point of \( ac \) with a point of \( b \) and join a point of \( ab \) with a point of \( c \). Let \( x_1 \) in \( ab \), \( x_2 \) in \( ac \), be the points where this line meets these spaces. The line then contains \( x, x_1, x_2 \) all in \( a \), where although \( x_1 \) and \( x_2 \) might coincide, neither could be \( x \). But then the line would lie wholly in \( a \), contrary to hypothesis. Hence \( x(ab+ac) = 0 \), and (2) is established. Likewise \( y \) cannot be in \( ab+bc \). For if it were then \( x+y \) would be in \( a+ab+bc = a+bc \), contrary to hypothesis. Thus (4) is established, and (6) follows similarly. Hence for \( a \) to fail to be distributive in the second sense implies Case A. Conversely given Case A, then \( a \) fails to be distributive with respect to \( b \) and \( c \) in the second sense. Indeed \( y \) will then be in \( a+b \) and also in \( x+y \) which is in \( a+c \). But \( y \) will not be in \( a+bc \). For \( y \) is in \( b \), but not in \( ab+bc \), hence not in \( ab \) nor \( bc \), hence not in \( a \) nor \( bc \). If \( y \) were yet in \( a+bc \), there would be a point \( u \) in \( a \), and a point \( v \) in \( bc \) such that \( y \) would be in \( u+v \). But \( y \) and \( v \) are then distinct and are both in \( b \). Hence \( u+v \) is in \( b \), and \( u \) is in \( b \). Hence \( u \) is in \( ab \). Hence \( y \) would be in \( ab+bc \) contrary to hypothesis. Hence Case A is a necessary and sufficient condition that \( a \) fail to be distributive with respect to \( b \) and \( c \) in the second sense.

Since Case B is necessary and sufficient for \( a \) to be distributive with respect to \( b \) and \( c \) in the first sense and again also in the second sense, Theorem 1 is proved. Since this Case B is symmetric in \( a, b, \) and \( c \), Theorem 2 is proved.

BROWN UNIVERSITY

---

ON FACTORING LARGE NUMBERS*

BY D. H. LEHMER† AND R. E. POWERS

1. Introduction. Various non-tentative methods of factoring a given odd number \( N \), based on the expansion of \( N^{1/2} \) in a regular continued fraction, have been described.† The success of most of these methods depends on the appearance of a perfect square among the denominators of the complete quotients. In practice, however, such an event occurs all too infrequently. More often
it happens that the product of two or more denominators is a square. In this case two methods are available for obtaining a factorization of $N$. These methods are described and compared in the present paper.

Sometimes a denominator $Q_n$ of the $n$th complete quotient has a prime factor in common with $N$. This factor appears also in the numerators of the $n$th and $(n+1)$st complete quotients, and is recognized by inspection. We are therefore justified in assuming that as far as the expansion has been carried out, the numerators and denominators of the complete quotients are prime to $N$. Under this assumption we prove that the two methods described below will both fail or both succeed in a given instance. We also show in §5 that a natural attempt to modify and combine the two methods is doomed to failure.

2. The Method Using the $P$’s. In expanding the square root of $N$ in a continued fraction we have for the general form of the $n$th complete quotient

$$x_n = \frac{P_n + N^{1/2}}{Q_n}, \quad (x_0 = N^{1/2}, \; [x_n] = q_n).$$

From the familiar relation $P_n^2 + Q_nQ_{n-1} = N$, we have

$$-Q_nQ_{n-1} \equiv P_n^2 \pmod{N}. \quad (1)$$

For $n = 1$ this becomes $-Q_1 \equiv P_1^2$, since $Q_0 = 1$, and for $n = 2$ we get

$$Q_2P_1^2 \equiv P_2^2 \pmod{N}.$$

In general, if we write $(-1)^nQ_n = Q_n^*$, we have

$$Q_n^*(P_{n-1} \cdot P_{n-5} \cdot P_{n-9} \cdots P_r)^2 \equiv (P_n \cdot P_{n-2} \cdot P_{n-4} \cdots P_s)^2 \pmod{N}, \quad (2)$$

