Continued Fractions Factoring method

Cryptology I
Trial division

Is there a good algorithm for factoring a given integer \( n \)?
Is there a good algorithm for factoring a given integer $n$?

Let $n$ be a number which is a product of two 50 digit prime numbers.
Is there a good algorithm for factoring a given integer $n$?

Let $n$ be a number which is a product of two 50 digit prime numbers.

- We need approximately $10^{50}$ steps of trial division.
Is there a good algorithm for factoring a given integer $n$?

Let $n$ be a number which is a product of two 50 digit prime numbers.

- We need approximately $10^{50}$ steps of trial division.
- Assume that every step takes $10^{-10}$ seconds.
Trial division

Is there a good algorithm for factoring a given integer $n$?

Let $n$ be a number which is a product of two 50 digit prime numbers.

- We need approximately $10^{50}$ steps of trial division.
- Assume that every step takes $10^{-10}$ seconds.
- We need to wait for $10^{40}$ seconds ($\sim 1032$ years).
RSA Factoring Challenge

The **RSA Challenge problem** is the problem of finding the factorization of the RSA modulus $n$.

---

The **RSA Challenge problem** is the problem of finding the factorization of the RSA modulus $n$.

- **RSA-100**: 1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

---

RSA Factoring Challenge

The **RSA Challenge problem** is the problem of finding the factorization of the RSA modulus $n$.

- **RSA-100**: 1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

- **RSA-768**: 1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

---

RSA Factoring Challenge

The **RSA Challenge problem** is the problem of finding the factorization of the RSA modulus $n$.

- **RSA-100:** $15226050279225333605356183781326374297180681149613\ 80688657908494580122963258952897654000350692006139$  
- **RSA-768:**
  - $1230186684530117755130494958384962720772853569595334\ 7921973224521517264005072636575187452021997864693899\ 5647494277406384592519255732630345373154826850791702\ 6122142913461670429214311602221240479274737794080665\ 351419597459856902143413$  

---

An expression of the form

$$x = a_0 + \frac{b_1}{a_1 + \frac{b_2}{a_2 + \frac{b_{n-1}}{a_{n-1} + \frac{b_n}{a_n}}}$$

is called a continued fraction.
It is called simple continued fraction if all the $b_i$'s are 1 and all the $a_i$'s are integers such that $a_1, a_2, \ldots \geq 1$. 
We can denote the simple continued fraction with

\[
[a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}
\]

\[C_k = [a_1, a_2, \ldots, a_k]\] for \(k \leq n\) is called the \textbf{k-th convergent of the simple continued fraction}. 

**Continued Fractions**
Infinite Continued fractions

The infinite continued fraction, \([a_1, a_2, ..., a_k, ...]\) is defined as a limit of the convergents \(C_k = [a_1, a_2, ..., a_k]\).

**Theorem**

*Every real number can be expressed as a continued fraction.*
The infinite continued fraction, \([a_1, a_2, ..., a_k, ...]\) is defined as a limit of the convergents \(C_k = [a_1, a_2, ..., a_k]\).

**Theorem**

*Every real number can be expressed as a continued fraction.*

**Theorem**

*Suppose that \(p_k/q_k\) is the \(k\)-th convergent of \(\sqrt{n}\). Then*
Infinite Continued fractions

The **infinite continued fraction**, \([a_1, a_2, \ldots, a_k, \ldots]\) is defined as a limit of the convergents \(C_k = [a_1, a_2, \ldots, a_k]\).

**Theorem**

*Every real number can be expressed as a continued fraction.*

**Theorem**

*Suppose that \(p_k/q_k\) is the \(k\)-th convergent of \(\sqrt{n}\). Then*

\[
p_k^2 - nq_k^2 = (-1)^{k+1} B_{k+1}.
\]
Continued Fractions

Continued Fraction Method CFRAC

3

Successfully factored $F_7 = 2^{128} + 1$.

First method with subexponential running time.

