# A Complete and Explicit Security Reduction Algorithm for RSA-based Cryptosystems

***Asiacrypt 2003, Taipei***

Kaoru Kurosawa [1], Katja Schmidt-Samoa [2], Tsuyoshi Takagi [2]

[1]Ibaraki University

[2]Technische Universität Darmstadt

# Introduction

**Problem:** Find "small" solutions $x, y$ of

$$\boxed{ax = y + c \bmod N}$$

Many applications in cryptanalysis and provable security

Previous solutions:

- Brute-force method
- Continued fraction methods
- Affine variant of Euclidian algorithm
- Lattice-based methods

# Outline of the talk

- PD-OW of RSA
- Features of the lattice-based solution
- Proposed algorithm
- Application to PD-OW of RSA
- Comparison
- Conclusion

# RSA: OW $\Rightarrow$ PD-OW

**Target:** Compute $m$ from $C = m^e \bmod N$

**PD-OW Oracle $\mathcal{O}$:** Gets $s_1$ from $(s_1 \cdot 2^k + s_2)^e \bmod N$

Fujisaki, Okamoto, Pointcheval, Stern 2001:

1. Choose $a \in \mathbb{Z}_N^\times$ at random
2. Define $C' = Ca^e \bmod N$ (encryption of $am \bmod N$)
3. $\mathcal{O}(C) = u$ and $\mathcal{O}(C') = v$
4. $m \bmod N = u \cdot 2^k + r$ and $am \bmod N = v \cdot 2^k + s$
   $\Rightarrow a \cdot (u \cdot 2^k + r) \bmod N = v \cdot 2^k + s$
   $\Rightarrow ar = s + c \bmod N,\ c = (v - ua) \cdot 2^k \bmod N.$

$$\Rightarrow \boxed{ax = y + c \bmod N}$$

# RSA: OW $\Rightarrow$ PD-OW, cont'd

**Problem**

$C = (u \cdot 2^k + r)^e \bmod N$, find $r$

We have $ar = s + c \bmod N,\ 0 \leq r, s < B < \sqrt{N}$

**General answer to the problem**

- Solve $ax = y + c \bmod N$ (small solutions)
- For each $(x, y)$: Check $C \stackrel{?}{=} \left(u \cdot 2^k + x\right)^e \bmod N$

**Questions**

- How to solve $ax = y + c \bmod N$?
- How many small solutions?

back

# Features of the lattice-based method

**Problem:** Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

Define lattice $L_{a,N} = \{(x, y) \in \mathbb{Z}^2 | ax = y \bmod N\}$

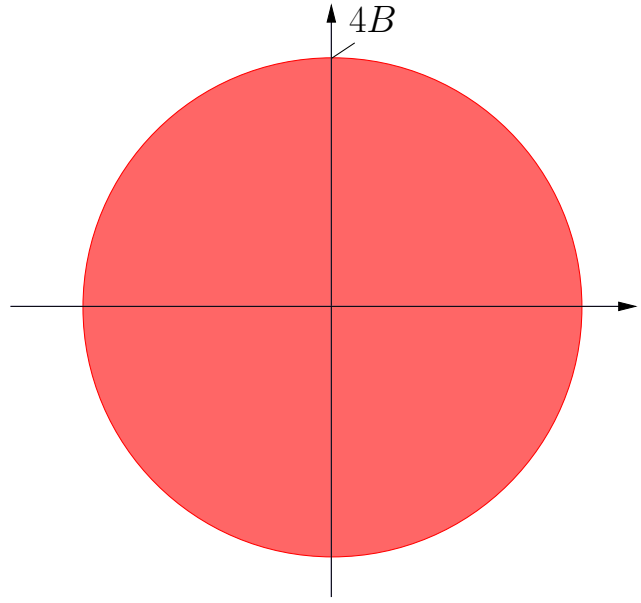
$\boxed{\text{Precondition: } L_{a,N} \text{ contains no } 0 \neq v, |v| < 4B}$

$\Downarrow$

1. unique small solution $(x, y)$ of $ax = y + c \bmod N$ ($\hookrightarrow$ no checks necessary)
2. $(x, y)$ can be found efficiently (lattice reduction)

# Critical area for lattice-based solution

Critical area of lattice $L_{a,N} = \{(x, y) \in \mathbb{Z}^2 | ax = y \bmod N\}$:
No non-zero vector inside critical area $\Rightarrow$ method works




**Target:** New algorithm for solving $ax = y + c \bmod N$ downsizes critical area

# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

**1st step: Specify the problem**

Find $x$-*minimal* solution w. r. t. $B$:

$$
\begin{array}{lcll}
x = 0 & \rightarrow & y = -c \bmod N \overset{?}{<} B & \text{no} \\
x = 1 & \rightarrow & y = -c + a \bmod N \overset{?}{<} B & \text{no} \\
\ldots & \ldots & \ldots \quad \ldots \quad \ldots & \ldots \\
x = \hat{x} & \rightarrow & \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B & \text{yes!}
\end{array}
$$

# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots \qquad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$

# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

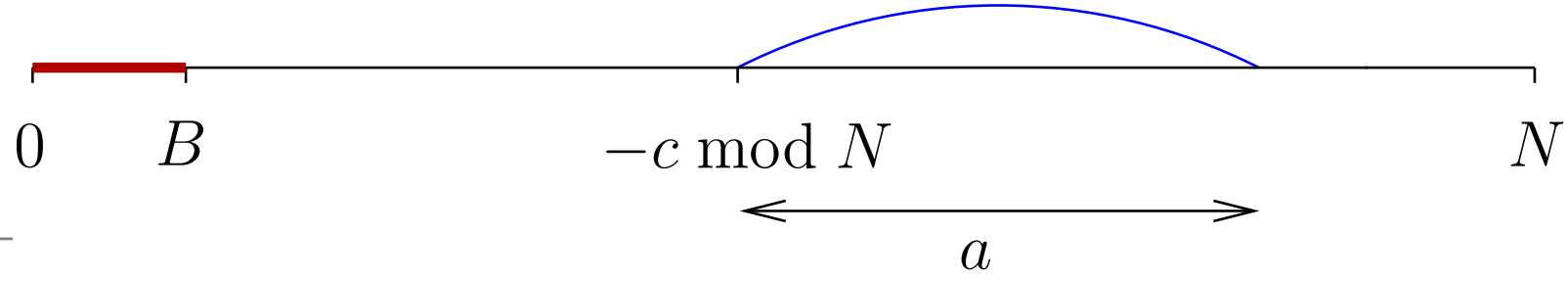
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

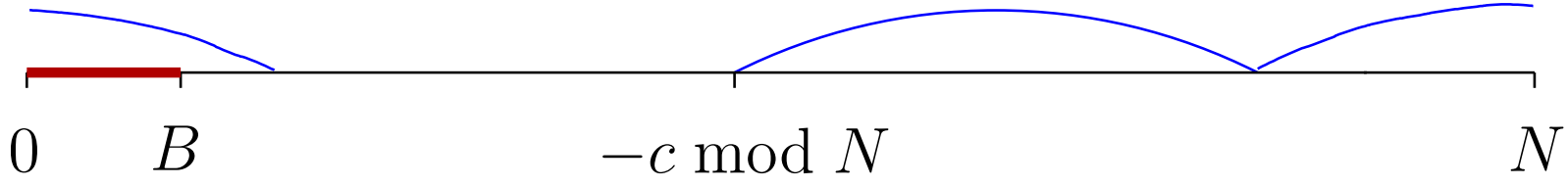
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots \qquad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

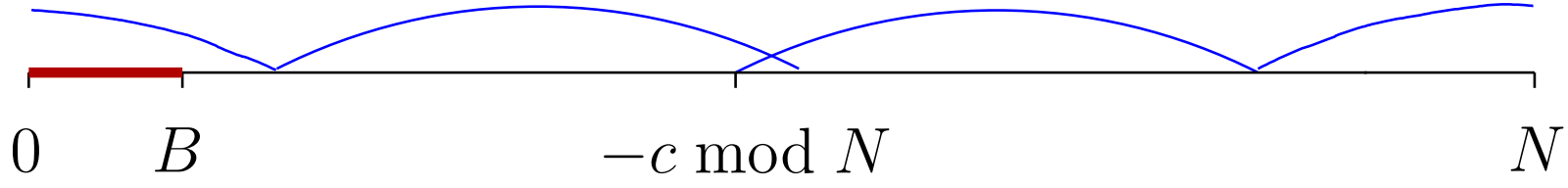
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

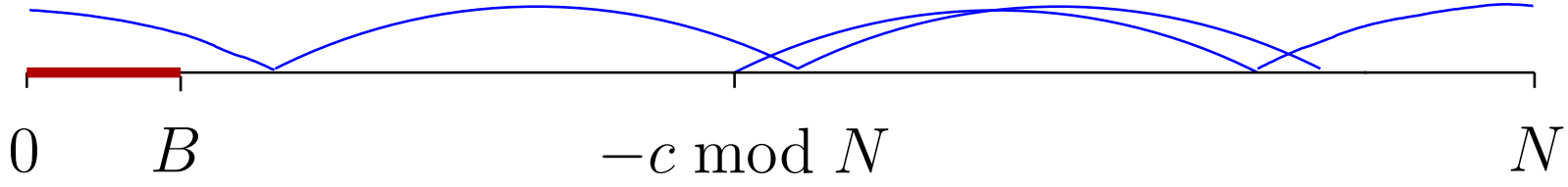
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

