Lattice Reduction Techniques To Attack RSA

David Wong

March 2015

University of Bordeaux

RSA

(e, N) is the **public key**

(d, N) is the **private key**

Encrypt a message m:

$$c = m^e \pmod{N}$$

Decrypt a ciphertext c:

$$m = c^d \pmod{N}$$

$$\begin{tikzcd} & \boldsymbol{N} = p \times q \arrow[dl] \arrow[dr] & \\ (\boldsymbol{e}, \boldsymbol{N}) & & (\boldsymbol{d}, \boldsymbol{N}) \end{tikzcd}$$

ATTACKS

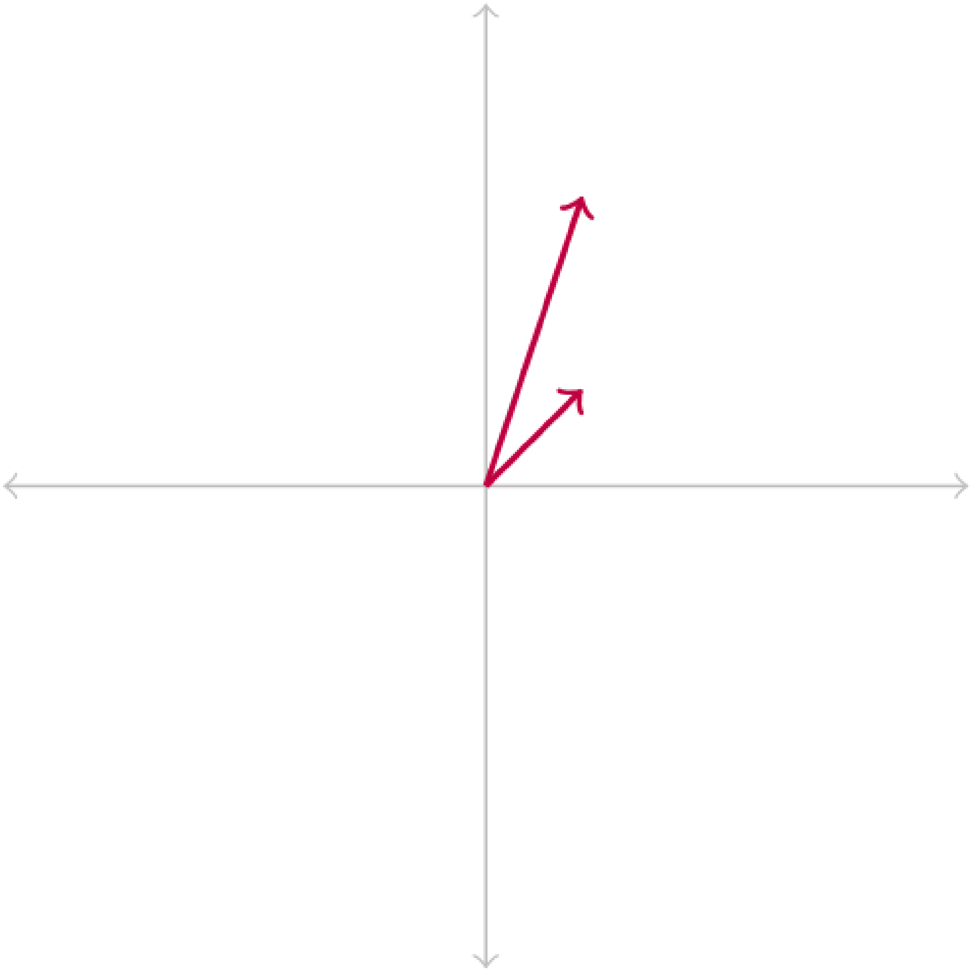
Attacks on the Implementation or the Mathematics.

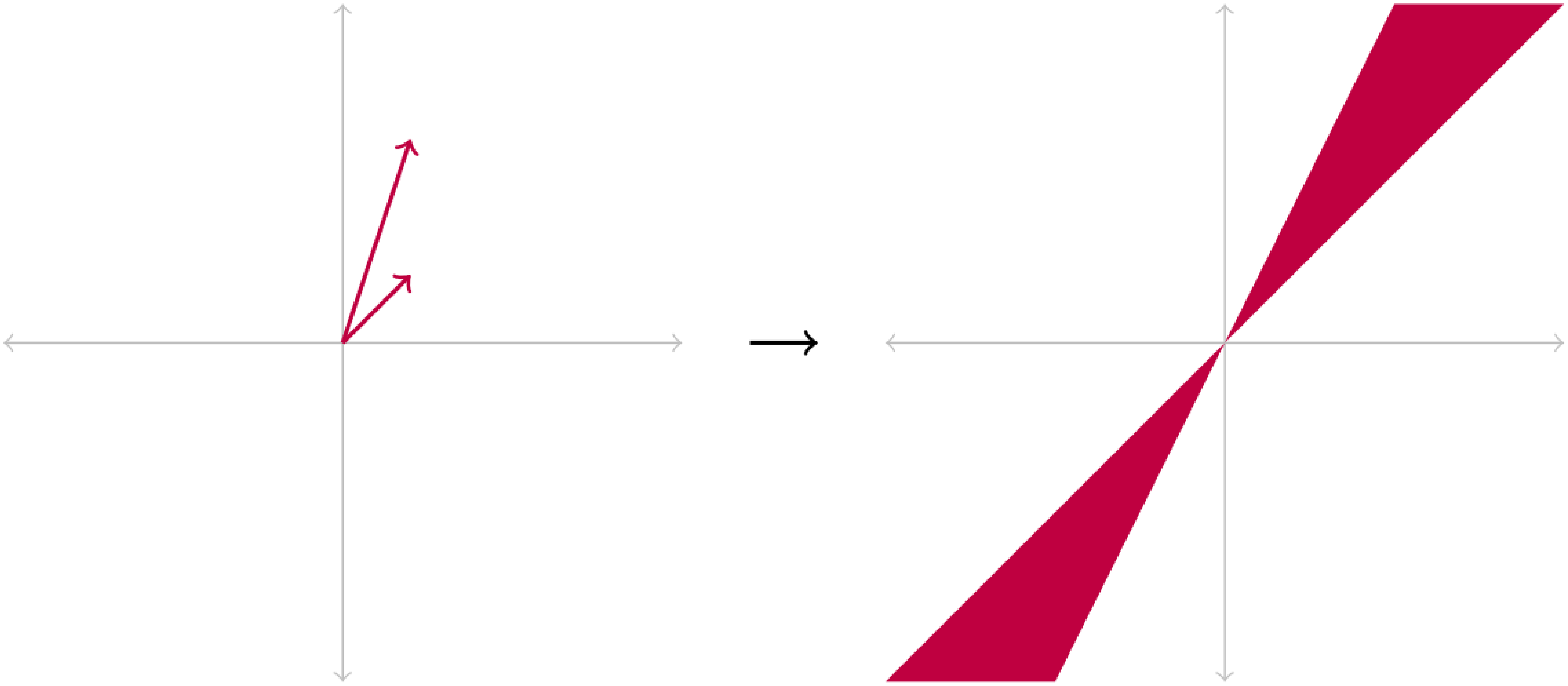
- Recover the plaintext
- Recover the private key