Most efficient general factorization method.


Foundation for QS and NFS factoring methods.

Successfully factored $F_7 = 2^{128} + 1$. 

---

Continued Fraction Method CFRAC \(^3\)

- Successfully factored \(F_7 = 2^{128} + 1\).
- First method with subexponential running time.

\(^3\) M.A. Morrison and J. Brillhart, “A method of factoring and Factorization of \(F_7\),” (1975)
Continued Fraction Method CFRAC

- Successfully factored $F_7 = 2^{128} + 1$.
- First method with subexponential running time.
- Most efficient general factorization method.

---

Continued Fraction Method CFRAC

- Successfully factored $F_7 = 2^{128} + 1$.
- First method with subexponential running time.
- Most efficient *general* factorization method.

---

Continued Fraction Method CFRAC

- Successfully factored $F_7 = 2^{128} + 1$.
- First method with subexponential running time.
- Most efficient general factorization method.
- Foundation for QS and NFS factoring methods.

---

Gaussian Elimination

**Gaussian elimination** is an efficient algorithm for solving system of linear equations.

\[
\begin{align*}
 a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
 a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
 & \vdots \quad \vdots \quad \vdots \\
 a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m.
\end{align*}
\]

where \(x_1, x_2, \ldots, x_n\) are the unknown variable, \(a_{11}, a_{12}, \ldots, a_{mn}\) are the coefficients of the system, and \(b_1, b_2, \ldots, b_m\) are the constant terms.
Gaussian Elimination

The system of linear equations is equivalent to a matrix equation of the form

\[ A \cdot x = b \]

where \( A \) is an \( m \times n \) matrix, \( x \) is a column vector with \( n \) entries, and \( b \) is a column vector with \( m \) entries.

\[
A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}
\]
Gaussian Elimination-Example

We have the following system of equations

\[
\begin{align*}
2x - 3y + z + 2w + 3v &= 4 \\
4x - 4y + z + 4w + 11v &= 4 \\
2x - 5y - 2z + 2w - v &= 9 \\
4 - 2y + z + 4v &= -5
\end{align*}
\]

http://www.sosmath.com
Gaussian Elimination - Example

We have the following system of equations

\[
\begin{align*}
2x - 3y + z + 2w + 3v &= 4 \\
4x - 4y + z + 4w + 11v &= 4 \\
2x - 5y - 2z + 2w - v &= 9 \\
4 - 2y + z + 4v &= -5 
\end{align*}
\]

The corresponding matrix equation is

\[
\begin{pmatrix}
2 & -3 & -1 & 2 & 3 & | & 4 \\
4 & -4 & -1 & 4 & 11 & | & 4 \\
2 & -5 & -2 & 2 & -1 & | & 9 \\
0 & 2 & 1 & 0 & 4 & | & -5
\end{pmatrix}
\]

\[\text{http://www.sosmath.com}\]
Gaussian Elimination-Example

5 We use elementary row operations to transform this matrix into a triangular one. We keep the first row and use it to produce all zeros elsewhere in the first column. We have

$$
\begin{pmatrix}
2 & -3 & -1 & 2 & 3 & 4 \\
0 & 2 & 1 & 0 & 5 & -4 \\
0 & -2 & -1 & 0 & -4 & 5 \\
0 & 2 & 1 & 0 & 4 & -5
\end{pmatrix}.
$$

\[5\text{ http://www.sosmath.com}\]
5 We use elementary row operations to transform this matrix into a triangular one. We keep the first row and use it to produce all zeros elsewhere in the first column. We have

\[
\begin{pmatrix}
2 & -3 & -1 & 2 & 3 & 4 \\
0 & 2 & 1 & 0 & 5 & -4 \\
0 & -2 & -1 & 0 & -4 & 5 \\
0 & 2 & 1 & 0 & 4 & -5
\end{pmatrix}.
\]

Continuing like this we get the following triangular matrix

\[
\begin{pmatrix}
2 & -3 & -1 & 2 & 3 & 4 \\
0 & 2 & 1 & 0 & 5 & -4 \\
0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
\]

\(^5\text{http://www.sosmath.com}\)
Legendre function

Definition
Let $0 < a < n$. We say that $a$ is a quadratic residue of $n$ if there is and $x$ such that $x^2 \mod n = a$. 
Legendre function

Definition
Let 0 < a < n. We say that a is a quadratic residue of n if there is and x such that \( x^2 \mod n = a \).