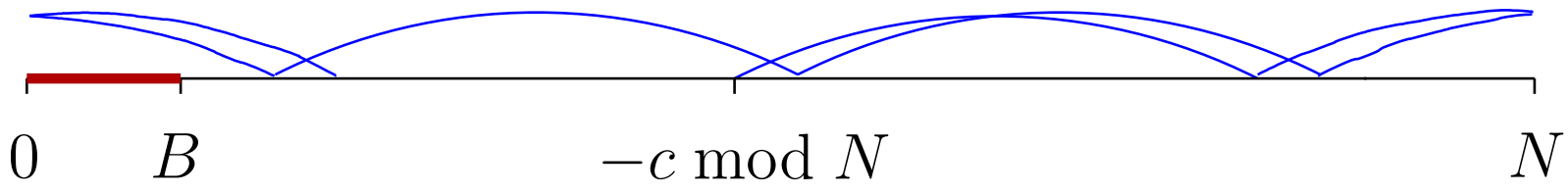
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

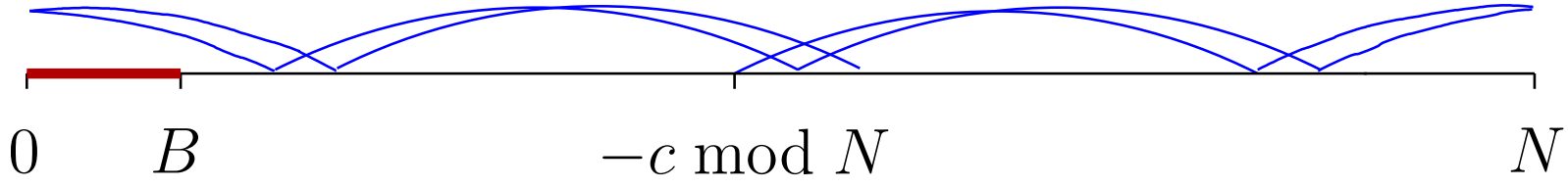
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots \qquad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

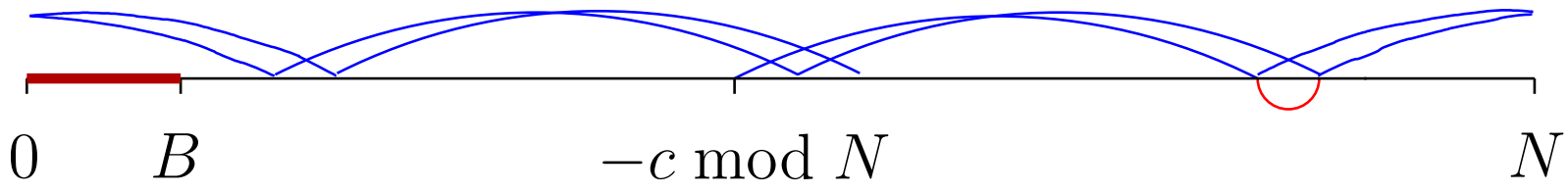
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

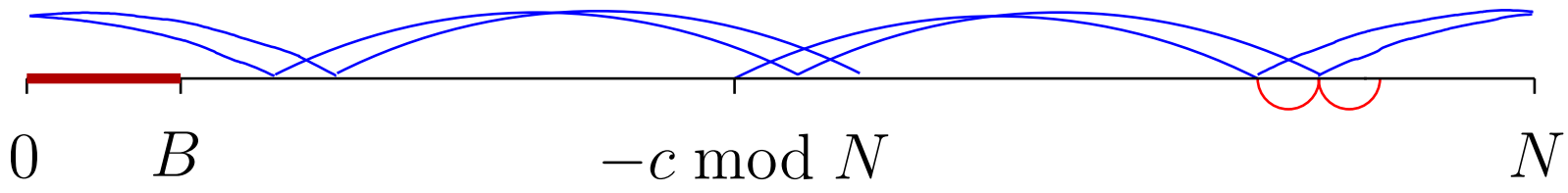
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

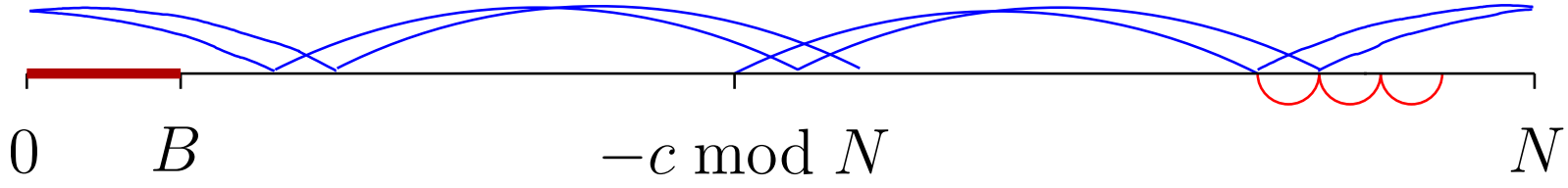
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