where $r = 1, s = 2$ or $r = 2, s = 1$, according as $n$ is even or odd. To prove this, we assume that (2) is true for $n - 1$, or

$$Q_{n-1}^*(P_{n-2} \cdot P_{n-4} \cdot P_{n-6} \cdots P_s)^2 \equiv (P_{n-1} \cdot P_{n-3} \cdot P_{n-5} \cdots P_r)^2, \quad (3)$$

and then show it true for $n$ as follows. Multiplying (1) by

$$(P_{n-1} \cdot P_{n-3} \cdots P_r)^2 \cdot (P_{n-2} \cdot P_{n-4} \cdots P_s)^2,$$

and dividing by (3), we get (2). But we have shown above that (2) is true for $n = 1, 2$; hence it is true in general.
Two \( Q^* \)'s are said to be equivalent if their product is a square, that is, \( Q^* \) is equivalent to \( Q_j^* \) if \( x^2Q_i^* = y^2Q_j^* \). From this equation we have by substituting \( n = i \) and \( n = j \) in (2), and noting that \( i \) and \( j \) are of the same parity,

\[
(4) \ (xP_{i+1}\cdot P_{i+3} \cdots P_{j-1})^2 - (yP_{i+2}\cdot P_{i+4} \cdots P_j)^2 \equiv 0 \pmod N.
\]

Unless \( N \) divides either \( (xP_{i+1}\cdot P_{i+3} \cdots P_{j-1}) \pm y(P_{i+2}\cdot P_{i+4} \cdots P_j) \), we obtain a factor of \( N \) by finding the G.C.D. of \( N \) and one of these numbers. If the two equivalent \( Q^* \)'s are near each other in the series of denominators, the factors of \( N \) will be disclosed with a minimum of effort.

This method may be extended to the case in which the product of more than two \( Q^* \)'s is a square. This involves a straightforward application of (2) as we illustrate later, and the ease with which the method may be applied depends again on the relative position of the \( Q^* \)'s and on the parities of their subscripts. It is of course unnecessary to compute the actual products of the \( P^* \)'s involved, since these products may be reduced modulo \( N \).

3. The Method Using the \( A^* \)'s. If \( A_n/B_n \) is the \( n \)th convergent to \( N^{1/2} \), we have the well known relation

\[
A_{n+1} - NB_n^2 = (-1)^nQ_n = Q_n^*,
\]

which can be written

\[
(5) \quad Q_n^* \equiv A_{n+1}^2 \pmod N.
\]

Hence if \( Q_i^* \) and \( Q_j^* \) are equivalent, so that \( x^2Q_i^* = y^2Q_j^* \), then

\[
(xA_{i-1})^2 - (yA_{j-1})^2 \equiv 0 \pmod N.
\]

Unless \( N \) divides either \( xA_{i-1} \pm yA_{j-1} \) it is possible by the greatest common divisor process to obtain a factorization of \( N \). In the same way more than two \( Q^* \)'s may be used. For example, if \( x^2Q_i^*Q_j^* = y^2Q_k^* \), then

\[
(xA_{i-1}A_{j-1})^2 - (yA_{k-1})^2 \equiv 0 \pmod N.
\]

The \( A^* \)'s are of course calculated by the familiar recurrence

\[
(6) \quad A_n = q_nA_{n-1} + A_{n-2}, \quad (A_{-2} = 0, A_{-1} = 1),
\]