Definition
Let \( p \) be a prime and \( a < p \) a positive integer. The Legendre symbol is a multiplicative function with values 1, -1, 0 that is a quadratic character modulo a prime number \( p \): its value on a quadratic residue mod \( p \) is 1 and on a non-quadratic residue is -1.
Fermat’s Theorem

Theorem

If \( x^2 \equiv y^2 \mod n \) and \( x \not\equiv \pm y \mod n \), then either \( \gcd(x + y, n) \) or \( \gcd(x - y, n) \) is a proper factor of \( n \).
Theorem

Suppose that $p_k/q_k$ is the $k$-th convergent of $\sqrt{n}$. Then

$$p_k^2 - nq_k^2 = (-1)^{k+1}B_{k+1}.$$
Theorem

Suppose that $p_k/q_k$ is the k-th convergent of $\sqrt{n}$. Then

$$p_k^2 - nq_k^2 = (-1)^{k+1} B_{k+1}.$$
CFRAC factoring method

Theorem

Suppose that \( \frac{p_k}{q_k} \) is the \( k \)-th convergent of \( \sqrt{n} \). Then

\[
p_k^2 - nq_k^2 = (-1)^{k+1} B_{k+1}.
\]

The theorem implies that

\[
p_k^2 = (-1)^{k+1} B_{k+1} \mod n
\]
Theorem

Suppose that $p_k/q_k$ is the $k$-th convergent of $\sqrt{n}$. Then

$$p_k^2 - nq_k^2 = (-1)^{k+1}B_{k+1}.$$

The theorem implies that

$$p_k^2 = (-1)^{k+1}B_{k+1} \mod n$$

To apply the Fermat theorem we need squares on both sides.
Suppose that $p_k/q_k$ is the $k$-th convergent of $\sqrt{n}$. Then

$$p_k^2 - nq_k^2 = (-1)^{k+1} B_{k+1}.$$ 

The theorem implies that

$$p_k^2 = (-1)^{k+1} B_{k+1} \pmod{n}$$

To apply the Fermat theorem we need squares on both sides. The idea of continued fractions is to generate pairs $(p_k, B_{k+1})$ and take suitable combinations to produce a square on the right and to possibly factor $n$. 
Theorem

Suppose that $p_k/q_k$ is the $k$-th convergent of $\sqrt{n}$. Then

$$p_k^2 - nq_k^2 = (-1)^{k+1} B_{k+1}.$$  

The theorem implies that

$$p_k^2 = (-1)^{k+1} B_{k+1} \mod n$$

To apply the Fermat theorem we need squares on both sides. The idea of continued fractions is to generate pairs $(p_k, B_{k+1})$ and take suitable combinations to produce a square on the right and to possibly factor $n$. Recall that the integer is a perfect square if and only the exponents in the prime factorization are all even.
CFRAC factoring method

Theorem

Suppose that $p_k/q_k$ is the $k$-th convergent of $\sqrt{n}$. Then

$$p_k^2 - nq_k^2 = (-1)^{k+1}B_{k+1}.$$ 

The theorem implies that

$$p_k^2 = (-1)^{k+1}B_{k+1} \mod n$$

To apply the Fermat theorem we need squares on both sides. The idea of continued fractions is to generate pairs $(p_k, B_{k+1})$ and take suitable combinations to produce a square on the right and to possibly factor $n$. Recall that the integer is a perfect square if and only the exponents in the prime factorization are all even.

