Analysis and Improvement of the Continued Fraction Method of Factorization

Daniel Shanks*

Contents

1 Introduction

Recently, Morrison and Brillhart [1], (henceforth M&B), gave a detailed account of a powerful factorization program based upon the continued fraction method of Lehmer and Powers [2]. For every n, one has

$$N = q_0 + \frac{1}{q_1+}\ \frac{1}{q_2+}\ \ldots\ + \frac{1}{q_{n-1}+}\ \frac{1}{(\sqrt{N}+P_n)/Q_n} \tag{1}$$

with known recurrences for computing the integers P_n, Q_n and also certain integers A_n, B_n such that

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

Thus

$$(-1)^n Q_n \equiv A_n^2 \pmod{N} \tag{3}$$

*Original paper, in mimeographed type-written form circa 1975, was never completed. Typed into latex by Stephen McMath in March, 2004. Equation numbers and sections match the original. Composition of forms is denoted here by $*$.

where A_n may be reduced (mod N). (Note: Our A_n is designated as A_{n-1} in [1].)

If the product of one or more selected $(-1)^n Q_n$ equals a perfect square, and

$$\Pi(-1)^n Q_n = Q^2,\ \Pi A_n \equiv A \pmod{N} \tag{4}$$

then

$$N \mid (A^2 - Q^2). \tag{5}$$

Now <u>if</u>

$$N \nmid (A - Q),\ N \nmid (A + Q) \tag{6}$$

the $GCD(A - Q, N)$ is a proper factor of N. If (6) does not hold, the square product (4) <u>fails</u> (unless $GCD(Q, N)$ is already > 1) and another product (4) must be sought.

M&B are prepared to accept several such failures until they find a case where (6) holds. They make no attempt to analyze the conditions for failure and do not even pose the question. Failure is accepted philosophically, even poetically: "...your butterfly net is empty". Our first purpose is to give an analysis of failure and thereby to gain understanding and to eliminate (most) false tries.

This factorization method is used primarily for very large N and has the advantage that all

$$P_n, Q_n = O(\sqrt{N}) \tag{7}$$

But the A_n are $O(N)$ even when reduced. Their multiprecision computation, reduction and multiplication, and the evaluation of $GCD(A - Q, N)$ are all lengthened correspondingly. Their storage requirements are likewise increased. Our second purpose is to show how all that may be avoided; the A_n are not needed at all. Their computation, reduction, multiplication and storage may all be dispensed with.

To understand how that can be done, one needs to reinterpret the continued fraction algorithm (1) as a period of reduced binary quadratic forms, or, alternatively, to utilize the concepts of the real quadratic field $\mathbb{Q}(\sqrt{N})$. We do this first.

Besides the two main purposes described above, we will conclude with some other commentary on [1] and its method.

2 The Principal Period

Consider the "knight's tour" diagram:

n			
0	Q_0	$2P_1$	
1		$2P_2$	$-Q_1$
2	Q_2	$2P_3$	
3		$2P_4$	$-Q_3$
4	Q_4 etc.		

The n^{th} end-coefficient is $(-1)^n Q_n$. The n^{th} form is

$$F_n = ((-1)^n Q_n, 2P_{n+1}, (-1)^{n+1} Q_{n+1}) \tag{8}$$

F_n is an indefinite quadratic form of discriminant

$$4(P_{n+1}^2 + Q_n Q_{n+1}) = 4N \tag{9}$$

(We are mostly following [1] here and thereby confine ourselves to even discriminants. Odd discriminants can also be used and are touched upon briefly below.)

If $Q_0 = 1$, $P_1 = \sqrt{N}$, and P_{n+1} and Q_{n+1} are chosen such that each P_{n+1} is the maximal integer for which

$$P_{n+1} \equiv -P_n \pmod{Q_n},\ N = P_{n+1}^2 + Q_n Q_{n+1},\ Q_{n+1} > 0, \tag{10}$$

then the sequence F_n constitutes the **principal period of reduced forms** of discriminant $4N$. For the example in [1], $N = 13290059$, the period begins as in Figure 1.