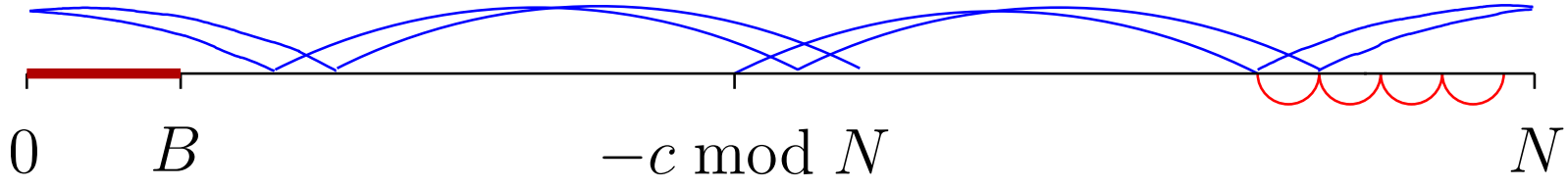
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

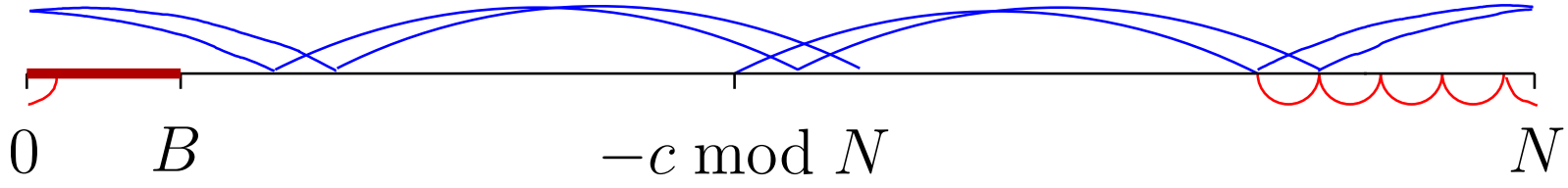
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Motivation of proposed algorithm

Problem: Find $0 \leq x, y < B < \sqrt{N}$ s.t. $\boxed{ax = y + c \bmod N}$

$$\Updownarrow$$

$$\boxed{y = ax - c \bmod N}$$

**1st step: Specify the problem**

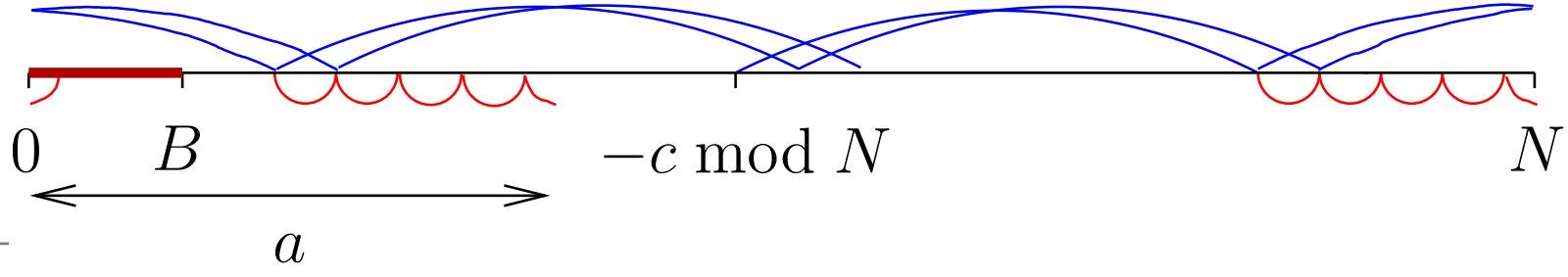
Find $x$-*minimal* solution w. r. t. $B$:

$$x = 0 \quad \rightarrow \quad y = -c \bmod N \overset{?}{<} B \qquad \text{no}$$

$$x = 1 \quad \rightarrow \quad y = -c + a \bmod N \overset{?}{<} B \qquad \text{no}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \qquad \ldots$$

$$x = \hat{x} \quad \rightarrow \quad \hat{y} = -c + \hat{x}a \bmod N \overset{?}{<} B \qquad \text{yes!}$$



# Idea of proposed algorithm

## 2nd step: Reduction to a smaller instance

$$a\hat{x} = \hat{y} + c \bmod N$$
$$\Rightarrow \quad a\hat{x} = \hat{y} + c + kN,\ k \in \mathbb{Z}$$

Euclidian division: $N = aq + r,\ 0 \leq r < a,\ q \in \mathbb{Z}^+$

$$\Rightarrow \quad a\hat{x} = \hat{y} + c + k(aq + r)$$
$$\Rightarrow \quad -rk = \hat{y} + c + a(kq - \hat{x})$$
$$\Rightarrow \quad -rk = \hat{y} + c \bmod a$$

# Idea of proposed algorithm

## 2nd step: Reduction to a smaller instance

$$a\hat{x} = \hat{y} + c \bmod N$$
$$\Rightarrow \quad a\hat{x} = \hat{y} + c + kN,\ k \in \mathbb{Z}$$