Thus, to find the products of $B_k$’s that yield perfect square we obtain their prime factorization and combine them so that the exponents become even.
CFRAC factoring method

Theorem

Suppose that \( p_k/q_k \) is the \( k \)-th convergent of \( \sqrt{n} \). Then

\[
p_k^2 - nq_k^2 = (-1)^{k+1} B_{k+1}.
\]

The theorem implies that

\[
p_k^2 = (-1)^{k+1} B_{k+1} \mod n
\]

To apply the Fermat theorem we need squares on both sides. The idea of continued fractions is to generate pairs \((p_k, B_{k+1})\) and take suitable combinations to produce a square on the right and to possibly factor \( n \).

Recall that the integer is a perfect square if and only the exponents in the prime factorization are all even.

Thus, to find the products of \( B_k \)’s that yield perfect square we obtain their prime factorization and combine them so that the exponents become even. The factorization of \( B_k \) is obtained by trial division.
Select a set of primes over which $B_k$ factors. If $p | B_k$ we have

$$p_k = nq_k^2 \mod p$$
Select a set of primes over which $B_k$ factors. If $p|B_k$ we have

$$p_k = nq_k^2 \mod p$$

So $n$ is a quadratic residue modulo $p$. Select a set of primes $q$ such that $\text{legendre}(n, q) = 1$. This set of primes is called a factor base.
### CFRAC Example

**Table:** Integer: $n = 4141$, Factor base: $2, 3, 5, 7, 11$

<table>
<thead>
<tr>
<th>$k + 1$</th>
<th>$p_k$</th>
<th>$B_{k+1}$</th>
<th>$B_{k+1}$ factored</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>129</td>
<td>77</td>
<td>$7^111^1$</td>
</tr>
<tr>
<td>3</td>
<td>193</td>
<td>20</td>
<td>$2^25^1$</td>
</tr>
<tr>
<td>6</td>
<td>814</td>
<td>36</td>
<td>$2^23^2$</td>
</tr>
<tr>
<td>8</td>
<td>3719</td>
<td>21</td>
<td>$3^17^1$</td>
</tr>
<tr>
<td>11</td>
<td>2266</td>
<td>84</td>
<td>$2^23^17^1$</td>
</tr>
<tr>
<td>12</td>
<td>3463</td>
<td>33</td>
<td>$3^111^1$</td>
</tr>
<tr>
<td>13</td>
<td>232</td>
<td>9</td>
<td>$3^2$</td>
</tr>
<tr>
<td>14</td>
<td>2570</td>
<td>5</td>
<td>$5^1$</td>
</tr>
<tr>
<td>15</td>
<td>2367</td>
<td>84</td>
<td>$2^23^17^1$</td>
</tr>
<tr>
<td>17</td>
<td>3959</td>
<td>4</td>
<td>$2^2$</td>
</tr>
<tr>
<td>18</td>
<td>3436</td>
<td>105</td>
<td>$3^15^17^1$</td>
</tr>
<tr>
<td>19</td>
<td>3254</td>
<td>21</td>
<td>$3^17^1$</td>
</tr>
<tr>
<td>20</td>
<td>3142</td>
<td>20</td>
<td>$2^25^1$</td>
</tr>
</tbody>
</table>
**Remark:** We have to include $-1$ as an element in the factor base to take into account the negative sign when $k + 1$ is odd.