$$N = 13290059$$

n			
0	1	7290	
1		778	−4034
2	3257	5736	
3		6704	−1555
4	1321	6506	
5		5794	−2050
6	2389	3762	
7		4402	−4082
8	2069	3874	
9		5346	−4610
10	1333	5318	
11		4014	−4666
12	1985	3926	
13		5582	−4754
14	1157	5988	
15		1490	−3739
16	3406	5322	
17		5616	−1823
18	2965	6244	
19		5706	−1195
20	4310	2914	
21		2268	−2591
22	4633	6998	
23		7014	−226
24	4385	1756	

Figure 1

The array may be interpreted as a sequence of infinite continued fractions. For every $n > 0$, one has

$$\frac{\sqrt{N} - P_n}{Q_{n-1}} = \frac{Q_n}{\sqrt{N} + P_n} = \frac{1}{q_n+}\ \frac{1}{q_{n+1}+}\ \frac{1}{q_{n+2}+}\ldots \tag{11}$$

where

$$q_n = \lfloor \frac{\sqrt{N} + P_n}{Q_n} \rfloor = \frac{P_n + P_{n+1}}{Q_n} \tag{12}$$

In particular, for $n = 1$, since $Q_0 = 1$,

$$\sqrt{N} = P_1 + \frac{1}{q_1+}\ \frac{1}{q_2+}\ \frac{1}{q_3+} \tag{13}$$

Any continued fraction (11) may be truncated, leaving an exact identity, by replacing any final q_m with the quadratic surd $(\sqrt{N} + P_m)/Q_m$ of which it is the integer part.

The three integers in (8) are the coefficients of a binary quadratic form in the variables U_n and V_n. The $(n-1)^{st}$ form:

$$F_{n-1}(U_{n-1}V_{n-1}) = (-1)^{n-1}Q_{n-1}U_{n-1}^2 + 2P_nU_{n-1}V_{n-1} + (-1)^nQ_nV_{n-1}^2 \tag{14}$$

transforms into the n^{th} form $F_n(U_n, V_n)$ by the liner substitutions

$$\begin{aligned} U_{n-1} &= \quad -V_n, \\ V_{n-1} &= U_n + (-1)^n q_n V_n, \end{aligned} \tag{15}$$

that is, by the unimodular matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & (-1)^n q_n \end{pmatrix} \tag{16}$$

This gives

$$\begin{cases} P_{n+1} = -P_n + q_nQ_n \\ Q_{n+1} = Q_{n-1} + q_n(P_n - P_{n+1}) \end{cases} \tag{17}$$

The two end-coefficients of F_n are equal to $F_{n-1}(U_{n-1}, V_{n-1})$ with the variables equal to the columns of (16); that is, with

$$\begin{cases} U_{n-1} = 0 & V_{n-1} = 1, \text{ or} \\ U_{n-1} = -1 & V_{n-1} = (-1)^n q_n, \end{cases} \tag{18}$$

respectively. Likewise, by compounding successive matrices (16), or their inverses, the end-coefficients of any F_n are given by any $F_n(U_m, V_m)$ for computable values of its two arguments.

Specifically, for

$$F_0 = (1, 2P_1, -Q_1) \tag{19}$$

there are integers α_n and β_n such that

$$\begin{aligned}(-1)^n Q_n &= \alpha_n^2 + 2P_1\alpha_n\beta_n - Q_1\beta_n^2 \\ &= (\alpha_n + P_1\beta_n)^2 - \beta_n^2 N \\ &= A_n^2 - B_n^2 N,\end{aligned} \tag{20}$$

as in (2). Or, we may write,

$$(-1)^n Q_n = N(A_n + B_n\sqrt{N}) \tag{21}$$

i.e., the end-coefficient is the norm of an algebraic integer $A_n + B_n\sqrt{N}$. Here, A_n and B_n are < 0 and $A_n + B_n\sqrt{N}$ increases monotonically with n. By Levy's Law for almost-all continued fractions, we can estimate (but only roughly)

$$\log(A_n + B_n\sqrt{N}) \approx n \cdot \frac{\pi^2}{12\log 2} \tag{22}$$

when n is large and the period of the continued fraction is large.

