Bull. Korean Math. Soc. **53** (2016), No. 1, pp. 1–20
http://dx.doi.org/10.4134/BKMS.2016.53.1.001

ON NONLINEAR POLYNOMIAL SELECTION AND GEOMETRIC PROGRESSION (MOD N) FOR NUMBER FIELD SIEVE

Gook Hwa Cho, Namhun Koo, and Soonhak Kwon

Abstract. The general number field sieve (GNFS) is asymptotically the fastest known factoring algorithm. One of the most important steps of GNFS is to select a good polynomial pair. A standard way of polynomial selection (being used in factoring RSA challenge numbers) is to select a nonlinear polynomial for algebraic sieving and a linear polynomial for rational sieving. There is another method called a nonlinear method which selects two polynomials of the same degree greater than one. In this paper, we generalize Montgomery's method [12] using geometric progression (GP) (mod N) to construct a pair of nonlinear polynomials. We also introduce GP of length $d+k$ with $1 \leq k \leq d-1$ and show that we can construct polynomials of degree d having common root (mod N), where the number of such polynomials and the size of the coefficients can be precisely determined.

1. Introduction

The number field sieve (NFS) [6, 10] is asymptotically the fastest known factoring algorithm for given composite integer N. One of the most exciting news on this topic is the factorization of RSA-768 by the collaboration of Kleinjung and many other researchers [9] using the technique of the general number field sieve (GNFS). Almost all of the factored RSA numbers with 100 digit size or more were tackled by using NFS algorithm so far. Recently the polynomial selection step of NFS is being studied widely since a good polynomial pair greatly reduces the entire running time of NFS algorithm.

Among several polynomial selection methods for NFS being proposed so far, the base-m method is one of the most standard ones. Murphy [13] proposed an improvement of the base-m method by refining the notion of polynomial yield. Murphy's method focuses on root property, which is a measurement of the efficiency of polynomial pair having roots modulo small primes. Kleinjung [8]

Received August 27, 2013; Revised August 27, 2015.
2010 *Mathematics Subject Classification.* 11Y05, 11Y16, 11B50.
Key words and phrases. polynomial selection, number field sieve, geometric progression, LLL algorithm.

proposed an improvement of Murphy's method to nonmonic linear polynomials. Both Murphy's and Kleinjung's methods were used on factorization of many RSA challenge numbers. We call all these polynomial selection methods linear method since it selects a nonlinear polynomial for algebraic sieving and a linear polynomial for rational sieving.

A nonlinear method refers the method of choosing two nonlinear polynomials (of degree ≥ 2) having a common zero (mod N). Several researchers focus on nonlinear polynomial selection methods. Montgomery [12] showed that one can find two nonlinear polynomials of degree d and size $O(N^{1/2d})$ having common root (mod N) if and only if one can find a geometric progression (GP) (mod N) of length $2d-1$ and size $O(N^{1-1/d})$. Montgomery succeeded in finding such GP (mod N) when $d=2$ but the case $d \geq 3$ is still unresolved. The quadratic method ($d=2$) is not competitive to linear method when the integer N is over 120 digits [13]. Prest and Zimmermann [15], and also Williams [17] proposed other nonlinear polynomial selection methods using GP (mod N) of length $d+1$, however these methods produce polynomials which have larger coefficients than the optimal bound $O(N^{1/2d})$ expected from Montgomery's method.

In this paper, we propose a polynomial selection method using a GP of length $d+k$ with $1 \leq k \leq d-1$ which generalizes Montgomery's method of GP with length $2d-1$ (i.e., $k=d-1$). Natural implication of our result is that one can generate polynomials with different degrees d for all $\frac{l}{2} < d < l$ having common root (mod N) from a GP of fixed length l. We also introduce a method of finding a GP of $(d+1)$-term with size $O(N^{1-1/d})$ and show that the proposed method has more flexibility than the usual base-m method. GP with length $d+2$ and size $O(N^{1-1/d})$ is difficult to find in general but we show that such GP can be found under certain conditions. We apply our result to construct explicit cubic polynomials having common roots (mod N).

The remaining part of this paper is organized as follows. We explain the existing polynomial selection methods in Section 2. We introduce an extension of Montgomery's GP method and explain a generalized polynomial selection method given GP of arbitrary length in Section 3. We introduce new classes of GP of length $d+1$ and $d+2$ and give examples of corresponding nonlinear polynomials in Section 4. Finally we give conclusive remarks in Section 5.

