# Continued Fraction Factorisation Algorithm

*Jean-Paul Hii*

## Abstract

In mathematics, especially number theory, continued fractions allow us to represent a real number by successive divisions of integers. Applications of continued fractions include constructing rational approximations to irrational numbers and helping to solve the Diophantine and Pell's equations. In particular, the continued fraction algorithm (CFRAC) is a powerful integer factorisation algorithm. It was described by D. H. Lehmer and R. E. Powers in 1931, whose theoretical basis will be explored today. It has been described as a general-purpose algorithm, meaning that it is suitable for factoring any integer $n$, independent of the number's properties. The CFRAC, in its operation, also helps us find congruences of the form $x^2 \equiv y^2 \pmod{n}$. I will introduce some statements about continued fractions to motivate the purpose of this report. This will be followed with an introduction of $n$-th complete quotients and how they produce the integers needed for the CFRAC. The CFRAC can be carried out via two methods which I will call the "A method" and "P method", whose strengths and weaknesses will be discussed. Lastly, a faster algorithm, described by Michael A. Morrison and John Brillhart, which computerised the A method, will also be examined.

## I. Basic Facts about Continued Fractions

I will present some basic facts about continued fractions here.

**Definition 1.1.** A continued fraction is of the form

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 \ldots}}} \tag{1}$$

*We can also identify continued fractions in sequence form as* $x = [q_0; q_1, q_2, \ldots], q_i \in \mathbb{Z}$.

The above is an example of an infinite continued fraction; a finite continued fraction in sequence form is $x = [q_0; q_1, q_2, \ldots, q_n], n \in \mathbb{N}$.

**Theorem 1.2.** Every $x \in \mathbb{Q}$ can be represented as a finite continued fraction.

**Example 1.3.** In order to represent $\frac{62}{23}$ as a finite continued fraction, we can apply the Euclidean algorithm to 62 and 23 to obtain:

$$\frac{62}{23} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \frac{1}{2}}}} = [2; 1,2,3,2] \tag{2}$$

**Definition 1.4.** *If* $[q_0, \ldots, q_n]$ *is a finite continued fraction, its* $k$*-th convergent is* $[q_0, \ldots, q_k]$ *where* $k \leq n$*. More generally, if* $[q_0, q_1, \ldots]$ *is an infinite continued fraction, then its k-th convergent is* $[q_0, \ldots, q_k]$ *for some k.*

**Definition 1.5.** $[q_0, q_1, \ldots] = \lim_{k\to\infty}[q_0, \ldots, q_k]$.

**Theorem 1.6.** Let $q_0, q_1, \ldots$ be a sequence such that $q_i > 0$ whenever $i > 0$. Define $A_0 = q_0$, $B_0 = 1$, $A_1 = q_0 q_1 + 1$, $B_1 = q_1$ and the following recurrence relations for $i > 1$:

$$A_i = q_i A_{i-1} + A_{i-2}. \tag{3}$$

$$B_i = q_i B_{i-1} + B_{i-2}. \tag{4}$$

*Then, the k-th convergent is* $[q_0; q_1, \ldots q_k] = \frac{A_k}{B_k}$.

Intuitively, if one considers $\frac{A_k}{B_k} = \frac{q_k A_{k-1} + A_{k-2}}{q_k B_{k-1} + B_{k-2}}$, then they can substitute all previous recurrence relations into the equation to get the continued fraction. We will prove this by induction on $k$, however.

*Proof of Theorem 1.6.* We proove this by induction on *k*.

Base case $k = 0$: $\frac{A_0}{B_0} = a_0 = [a_0]$.

Induction hypothesis: Suppose the theorem holds for some $k = n$.