3 Batting 500

In factoring $2^{128} + 1$ M&B encountered four failures before (6) was satisfied. For their illustrative example $N = 13290059$, they give four products (4), two successes and two failures:

"Product" I. Going beyond our table to $n = 52$ one finds the square:

$$(-1)^{52} Q_{52} = 25, A_{52} \pmod N = 2467124.$$

Then, with $A = 2467124$, $Q = 5$, $(A - Q, N) = 4261$. So 4261 divides N.

Product II. Suppose we do not go as far as $n = 52$. Try this:

n	$(-1)^n Q_n$	$A_n \pmod N$
10	$1333 = 31 \cdot 43$	6700527
26	$3286 = 2 \cdot 31 \cdot 53$	11455708
40	$4558 = 2 \cdot 43 \cdot 53$	3213960.

Then $Q = 2 \cdot 31 \cdot 43 \cdot 53 = 141298$ and A (reduced) also equals 141298. So $N = (141298 - 141298, N)$ and $N \mid N$. Failure; that we already know.

Product III. Again, take

n	$(-1)^n Q_n$	$A_n \pmod N$
5	$-2050 = -2 \cdot 5^2 \cdot 41$	171341
22	$4653 = 41 \cdot 113$	5235158
31	$-5650 = -2 \cdot 5^2 \cdot 113$	1895246.

Then $Q = 2 \cdot 5^2 \cdot 41 \cdot 113 = 231650$ and $A = 13058409$. Since $1 = (13058409 - 231650, N)$ we have $1 \mid N$. That we also know. M&B refer to this as a different "type of failure" than that in the previous product. Actually, it is essentially the same, merely a sign change in Q. We now have $N = (13058409 + 231650, N)$ because $A - (-Q) = N$.

Product IV. Finally, try

n	$(-1)^n Q_n$	$A_n \pmod N$
5	$-2050 = -2 \cdot 5^2 \cdot 41$	171341
22	$4653 = 41 \cdot 113$	5235158
23	$-226 = -2 \cdot 113$	1914221.

$Q = 2 \cdot 5 \cdot 41 \cdot 113 = 46330$, $A = 1469504$ and $4261 = (A - Q, N)$. So $4261 \mid N$ as in Product I.

4 Failure and Equivalence

One can always obtain a square product (4) simply by squaring any $(-1)^n Q_n$. But that always leads to failure; we call it the trivial failure. If

$$(-1)^n Q_n = N(A_n + B_n\sqrt{N})$$

its square is

$$Q_n^2 = N(A_n^2 + B_n^2 N + 2A_n B_n \sqrt{N})$$

Therefore, either $A-Q$ or $A+Q$ equals $2B_n^2 N$ and so we have failure unless (Q, N) is already > 1.

Now the failures of products II and III above are not much deeper than the trivial failure. In II we have

$$31 \cdot 41 = Q_{10} = N(6700527 + 1838\sqrt{N})$$

$$2 \cdot 31 \cdot 53 = Q_{26} = N(17435545529165 + 4782688389\sqrt{N})$$

with A_n, B_n unreduced (mod N). Since

$$A_{10}A_{26} + B_{10}B_{26}N \equiv A_{10}B_{26} + A_{26}B_{10} \equiv 0 \pmod{31}$$

we have the product

$$Q_{10}Q_{26} = 2 \cdot 43 \cdot 53 \cdot (31^2) = (31^2) \cdot N(A + B\sqrt{N})$$

where

$$31A = A_{10}A_{26} + B_{10}B_{26}N,\ 31B = A_{10}B_{26} + A_{26}B_{10}.$$

But it may be verified that $A = A_{40}$ and $B = B_{40}$ and so we also have

$$Q_{40} = 2 \cdot 43 \cdot 53 = N(A + B\sqrt{N}).$$

Therefore, the product $Q_{10}Q_{26}Q_{40}$ differs from the trivial failure only by the additional factor 31^2 on both sides of the equation.

Similarly, for III, one could verify that

$$(A_5 + B_5\sqrt{N})(A_{22} + B_{22}\sqrt{N}) = 41(A_{31} + B_{31}\sqrt{N}) \tag{23}$$

and $Q_5Q_{22}Q_{31}$ differs from the trivial failure only by the common factor of 41^2.