and when necessary the \( A^* \)'s may be reduced modulo \( N \).
4. Comparison of the Methods. The two methods are best compared by a numerical example. Consider the case \( N = 13290059 \). The elements for \( N^{1/2} \) are as follows.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( P_n )</th>
<th>( Q_n^* )</th>
<th>( q_n )</th>
<th>( A_n(\text{mod } N) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3645</td>
<td>3645</td>
</tr>
<tr>
<td>1</td>
<td>3645</td>
<td>-2 \cdot 2017</td>
<td>1</td>
<td>3646</td>
</tr>
<tr>
<td>2</td>
<td>389</td>
<td>3257</td>
<td>1</td>
<td>7291</td>
</tr>
<tr>
<td>3</td>
<td>2868</td>
<td>-5 \cdot 311</td>
<td>4</td>
<td>32810</td>
</tr>
<tr>
<td>4</td>
<td>3352</td>
<td>1321</td>
<td>5</td>
<td>171341</td>
</tr>
<tr>
<td>5</td>
<td>3253</td>
<td>-2 \cdot 5^2 \cdot 41</td>
<td>3</td>
<td>546833</td>
</tr>
<tr>
<td>6</td>
<td>2897</td>
<td>2389</td>
<td>2</td>
<td>1265007</td>
</tr>
<tr>
<td>7</td>
<td>1881</td>
<td>-2 \cdot 13 \cdot 157</td>
<td>1</td>
<td>1811840</td>
</tr>
<tr>
<td>8</td>
<td>2201</td>
<td>2069</td>
<td>2</td>
<td>4888687</td>
</tr>
<tr>
<td>9</td>
<td>1937</td>
<td>-2 \cdot 5 \cdot 461</td>
<td>1</td>
<td>6700527</td>
</tr>
<tr>
<td>10</td>
<td>2673</td>
<td>31 \cdot 43</td>
<td>4</td>
<td>5110677</td>
</tr>
<tr>
<td>11</td>
<td>2659</td>
<td>-2 \cdot 2333</td>
<td>1</td>
<td>11811204</td>
</tr>
<tr>
<td>12</td>
<td>2007</td>
<td>5 \cdot 397</td>
<td>2</td>
<td>2152967</td>
</tr>
<tr>
<td>13</td>
<td>1963</td>
<td>-2 \cdot 2377</td>
<td>1</td>
<td>674112</td>
</tr>
<tr>
<td>14</td>
<td>2791</td>
<td>13 \cdot 89</td>
<td>5</td>
<td>5523527</td>
</tr>
<tr>
<td>15</td>
<td>2994</td>
<td>-3739</td>
<td>1</td>
<td>6197639</td>
</tr>
<tr>
<td>16</td>
<td>745</td>
<td>2 \cdot 13 \cdot 131</td>
<td>1</td>
<td>11721166</td>
</tr>
<tr>
<td>17</td>
<td>2661</td>
<td>-1823</td>
<td>3</td>
<td>1490960</td>
</tr>
<tr>
<td>18</td>
<td>2808</td>
<td>5 \cdot 593</td>
<td>2</td>
<td>1413027</td>
</tr>
<tr>
<td>19</td>
<td>3122</td>
<td>-5 \cdot 239</td>
<td>5</td>
<td>8556095</td>
</tr>
<tr>
<td>20</td>
<td>2853</td>
<td>2 \cdot 5 \cdot 431</td>
<td>1</td>
<td>9969122</td>
</tr>
<tr>
<td>21</td>
<td>1457</td>
<td>-2591</td>
<td>1</td>
<td>5235158</td>
</tr>
<tr>
<td>22</td>
<td>1134</td>
<td>41 \cdot 113</td>
<td>1</td>
<td>1914221</td>
</tr>
<tr>
<td>23</td>
<td>3499</td>
<td>-2 \cdot 113</td>
<td>31</td>
<td>11415773</td>
</tr>
<tr>
<td>24</td>
<td>3507</td>
<td>5 \cdot 877</td>
<td>1</td>
<td>39935</td>
</tr>
<tr>
<td>25</td>
<td>878</td>
<td>-5 \cdot 571</td>
<td>1</td>
<td>11455708</td>
</tr>
<tr>
<td>26</td>
<td>1977</td>
<td>2 \cdot 31 \cdot 53</td>
<td>1</td>
<td>11495643</td>
</tr>
<tr>
<td>27</td>
<td>1309</td>
<td>-13 \cdot 271</td>
<td>1</td>
<td>9661292</td>
</tr>
<tr>
<td>28</td>
<td>2214</td>
<td>2381</td>
<td>2</td>
<td>4238109</td>
</tr>
<tr>
<td>29</td>
<td>2548</td>
<td>-5 \cdot 571</td>
<td>2</td>
<td>4847451</td>
</tr>
<tr>
<td>30</td>
<td>3162</td>
<td>1153</td>
<td>5</td>
<td>1895246</td>
</tr>
<tr>
<td>31</td>
<td>2603</td>
<td>-2 \cdot 5^2 \cdot 113</td>
<td>1</td>
<td>6742697</td>
</tr>
<tr>
<td>32</td>
<td>3047</td>
<td>709</td>
<td>9</td>
<td>9419283</td>
</tr>
<tr>
<td>33</td>
<td>3334</td>
<td>-3067</td>
<td>2</td>
<td>12291204</td>
</tr>
<tr>
<td>34</td>
<td>2800</td>
<td>1777</td>
<td>3</td>
<td>6422718</td>
</tr>
<tr>
<td>35</td>
<td>2531</td>
<td>-2 \cdot 13 \cdot 149</td>
<td>1</td>
<td>5423863</td>
</tr>
<tr>
<td>36</td>
<td>1343</td>
<td>5 \cdot 593</td>
<td>1</td>
<td>11846581</td>
</tr>
</tbody>
</table>