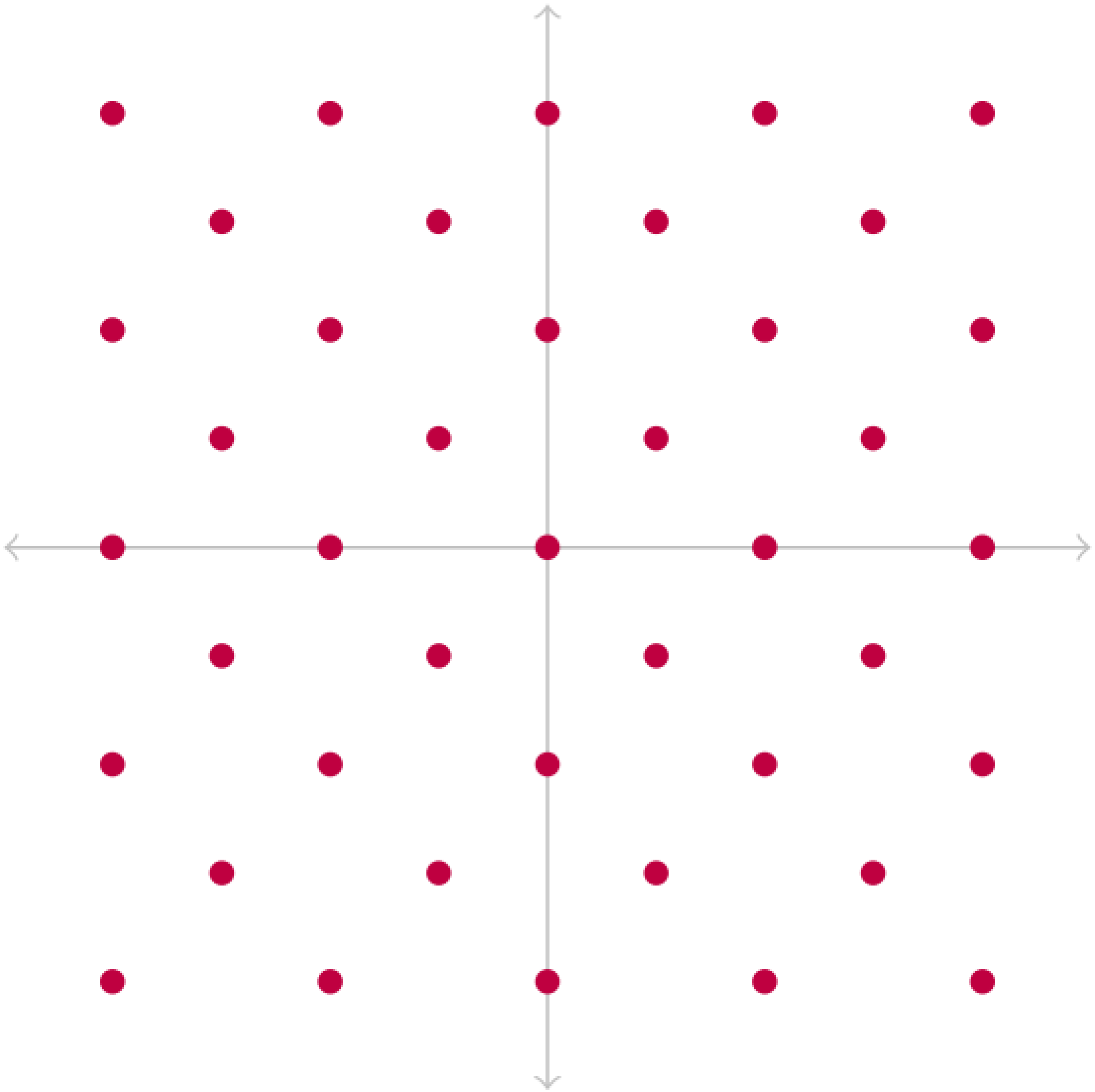
A Relaxed Model

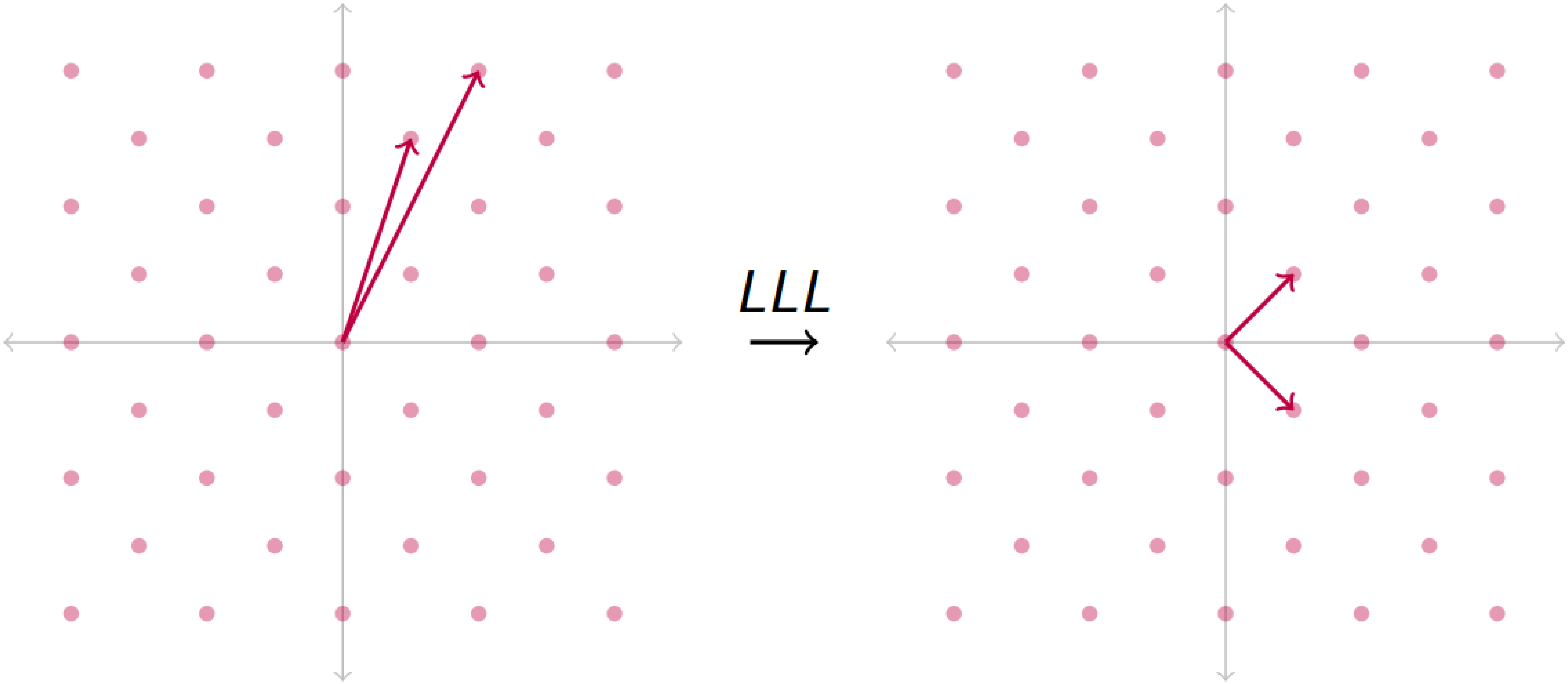
- We know a part of the message
- We know an approximation of one of the prime
- The private exponent is too small