In general, suppose we have the factorization of $B_k$'s:

\[
B_1 = p_{1}^{a_{11}} p_{2}^{a_{12}} \ldots p_{r}^{a_{1r}}
\]

\[
B_s = p_{1}^{a_{s1}} p_{2}^{a_{s2}} \ldots p_{r}^{a_{sr}}
\]

where $p_1, p_2, \ldots, p_s$ are the primes of the factor base with $p_1 = -1$. 
We need to find numbers $e_1, e_2, \ldots, e_s$ that are either 0 or 1 such that

$$B_1^{e_1} B_2^{e_2} \ldots B_s^{e_s}$$

is a perfect square.
We need to find numbers $e_1, e_2, ..., e_s$ that are either 0 or 1 such that

$$B_1^{e_1} B_2^{e_2} ... B_s^{e_s}$$

is a perfect square.
We need to find numbers $e_1, e_2, \ldots, e_s$ that are either 0 or 1 such that

$$B_1^{e_1} B_2^{e_2} \ldots B_s^{e_s}$$

is a perfect square.

$$B_1^{e_1} B_2^{e_2} \ldots B_s^{e_s} = (p_1^{a_{11}} p_2^{a_{21}} \ldots p_k^{a_{k1}})^{e_1} \cdot \ldots \cdot (p_1^{a_{1s}} p_2^{a_{2s}} \ldots p_k^{a_{ks}})^{e_s} =$$
We need to find numbers $e_1, e_2, \ldots, e_s$ that are either 0 or 1 such that

$$B_1^{e_1} B_2^{e_2} \cdots B_s^{e_s}$$

is a perfect square.

$$B_1^{e_1} B_2^{e_2} \cdots B_s^{e_s} = (p_1^{a_{11}} p_2^{a_{21}} \cdots p_k^{a_{k1}})^{e_1} \cdot \cdots \cdot (p_1^{a_{1s}} p_2^{a_{2s}} \cdots p_k^{a_{ks}})^{e_s} =$$

$$= p_1^{a_{11}e_1 + a_{12}e_2 + \cdots + a_{1s}e_s} \cdot \cdots \cdot p_k^{a_{k1}e_1 + a_{k2}e_2 + \cdots + a_{ks}e_s}$$
We need to find numbers $e_1, e_2, \ldots, e_s$ that are either 0 or 1 such that

$$B_1^{e_1} B_2^{e_2} \cdots B_s^{e_s}$$

is a perfect square.

$$B_1^{e_1} B_2^{e_2} \cdots B_s^{e_s} = (p_1^{a_{11}} p_2^{a_{21}} \cdots p_k^{a_{k1}})^{e_1} \cdot \cdots \cdot (p_1^{a_{1s}} p_2^{a_{2s}} \cdots p_k^{a_{ks}})^{e_s} =

= p_1^{a_{11} e_1 + a_{12} e_2 + \cdots + a_{1s} e_s} \cdot \cdots \cdot p_k^{a_{k1} e_1 + a_{k2} e_2 + \cdots + a_{ks} e_s}$$

We need to find $e_1, e_2, \ldots, e_s$ such that $e_1 a_{1i} + e_2 a_{2i} + \cdots + e_s a_{si}$ is even for all $i$. 
CFRAC factoring method

We need to solve the system of linear equation

\[ a_{11}e_1 + a_{12}e_2 + \ldots + a_{1s}e_s = 0 \mod 2 \]
\[ a_{21}e_1 + a_{22}e_2 + \ldots + a_{2s}e_s = 0 \mod 2 \]
\[ \ldots \]
\[ a_{k1}e_1 + a_{k2}e_2 + \ldots + a_{ks}e_s = 0 \mod 2 \]

i.e. to solve the matrix equation \( Ae = 0 \), where \( e = (e_1, e_2, \ldots, e_s) \) and \( A \) is the matrix whose \( ij \)-th entry is \( a_{ij} \).
We need to solve the system of linear equation

\[
\begin{align*}
a_{11}e_1 + a_{12}e_2 + \ldots + a_{1s}e_s &= 0 \mod 2 \\
a_{21}e_1 + a_{22}e_2 + \ldots + a_{2s}e_s &= 0 \mod 2 \\
\vdots \\
a_{k1}e_1 + a_{k2}e_2 + \ldots + a_{ks}e_s &= 0 \mod 2
\end{align*}
\]

i.e. to solve the matrix equation \( A\mathbf{e} = 0 \), where \( \mathbf{e} = (e_1, e_2, \ldots, e_s) \) and \( A \) is the matrix whose \( ij \)-th entry is \( a_{ij} \).