Induction step: We want to show that $[q_0; q_1, \dots q_k, q_{k+1}] = \frac{A_{k+1}}{B_{k+1}}$. Since $[q_0; q_1, \dots q_k, q_{k+1}] = \left[q_0; q_1, \dots q_k + \frac{1}{q_{k+1}}\right]$, we have:

$$\begin{aligned}\left[q_0; q_1, \dots q_k + \frac{1}{q_{k+1}}\right] &= \frac{\left(q_k + \frac{1}{q_{k+1}}\right) A_{k-1} + A_{k-2}}{\left(q_k + \frac{1}{q_{k+1}}\right) B_{k-1} + B_{k-2}} \\ &= \frac{q_k A_{k-1} + A_{k-2} + \frac{A_{k-1}}{q_{k+1}}}{q_k B_{k-1} + B_{k-2} + \frac{B_{k-1}}{q_{k+1}}} \\ &= \frac{q_{k+1} A_k + A_{k-1}}{q_{k+1} B_k + B_{k-1}} \\ &= \frac{A_{k+1}}{B_{k+1}}\end{aligned}$$

□

# II. Periodic Continued Fractions

When is an infinite continued fraction periodic? That is, if $x$ is irrational, when is $x = \left[q_0; q_1, \dots q_j, \overline{q_{j+1}, \dots q_{j+p}}\right]$? Here, $p$ denotes the periodicity of the terms repeated.

**Definition 2.1.** An element $a \in \mathbb{R}$ is a quadratic surd if it is irrational and there exists a quadratic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(a) = 0$.

**Theorem 2.2.** Let x ∈ ℝ, then the continued fraction for x is infinite and periodic if and only if x is a quadratic surd.

**Example 2.3.** The golden ratio $\phi = \frac{1+\sqrt{5}}{2}$ is a solution to the quadratic equation $x^2 - x - 1 = 0$ and its continued fraction is $[1; 1,1, \dots]$.

In the case of $x = \sqrt{N}$, where $N$ is a square free positive integer, we get an interesting result.

**Theorem 2.4.** Let $N$ be a square free positive integer, then the period starts after the first term in the continued fraction for $\sqrt{N}$, i.e. $\sqrt{N} = \left[q_0; \overline{q_1, q_2, \dots, q_{p-1}, 2q_0}\right]$. Moreover, the sequence $q_1, q_2, \dots, q_{p-1}$ has the property that $q_{p-i} = q_i$ for $1 \leq i \leq p-1$.

**Example 2.5.** $\sqrt{7} = \left[2; \overline{1,1,1,4}\right]$.

We now move on to the main part of this report. There is a simple algorithm which computes the $q_i$'s in the continued fraction of $\sqrt{N}$ using only integer arithmetic. However, the downside is that several other integers will also be computed, which add extra calculations when attempting to factor an integer using CFRAC. These integers are shown in Equations (6) and (7).

**Definition 2.6.** The $n$-th complete quotient of $x_n$, where $x_n$ is the $n$-th convergent of $\sqrt{N}$ is defined as

$$x_n = \begin{cases} \sqrt{N}, & \text{if } n = 0 \\ \dfrac{1}{x_{i-1} - q_{i-1}}, & \text{if } n \geq 1 \end{cases} \tag{5}$$

The work done until now implies that if we want to factor an integer $N$, we should consider the continued fraction expansion of $\sqrt{N}$, which the CFRAC does. The trouble is that we need the presence of perfect squares among the denominators of our complete quotients. However,

the product of two or more distinct denominators is often a square, which will lead to the A and P methods.

We will now rewrite our complete quotients into something which will be useful down the road. With enough algebraic manipulation, one can check that $x_n = \frac{P_n+\sqrt{N}}{Q_n}$ for $n \geq 0$, where:

$$P_n = \begin{cases} 0 & \text{if } n = 0 \\ q_0 & \text{if } n = 1 \\ q_{n-1}Q_{n-1} - P_{n-1} & \text{if } n \geq 2, \end{cases} \tag{6}$$

and

$$Q_n = \begin{cases} 1 & \text{if } n = 0 \\ N - q_0^2 & \text{if } n = 1 \\ Q_{n-2} + (P_{n-1} - P_n)q_{n-1} & \text{if } n \geq 2. \end{cases} \tag{7}$$

Finally, the $q_n$'s can be computed by

$$q_n = \lfloor x_n \rfloor = \begin{cases} \lfloor \sqrt{N} \rfloor, & \text{if } n = 0 \\ \left\lfloor \dfrac{\sqrt{N} + P_n}{Q_n} \right\rfloor, & \text{if } n \geq 1 \end{cases} \tag{8}$$

With $A_n$ and $B_n$ defined as in Theorem 1.6, we have the following two equalities:

$$(-1)^n Q_n = A_{n-1}^2 - B_{n-1}^2 N, \tag{9}$$

and

$$N = P_n^2 + Q_n Q_{n-1}. \tag{10}$$

Equations (9) and (10) will be the key drivers in the A and P method respectively; the $Q_n$'s are particularly significant in both methods.