LATTICE








LLL

$$B = \begin{pmatrix} \vec{b_1} \\ \vdots \\ \vec{b_n} \end{pmatrix} \xrightarrow{\textbf{LLL}} B' = \begin{pmatrix} \vec{b'_1} \\ \vdots \\ \vec{b'_n} \end{pmatrix}$$

$$B = \begin{pmatrix} \vec{b_1} \\ \vdots \\ \vec{b_n} \end{pmatrix} \xrightarrow{\quad\textbf{LLL}\quad} B' = \begin{pmatrix} \vec{b'_1} \\ \vdots \\ \vec{b'_n} \end{pmatrix}$$

$$\|b'_1\| \leq \|b'_2\| \leq \ldots \leq \|b'_i\| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \cdot det(L)^{\frac{1}{n+1-i}}$$

COPPERSMITH

$$c = m^e \pmod{N}$$

$$c = m^e \pmod{N}$$

$$m = m_0 + x_0$$

« le password du jour : cupcake »

$$c = m^e \pmod{N}$$

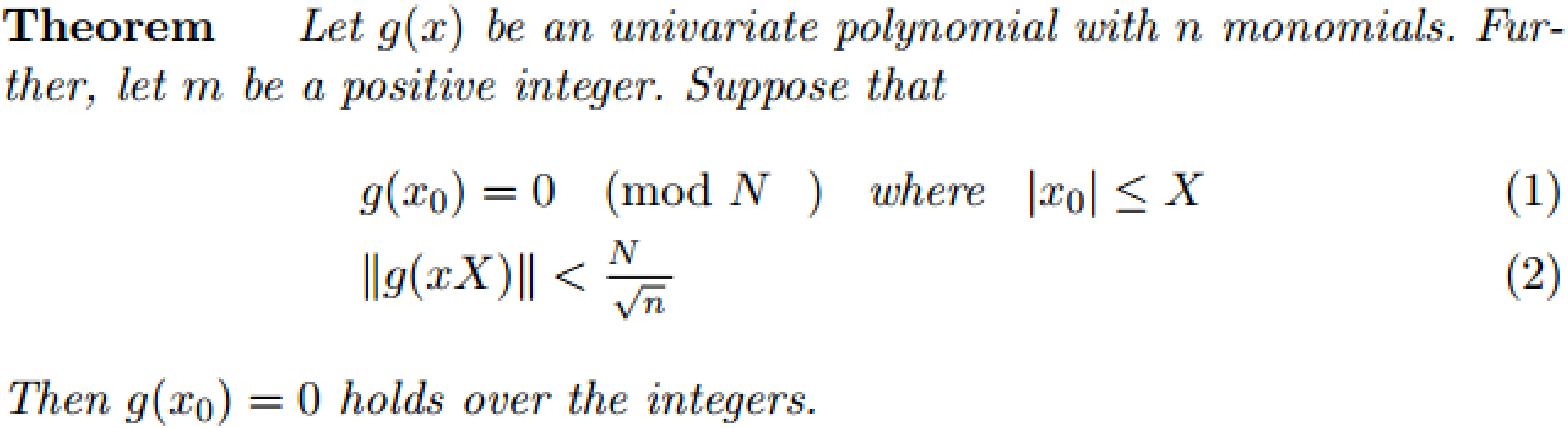
$$m = m_0 + x_0$$

« le password du jour : cupcake »

$$f(x) = c - (m_0 + x)^e \pmod{N}$$

$$\begin{tikzcd}
f(x) = 0 \pmod{N} \text{ with } |x| < X \arrow[d] \\
g(x) = 0 \text{ over } \mathbb{Z}
\end{tikzcd}$$

HOWGRAVE-GRAHAM



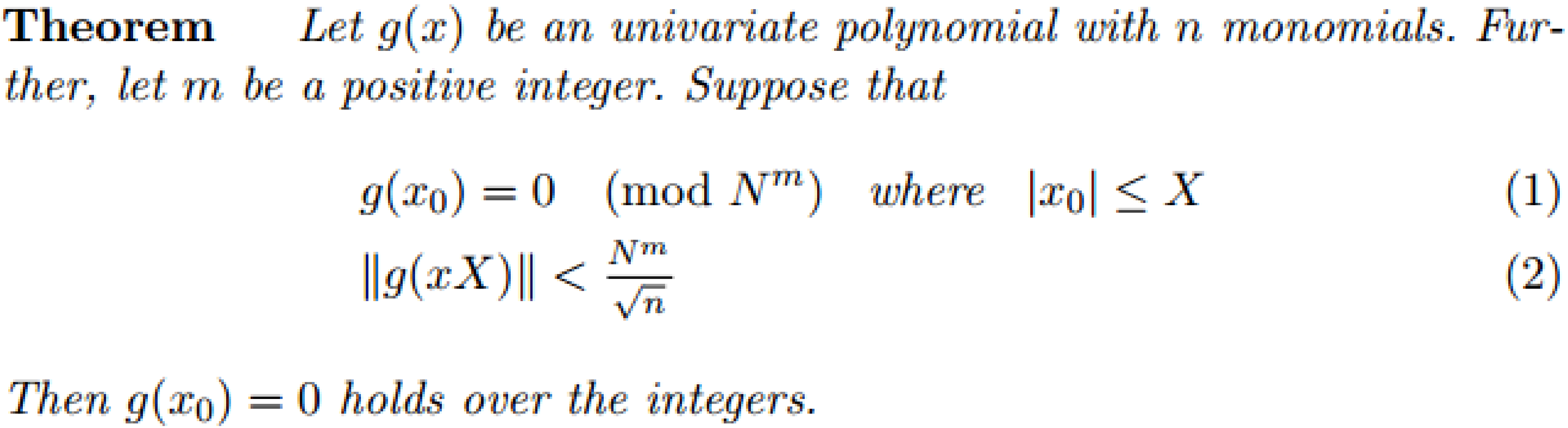
Theorem *Let $g(x)$ be an univariate polynomial with n monomials. Further, let m be a positive integer. Suppose that*

$$g(x_0) = 0 \pmod{N} \quad \textit{where} \quad |x_0| \leq X \tag{1}$$

$$\|g(xX)\| < \frac{N}{\sqrt{n}} \tag{2}$$

Then $g(x_0) = 0$ holds over the integers.