2. Existing polynomial selection methods

2.1. Linear polynomial selection method

2.1.1. *Base-m method.* Let $N^{1/(d+1)} < m \leq N^{1/d}$ and let $N = \sum_{i=0}^{d} a_i m^i$ ($0 \leq a_i < m$) be the base m-expansion of N. Then

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0, \quad g(x) = x - m$$

are two polynomials having common root m (mod N). There are other improvements to reduce the size of coefficients of f with the property $f(m) \equiv 0$

(mod N) being preserved. For example, if $a_i > m/2$, then the substitution

$$a_i \leftarrow a_i - m \text{ and } a_{i+1} \leftarrow a_{i+1} + 1,$$

makes $|a_i| < m/2$ for every i. For more detail, refer [10, 13].

2.1.2. *Murphy's method.* Murphy's method [13] is an improvement of the base-m method to generate skewed polynomials having good root property using rotations and translations. For given polynomial pair $(f(x), g(x))$ with common root m (mod N), rotation by $r(x)$ refers another polynomial pair $(f(x) + r(x)g(x), g(x))$. Also translation by t refers a polynomial pair $(f(x-t), g(x-t))$ having common root $m + t$ (mod N).

The root property measures the smoothness of given polynomial, i.e., it tells how many roots the polynomial has modulo small primes. To measure the root property of a polynomial f, one defines

$$\alpha(f) = \sum_{p \le B} (1 - q_p) \frac{\log p}{p - 1}, \tag{1}$$

where B is the given bound and q_p is the number of root of $f(x) \equiv 0 \pmod{p}$. Sufficiently many zeros of f (mod p) implies that one has negative $\alpha(f)$ with larger absolute value. Similarly one can also define α value for a bivariate homogeneous polynomial $F(x, y)$ with $f(x) = F(x, 1)$. In this case, projective roots p dividing the leading coefficient a_d of f should also be considered. That is, if the leading coefficient of f has many small prime factors, then f may have a good root property. Therefore one may select m with $a_d m^d \le N < (a_d + 1)m^d$ with a_d having many small prime factors. By using the techniques of translation and rotation, one may generate skewed polynomials having good root properties. In Murphy's method, rotation by linear polynomial $r(x)$ was used. Rotation by nonlinear polynomials using the Chinese remainder theorem was proposed in [7].

2.1.3. *Kleinjung's method and improvements.* Kleinjung [8] proposed an improvement of Murphy's method to nonmonic linear g. This method first selects a positive integer a_d which has many small prime factors. Next, one chooses an integer p such that $a_d x^d \equiv N \pmod{p}$ is solvable. Now let m be a solution of $a_d x^d \equiv N \pmod{p}$ close to $\widetilde{m} = (N/a_d)^{1/d}$. Then there is an expression

$$N = a_d m^d + a_{d-1} m^{d-1} p + \cdots + a_1 m p^{d-1} + a_0 p^d,$$

with $|a_{d-1}| < d a_d \frac{m - \widetilde{m}}{p} + p$ and $|a_i| < m + p$ for $i = 0, \ldots, d-2$ (see Lemma 2.1 of [8]). Thus

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0, \quad g(x) = px - m$$

is a polynomial pair having common root $p^{-1}m$ (mod N), where a_{d-1} and a_{d-2} can be bounded in terms of a_d, p and m. Considering plenty of optimal triples (a_d, p, m), Kleinjung found polynomial pairs with nonmonic g having

better yields than that of Murphy's method. This method was used for the factorization of RSA-768 [9].

Two methods which improve Kleinjung's method are recently introduced in [2, 3]. In [3], Bai et al. focused on fast computation of α value in (1) and proposed a new method to compute α value of $f_{u,v} = f(x) + (ux + v)g(x)$ using root property of f and applying Hensel's Lemma. In [2], Bai et al. introduced a method to refine rotation and translation procedure. To get a better rotated polynomial, the authors used the LLL lattice reduction algorithm [11]. Combined with some resultant technique, they found a better polynomial pair than the previous proposed methods.