**Definition 2.7.** Let $(-1)^n Q_n = Q_n^*$. Two $Q_n^*$'s are equivalent if their product is a square, that is, $Q_i *$ is equivalent to $Q_j *$ if $x^2 Q_i^* = y^2 Q_j^*$ for $x, y \in \mathbb{Z}$.

# III. LEHMER AND POWERS

## A. The A method

Let $\frac{A_n}{B_n}$ be the $n$-th convergent of the continued fraction expansion of $\sqrt{N}$. Then Equation (9) gives us

$$(-1)^n Q_n \equiv A_{n-1}^2 \pmod{N}. \tag{11}$$

Thus, if $Q_i^*$ is equivalent to $Q_j^*$, then

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

This relates to the general strategy we will try to use to factor $N$:

**Theorem 3.1.** If N is a composite integer, $x, y \in \mathbb{Z}$, and $x^2 \equiv y^2 \pmod{N}$, but $x \not\equiv \pm y \pmod{N}$, then $gcd(x-y, N)$ and $gcd(x+y, N)$ are proper factors of N.

*Proof of Theorem 3.1.* The assumption implies that $N$ divides $x^2 - y^2 = (x+y)(x-y)$, but $N$ does not divide either of the factors. Since $N$ is composite, at least one of its prime factors does not divide $x+y$, so those prime factors must divide $x-y$ instead, and the same argument goes for $x-y$. Thus $\gcd(x-y, N)$ and $\gcd(x+y, N)$ are both greater than 1 and less than $N$.

Therefore, unless $N$ divides either $xA_{i-1} \pm yA_{j-1}$, it is possible to obtain a factorisation of $N$.

The A method allows for multiple $Q_n$'s to be used, that is, if $x^2 Q_i^* Q_j^*$ is equivalent to $y^2 Q_k^*$, then

$$(xA_{i-1}A_{j-1})^2 \equiv (yA_{k-1})^2 \pmod{N} \tag{12}$$

which is an instance of Theorem 3.1.

□

One may wonder what is the chance of choosing $x$ and $y$ such that they satisfy Definition 2.7. It turns out the probability is better than 50-50.

**Theorem 3.2.** If N is a odd composite integer with at least two different prime factors and $x, y \in \mathbb{Z}$ are randomly chosen subject to $x^2 \equiv y^2$ (mod N), then gcd(x-y, N) is a proper factor of N with probability greater than or equal to $\frac{1}{2}$.

*Proof of Thoerem 3.2.* Suppose $N$ is odd and has more than two different prime factors. Let $x, y \in \mathbb{Z}$ be such that $x^2 \equiv y^2 \pmod{N}$. By the Chinese Remainder Theorem, $x^2 \equiv y^2 \pmod{p^k}$ for a prime factor $p$ of $N$ and $k \in \mathbb{N}$. $y^2$ is then a quadratic residue mod $p$, and so the congruence $x^2 \equiv y^2 \pmod{p^k}$ has two solutions $x = \pm y$. Hence, there are $2^k$ solutions to $x^2 \equiv y^2 \pmod{N}$. Therefore, if we choose $x$ and $y$ randomly, the probability that $x^2 \not\equiv y^2 \pmod{N}$ would be $\frac{2^k-2}{2^k} = 1 - 2^{k-1}$. Thus, the probability that $x^2 \equiv y^2 \pmod{N}$ is greater than or equal to $\frac{1}{2}$.

□

## B. The P method

From Equation (10), we have

$$-Q_n Q_{n-1} \equiv P_n^2 \pmod{N}. \tag{12}$$

Let's substitute in different $n \in \mathbb{N}$ to see how Equation (13) behaves. If $n = 1$, we get

$$-Q_1 \equiv P_1^2 \pmod{N}.$$

If $n = 2$, we get

$$Q_2 P_1^2 \equiv P_2^2 \pmod{N}.$$

If $n = 3$, we get

$$-Q_3 P_2^2 \equiv (P_3 P_1)^2 \pmod{N}.$$

Proposition 3.3.

$$(-1)^k Q_k (P_{k-1} P_{k-3} \dots P_r)^2 \equiv (P_k P_{k-2} \dots P_s)^2 \pmod{N},$$