HOWGRAVE-GRAHAM



Theorem *Let $g(x)$ be an univariate polynomial with n monomials. Further, let m be a positive integer. Suppose that*

$$g(x_0) = 0 \pmod{N^m} \quad \textit{where} \quad |x_0| \leq X \tag{1}$$

$$\|g(xX)\| < \frac{N^m}{\sqrt{n}} \tag{2}$$

Then $g(x_0) = 0$ holds over the integers.

$$\begin{tikzcd}
f(x_0) = 0 \pmod{N} \arrow[dd] & \text{with } |x_0| < X \arrow[d] \\
{} & \begin{array}{l} g(x_0) = 0 \pmod{N^m} \\ \|g(xX)\| < \frac{N^m}{\sqrt{n}} \end{array} \arrow[l] \\
g(x_0) = 0 \text{ over } \mathbb{Z} &
\end{tikzcd}$$

LLL reduction:

- It only does integer linear operations on the basis vectors
- The shortest vector of the output basis is bound

$$B = \begin{pmatrix} \vec{b_1} \\ \vdots \\ \vec{b_n} \end{pmatrix} \xrightarrow{\quad\textbf{LLL}\quad} B' = \begin{pmatrix} \vec{b'_1} \\ \vdots \\ \vec{b'_n} \end{pmatrix}$$

$$\|b'_1\| \leq \|b'_2\| \leq \ldots \leq \|b'_i\| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \cdot det(L)^{\frac{1}{n+1-i}}$$

$$B = \begin{pmatrix} \vec{b_1} \\ \vdots \\ \vec{b_n} \end{pmatrix} \xrightarrow{\textbf{LLL}} B' = \begin{pmatrix} \vec{b'_1} \\ \vdots \\ \vec{b'_n} \end{pmatrix}$$

$$\|b'_1\| \leq \|b'_2\| \leq \ldots \leq \|b'_i\| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \cdot det(L)^{\frac{1}{n+1-i}}$$

$$\|b'_1\| \leq 2^{\frac{n(n-1)}{4(n)}} \cdot det(L)^{\frac{1}{n}}$$

$$g_{i,j}(x) = x^j \cdot N^i \cdot f^{m-i}(x)$$

$$\text{for } i = 0, \ldots, m-1, \quad j = 0, \ldots, \delta - 1$$

$$h_i(x) = x^i \cdot f^m(x)$$

$$\text{for } i = 0, \ldots, t-1$$

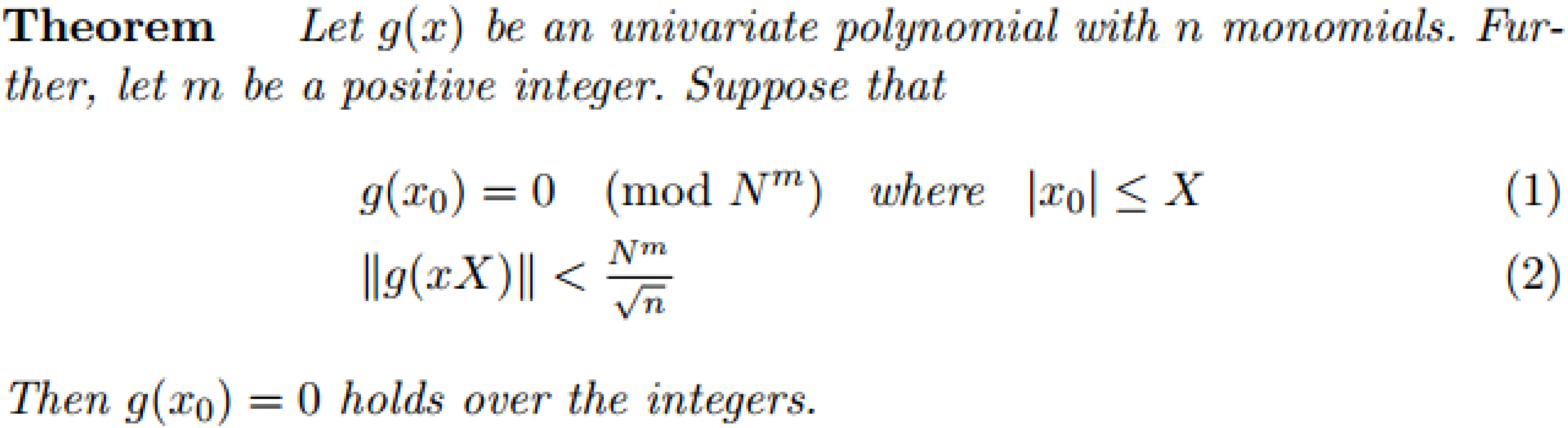
Those polynomials achieve two things:

- They have the same root x_0 but modulo N^m
- Each iteration introduce a new polynomial

$$\begin{tikzcd}
f(x_0) = 0 \pmod{N} \arrow[dd] & \text{with } |x_0| < X \arrow[d] \\
 & \begin{array}{l} g(x_0) = 0 \pmod{N^m} \\ \|g(xX)\| < \frac{N^m}{\sqrt{n}} \end{array} \arrow[l] \\
g(x_0) = 0 \text{ over } \mathbb{Z} &
\end{tikzcd}$$

$$\begin{tikzcd}
 & f(x_0) = 0 \pmod{N} \text{ with } |x_0| < X \arrow[dr] \arrow[ddddl] & \\
 & & \text{generate } f_i \text{ s.t. } f_i(x_0) = 0 \pmod{N^m} \arrow[d] \\
 & & B = \begin{pmatrix} f_i(xX) \\ \vdots \\ f_n(xX) \end{pmatrix} \arrow[d, "\text{LLL}"] \\
 & & B' = \begin{pmatrix} b_1 = g(xX) \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \arrow[d] \\
g(x_0) = 0 \text{ over } \mathbb{Z} & & g(x_0) = 0 \pmod{N^m} \text{ and } \|g(xX)\| < \frac{N^m}{\sqrt{n}} \arrow[ll]
\end{tikzcd}$$

HOWGRAVE-GRAHAM



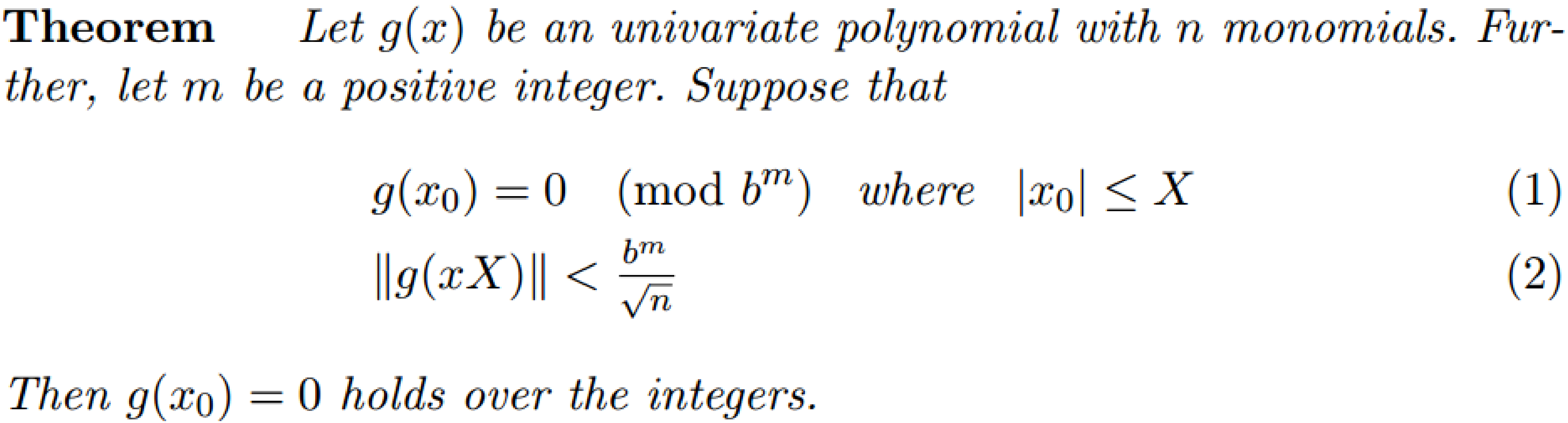
Theorem *Let $g(x)$ be an univariate polynomial with n monomials. Further, let m be a positive integer. Suppose that*