† This number is a factor of 254903331620, which in turn is the 55th term of the sequence 276, 396, 696, \ldots, in which each term is the sum of the aliquot parts of its predecessor.
The easiest method of factoring $N$ is to apply the $P$ method to the equal denominators $Q_{25}^* = Q_{29}^* = -2855$. For this case (4) reduces to

$$(P_{26} \cdot P_{28})^2 - (P_{27} \cdot P_{29})^2 \equiv 0 \pmod{N}.\]$$

The G.C.D. of $N$ and $P_{26} \cdot P_{28} - P_{27} \cdot P_{29}$ is found to be 3119, and

$$N = 13290059 = 3119 \cdot 4261.$$

Similarly it is found that $Q_{18}^* = Q_{36}^* = 2965$, and the factors of $N$ can be obtained in the same way, but with more effort, since these $Q^*$'s are 18 terms apart and hence more $P$'s are involved. Also $Q_{23}^* = -2 \cdot 113$ is equivalent to $Q_{31}^* = -2 \cdot 5^2 \cdot 113$, from which the factors of $N$ may be found.

The case in which three $Q^*$'s are involved is illustrated by $Q_{5}^*, Q_{22}^*$ and $Q_{23}^*$, where the difference $5 \cdot P_3 P_4 P_{23} - 113 \cdot P_1 P_3 P_6$ has the factor 3119 in common with $N$. In each of these instances the $A$ method is applicable. In the last case, for instance, we can write

$$(5 \cdot A_{21} \cdot A_{22})^2 - (113 \cdot A_4)^2 \equiv 0 \pmod{N},$$

from which the factors of $N$ follow. This example shows the advantages of the $P$ method when two equivalent $Q^*$'s appear near each other. When this is not the case, however, the method using the $A$'s is more expeditious since the calculations are simpler.

We now show that the ease of application is the only deciding factor in choosing one of the two methods. To do this we make use of the following lemma.

**Lemma.** If $n$ is any integer, then

$$P_n + (-1)^n A_{n-1} A_{n-2} \equiv 0 \pmod{N},$$

**Proof.** For $n = 0, 1, 2$ this is true, though trivial. Supposing the lemma is true for $n - 1$, we show it true for $n$ itself as follows:

We have by assumption

$$P_{n-1} + (-1)^{n-1} A_{n-2} A_{n-3} \equiv 0 \pmod{N}.$$

Adding and subtracting $Q_{n-1} q_{n-1}$ and using the recurrence

$$(7) \quad P_n = Q_{n-1} q_{n-1} - P_{n-1},$$
we find
\[ 0 = P_{n-1} - Q_{n-1}q_{n-1} + (-1)^{n-1}A_{n-2}A_{n-3} + Q_{n-1}q_{n-1} \]
\[ = -P_n + (-1)^{n-1}A_{n-2}(A_{n-3} + A_{n-2}q_{n-1}) \]
\[ = -P_n + (-1)^{n-1}A_{n-2}A_{n-1}. \]

That is
\[ P_n + (-1)^n A_{n-1} A_{n-2} \equiv 0 \pmod{N}, \]
which is the lemma.