*where* $r = 1$ *and* $s = 2$ *when* $k$ *is even and* $r = 2$ *and* $s = 1$ *when* $k$ *is odd.*

*Proof of Proposition 3.3.* We prove this by induction on $k$.
Base case $k = 1$: already shown above.
Induction hypothesis: suppose the statement is true for $k = n - 1$. That is,

$$(-1)^{n-1} Q_{n-1} (P_{n-2} P_{n-4} \dots P_s)^2 \equiv (P_{n-1} P_{n-3} \dots P_r)^2 \pmod{N}. \tag{13}$$

Observe that $r$ and $s$ swapped positions because the parity of $k$ changed.
Induction step: multiply both sides of Equation (13) by $(P_{n-2} P_{n-4} \dots P_s)^2 \cdot (P_{n-1} P_{n-3} \dots P_r)^2$. Then, divide the LHS by the LHS from Equation (14) and divide the RHS by the RHS from Equation (14). If done right, this should look like:

$$(-1)^n Q_n (P_{n-1} P_{n-3} \dots P_r)^2 \equiv (P_n P_{n-2} \dots P_s)^2 \pmod{N}$$

which finishes the proof.
□

**Remark 3.4.** Recalling what it takes for two $Q_k^*$'s to be equivalent, we want to try and find instances where $i$ and $j$ are of the same parity so that

$$(x P_{i+1} P_{i+3} \dots P_{j-1})^2 \equiv (y P_{i+2} P_{i+4} \dots P_j)^2 \pmod{N} \tag{15}$$

*which is an instance of Theorem 3.1. Then, as with the A method, unless* $N$ *divides either* $x P_{i+1} P_{i+3} \dots P_{j-1} \pm y P_{i+2} P_{i+4} \dots P_j$*, it is possible to obtain a factorisation of* $N$.

# IV. COMPARISON OF A METHOD AND P METHOD

It is now appropriate to do an example. I will use the integer $N = 13290059$. This was the number used in the resources, but several $n$

values were missed out, I will fill them in to provide a better view on how each $q_n$, $P_n$, $Q_n^*$ and $A_{n-1} \pmod N$ are calculated.
Since $\lfloor \sqrt{13290059} \rfloor = 3645, q_0 = 3645$. We then use Equations (6), (7), (8) and (11) to calculate all desired values. Observe that the $Q_n^*$'s are factored, and the ones that are not imply that those $Q_n$'s are prime, this observation will become significant later on.
According to Remark 3.4, we want to find instances where two indices are of the same parity for the P method. Looking at Table 1, observe that $Q_{25} = Q_{29}$ and both 25 and 29 are odd. Therefore, Equation (14) tells us that

$$(P_{26}P_{28})^2 \equiv (P_{27}P_{29})^2 \ (mod\ N).$$

In this case, $x$ and $y$ have cancelled each other out, because they equal $5 \cdot 571$. We see $P_{26}P_{28} \not\equiv P_{27}P_{29} \pmod N$. Therefore, by Theorem 3.1, we conclude that $\gcd(P_{26}P_{28} - P_{27}P_{29}, N) = 3119$ is a proper factor of $N$.

To use more than two $Q_n^*$'s, we look at the $Q_n^*$ column and choose the values whose product gives a square. For example, we can choose $Q_5^*$, $Q_{22}^*$ and $Q_{23}^*$, because their product gives $(2 \cdot 5 \cdot 41 \cdot 113)^2$. By Proposition 3.3, we have the following congruences:

$$(-1)^5 Q_5 (P_4P_2)^2 \equiv (P_5P_3P_1)^2 \pmod N, \tag{16}$$

$$(-1)^{22} Q_{22} (P_{21}P_{19} \dots P_1)^2 \equiv (P_{22}P_{20} \dots P_2)^2 \pmod N, \tag{17}$$

and

$$(-1)^{23} Q_{23} (P_{22}P_{20} \dots P_2)^2 \equiv (P_{23}P_{21} \dots P_1)^2 \pmod N. \tag{18}$$

By switching the LHS and RHS of Equations (17) and (18), multiplying all three equations together and cancelling out appropriately, we have

$$(5P_2P_4P_{23})^2 \equiv (113P_1P_3P_5)^2 \pmod N,$$

implying that $\gcd(5P_2P_4P_{23} - 113P_1P_3P_5, N) = 3119$ is a proper factor of $N$.