$$g(x_0) = 0 \pmod{N^m} \quad \textit{where} \quad |x_0| \leq X \tag{1}$$

$$\|g(xX)\| < \frac{N^m}{\sqrt{n}} \tag{2}$$

Then $g(x_0) = 0$ holds over the integers.

HOWGRAVE-GRAHAM



Theorem *Let $g(x)$ be an univariate polynomial with n monomials. Further, let m be a positive integer. Suppose that*

$$g(x_0) = 0 \pmod{b^m} \quad \textit{where} \quad |x_0| \le X \tag{1}$$

$$\|g(xX)\| < \frac{b^m}{\sqrt{n}} \tag{2}$$

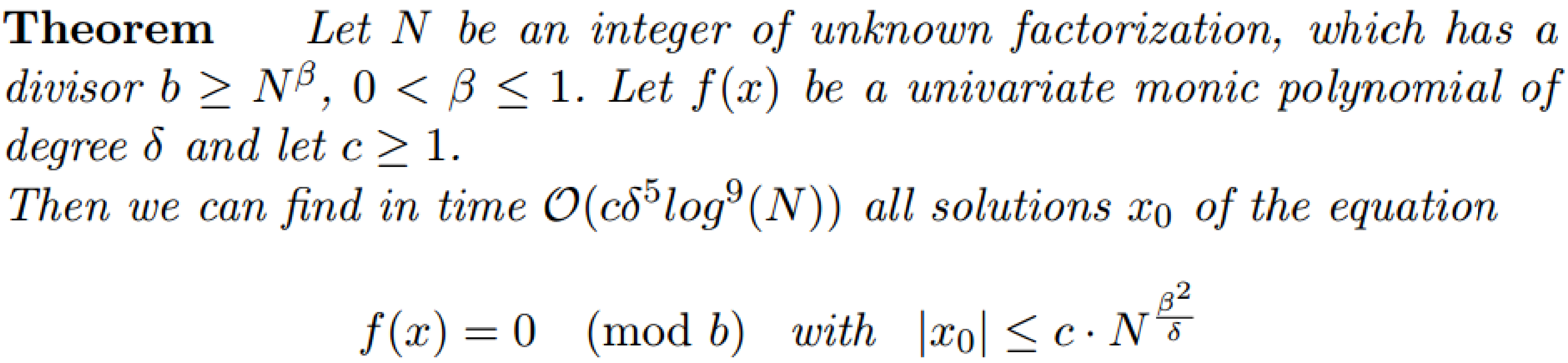
Then $g(x_0) = 0$ holds over the integers.

$$|\tilde{p} - p| < \boldsymbol{N}^{\frac{1}{4}}$$

$$|\tilde{p} - p| < \boldsymbol{N}^{\frac{1}{4}}$$

$$\tilde{p} = x_0 \pmod{p}$$

COPPERSMITH



Theorem *Let N be an integer of unknown factorization, which has a divisor $b \geq N^{\beta}$, $0 < \beta \leq 1$. Let $f(x)$ be a univariate monic polynomial of degree δ and let $c \geq 1$.*

Then we can find in time $\mathcal{O}(c\delta^5 log^9(N))$ all solutions x_0 of the equation

$$f(x) = 0 \pmod{b} \quad \textit{with} \quad |x_0| \leq c \cdot N^{\frac{\beta^2}{\delta}}$$

BONEH-DURFEE

$$\begin{tikzcd}
& \boldsymbol{N} = p \times q \arrow[dl] \arrow[dr] & \\
(\boldsymbol{e}, \boldsymbol{N}) & & (\boldsymbol{d}, \boldsymbol{N})
\end{tikzcd}$$

$$e \cdot d = 1 \pmod{\varphi(N)}$$

$$e \cdot d = 1 \pmod{\varphi(N)}$$

$$\implies e \cdot d = k \cdot \varphi(N) + 1$$

$$
\begin{aligned}
& e \cdot d = 1 \pmod{\varphi(N)} \\
\implies & e \cdot d = k \cdot \varphi(N) + 1 \\
\implies & k \cdot \varphi(N) + 1 = 0 \pmod{e}
\end{aligned}
$$

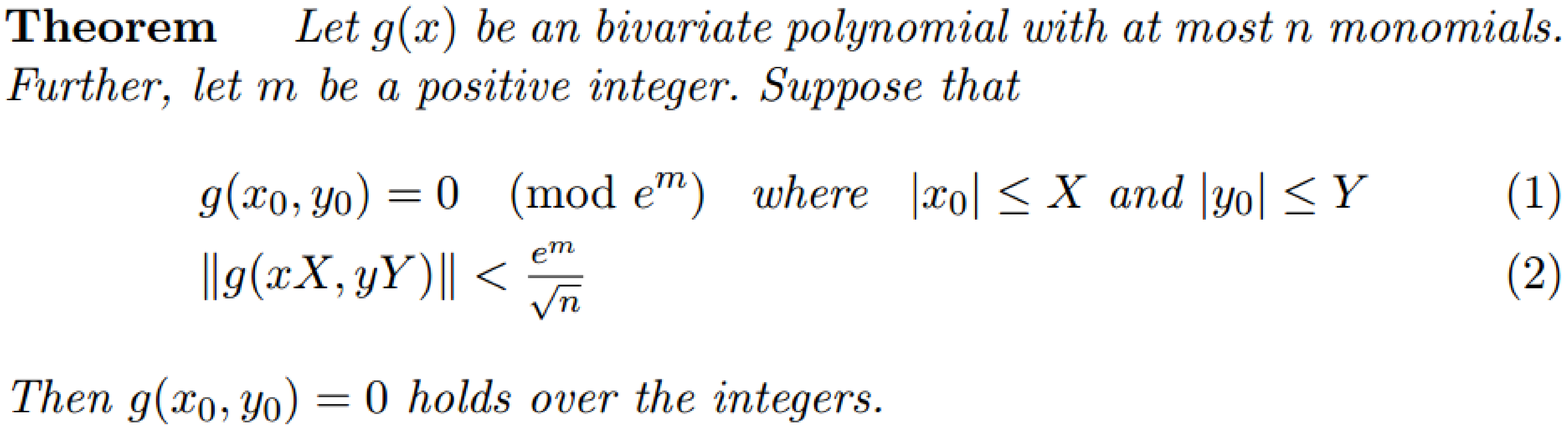
$$
\begin{aligned}
& e \cdot d = 1 \pmod{\varphi(N)} \\
\implies & e \cdot d = k \cdot \varphi(N) + 1 \\
\implies & k \cdot \varphi(N) + 1 = 0 \pmod{e} \\
\implies & k \cdot (N + 1 - p - q) + 1 = 0 \pmod{e}
\end{aligned}
$$