On the other hand, one could verify that

$$(A_5 + B_5\sqrt{N})(A_{22} + B_{22}\sqrt{N})(A_{23} + B_{23}\sqrt{N}) = 2 \cdot 41 \cdot 113(A_{52} + B_{52}\sqrt{N}) \tag{24}$$

and so product IV will succeed (or fail) together with product I; they are equivalent.

Note that, to the extent (22) is valid, the indices n in (23) and (24) should be roughly additive. They are:

$$5 + 22 \approx 31, \;\; 5 + 22 + 23 \approx 52.$$

For large n, A_n and B_n get very large (roughly, as in (22)) and if we really needed these unreduced numbers to predict failure, as in (23), this criterion would not be very practical. But we have already stated that we do not need the A_n at all, reduced or unreduced; we need only the P_n and Q_n and so we now give a second theory of failure.

From the table above we read

$$F_5 = (-2 \cdot 5^2 \cdot 41, 5795, 2389),$$

$$F_{22} = (41 \cdot 113, 6998, -226).$$

The composition $F_5 * F_{22}$ of these two quadratic forms (see [3, Appendix 1]) is found to be

$$F = (-2 \cdot 5^2 \cdot 113, 6094, 709).$$

This is already reduced, and if we extend the table we would find that $F = F_{31}$. And so

$$F_5 * F_{22} = F_{31} \tag{25}$$

is analogous to (23) but does not require the A_n in its calculation - only the P_n and Q_n. The main point in the calculation is that the factors 41 on the left of F_5 and F_{22} cancel each other in their product $F = F_{31}$. Why?

In general (see [3, Appendix 1]), if

$$F_1 * F_2 = (X_1, Y_1, Z_1)(X_2, Y_2, Z_2) = (X_3, Y_3, Z_3) = F_3$$

prior to any reduction of F_3, and if

$$X_1 = M_1 p_1^{a_1} ... p_m^{a_m}, \;\; X_2 = M_2 p_1^{b_1} ... p_m^{b_m}$$

where $(M_1, M_2) = 1$, then

$$X_3 = M_1 M_2 p_1^{c_1} ... p_m^{c_m}$$

with

$$c_i = a_i + b_i \text{ if } p_i \nmid (Y_1 + Y_2)/2,$$

while

$$c_i = |a_i - b_i| \text{ if } p_i \mid (Y_1 + Y_2)/2.$$

Since $41 \mid (5794 + 6998)$ in F_5 and F_{22}, the factors 41 cancel in their composition (25).

Similarly,

$$F_5 * F_{22} * F_{23} = F_{52} \tag{26}$$

is analogous to (24). Composition is commutative and associative and we may carry out (26) in several ways: via (25) and $F_{31} * F_{23}$ or via $F_{22} * F_{23} = (-2 \cdot 41, 7162, 5689) = F_{45}$ and then $F_5 * F_{45}$. But $F = F_5 * F_{23}$ is not yet reduced since $5^2 \cdot 41 \cdot 113 = 115825 > 2\sqrt{N}$, and so F would not be found in the period of reduced forms unless it were first reduced. It is useful to note that the cancellation of 113 in $F_{22} * F_{23}$ is clear a priori since Q_{23} divides $P_{22} + P_{23}$ from (12) and ipso facto 113 also divides $P_{22} + P_{23}$.

Our third criterion for failure is by far the simplest arithmetically; it relates to both previous criteria but is based upon conjugate prime ideals in the real field $\mathbb{Q}(\sqrt{N})$. Consider the equal-valued

$$-Q_{55} = -Q_{109} = -Q_{321} = -Q_{363} = -2015 = -5 \cdot 13 \cdot 31. \tag{27}$$

A product of any distinct pair of these is not the trivial failure. It may succeed or fail, but if it fails it is not the trivial failure described above. The corresponding F_n are all distinct:

$$\begin{aligned} F_{55} &= (-2015, 5036, 3449),\ F_{109} = (-2015, 3424, 5141), \\ F_{321} &= (-2015, 6586, 1214),\ F_{363} = (-2015, 4974, 3526). \end{aligned} \tag{28}$$

The rational primes p dividing Q_n are of two types[1], those that divide the discriminant $4N$ and have $(4N \mid p) = 0$, and those that do not have $(4N \mid p) = +1$. The first type ramify; the second split. In the first, there is only one prime ideal of norm p; call it P. In the second, there are two; call them P and $\overline{P}$. The product $P \cdot \overline{P}$ equals the principal ideal (p) in the second type, while $P^2 = (p)$ in the first.