| $n$ | $q_n$ | $P_n$ | $Q_n^*$ | $A_{n-1} \pmod N$ |
|---|---|---|---|---|
| 0 | 3645 | 0 | 1 | 1 |
| 1 | 1 | 3645 | -2·2017 | 3645 |

| | | | | |
|---|---|---|---|---|
| 2 | 1 | 389 | 3257 | 3646 |
| 3 | 4 | 2868 | -5·311 | 7291 |
| 4 | 5 | 3352 | 1321 | 32810 |
| 5 | 3 | 3253 | $-2 \cdot 5^2 \cdot 41$ | 171341 |
| 6 | 2 | 2897 | 2389 | 546833 |
| 7 | 1 | 1881 | $-2 \cdot 13 \cdot 157$ | 1265007 |
| 8 | 2 | 2201 | 2069 | 1811840 |
| 9 | 1 | 1937 | $-2 \cdot 5 \cdot 461$ | 4888687 |
| 10 | 4 | 2673 | $31 \cdot 43$ | 6700527 |
| 11 | 1 | 2659 | $-2 \cdot 2333$ | 5110677 |
| 12 | 2 | 2007 | $5 \cdot 397$ | 11811204 |
| 13 | 1 | 1963 | $-2 \cdot 2377$ | 2152967 |
| 14 | 5 | 2791 | $13 \cdot 89$ | 674112 |
| 15 | 1 | 2994 | -3739 | 5523527 |
| 16 | 1 | 745 | $2 \cdot 13 \cdot 131$ | 6197639 |
| 17 | 3 | 2661 | -1823 | 11721166 |
| 18 | 2 | 2808 | $5 \cdot 593$ | 1490960 |
| 19 | 5 | 3122 | $-5 \cdot 239$ | 1413027 |
| 20 | 1 | 2853 | $2 \cdot 5 \cdot 431$ | 8556095 |
| 21 | 1 | 1457 | -2591 | 9969122 |
| 22 | 1 | 1134 | $41 \cdot 113$ | 5235158 |
| 23 | 31 | 3499 | $-2 \cdot 113$ | 1914221 |
| 24 | 1 | 3507 | $5 \cdot 877$ | 11415773 |
| 25 | 1 | 878 | $-5 \cdot 571$ | 39935 |
| 26 | 1 | 1977 | $2 \cdot 31 \cdot 53$ | 11455708 |
| 27 | 1 | 1309 | $-13 \cdot 271$ | 11495643 |
| 28 | 2 | 2214 | 2381 | 9661292 |
| 29 | 2 | 2548 | $-5 \cdot 571$ | 4238109 |
| 30 | 5 | 3162 | 1153 | 4847451 |
| 31 | 1 | 2603 | $-2 \cdot 5^2 \cdot 113$ | 1895246 |
| 32 | 9 | 3047 | 709 | 6742697 |
| 33 | 2 | 3334 | -3067 | 9419283 |
| 34 | 3 | 2800 | 1777 | 12291204 |
| 35 | 1 | 2531 | $-2 \cdot 13 \cdot 149$ | 6422718 |
| 36 | 1 | 1343 | $5 \cdot 593$ | 5423863 |
| 37 | 1 | 1622 | -5·719 | 11846581 |
| 38 | 2 | 1973 | 2·1307 | 2463469 |
| 39 | 6 | 3255 | -1031 | 5899447 |
| 40 | 1 | 2931 | $2 \cdot 43 \cdot 53$ | 3213960 |

Table 1: Continued fraction for $\sqrt{13290059}$.

Since we took the time to calculate $A_{n-1} \pmod N$, we can also use the A method to greatly simplify our work above. If we take $Q_5^*$, $Q_{22}^*$ and

$Q_{23}^*$ again, this time we look at the $A_{n-1} \pmod N$ and pick out $A_4$, $A_{21}$ and $A_{22}$ as the values to Equation (12), doing so implies

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

and thus $\gcd(5A_{21}A_{22} - 113A_4, N) = 3119$ is a proper factor of $N$.
From Table 1, we can see that it really only depends on the ease of application. For the P method, if we see two equivalent $Q_n^*$'s whose $n$ are close to each other ("close" is up to the reader's discretion), it will be efficient; we can also use the P method for more than two $Q_n^*$'s, it will just take a longer calculation, which is where the A method becomes more beneficial, since it requires simpler calculations. However, to calculate the values needed for the A method is arguably harder than calculating the values needed for the P method because Equation (11) is a quadratic equation.

