Takagi/Naito’s algorithm revisited

M. Joye, F. Koeune and J.-J. Quisquater
Takagi/Naito’s algorithm revisited

M. Joye\textsuperscript{1)}, F. Koene\textsuperscript{2)} and J.-J. Quisquater\textsuperscript{2)}

March 29, 1997

\textsuperscript{1)} Département de Mathématique (AGEL), Université catholique de Louvain
Chemin du Cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
E-mail: joye@agel.ucl.ac.be

\textsuperscript{2)} Département d’Électricité (DICE), Université catholique de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
E-mail: \{fkoene,jjq\}@dice.ucl.ac.be

\textbf{Abstract.} Recently, Takagi and Naito extended the Håstad algorithm to the multivariate case. In this report, we simplify the proof of their theorem. We also significantly improve their bound.

\section{Introduction}

In [2], Håstad presented a way to solve a system of univariate modular polynomial equations. His method was based on the use of LLL to reduce a lattice of dimension $k + \epsilon + 1$, where $k$ is the number of equations and $\epsilon$ is the maximal degree of the polynomial equations. After publication, Rivest suggested a great simplification of the proof, reducing the lattice dimension to $\epsilon + 2$ and yielding a significant improvement of some bound (see below for more details). This improved version was published in [3].

Recently, Takagi and Naito [4] extended the initial Håstad algorithm to the multivariate case. We will show that the same improvement as Rivest suggested can be applied to the extended algorithm, resulting in the same proof simplification and bound improvement.

\section{Improvement}

The theorem we are going to prove is the following.
Theorem 1. Consider the system of $k$ modular polynomial equations of degree $\leq e$ with $l$ variables

$$
\sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \cdots + j_l \leq e} a_{i, j_1, j_2, \ldots, j_l} x_1^{j_1} x_2^{j_2} \cdots x_l^{j_l} \equiv 0 \pmod{n_i} \quad \text{for } i = 1, 2, \ldots, k
$$

(1)

where $x_1, \ldots, x_l < n$ and $n = \min n_i$.

Suppose that the moduli $n_i$ are coprime and that

$$
\gcd(a_{i, j_1, j_2, \ldots, j_l}^{j_1 + j_2 + \cdots + j_l \leq e}, n_i) = 1 \quad (\forall 1 \leq i \leq k)
$$

* Let $g$ be the (max.) number of different terms, $f$ be the (max.) sum of the degrees in $x_1, x_2, \ldots, x_l$ through all of the different terms, and $N = \prod_{i=1}^{k} n_i$.

If $N > n^f 2^{k+1} g^2$, then we can get in polynomial time a real-valued equation which is equivalent to (1).

Remarks. 1) This bound has to be compared with Takagi-Naito’s bound, i.e.

$$
N > n^f (k + g)^{\frac{e}{2} + \frac{(e+g)^2}{2}}
$$

2) Theorem 1 includes the improved Håstad attack as a special case by reducing the number of variables to one.

Our proof will be based on the following simple lemma.

Lemma 2. The polynomial modular equation

$$
\sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \cdots + j_l \leq e} c_{j_1, j_2, \ldots, j_l} x_1^{j_1} x_2^{j_2} \cdots x_l^{j_l} \equiv 0 \pmod{N}
$$

(2)

is equivalent to its real-valued corresponding if

$$
|c_{j_1, j_2, \ldots, j_l}| \leq \frac{N}{g n^{j_1 + j_2 + \cdots + j_l}} \quad (\forall j_1, j_2, \ldots, j_l).
$$

(3)

*By this notation, we mean that the greatest common divisor of $n_i$ and all $a_{i, j_1, \ldots, j_l}$ is equal to 1.

†One can easily show that

$$
f = \sum_{m=1}^{e} m \binom{m+l-1}{m} \quad \text{and} \quad g = \sum_{m=0}^{e} \binom{l+m-1}{m}.
$$

CG–1997/3.2
Proof. Since $x_1, x_2, \ldots, x_l < n$, we have

\[
\left| \sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \ldots + j_l \leq e} c_{j_1, j_2, \ldots, j_l} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \right| < \sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \ldots + j_l \leq e} |c_{j_1, j_2, \ldots, j_l}| n^{j_1 + j_2 + \ldots + j_l} \leq \sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \ldots + j_l \leq e} \frac{N}{g} = N.
\]

Therefore, we can simply consider Eq. (2) as a real-valued equation. \hfill \Box

Proof (Theorem 1). Let $u_j = \delta_{ij} \pmod{n_i}$, where $\delta_{ij}$ is Kronecker’s delta.

