5 and added to the first number. Note that

$$\frac{5}{53} < \frac{1}{2}, \ \frac{3}{11} < \frac{1}{2}, \ \frac{8}{13} > \frac{1}{2}$$

tells us, at once, that the primes dividing the corresponding Q_n are 53, 11 and $\overline{13}$.

Next we come to the square-form F_{316}. Since $P_{316} = 5093 \equiv 5 \pmod{53}$, F_{316} gives us 53.00005 which is at the top of the queue. We have kept no record as to specifically how it got there: that is, we no longer know (at $N = 3/6$) whether it came from a

$$(-1)^n Q_n = 53 \ \text{ or } \ -53 \ \text{ or } \ 106 \ \text{ or } \ -106 \tag{78}$$

at $d_n = \frac{1}{2} d_{316}$ in F_n. But that is irrelevant since, in any case, the G_0 for F_{316} will lead us to one of the four symmetry points $\pm s = \pm 1$ or ± 2, and therefore to an improper factor $f = 1$ or 2. Obviously, whichever is correct in (78),

$(-1)^{n+1}Q_n$ will be at the same distance below -1 in $-F_n$. Further, by the composition of forms and (59), $\pm Q_n/w$ or $\pm 2Q_n$ will be at $\overline{d}_n = \overline{d}_{421} + \frac{1}{2}d_{316}$ in $\overline{F}_n$ or $-\overline{F}_n$ (see Table II) according as Q_n is even or odd. Therefore, in any of the four cases, F_{316} must be improper. We save its 53.00005 in a register $L1S$ called "last improper square-form" and continue.

We must digress briefly and we have not yet defined $\overline{d}_n$. There are two ways to do that. Lenstra [L][3]

References

[Sh1] D. Shanks, ??

[Sh2] D. Shanks, "Analysis and Improvement of the Continued Fraction Method of Factorization," unpublished.

[BM] Brillart and Morrison, Math. Comp., ?

[4] Lehmer and Powers, ?

[5] ??

[6] ??

[7] ??

[8] ??

[9] ??

[L] Lenstra, ?

[11] ??

[12] ??

[13] Dickson

[14] ??

[15] Shanks??

[3]Here the paper ends at the bottom of a hand-written page. No lists of references or other pages of this manuscript are known. [S.M.