For any $(-1)^n Q_n$ in question, we want to factor the principal ideal $(A_n + B_n\sqrt{N})$ into a product f_n of prime ideals. If any splitting p divides Q_n, we adopt the convention that P divides $(A_n + B_n\sqrt{N})$, or $\overline{P}$ does, according as the fractional part

$$\frac{2P_{n+1}}{P} - \left\lfloor \frac{2P_{n+1}}{P} \right\rfloor < \frac{1}{2}, \text{ or } > \frac{1}{2}, \tag{29}$$

respectively. Whereas the four $-Q_n$ in (27) are all equal, from (28) we find that the four f_n are all distinct:

$$\begin{aligned} f_{55} &= -5 \cdot 13 \cdot 31, \quad f_{109} = -\overline{5} \cdot 13 \cdot 31, \\ f_{321} &= -5 \cdot \overline{13} \cdot 31, \quad f_{363} = -\overline{5} \cdot \overline{13} \cdot 31. \end{aligned} \tag{30}$$

And as our first criterion was based upon $A_n + B_n\sqrt{N}$ and our second upon F_n, our third criterion is based upon f_n.

Returning to Product III, we now have

[1] Grammatically, Shanks may have restated the second type as "those that have $(4N \mid p) = +1$" [SM].

$$f_5 = -2 \cdot \overline{5}^2 \cdot 41,\ f_{22} = \overline{41} \cdot 113,\ f_{31} = -2 \cdot \overline{5}^2 \cdot 113,$$

and the analogue to (23) and (25) is now

$$f_5 \cdot f_{22} = (41) f_{31}. \tag{31}$$

So our criterion is this: With a proviso (36) given below, if the factors in a product (4) can be split into two disjoint sets S_1 and S_2 such that

$$\prod_{S_1} f_n = \prod_{S_2} f_n, \tag{32}$$

except for some principal ideals (p) on either or both sides, then the product (4) fails. Note that when Q_n is treated as an integer having unique factorization into rational primes, as in [1], without distinguishing the underlying conjugate ideals P and $\overline{P}$, all of this structure is lost.

Whereas $A_n + B_n\sqrt{N}$ increases monotonically, F_n and f_n will repeat periodically. For our example $N = 13290059$, the period is 1068. Therefore, if

$$n = m + 1068k, \tag{33}$$

we have $F_n = F_m$, $f_n = f_m$ but

$$A_n + B_n\sqrt{N} = \epsilon^k (A_m + B_n\sqrt{N}) \tag{34}$$

where

$$\epsilon = A_{1068} + B_{1068}\sqrt{N} \tag{35}$$

is the fundamental unit. Now a square

$$(-1)^n Q_n \cdot (-1)^m Q_m$$

for such an n and m is not a trivial failure and so our proviso is that the two products in (32) are in the same period. This means that one has

$$\sum_{S_1} n \approx \sum_{S_2} n \tag{36}$$

for the corresponding indices n, and not that the sums differ by an approximate multiple of 1068. For very large N, the period is usually very large, and the individual n in (36) will be very small in comparison. So (36) cannot fail unless there are very many n in one S_i.

I give no conclusion here concerning the practicality of programming this test: (32), (36). If there are only a few factors in (4), as in (31), the test is almost immediate, but many factors would allow many possible partitions into S_1 and S_2.

5 Success

If the test (32), (36) fails on a square (4), the probability of success in obtaining a proper factor of N will be shown to be at least $1/2$ if N is divisible by two distinct primes, and the probability increases as the number of prime dividsors of N increases. To illustrate the fact that failure may still occur, consider $Q^2 = (-Q_{55}) \cdot (-Q_{321})$ from (27). This product does not satisfy (32) or (36). Nonetheless, it fails since there is an $f_{193} = -5 \cdot 31$. Therefore

$$f_{55} \cdot f_{321} = (13) f_{193}^2$$

and Q^2 is equivalent to a trivial failure. Note that $2 \cdot 193 \approx 55 + 321$.