The equation \( A\mathbf{e} = 0 \) can be solved by Gaussian elimination modulo 2.
We need to solve the system of linear equations

\[
\begin{align*}
    a_{11}e_1 + a_{12}e_2 + \ldots + a_{1s}e_s &= 0 \mod 2 \\
    a_{21}e_1 + a_{22}e_2 + \ldots + a_{2s}e_s &= 0 \mod 2 \\
    \vdots \\
    a_{k1}e_1 + a_{k2}e_2 + \ldots + a_{ks}e_s &= 0 \mod 2
\end{align*}
\]

i.e. to solve the matrix equation \( Ae = 0 \), where \( e = (e_1, e_2, \ldots, e_s) \) and \( A \) is the matrix whose \( ij \)-th entry is \( a_{ij} \).

The equation \( Ae = 0 \) can be solved by Gaussian elimination modulo 2.

If \( s > r \) then we are guaranteed a nontrivial solution.
Matrix of exponents modulo 2 for $n = 4141$

$$
A = \begin{pmatrix}
-1 & 2 & 3 & 5 & 7 & 11 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 
\end{pmatrix}
$$
The solutions yield combinations that will produce

\[ p_{i_1}^2 p_{i_2}^2 \ldots p_{i_k}^2 = B_{i_1+1} B_{i_2+1} \ldots B_{i_k+1} \mod n \]
The solutions yield combinations that will produce

\[ p_{i_1}^2 p_{i_2}^2 ... p_{i_k}^2 = B_{i_1+1} B_{i_2+1} ... B_{i_k+1} \mod n \]

where the expression \( B_{i_1+1} B_{i_2+1} ... B_{i_k+1} \) is a square.
The solutions yield combinations that will produce

\[ p_{i_1}^2 p_{i_2}^2 \ldots p_{i_k}^2 = B_{i_1+1} B_{i_2+1} \ldots B_{i_k+1} \mod n \]

where the expression \( B_{i_1+1} B_{i_2+1} \ldots B_{i_k+1} \) is a square. It is possible that such combination does not yield a proper factor of \( n \).
Computing $gcd$’s:
Computing $gcd$'s:

- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 4141$
Computing $gcd$'s:

- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 4141$
- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 1$
Computing $gcd$’s:

- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 4141$
- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 1$
- $gcd(2266 \cdot 3254 - 2 \cdot 3 \cdot 7, n) = 41$
Computing \( \text{gcd}'s: \)

- \( \text{gcd}(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 4141 \)
- \( \text{gcd}(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 1 \)
- \( \text{gcd}(2266 \cdot 3254 - 2 \cdot 3 \cdot 7, n) = 41 \)
- \( \text{gcd}(2266 \cdot 3254 + 2 \cdot 3 \cdot 7, n) = 101 \)
Step 1  Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, \ldots, a_m]$. 
The CFRAC method

Step 1  Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, ..., a_m]$.

Step 2  Generate “$p_k - B_k$ pairs”.

Step 3  Find among the set of “$p_k - B_k$ pairs” generated in the previous step certain subsets (called “$S$-sets”) each having the property that the product $\prod_i (-1)^i B_i$ of its $B_i$’s is a square. If no such set is found go to Step 1 and expand $\sqrt{n}$.

Step 4  Each $S$-set found in Step 3 gives rise to the congruence $X^2 \equiv \prod_i p_i \equiv \prod_i (-1)^i B_i \equiv Y^2 \pmod{n}$, where $1 \leq X < n$.

Step 5  Compute $Y$ and the gcd($X - Y, n$) = $d$ for the $S$-sets produced in Step 4. If $1 < d < n$ for some $S$-set, the method succeeds and $d$ is non-trivial factor of $n$. Otherwise, return to Step 1.
The CFRAC method

Step 1 Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, ..., a_m]$. 