**Theorem 1.** The success of one method in a particular instance implies the success of the other.

**Proof.** For simplicity the proof is given for the case of two equivalent \( Q^* \)'s. It can be easily amplified to cover the general case. Let \( Q_i^* \) and \( Q_j^* \) be equivalent, so that
\[ x^2 Q_i^* = y^2 Q_j^*. \]

Suppose now that the \( A \) method succeeds and that the \( P \) method fails. Then \( N \) will divide either
\[ (xP_{i+1}P_{i+3}P_{i+5} \cdots P_{j-1}) \pm y(P_{i+2}P_{i+4}P_{i+6} \cdots P_j). \]

Substituting for each \( P \) its value in terms of the \( A \)'s as given by the lemma we have, after simplifying, either
\[ xA_{i-1} \pm yA_{j-1} \equiv 0 \pmod{N}. \]

This implies the failure of the \( A \) method contrary to hypothesis. Therefore the \( P \) method succeeds.

By reversing the argument we may show that the success of the \( P \) method implies the success of the \( A \) method. This is done without using the assumption of §1 that the \( P \)'s are prime to \( N \). Hence we may restate Theorem 1 in a more precise form as follows.

The only instance of the success of one method and the failure of the other is that in which the \( A \) method succeeds, the \( P \) method fails, and a factor of \( N \) appears among the \( P \)'s and \( Q \)'s.

\[ \dagger \] The ± signs do not necessarily correspond to those in (8).

\[ \ddagger \] An example of this instance is offered by \( N = 611, Q_6 = Q_8 = 17 \). Of course both methods fail when \( N \) is a prime, but the failure of either method should not be taken as an indication of the primality of \( N \).
5. Simultaneous Use of Both Methods. Since each method finds a square to which \( Q^*_n \) is congruent mod \( N \), one is naturally tempted to use both methods with any fixed \( Q \) whatsoever to obtain at once a difference of squares divisible by \( N \). Unfortunately we have the following result.

**Theorem 2.** The two different methods for obtaining squares congruent to a particular denominator \( Q^*_k \) will not give a factorization of \( N \) if used together.

**Proof.** By the \( P \) method we have

\[
P^2_{k-1} \cdot Q^*_k = P^2_k \cdot Q^*_{k-2}.
\]

This follows by writing (2) for \( n = k \) and \( n = k - 2 \) and taking their ratio. By the \( A \) method we have for the same \( Q^*_k \)

\[
Q^*_k \equiv A^2_{k-1} \quad \text{(mod \( N \))}.
\]

Eliminating the \( Q^*_k \)'s from (9) and (10), we have the desired difference of squares

\[
P^2_{k-1} A^2_{k-2} - P^2_k A^2_{k-1} \equiv 0 \quad \text{(mod \( N \))}.
\]

But we now show that \( N \) always divides the sum

\[
P_k A_{k-3} + P_{k-1} A_{k-1}.
\]

In fact this sum, in view of (5), (6) and (7), is congruent to

\[
q_{k-1} A^2_{k-2} \{ P_{k-1} + ( -1)^{k-1} \cdot A_{k-2} A_{k-3} \}.
\]

By the lemma with \( n = k - 1 \), the quantity in brackets is divisible by \( N \), hence \( N \) divides the sum (11).

Factorization is therefore possible only if \( N \) has a factor in common with the difference

\[
A_{k-1} P_{k-1} - A_{k-3} P_k.
\]

Such a factor would be common to

\[
A_{k-1} P_{k-1} - A_{k-3} P_k + ( A_{k-1} P_{k-1} + A_{k-3} P_k ) = 2 A_{k-1} P_{k-1}.
\]

But \( N \) is odd and prime to the \( P \)'s and \( Q \)'s, and, from (5), to the \( A \)'s, hence the theorem.

Stanford University and Denver Colorado