Will $\overline{Q^2 = (-Q_{55})} \cdot (-Q_{109})$ from (27) succeed? If there were an $f_n = \pm 13 \cdot 31$ with $n \approx 82 = \frac{1}{2}(55 + 109)$, this $Q * 2$ would fail in the same way. But there is no such n; one finds that $f_{605} = -13 \cdot 31$ is located about one-half a period away from $n \approx 82$. In the same way, in our equivalent products I and IV, with $\overline{5}^2$ at $n = 52$, one finds that $\overline{5} = f_{558}$ occurs about one-half a period away from $n = 26$.

Either by continuing Figure 1 to $n = 52$, or by composition of F_5, F_{22}, and F_{23} as in (26), we obtain

$$F_{52} = (25, 7244, -6847) \tag{37}$$

corresponding to the prime ideal product $\overline{5}^2$. A square-root of F_{52} is obtained immediately by

$$(5, 7244, -5 \cdot 6847)$$

and we reduce this by adding the largest even multiple of 5 to 7244 that keeps the sum less than $2\sqrt{N}$. We thereby obtain the reduced form

$$(5, 7284, -5179), \tag{38}$$

corresponding to $\overline{5}$. Now compute the period of (38) going backwards for about $26 = 52/2$ forms as in Figure 2

	6238	-571
6238	6238	
	6324	-571
5764	...	
	6980	-311
3569	158	
	7286	-3722
5	7284	
		-5179

Figure 2

We find that 24 forms before (38) there is an ambiguous form

$$(6238, 6238, -571) \tag{39}$$

where an end-coefficient (6238) divides the center coefficient (6238) and therefore also divides the discriminant $4N$. So 3119 divides N and we have

$$N = 3119 \cdot 4261$$

with no use of the A_n whatsoever. One knows when one is at the ambiguous form in Figure 2 by the symmetry there; the adjacent center coefficients are equal.

The forms (38) and (39) are, in fact, F_{558} and F_{534}, respectively. We are still in the principal period although we would not have known that if we had merely computed the period down to F_{23}, or even to F_{52}.

In much the same way, from our previous discussion and (28), the square

$$F_{55} * F_{109} = (-403)^2, 50172, 3793) \quad \text{(unreduced)}$$

has a square-root

$$(-403, 6648, 5561) \quad \text{(reduced)}, \tag{40}$$

and 71 forms before it in its period one again finds F_{534} since (40), as suggested above, if F_{605}. On the other hand, as explained above, a square-root of $F_{55} * F_{321}$ is

$$(-155, 7206, 1990), \tag{41}$$

and going back 193 forms leads us not to F_{534} but rather to $F_0 = (1, 7290, -4034)$ since (41) is, in fact, F_{193}. But <u>this</u> ambiguous form F_0 is a failure; it merely yields the trivial factor $1 \mid N$. (In other words, failure does not mean no factor of N; it means no proper factor.)

In all of the foregoing, we remained within the principal period. To obtain the full picture, we will soon compute examples that take us into other equivalence classes. But first we recompute the factor of N from (38), and from (40), in a different, usually faster way.

Instead of going <u>backwards</u> from (38), as in Figure 2, let us go <u>forward</u> from its <u>inverse</u>:

$$(5, 7286, -3722) \tag{42}$$

This form is seen in Figure 2 as the predecessor of (38) read backwards. It is $F_{510} = F_{1068-558}$ and has $f_{510} = 5$, not $\overline{5}$. We want to go forward from (42) the equivalent of about $\frac{1}{2} \cdot 52 = 26$ forms and so we compose (42) with

$$F_{26} = (3286, 2618, -3523) \tag{43}$$

This composition is readily computed [3, Appendix 1] to be

$$(5 \cdot 3286, -3954, -571)$$

which we reduce to

$$F = (5765, 6324, -571) \tag{44}$$

Now F should be close to an ambiguous form. It is, in fact F_{532} and therefore only one form away from the ambiguous form F_{533}.

Similarly, we compose the inverse of (40):

$$(-403, 7054, 2110) \tag{45}$$

(which happens to be $F_{463} = F_{1068-605}$ although we need not know that to factor N) together with

$$F_{82} = (3134, 2120, -3851) \tag{46}$$

We get

$$(-403 \cdot 3134, -54202, -572)$$

which again reduces to (44).