$$\underbrace{k}_{x} \cdot (\underbrace{N + 1}_{A} \underbrace{-p - q}_{y}) + 1 = 0 \pmod{e}$$

$$\underbrace{k}_{x} \cdot (\underbrace{N+1}_{A} \underbrace{-p-q}_{y}) + 1 = 0 \pmod{e}$$

$$f(x,y) = x(A+y)+1$$

HOWGRAVE-GRAHAM



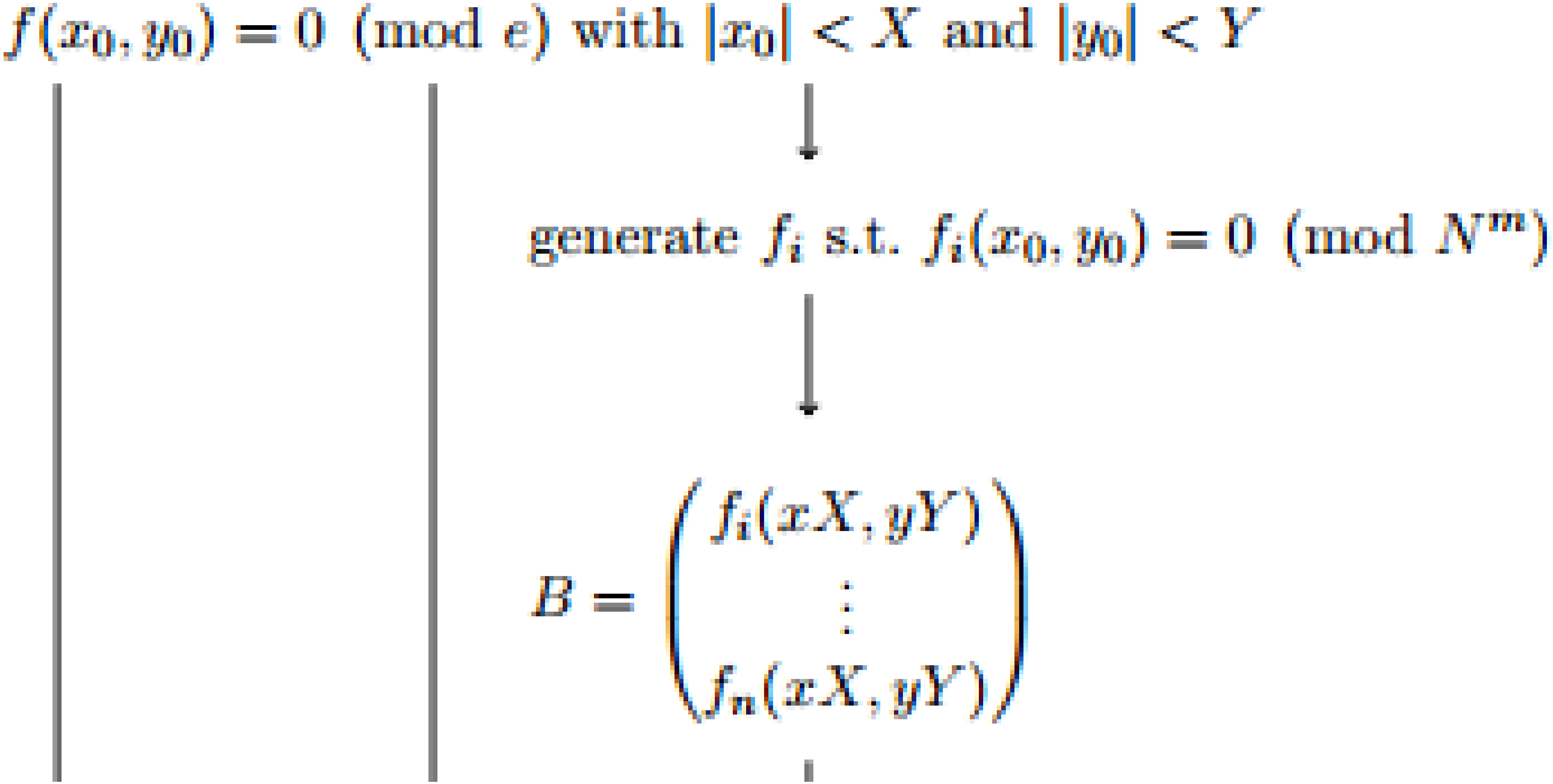
Theorem *Let $g(x)$ be an bivariate polynomial with at most n monomials. Further, let m be a positive integer. Suppose that*

$$g(x_0, y_0) = 0 \pmod{e^m} \quad \textit{where} \quad |x_0| \le X \textit{ and } |y_0| \le Y \tag{1}$$

$$\|g(xX, yY)\| < \frac{e^m}{\sqrt{n}} \tag{2}$$

Then $g(x_0, y_0) = 0$ holds over the integers.

$$\begin{tikzcd}
f(x_0, y_0) = 0 \pmod{e} \text{ with } |x_0| < X \text{ and } |y_0| < Y \arrow[d] \\
\text{generate } f_i \text{ s.t. } f_i(x_0, y_0) = 0 \pmod{N^m} \arrow[d] \\
B = \begin{pmatrix} f_i(xX, yY) \\ \vdots \\ f_n(xX, yY) \end{pmatrix} \arrow[d, "\text{LLL}"] \\
B' = \begin{pmatrix} b_1 = g_1(xX, yY) \\ b_2 = g_2(xX, yY) \\ \vdots \\ b_n \end{pmatrix} \arrow[d] \\
\begin{array}{l} g_1(x_0, y_0) = 0 \pmod{e^m} \text{ and } \|g_1(xX, yY)\| < \frac{e^m}{\sqrt{n}} \\ g_2(x_0, y_0) = 0 \pmod{e^m} \text{ and } \|g_2(xX, yY)\| < \frac{e^m}{\sqrt{n}} \end{array} \arrow[d] \\
\begin{array}{l} g_1(x_0, y_0) = 0 \text{ over } \mathbb{Z} \\ g_2(x_0, y_0) = 0 \text{ over } \mathbb{Z} \end{array} \arrow[d] \\
r(x) = resultant_x(g_1, g_2)
\end{tikzcd}$$