# V. MORRISON AND BRILLHART

Morrison and Brillhart reprised the A method of the CFRAC discovered by Lehmer and Powers and improved it by using Gaussian elimination on vectors of exponents modulo 2. Before exploring how they used Gaussian elimination, we introduce the concept of smoothness of numbers:

**Definition 5.1.** A positive integer is $B$-smooth if there exists $B \in \mathbb{N}$ such that the integer's prime factors are all less than or equal to $B$.
These were the steps Morrison and Brillhart took in order use vectors:

1. Recall that some of the $Q_n$s were composite. Pick an upper bound $B \in \mathbb{N}$.

2. Keep the $Q_n^*$s whose $Q_n$s factored into primes less than or equal to $B$. In other words, we want to find the $Q_n$s that are $B$-smooth.

3. Those primes form a set called the factor base. For convenience, we add -1 as a "prime" into the factor base because we want to square the $Q_n^*$s.

4. When $Q_n$ is $B$-smooth, define the vector $\vec{v}_n$ whose entries are made up of the multiplicity modulo 2 of those prime factors. That is, if the prime factors of $Q_n$ are ordered and the $i$-th prime has an even or odd power, then the $i$-th entry of $\vec{v}_n$ is 0 or 1 respectively.

5. Form a matrix whose rows are the $\vec{v}_n$s for which $Q_n$ is $B$-smooth.

6. Since $\{0,1\} \in \mathbb{Z}_2$, these are the only possible coefficients for our linear combinations.

7. Let $S$ be the set of $i$ for which $\vec{v}_i$ is in dependency. Then $\prod_{i \in S} Q_n^* = y^2$ for some $y \in Z$.

8. Let $x = \prod_{i \in S} A_{n-1} \pmod N$, then we get $x^2 \equiv y^2 \pmod N$, which by Equation (15) leads to an instance of Theorem 3.1.

Let's use this algorithm on $N = 13290059$. Again, I will replicate the work done in the resources provided but give more details. Choose our upper bound $B = 113$ and find all primes less than or equal to 113 (there are 30 in total). Choose our factor base to be the set $\{-1,2,5,31,43,53,113\}$. Observe that we could've added other primes in such as 3 or 7 but notice that those primes never occurred in Table 1, implying that they rarely or never occur in the factorisations of the $Q_n$s. Thus, using them is redundant.

We now want to choose $n$ such that the factorisation of $Q_n$ gives us prime factors in the factor base. For example, we do not want to choose $Q_2$ because 2017 is not in our factor base; had 41 been in the factor base, we could've chosen $Q_5$.

Let's choose $Q_{10}$, $Q_{23}$, $Q_{26}$, $Q_{31}$ and $Q_{40}$, referring back to Table 1 for their factorisations. We can choose more, but keep in mind that we want more rows than columns in our matrix.

| $n$/factor base | $-1$ | 2 | 5 | 31 | 43 | 53 | 113 | |
|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | $= \vec{v}_{10}$ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 23 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | $= \vec{v}_{23}$ |
| 26 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | $= \vec{v}_{26}$ |
| 31 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | $= \vec{v}_{31}$ |
| 40 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | $= \vec{v}_{40}$ |

Table 2: Factor base and the $\vec{v}_n$s

We now construct the 5 x 7 matrix whose rows are made up of the $\vec{v}_n$s:

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Here, we see that the first, third and fifth rows are linearly dependent and the second and fourth rows are linearly dependent. The first dependency gives

$$(6700527 \cdot 11455708 \cdot 3213960)^2 \equiv (2 \cdot 31 \cdot 43 \cdot 53)^2 \pmod{N},$$

but neither

$$\gcd\left((6700527 \cdot 11455708 \cdot 3213960)^2 - (2 \cdot 31 \cdot 43 \cdot 53)^2, N\right)$$

nor

$$\gcd\left((6700527 \cdot 11455708 \cdot 3213960)^2 + (2 \cdot 31 \cdot 43 \cdot 53)^2, N\right)$$

factor *N*. The second dependency gives

$$(1914221 \cdot 1895246)^2 \equiv (2 \cdot 5 \cdot 113)^2 \pmod{N}.$$

We, then, have

$$\gcd\left((1914221 \cdot 1895246)^2 - (2 \cdot 5 \cdot 113)^2, N\right) = 4261$$

and

$$\gcd\left((1914221 \cdot 1895246)^2 + (2 \cdot 5 \cdot 113)^2, N\right) = 3119.$$

These are the proper factors of $N$.