Now suppose that N is very much larger. If we are lucky and encounter a square form such as (37) early, we can go backwards from the square-root, as in Figure 2, and factor N with the P_n and Q_n alone, and with no composition of forms needed either. But, in general, we should anticipate that our square product (4) will involve several or many indices n with Σn beyond, or even much beyond, our last index n computed. We would therefore compute the product πF_n by composition as in (26). This product would remain in the principal equivalence class and would be

$$F = (\frac{Q^2}{K^2}, B, C) \tag{47}$$

for a K^2 caused by the cancellation of the conjugate prime ideals as in (26). (Usually, there will be considerable cancellation and Q^2 will be correspondingly much reduced in magnitude.) IF the product F were reduced, it would become F_m with $m \approx \Sigma n$. But we do <u>not</u> reduce F; we reduce the square-root

$$G = (\frac{Q}{K}, B, \frac{QC}{K}) \tag{48}$$

instead and compose its inverse G^{-1} with F_r where $r \approx m/2$. Then, somewhere in the vicinity of $G^{-1} * F_r$, we find an ambiguous form which gives us a proper or a trivial factor of $4N$.

Where do we get F_r? We may have already computed it, but, if so, we may have also discarded it. If we save F_{2^s} for $s = 0, 1, 2, ...$, and express r in binary, we can obtain an $F_{r'}$ by the composition of all those F_{2^s} where 2^s appears in this binary representation. If we need some F_{2^s} beyond the last F_{2^s} encountered, we may repeatedly square (and reduce) this last F_{2^s}. The resulting $F_{r'}$ will be close enough since we can only expect to put $G^{-1} * F_r$ into the vicinity of an ambiguous form. If r is large, say 10^6, we may, in fact, have to search the period of $G^{-1} * F_r$ for some way, in both directions, to find the ambiguous form. But that should be relatively fast since one merely computes the P and Q (without any factorization of the Q) until one find $2P_n = 2P_{n+1}$.

6 Other Equivalence Classes; the Whole Picture

Although (47) is in the principal equivalence class, all that we immediately know about (48) is that it is in some equivalence class whose square is the identity of the class group. The identity is represented by the principal period, and (48) (when reduced if necessary) may, or may not, lie in that period. Returning to $N = 13290059$, consider two other square reduced forms:

$$F_{370} = (53^2, 4272, -3107) \tag{49}$$
$$F_{88} = (41^2, 4702, -4618) \tag{50}$$

They have the reduced square-roots:

$$G = (53, 7240, -3503), \tag{51}$$
$$H = (41, 7244, -4175). \tag{52}$$

We first compute

$$G^{-1} * F_{185} = (53, 7282, -626) * (-179, 7170, 2446) = (-179 \cdot 53, 15762, -5146)$$

The product shown reduces to $(1129, 5470, -5146)$ and nine forms later in its period:

$$\begin{array}{llll} 1129 & 5470 & & \\ & \ldots & -5146 & \\ & \ldots & & \\ 1142 & 6238 & & \\ & 6238 & -3119 & \\ 1142 & & & \end{array}$$

we find the ambiguous form

$$G_m = (-3119, 6238, 1142) \tag{53}$$

which again gives $3119 \mid N$. But G and G_m do not lie in the principal period. In fact, no end-coefficient in the new period occurs as a $(-1)^n Q_n$ in the continued fraction algorithm as given in [1]. G and G_m lie in a nonprincipal period that "begins" as follows:

$$\begin{array}{llll} n & & & \\ 0 & -2 & 7290 & \\ 1 & & 4812 & 2017 \\ 2 & -3719 & \ldots & \end{array}$$

It has a period equal to some $2m \approx 1068$ whose exact value was not determined[2]. G_m is at its midpoint while $G = G_{m+r}$ with r some odd number ≈ 185.

[2] 1072, actually [SM]

Next we compute

$$H^{-1} * F_{44} = (41, 7270, -1874) * (937, 7270, -82).$$

The second form is equivalent to $(-82, -7270, 937)$ since (A, B, C) is always equivalent to $(C, -B, A)$, and so the required composition is immediately found to be the ambiguous form

$$G_0 = (-2, 7290, 2017) \tag{54}$$

seen above. Therefore, $2 \mid 4N$ and we have a failure - a trivial factor.

