# Continued Fractions Factoring method

Cryptology I

# Trial division

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

# 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.

# 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.

# 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 $n$.

[1] B.Dixon & A.Lenstra, "Factoring integers using SIMD sieves" (1994)

[2] A.Lenstra et al., " Factoring RSA-768", (2009)

# RSA Factoring Challenge

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

- **RSA-100:** 152260502792253336053561837813263742971806811496138068865790849458012296325895289765400035069200613 9

[1] B.Dixon & A.Lenstra, "Factoring integers using SIMD sieves" (1994)

[2] A.Lenstra et al., " Factoring RSA-768", (2009)

# RSA Factoring Challenge

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

- **RSA-100:** 152260502792253336053561837813263742971806811496138068865790849458012296325895289765400035069200613 [1]
- **RSA-768:**
  123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3 [2]

[1] B.Dixon & A.Lenstra, "Factoring integers using SIMD sieves" (1994)

[2] A.Lenstra et al., " Factoring RSA-768", (2009)

# RSA Factoring Challenge

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

- **RSA-100:** 152260502792253336053561837813263742971806811496138068865790849458012296325895289765400035069200613 [1]
- **RSA-768:**
  123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3 [2]

[1] B.Dixon & A.Lenstra, "Factoring integers using SIMD sieves" (1994)

[2] A.Lenstra et al., " Factoring RSA-768", (2009)

# Continued Fractions

An expression of the form

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

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 $a_1, a_2, \ldots \geq 1$.

# Continued Fractions

We can denote the simple continued fraction with

$$[a_1, a_2, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 ... + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

$C_k = [a_1, a_2, ..., a_k]$ for $k \leq n$ is called **k-th convergent of the simple continued fraction**.

# 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.*

# 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.*

**Theorem**

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

# Infinite Continued fractions

The **infinite continued fraction**, $[a_1, a_2, ..., a_k, ...]$ 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*

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

# Continued Fraction Method CFRAC [3]

[3] M.A. Morrison and J. Brillhart, "A method of factoring and Factorization of $F_7$", (1975)

# Continued Fraction Method CFRAC [3]

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

[3] M.A. Morrison and J. Brillhart, "A method of factoring and Factorization of $F_7$", (1975)

# 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 [3]

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

[3] M.A. Morrison and J. Brillhart, "A method of factoring and Factorization of $F_7$", (1975)

# Continued Fraction Method CFRAC [3]

- Successfully factored $F_7 = 2^{128} + 1$.
- First method with subexponential running time.
- Most efficient *general* factorization method.
- Main factoring method in use during 1970-1985.

[3] M.A. Morrison and J. Brillhart, "A method of factoring and Factorization of $F_7$", (1975)

# Continued Fraction Method CFRAC [3]

- Successfully factored $F_7 = 2^{128} + 1$.
- First method with subexponential running time.
- Most efficient *general* factorization method.
- Main factoring method in use during 1970-1985.
- Foundation for QS and NFS factoring methods.

[3] M.A. Morrison and J. Brillhart, "A method of factoring and Factorization of $F_7$", (1975)

# Gaussian Elimination

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

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

where $x_1, x_2, ..., x_n$ are the unknown variable, $a_{11}, a_{12}, ..., a_{mn}$ are the coefficients of the system, and $b_1, b_2, ..., b_m$ are the constant terms.

# Gaussian Elimination

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

$$\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$$

where $\mathbf{A}$ is an $m \times n$ matrix, $\mathbf{x}$ is a column vector with $n$ entries, and $\mathbf{b}$ is a column vector with $m$ entries.

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

# Gaussian Elimination-Example

We have the following system of equations

$$4\begin{cases} 2x- & 3y-z+ & 2w & +3v & = & 4 \\ 4x- & 4y-z+ & 4w & +11v & = & 4 \\ 2x- & 5y-2z+ & 2w & -v & = & 9 \\ & 2y+z & & +4v & = & -5 \end{cases}$$

[4] http://www.sosmath.com

# Gaussian Elimination-Example

We have the following system of equations

$$4\begin{cases} 2x- & 3y-z+ & 2w & +3v & = & 4 \\ 4x- & 4y-z+ & 4w & +11v & = & 4 \\ 2x- & 5y-2z+ & 2w & -v & = & 9 \\ & 2y+z & & +4v & = & -5 \end{cases}$$

The corresponding matrix equation is

$$\left(\begin{array}{rrrrr|r} 2 & -3 & -1 & 2 & 3 & 4 \\ 4 & -4 & -1 & 4 & 11 & 4 \\ 2 & -5 & -2 & 2 & -1 & 9 \\ 0 & 2 & 1 & 0 & 4 & -5 \end{array}\right).$$

[4] 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

$$\left(\begin{array}{rrrrr|r} 2 & -3 & -1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 0 & 5 & -4 \\ 0 & -2 & -1 & 0 & -4 & 5 \\ 0 & 2 & 1 & 0 & 4 & -5 \end{array}\right).$$

[5] 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

$$\left(\begin{array}{rrrrr|r} 2 & -3 & -1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 0 & 5 & -4 \\ 0 & -2 & -1 & 0 & -4 & 5 \\ 0 & 2 & 1 & 0 & 4 & -5 \end{array}\right).$$

Continuing like this we get the following triangular matrix

$$\left(\begin{array}{rrrrr|r} 2 & -3 & -1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 0 & 5 & -4 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

[5] 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* $x^2 \equiv y^2 \bmod n$ *and* $x \not\equiv \pm y \bmod n$, *then either* $gcd(x + y, n)$ *or* $gcd(x - y, n)$ *is a proper factor of* $n$.