Using the Chinese remainder theorem, we obtain

\[
0 \equiv \sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \ldots + j_l \leq e} \left( \sum_{i=1}^{k} a_{i, j_1, j_2, \ldots, j_l} u_i \right) x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \equiv \sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \ldots + j_l \leq e} c_{j_1, j_2, \ldots, j_l} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \pmod{N},
\]

which is equivalent to Eq. (1).

The idea is to multiply Eq. (4) by a constant factor in order to meet the conditions of Lemma 2. Therefore, we will consider a lattice $L$ whose basis is given by

\[
\begin{align*}
\mathbf{b}_1 &= (c_0, 0, \ldots, 0, c_0, 0, \ldots, 0, \ldots, \ldots, 0, \ldots, 0, 1/2) \\
\mathbf{b}_2 &= (N, 0, 0, \ldots, 0, \ldots, 0, \ldots, 0, 0) \\
\mathbf{b}_3 &= (0, nN, 0, \ldots, 0, \ldots, 0, \ldots, 0) \\
\mathbf{b}_4 &= (0, 0, nN, \ldots, 0, \ldots, 0, \ldots, 0) \\
&\vdots
\mathbf{b}_{i+1} &= (0, 0, 0, \ldots, 0, \ldots, 0, \ldots, 0, n^{i+1} N) \\
\mathbf{b}_{g+1} &= (0, 0, 0, \ldots, 0, \ldots, 0, \ldots, 0, n^g N)
\end{align*}
\]

A vector of this lattice is of the form $\mathbf{V} = S \mathbf{b}_1^* + \sum_{i=1}^{g} s_i \mathbf{b}_{i+1}^*$. Its $i$th coordinate (apart from the last one) is given by

\[
V_i = n^{i+1} \cdots i (Sc_{j_1, \ldots, j_l} + s_i N).
\]

Suppose that we find a vector $\mathbf{V}$ such that $\|\mathbf{V}\| < N/g$, then $|V_i| < N/g$. So,

\[
\frac{|V_i|}{n^{i+1} \cdots i} = \frac{V_i}{n^{i+1} \cdots i \mod{N}} = |Sc_{j_1, \ldots, j_l} \mod{N}| < \frac{N}{g n^{i+1} \cdots i}.
\]

CG–1997/3.2
for all \( j_1, \ldots, j_l \). \( S \) would thus be an appropriate constant for our purpose.

So, all we have to do is to find a sufficiently small vector \( \tilde{V} \). As proved in [1, pp. 84-85], we can, using the LLL algorithm, find within polynomial time a vector \( \tilde{V} \) such that

\[
\|\tilde{V}\| \leq 2^{9/4} (\det L)^{1/(g+1)}.
\]

Therefore, LLL will provide us the required vector \( \tilde{V} \) if

\[
2^{9/4} \left( \frac{N^{g/n^f}}{g} \right)^{1/(g+1)} < \frac{N}{g} \iff 2^{9(g+1)/4} g^{9/n^f} < N,
\]

which is the announced condition.

To finish the proof, we must now show that the equation we obtain, namely

\[
\sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \cdots + j_l \leq \epsilon} S c_{j_1, j_2, \ldots, j_l} x_1^{j_1} x_2^{j_2} \cdots x_l^{j_l} \equiv 0 \pmod{N} \quad (5)
\]

is non-trivial.

First note that the last coefficient of \( \tilde{V} \) is equal to \( S/g \), and therefore \( |S| < N \), since \( \|\tilde{V}\| < N/g \). Note also that \( S \neq 0 \), because all nonzero vectors \( \tilde{V} \) with \( S = 0 \) are of length at least \( N \). So, \( 0 < |S| < N \), whence \( S \equiv 0 \pmod{N} \), and thus \( S \neq 0 \pmod{n_i} \) for some \( i \). Furthermore, since \( c_{j_1, j_2, \ldots, j_l} \equiv a_{i_1, i_2, \ldots, i_l} \pmod{n_i} \) and \( \gcd(a_{i_1, i_2, \ldots, i_l}, n_i) = 1 \) for at least one \( (j_1, j_2, \ldots, j_l) \), there exists at least one \( c_{j_1, j_2, \ldots, j_l} \neq 0 \pmod{n_i} \). Consequently, Eq. (5) is nontrivial and the proof is complete.

\[ \square \]

### References


\[\dagger\] The notation \( a = b \mod N \) means that \( a \) is the unique integer congruent to \( b \) modulo \( N \) such that \( -[N/2] + 1 \leq a \leq [N/2] \).