Euclidian division: $N = aq + r,\ 0 \leq r < a,\ q \in \mathbb{Z}^+$

$$\Rightarrow \quad a\hat{x} = \hat{y} + c + k(aq + r)$$
$$\Rightarrow \quad -rk = \hat{y} + c + a(kq - \hat{x})$$
$$\Rightarrow \quad -rk = \hat{y} + c \bmod a$$

# Idea of proposed algorithm

## 2nd step: Reduction to a smaller instance

$$a\hat{x} = \hat{y} + c \bmod N$$
$$\Rightarrow \quad a\hat{x} = \hat{y} + c + kN,\ k \in \mathbb{Z}$$

Euclidian division: $N = aq + r,\ 0 \leq r < a,\ q \in \mathbb{Z}^+$

$$\Rightarrow \quad a\hat{x} = \hat{y} + c + k(aq + r)$$
$$\Rightarrow \quad -rk = \hat{y} + c + a(kq - \hat{x})$$
$$\Rightarrow \quad -rk = \hat{y} + c \bmod a$$

## 3rd step: Iterating this process

$N_0 = N$ $\quad a_0 = a$ $\quad c_0 = c$ $\quad x_0 = \hat{x}$

$N_{i+1} = a_i$ $\quad a_{i+1} = -N_i \bmod a_i$ $\quad c_{i+1} = c_i \bmod N_{i+1}$ $\quad x_{i+1} = \frac{a_i x_i - \hat{y} - c_i}{N_i}$

# Idea of proposed algorithm, cont'd

**Iteration process (sequence of congruences):**

$$N_0 = N \qquad a_0 = a \qquad c_0 = c \qquad x_0 = \hat{x}$$

$$N_{i+1} = a_i \qquad a_{i+1} = -N_i \bmod a_i \qquad c_{i+1} = c_i \bmod N_{i+1} \qquad x_{i+1} = \frac{a_i x_i - \hat{y} - c_i}{N_i}$$

Define $(\text{cong}_i) : a_i x = y + c_i \bmod N_i$.

$(x_i, \hat{y})$ is $x$-minimal solution of $(\text{cong}_i)$ w.r.t. $B$, $x_i > 0$

$\Rightarrow$ $(x_{i+1}, \hat{y})$ is $x$-minimal solution of $(\text{cong}_{i+1})$ w.r.t. $B$

For each $i$:

$$-c_i \bmod N_i \overset{?}{<} B \quad \begin{cases} \xrightarrow{\text{yes}} & \hat{y} = -c_i \bmod N_i \\ \xrightarrow{\text{no}} & \text{iterate} \end{cases}$$

# Proposed algorithm, outline

Lin_Cong (Outline)

Input: $a, c, N, B$, gcd$(a, N) = 1$

Output: $x$-minimal solution $(\hat{x}, \hat{y})$ of $ax = y + c \bmod N$

1. set $a' = a,\ c' = c,\ N' = N,\ y' = -c' \bmod N'$
2. while $y' \geq B$ do
3. set $(a', N') = (-N' \bmod a', a')$ (parallel assignment)
4. set $c' = c' \bmod N', y' = -c' \bmod N'$
5. set $\hat{y} = y', \hat{x} = a^{-1} \cdot (\hat{y} + c) \bmod N$
6. return $(\hat{x}, \hat{y})$

# Proposed algorithm, outline

**Lin_Cong (Outline)**

Input: $a, c, N, B$, gcd$(a, N) = 1$

Output: $x$-minimal solution $(\hat{x}, \hat{y})$ of $ax = y + c \bmod N$

1. set $a' = a,\ c' = c,\ N' = N,\ y' = -c' \bmod N'$
2. while $y' \geq B$ do
3. set $(a', N') = (-N' \bmod a', a')$ (parallel assignment)
4. set $c' = c' \bmod N', y' = -c' \bmod N'$
5. set $\hat{y} = y', \hat{x} = a^{-1} \cdot (\hat{y} + c) \bmod N$
6. return $(\hat{x}, \hat{y})$

# Proposed algorithm, outline

Lin_Cong (Outline)

Input: $a, c, N, B$, gcd$(a, N) = 1$

Output: $x$-minimal solution $(\hat{x}, \hat{y})$ of $ax = y + c \bmod N$

1. set $a' = a,\ c' = c,\ N' = N,\ y' = -c' \bmod N'$
2. while $y' \geq B$ do
3. set $(a', N') = (-N' \bmod a', a')$ (parallel assignment)
4. set $c' = c' \bmod N', y' = -c' \bmod N'$
5. set $\hat{y} = y', \hat{x} = a^{-1} \cdot (\hat{y} + c) \bmod N$
6. return $(\hat{x}, \hat{y})$