# CFRAC factoring method

## Theorem

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

# CFRAC factoring method

## Theorem

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

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

# 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

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

# 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.

# 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 $n$.

# 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.

# 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.

# CFRAC factoring method

Select a set of primes over which $B_k$ factors. If $p|B_k$ we have

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

# CFRAC factoring method

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 $legendre(n, q) = 1$. This set of primes is called a **factor base**.

## CFRAC example

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

| $k+1$ | $p_k$ | $B_{k+1}$ | $B_{k+1}$ factored |
|---|---|---|---|
| 2 | 129 | 77 | $7^1 11^1$ |
| 3 | 193 | 20 | $2^2 5^1$ |
| 6 | 814 | 36 | $2^2 3^2$ |
| 8 | 3719 | 21 | $3^1 7^1$ |
| 11 | 2266 | 84 | $2^2 3^1 7^1$ |
| 12 | 3463 | 33 | $3^1 11^1$ |
| 13 | 232 | 9 | $3^2$ |
| 14 | 2570 | 5 | $5^1$ |
| 15 | 2367 | 84 | $2^2 3^1 7^1$ |
| 17 | 3959 | 4 | $2^2$ |
| 18 | 3436 | 105 | $3^1 5^1 7^1$ |
| 19 | 3254 | 21 | $3^1 7^1$ |
| 20 | 3142 | 20 | $2^2 5^1$ |

▸ go to this page

# CFRAC factoring method

**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:

$$B_1 = p_1^{a_{11}} p_2^{a_{12}} \ldots p_r^{a_{1r}}$$

$$\vdots$$

$$B_s = p_1^{a_{s1}} p_2^{a_{s2}} \ldots p_r^{a_{sr}}$$

where $p_1, p_2, \ldots, p_s$ are the primes of the factor base with $p_1 = -1$.

# CFRAC factoring method

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.

# CFRAC factoring method

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.

# CFRAC factoring method

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.

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

# CFRAC factoring method

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.

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

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

# CFRAC factoring method

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.

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

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

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

# CFRAC factoring method

We need to solve the system of linear equation

$$a_{11}e_1 + a_{12}e_2 + ... + a_{1s}e_s = 0 \ mod \ 2$$
$$a_{21}e_1 + a_{22}e_2 + ... + a_{2s}e_s = 0 \ mod \ 2$$
$$\dots$$
$$a_{k1}e_1 + a_{k2}e_2 + ... + a_{ks}e_s = 0 \ mod \ 2$$

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

# CFRAC factoring method

We need to solve the system of linear equation

$$a_{11}e_1 + a_{12}e_2 + ... + a_{1s}e_s = 0 \ mod \ 2$$
$$a_{21}e_1 + a_{22}e_2 + ... + a_{2s}e_s = 0 \ mod \ 2$$
$$\dots$$
$$a_{k1}e_1 + a_{k2}e_2 + ... + a_{ks}e_s = 0 \ mod \ 2$$

i.e. to solve the matrix equation $A\mathbf{e} = 0$, where $\mathbf{e} = (e_1, e_2, ..., e_s)$ 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.

# 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 $A\mathbf{e} = 0$, 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.

If $s > r$ then we are guaranteed a nontrivial solution.

## Matrix of exponents modulo 2 for $n = 4141$

$$A = \begin{array}{c} \begin{matrix} -1 & 2 & 3 & 5 & 7 & 11 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

example

# CFRAC factoring method

The solutions yield combinations that will produce

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

# CFRAC factoring method

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.

# CFRAC factoring method

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 $n$.

# CFRAC factoring method-Example

▸ example

Computing *gcd*'s:

# CFRAC factoring method-Example

▸ example

Computing *gcd*'s:

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

# CFRAC factoring method-Example

▸ example

Computing *gcd*'s:

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

# CFRAC factoring method-Example

▸ example

Computing *gcd*'s:

- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 4141$
- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 1$
- $gcd(2266 \cdot 3254 - 2 \cdot 3 \cdot 7, n) = 41$

# CFRAC factoring method-Example

▸ example

Computing *gcd*'s:

- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 4141$
- $gcd(193 \cdot 3719 \cdot 2266 \cdot 3142 - 20 \cdot 3 \cdot 2 \cdot 7, n) = 1$
- $gcd(2266 \cdot 3254 - 2 \cdot 3 \cdot 7, n) = 41$
- $gcd(2266 \cdot 3254 + 2 \cdot 3 \cdot 7, n) = 101$

# The CFRAC method

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

# 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".

# 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 $\sqrt{n}$.

# 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 $1 \leq X < n$.

# 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.

# 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.