$f(x_0, y_0) = 0 \pmod{e}$ with $|x_0| < X$ and $|y_0| < Y$

generate f_i s.t. $f_i(x_0, y_0) = 0 \pmod{N^m}$

$$B = \begin{pmatrix} f_i(xX, yY) \\ \vdots \\ f_n(xX, yY) \end{pmatrix}$$

$$\begin{tikzcd}
B = \begin{pmatrix} f_1(xX, yY) \\ \vdots \\ f_n(xX, yY) \end{pmatrix} \arrow[d, "\textbf{LLL}"] \\
B' = \begin{pmatrix} b_1 = g_1(xX, yY) \\ b_2 = g_2(xX, yY) \\ \vdots \\ b_n \end{pmatrix}
\end{tikzcd}$$

$$B' = \begin{pmatrix} b_1 = g_1(xX, yY) \\ b_2 = g_2(xX, yY) \\ \vdots \\ b_n \end{pmatrix}$$

$$g_1(x_0, y_0) = 0 \pmod{e^m} \text{ and } \|g_1(xX, yY)\| < \frac{e^m}{\sqrt{n}}$$

$$g_2(x_0, y_0) = 0 \pmod{e^m} \text{ and } \|g_2(xX, yY)\| < \frac{e^m}{\sqrt{n}}$$

$$g_1(x_0, y_0) = 0 \text{ over } \mathbb{Z}$$

$$g_2(x_0, y_0) = 0 \text{ over } \mathbb{Z}$$

$$g_1(x_0, y_0) = 0 \pmod{e^m} \text{ and } \|g_1(xX, yY)\| < \frac{e^m}{\sqrt{n}}$$

$$g_2(x_0, y_0) = 0 \pmod{e^m} \text{ and } \|g_2(xX, yY)\| < \frac{e^m}{\sqrt{n}}$$

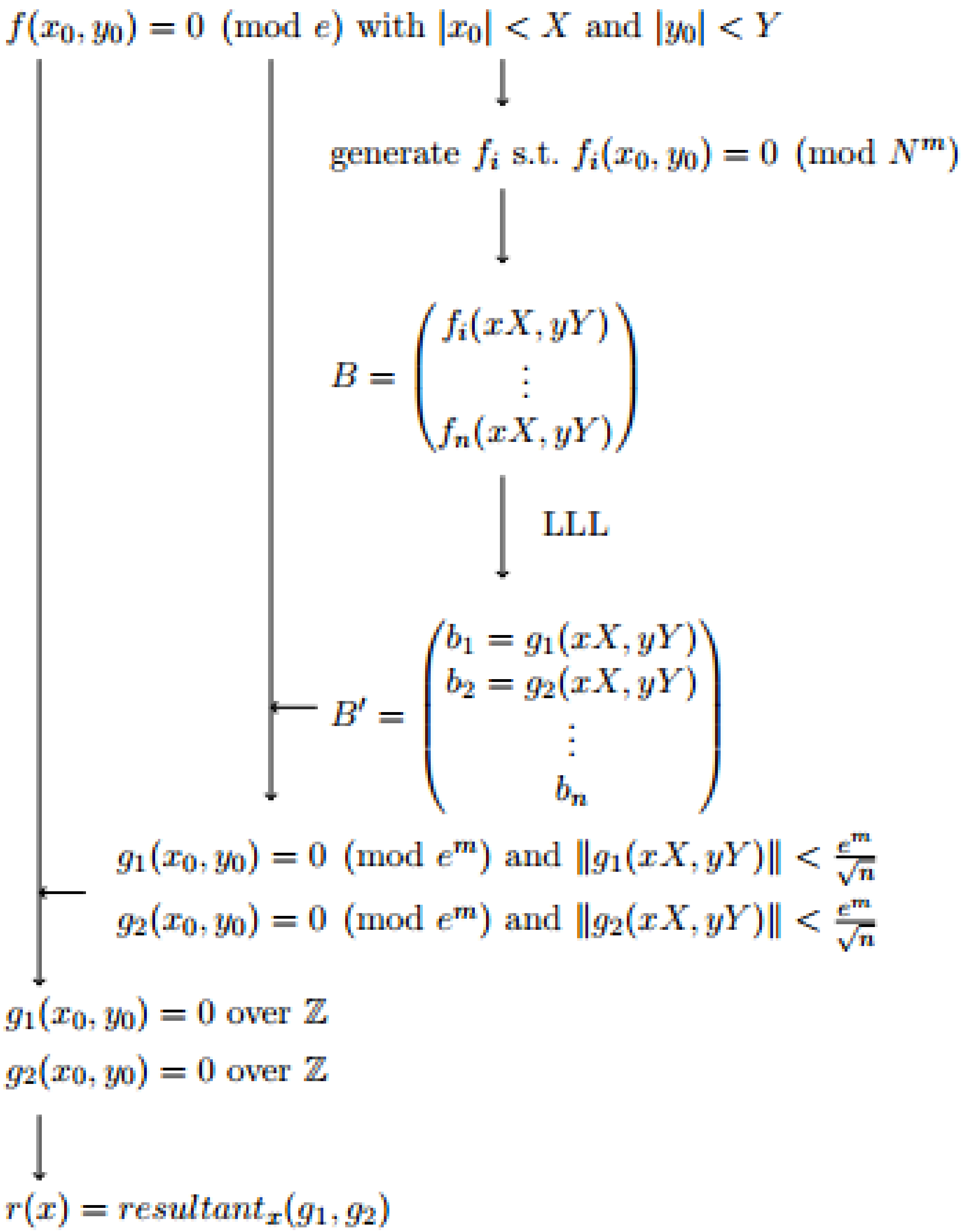
$$\Big\downarrow$$

$$g_1(x_0, y_0) = 0 \text{ over } \mathbb{Z}$$

$$g_2(x_0, y_0) = 0 \text{ over } \mathbb{Z}$$

$$\Big\downarrow$$

$$r(x) = resultant_x(g_1, g_2)$$


$f(x_0, y_0) = 0 \pmod{e}$ with $|x_0| < X$ and $|y_0| < Y$
generate f_i s.t. $f_i(x_0, y_0) = 0 \pmod{N^m}$
$B = \begin{pmatrix} f_i(xX, yY) \\ \vdots \\ f_n(xX, yY) \end{pmatrix}$
LLL
$B' = \begin{pmatrix} b_1 = g_1(xX, yY) \\ b_2 = g_2(xX, yY) \\ \vdots \\ b_n \end{pmatrix}$
$g_1(x_0, y_0) = 0 \pmod{e^m}$ and $\|g_1(xX, yY)\| < \frac{e^m}{\sqrt{n}}$
$g_2(x_0, y_0) = 0 \pmod{e^m}$ and $\|g_2(xX, yY)\| < \frac{e^m}{\sqrt{n}}$
$g_1(x_0, y_0) = 0$ over $\mathbb{Z}$
$g_2(x_0, y_0) = 0$ over $\mathbb{Z}$
$r(x) = resultant_x(g_1, g_2)$

$$\begin{array}{c|ccccccccc}
 & 1 & x & xy & x^2 & x^2y & x^2y^2 & y & xy^2 & x^2y^3 \\
\hline
e^2 & e^2 & & & & & & & & \\
xe^2 & & e^2X & & & & & & & \\
fe & e & eAX & eXY & & & & & & \\
x^2e^2 & & & & e^2X^2 & & & & & \\
xfe & & eX & & eAX^2 & eX^2Y & & & & \\
f^2 & 1 & 2AX & 2XY & A^2X^2 & 2AX^2Y & X^2Y^2 & & & \\
ye^2 & & & & & & e^2Y & & & \\
yfe & & & eAXY & & & & eY & eXY^2 & \\
yf^2 & & & 2AXY & & A^2X^2Y & 2AX^2Y^2 & Y & 2XY^2 & X^2Y^3
\end{array}$$