**Improvements:** Efficient variant, extension for finding all small solutions, . . .

# Application to OW $\Rightarrow$ PD-OW (RSA)

Remember two questions: Click here

1. How to solve $ax = y + c \bmod N$?
2. How many small solutions (bound $B$)?

# Application to OW $\Rightarrow$ PD-OW (RSA)

Remember two questions: Click here

1. How to solve $ax = y + c \bmod N$?
2. How many small solutions (bound $B$)?

ad 1. Lin_Cong succeeds for any input

# Application to OW $\Rightarrow$ PD-OW (RSA)

Remember two questions: Click here

1. How to solve $ax = y + c \bmod N$?
2. How many small solutions (bound $B$)?

ad 1. Lin_Cong succeeds for any input ✓

# Application to OW $\Rightarrow$ PD-OW (RSA)

Remember two questions: Click here

1. How to solve $ax = y + c \bmod N$?
2. How many small solutions (bound $B$)?

ad 1. Lin_Cong succeeds for any input ✓

ad 2. precondition on $a \Rightarrow$ not too many small solutions

# Application to OW $\Rightarrow$ PD-OW (RSA)

Remember two questions: Click here

1. How to solve $ax = y + c \bmod N$?
2. How many small solutions (bound $B$)?

ad 1. Lin_Cong succeeds for any input ✓

ad 2. precondition on $a \Rightarrow$ not too many small solutions

$L_{a,N}$ contains no $(x, y), 0 < x < B/l, -B/l < y < B/l$

$\Leftrightarrow$

at most $l$ small solutions of $ax = y + c \bmod N$

# Application to OW $\Rightarrow$ PD-OW (RSA)

Remember two questions: Click here

1. How to solve $ax = y + c \bmod N$?
2. How many small solutions (bound $B$)?

ad 1. Lin_Cong succeeds for any input ✓

ad 2. precondition on $a \Rightarrow$ not too many small solutions ✓

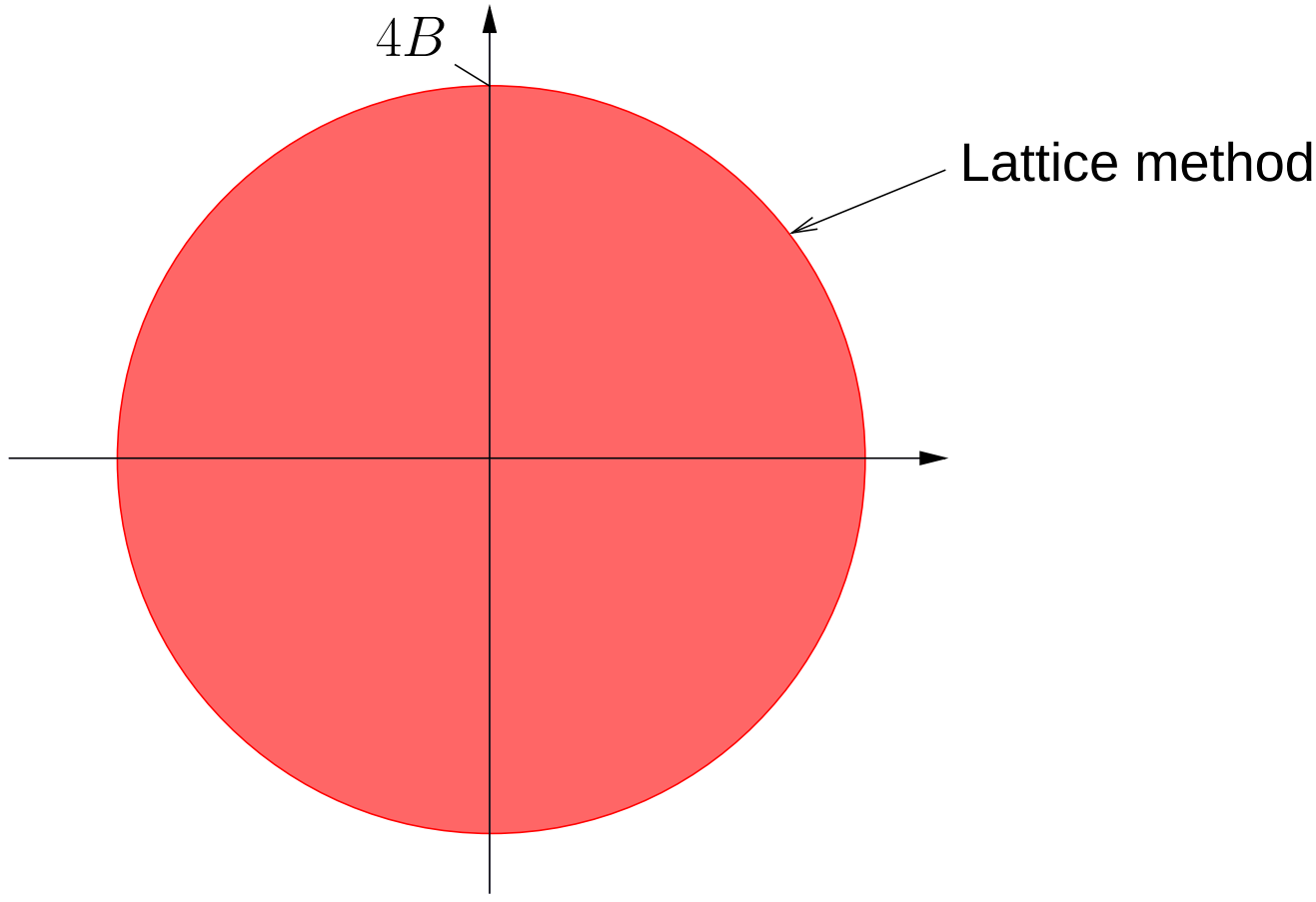
$L_{a,N}$ contains no $(x, y), 0 < x < B/l, -B/l < y < B/l$