Since 2 ramifies and $(-1)^2 = 1$, any square reduced form such as (50) has at least four reduced square-roots, and the H of (52) is only one of these for (50). The four are

$$(\pm 41, 7244, \mp 4175) \text{ and } (\pm 82, 7162, \mp 5689) \tag{55}$$

and the last of these may be identified as

$$F_{45} = F_{22} * F_{23} = (-82, 7162, +5689),$$

as had been computed in Section 4 after (26). Now F_{45} does lie in the principal period, and $F_{45}^2 = F_{88}$, so F_{88} is seen to be equivalent to a trivial failure.

For this N, or any $N \equiv -1 \pmod 4$, $-1 = (-1)^n Q_n$ for no n in the principal period; or equivalently, $N(\epsilon) = +1$ for the ϵ of (35). Therefore, all four forms in (55) lie in distinct periods. The four periods begin, respectively, with the ambiguous forms

$$\pm F_0 = (\pm 1, 7290, \mp 4034), \ \pm G_0 = (\mp 2, 7290, \pm 2017) \tag{56}$$

and contain, respectively, four other ambiguous forms

$$\pm F_{534} = (\pm 6238, 6238, \mp 4034), \ \pm G_m = (\mp 3119, 6238, \pm 1142) \tag{57}$$

at their half-periods. So the principal form F_0 has eight reduced square-roots, one-half yielding proper factors and one-half yielding trivial factors.

These four periods having the discriminant $d = 4 \cdot 13290059$ are the only periods that occur for this d; i.e., the quadratic form class number equals 4. But the ideal class number equals 2 here. Multiplication by -1 leaves an ideal in the same equivalence class and so whenever $N(\epsilon) = +1$ the ideal class number is one-half of the quadratic form class number. The ideal class number h satisfies

$$\frac{2h \log \epsilon}{\sqrt{d}} = \prod_{p=2}^{\infty} \frac{p}{p - (\frac{d}{p})}.$$

For our d above, $(d/p) = 0$ for $p = 2$, $+1$ for $p = 5, 13, 31$, and -1 for other $p < 37$. Since we can roughly estimate $\log \epsilon$ from (35) and (22), we can roughly estimate h by

$$h \approx \frac{\sqrt{d} \cdot 12 \log 2}{2 \cdot 1068 \pi^2} \prod_{p=2}^{31} \frac{p}{p - (\frac{d}{p})} = 2.013$$

for this d.

Any other $N \equiv -1 \pmod 4$ that is divisible by exactly two distinct primes will again have four ambiguous periods, beginning as in (56), and having midpoints as in (57), but if the ideal class number of $\mathbb{Q}(\sqrt{N}) > 2$ there will be additional, nonambiguous periods that do not enter into our factorization process. The corresponding equivalence classes are not square-roots of the identity in the class group. If $N \equiv -1 \pmod 4$ is divisible by exactly k distinct primes, there will be 2^k ambiguous periods and 2^{k+1} reduced ambiguous forms. Of the latter, only those four with $\pm 1, \pm 2$ on the left will give trivial factors; all other factors are proper. So the probability of finding a proper factor increases with k.

These 2^k ambiguous periods include the principal period F that begins with F_0, and $2^k - 1$ periods $G^{(i)}$, for $i = 2$ to 2^k, that begin with ambiguous forms $G_0^{(i)}$ and have other ambiguous forms $G_{m_i}^{(i)}$, for certain m_i, at their midpoints. Then the composition $F_n F_m$, when reduced, equals F_r for some $r \approx n + m$, and similarly $G_n^{(i)} * G_m^{(i)}$ gives F_r while $F_n * G_m^{(i)}$ gives $G_r^{(i)}$. The resulting period, F or $G^{(i)}$, reflects the group structure, while the location of the product within its period $r \approx n + m$ reflects the infrastructure, cf. [4]. All of our analysis of failure above and both of our rules for finding factors of N are merely special cases of these laws of composition. Since the factors of N are end-coefficients of ambiguous forms, we do not need the A_n to compute them; we merely need to know how far away they are from our square-roots (48).

References

[1]

[2]

[3]

[4]