Boneh-Durfee basis matrix for $m = 2$, $t = 1$

$$\begin{array}{c|ccccccccc}
 & 1 & x & xy & x^2 & x^2y & x^2y^2 & y & xy^2 & x^2y^3 \\
\hline
e^2 & e^2 & & & & & & & & \\
xe^2 & & e^2X & & & & & & & \\
fe & e & eAX & eXY & & & & & & \\
x^2e^2 & & & & e^2X^2 & & & & & \\
xfe & & eX & & eAX^2 & eX^2Y & & & & \\
f^2 & 1 & 2AX & 2XY & A^2X^2 & 2AX^2Y & X^2Y^2 & & & \\
ye^2 & & & & & & e^2Y & & & \\
yfe & & & eAXY & & & & eY & eXY^2 & \\
yf^2 & & & 2AXY & & A^2X^2Y & 2AX^2Y^2 & Y & 2XY^2 & X^2Y^3
\end{array}$$

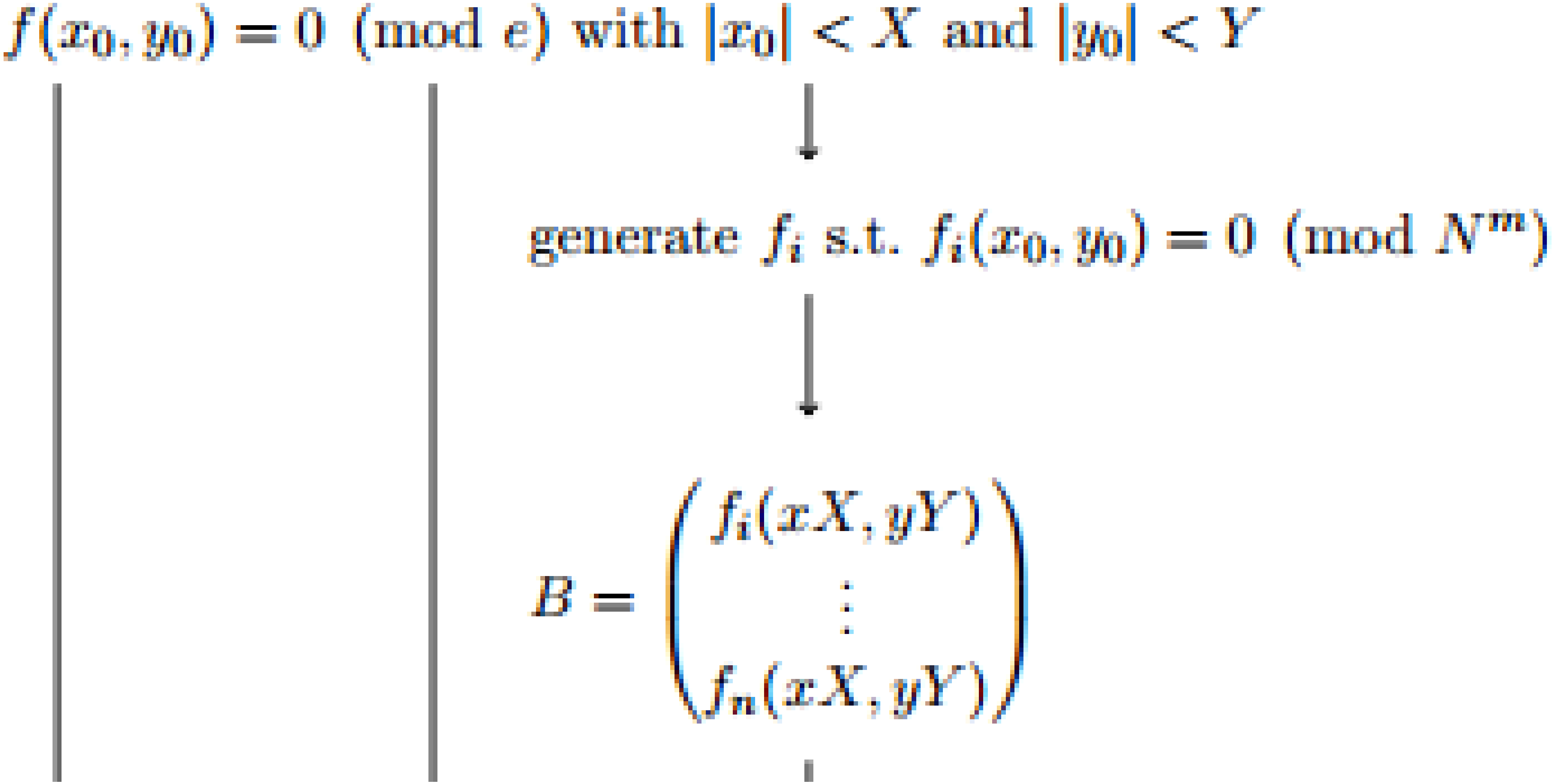
Boneh-Durfee basis matrix for $m = 2$, $t = 1$

$$\begin{array}{c|ccccccccc}
 & 1 & x & xy & x^2 & x^2y & x^2y^2 & y & xy^2 & x^2y^3 \\
\hline
e^2 & e^2 & & & & & & & & \\
xe^2 & & e^2X & & & & & & & \\
fe & e & eAX & eXY & & & & & & \\
x^2e^2 & & & & e^2X^2 & & & & & \\
xfe & & eX & & eAX^2 & eX^2Y & & & & \\
f^2 & 1 & 2AX & 2XY & A^2X^2 & 2AX^2Y & X^2Y^2 & & & \\
yf^2 & & & 2AXY & & A^2X^2Y & 2AX^2Y^2 & Y & 2XY^2 & X^2Y^3
\end{array}$$

After removing the damaging y-shifts' coefficient vectors

HERRMAN AND MAY:
UNRAVELLED LINEARIZATION

$$f(x,y) = \underbrace{1 + xy}_{u} + Ax \pmod e$$



$f(x_0, y_0) = 0 \pmod{e}$ with $|x_0| < X$ and $|y_0| < Y$

generate f_i s.t. $f_i(x_0, y_0) = 0 \pmod{N^m}$

$$B = \begin{pmatrix} f_i(xX, yY) \\ \vdots \\ f_n(xX, yY) \end{pmatrix}$$

$$\begin{array}{cccccccc}
 & 1 & x & u & x^2 & ux & u^2 & u^2y \\
e^2 & e^2 & & & & & & \\
xe^2 & & e^2X & & & & & \\
\bar{f}e & & eAX & eU & & & & \\
x^2e^2 & & & & e^2X^2 & & & \\
x\bar{f}e & & & & eAX^2 & eUX & & \\
\bar{f}^2 & & & & A^2X^2 & 2AUX & U^2 & \\
y\bar{f}^2 & & -A^2X & -2AU & & A^2UX & 2AU^2 & U^2Y
\end{array}$$

$$d < N^{0.292}$$

BONEH-DURFEE BOUND

CONCLUSIONS