$\Leftrightarrow$

at most $l$ small solutions of $ax = y + c \bmod N$

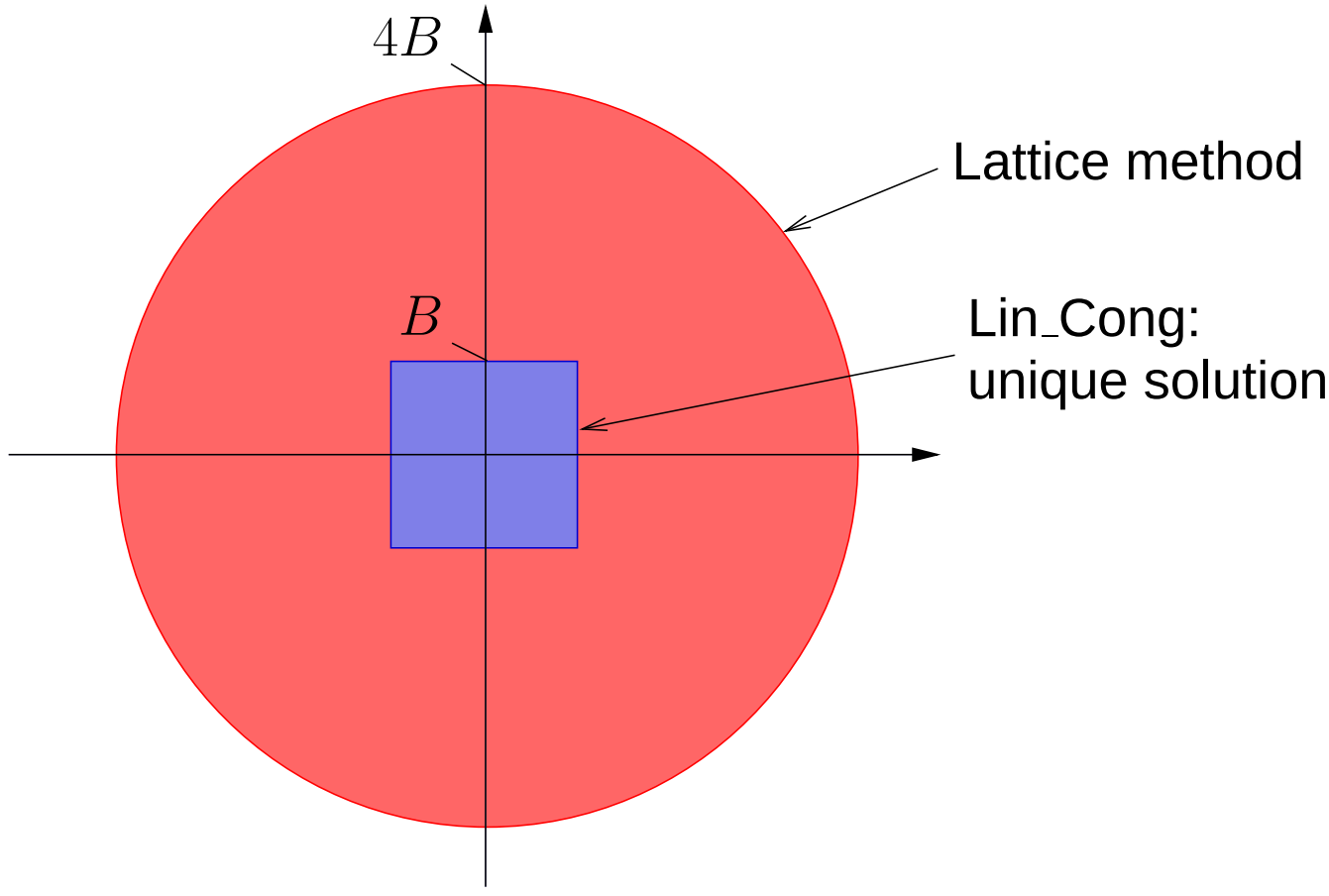
# Comparison

Critical area of lattice $L_{a,N} = \{(x, y) \in \mathbb{Z}^2 | ax = y \bmod N\}$:
No non-zero vector inside critical area $\Rightarrow$ method works