We now present the algorithm:

Algorithm 1 CFRAC

1: procedure
2: **input:** a composite integer *N*
3: Choose your factor base and an upper bound $B$.
4: $p_0 \leftarrow 0$.
5: $R \leftarrow 0$.
6: $i \leftarrow 0$.

7: **while** $R < K + 10$ **do**
8: Compute $P_i$, $Q_i^*$, $q_i$ and $A_{i-1} \pmod N$.
9: **if** $Q_i^*$ is factored using primes in the factor base **then**
10: Save $i$, $Q_i^*$ and $A_{i-1} \pmod N$ in a file
11: $R \leftarrow R + 1$.
12: $i \leftarrow i + 1$.
13: Form the matrix whose rows are the vectors $\vec{v}_i$.
14: Find linear dependencies amoung the $\vec{v}_i$'s.
15: Let $S = \{i \in \mathbb{N}: Q_i$ factors into primes in the factor base, $\prod_{i \in S} \vec{v}_i =$
16: **for** each dependency $\prod_{i \in S} \vec{v}_i = 0$ **do**
17: $y^2 = \prod_{i \in S} Q_n^*$ and $x = \prod_{i \in S} A_{n-1} \pmod N$.
18: **if** If $\gcd(x - y, N)$ is a proper factor of N **then**
19: **break**
20: **Output**: a factor of $N$.

# VI. FINAL REMARKS

The time complexity on the algorithm presented by Morrison and Brillhart is $O\left(e^{\sqrt{2\log n \cdot \log(\log n)}}\right)$[134]. Even though this is exponential time, the log$n$ prevents the running time from growing too big in proportion to the size of $n$. Recall that the A method and P method are the foundations to the CFRAC; indeed, they are related by the following theorem:

**Theorem 6.1.** The A method successfully yields a factor of $N$ if and only if the P method successfully yields a factor of $N$.
To prove this, we need a lemma:

**Lemma 6.2.** For $k \geq 2$, we have

[134] Pomerance, Carl (December 1996). "A Tale of Two Sieves" (PDF). *Notices of the AMS*. **43** (12). pp. 1473-1485

$$P_k + (-1)^k A_{k-1} A_{k-2} \equiv 0 \pmod{N}.$$

*Proof. Of Lemma 6.2.* We prove this by induction on $k$.

Base case $k = 2$:

$$\begin{aligned} P_2 + A_1 A_0 &= (q_1 Q_1 - P_1) + (q_0 q_1 + 1) q_0 \\ &= q_1 (N - q_0^2) - q_0 + (q_0 q_1 + 1) q_0 \\ &\equiv 0 \pmod{N}. \end{aligned}$$

Induction hypothesis: Suppose the lemma is true for $n - 1$. So

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

Induction step: Since $P_n = q_{n-1} Q_{n-1} - P_{n-1}$, we have

$$\begin{aligned} 0 &\equiv P_{n-1} - Q_{n-1} q_{n-1} + (-1)^{n-1} A_{n-2} A_{n-3} + Q_{n-1} q_{n-1} \\ &\equiv -P_n + (-1)^{n-1} A_{n-2} (A_{n-3} + A_{n-2} q_{n-1}) \\ &\equiv -P_n + (-1)^{n-1} A_{n-1} A_{n-2} \pmod{N}. \end{aligned}$$

□

*Proof of Theorem 6.1.* Assume the contrapositive: that the P method fails. Then, $N$ divides either $xP_{i+1}P_{i+3} \ldots P_{j-1} \pm yP_{i+2}P_{i+4} \ldots P_j$. Substituting the equation from Lemma 6.2 into the $P_i$'s appropriately and simplifying imply that N divides either $xA_{i-1} \pm yA_{j-1}$, which means the A method fails. The converse is true by reversing the above argument.