Step 2 Generate "$p_k - B_k$ pairs".

Step 3 Find among the set of "$p_k - B_k$ pairs" generated in the previous step certain subsets (called "S-sets") each having the property that the product $\prod_i (-1)^i B_i$ of its $B_i$'s is a square.
The CFRAC method

Step 1 Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, ..., a_m]$.

Step 2 Generate “$p_k - B_k$ pairs”.

Step 3 Find among the set of “$p_k - B_k$ pairs” generated in the previous step certain subsets (called “S-sets”) each having the property that the product $\prod_i (-1)^i B_i$ of its $B_i$’s is a square. If no such set is found go to Step 1 and expand $\sqrt{n}$. 

Step 4 Each S-set found in Step 3 gives rise to the congruence $X^2 \equiv \prod_i p_i \equiv \prod_i (-1)^i B_i \equiv Y^2 \pmod{n}$, where $1 \leq X < n$.

Step 5 Compute $Y$ and the $\gcd(X - Y, n) = d$ for the S-sets produced in Step 4. If $1 < d < n$ for some S-set, the method succeeds and $d$ is a non-trivial factor of $n$. Otherwise, return to Step 1.
The CFRAC method

Step 1: Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, ..., a_m]$.

Step 2: Generate “$p_k - B_k$ pairs”.

Step 3: Find among the set of “$p_k - B_k$ pairs” generated in the previous step certain subsets (called “S-sets”) each having the property that the product $\prod_i (-1)^i B_i$ of its $B_i$’s is a square. If no such set is found go to Step 1 and expand $\sqrt{n}$.

Step 4: Each S-set found in Step 3 gives rise to the congruence $X^2 \equiv \prod_i p_i \equiv \prod_i (-1)^i B_i = Y^2 \mod n$, where $1 \leq X < n$. 

(Cryptology I) Continued Fractions Factoring method
The CFRAC method

Step 1  Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, \ldots, a_m]$.

Step 2  Generate “$p_k - B_k$ pairs”.

Step 3  Find among the set of “$p_k - B_k$ pairs” generated in the previous step certain subsets (called “S-sets”) each having the property that the product $\prod_i (-1)^i B_i$ of its $B_i$’s is a square. If no such set is found go to Step 1 and expand $\sqrt{n}$.

Step 4  Each S-set found in Step 3 gives rise to the congruence $X^2 \equiv \prod_i p_i \equiv \prod_i (-1)^i B_i \equiv Y^2 \mod n$, where $1 \leq X < n$.

Step 5  Compute $Y$ and the $gcd(X - Y, n) = d$ for the S-sets produced in Step 4. If $1 < d < n$ for some S-set, the method succeeds and $d$ is non-trivial factor of $n$. Otherwise, return to Step 1.
The CFRAC method

Step 1. Expand $\sqrt{n}$ (or $\sqrt{cn}$) into a simple continued fraction expansion to some point $m$ i.e. $\sqrt{n} = [a_0, a_1, a_2, ..., a_m]$.

Step 2. Generate “$p_k - B_k$ pairs”.

Step 3. Find among the set of “$p_k - B_k$ pairs” generated in the previous step certain subsets (called “S-sets”) each having the property that the product $\prod_i (-1)^i B_i$ of its $B_i$’s is a square. If no such set is found go to Step 1 and expand $\sqrt{n}$.

Step 4. Each S-set found in Step 3 gives rise to the congruence

$$X^2 \equiv \prod_i p_i \equiv \prod_i (-1)^i B_i = Y^2 \mod n,$$

where $1 \leq X < n$.

Step 5. Compute $Y$ and the $gcd(X - Y, n) = d$ for the S-sets produced in Step 4. If $1 < d < n$ for some S-set, the method succeeds and $d$ is non-trivial factor of $n$. Otherwise, return to Step 1.