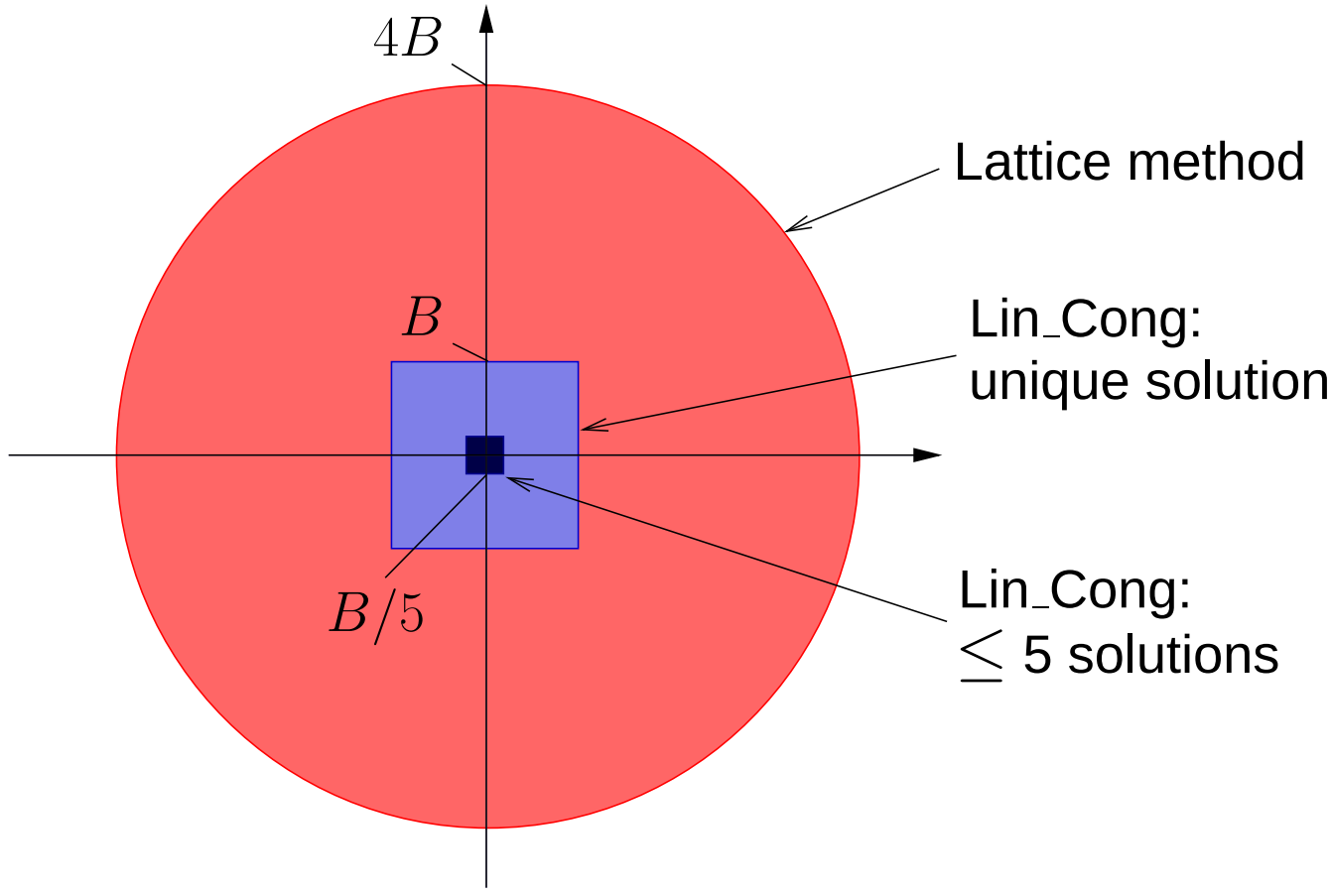
# Comparison

Critical area of lattice $L_{a,N} = \{(x, y) \in \mathbb{Z}^2 | ax = y \bmod N\}$:
No non-zero vector inside critical area $\Rightarrow$ method works



# Comparison

Critical area of lattice $L_{a,N} = \{(x, y) \in \mathbb{Z}^2 | ax = y \bmod N\}$:
No non-zero vector inside critical area $\Rightarrow$ method works



# Conclusion and further work

- Proposed algorithm always finds small solutions, provided small solutions exist at all
- Proposed algorithm is simple and efficient
- Proposed algorithm is flexible
- Further work: Find new applications!

# Conclusion and further work

- Proposed algorithm always finds small solutions, provided small solutions exist at all
- Proposed algorithm is simple and efficient
- Proposed algorithm is flexible
- Further work: Find new applications!

Thank you for your attention!