2.2. Nonlinear polynomial selection method

2.2.1. *Montgomery's method.* Montgomery [12] proposed a nonlinear method which produces two polynomials of the same degree d using a small GP (mod N). We say a sequence $\{c_i\}$ is a GP (mod N) if $c_{i+1} \equiv rc_i \pmod N$ for some fixed ratio r. If there exists a GP (mod N) of length $2d-1$ with $c_i = O(N^{1-1/d})$ written in vector notation as

$$\vec{c} = [c_0, c_1, \ldots, c_{2d-2}],$$

which is not a linear recurrence of order $d-1$ over $\mathbb{Q}$, then by looking at the two dimensional sublattice of $\mathbb{Z}^{d+1}$ which is orthogonal to $d-1$ vectors in $\mathbb{Z}^{d+1}$ spanned by

$$[c_0, c_1, \ldots, c_d], [c_1, c_2, \ldots, c_{d+1}], \ldots, [c_{d-2}, c_{d-1}, \ldots, c_{2d-2}],$$

one can construct two polynomials $f_1(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ and $f_2(x) = b_d x^d + b_{d-1}x^{d-1} + \cdots + b_0$ of degree d with common root r (mod N), where r is the geometric ratio of GP $\vec{c}$ and the coefficients of f_1 and f_2 are of $O(N^{1/2d})$.

At this moment, it is still an open problem whether one can find such GP (mod N) with length $2d-1$ and size $c_i = O(N^{1-1/d})$ for general d. However, when $d = 2$, Montgomery presented a GP (mod N) satisfying the above conditions. That is, letting p be a prime satisfying

$$\text{(i) } p < \sqrt{N}, \qquad \text{(ii) } \left(\frac{N}{p}\right) = 1.$$

Montgomery finds a solution c_1 of $x^2 \equiv N \pmod p$ with $|c_1 - \sqrt{N}| \le p/2$, and thus

$$[c_0, c_1, c_2] = [p, c_1, (c_1^2 - N)/p] \tag{2}$$

is a desired GP (mod N) with ratio $r \equiv p^{-1}c_1 \pmod N$. It seems difficult to extend the idea of Montgomery to general $d \ge 3$. A positive answer for the case $d = 3$ would imply that we may replace the sieving polynomial pair $(f(x), l(x))$ with linear $l(x)$ and $\deg f = 5$ or 6 by two cubic polynomials. For details, refer [13].

2.2.2. *The method of Prest and Zimmermann.* According to Montgomery's idea, we need a GP (mod N) with length $2d-1$ and size $O(N^{1-1/d})$ to generate two polynomials of degree d with common root (mod N) and coefficients of $O(N^{1/2d})$. In the case that we have only $(d+1)$-term of GP, we may still generate two polynomials of degree d with common root (mod N). Williams [17] showed that a GP of length 4 (i.e., $d=3$) of size $O(N^{2/3})$ gives two cubic polynomials having common root (mod N) with coefficients $O(N^{2/9})$. Therefore the resultant of two polynomials is $O(N^{4/3})$, while $O(N)$ is the optimal resultant size expected from two polynomials with coefficients $O(N^{1/2d})$. Prest and Zimmermann [15] considered the case of arbitrary degree to generate skewed polynomials. Choosing a GP of the form $[1, m, \ldots, m^{d-1}, m^d - N]$ with m near $N^{1/d}$, and applying LLL algorithm [11] on the lattice spanned by the column vectors of the following matrix

$$\begin{pmatrix} m & \cdots & m^{d-1} & m^d - N \\ s & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & s^{d-1} & 0 \\ 0 & \cdots & 0 & s^d \end{pmatrix},$$

where s is the skewness parameter, they get two short vectors of the form

$$\begin{bmatrix} -a_0 \\ a_1 s \\ \vdots \\ a_d s^d \end{bmatrix}.$$

Thus the polynomials $a_0 + \cdots + a_d x^d$ have m as a common root (mod N). They showed that, by selecting $s = O(N^{\frac{2}{d(d^2-d+2)}})$, the skewed polynomials have medium coefficients of size $O(N^{\frac{d^2-2d+2}{d^3-d^2+2d}})$ and resultant of size $O(N^{\frac{2(d^2-2d+2)}{d^2-d+2}})$. When $d=3$, this method gives two cubic polynomials whose resultant is of $O(N^{5/4})$ and medium coefficients of $O(N^{5/24})$.

2.2.3. *Coxon's analysis of Montgomery's method.* In [5], Coxon focused on two subjects from Montgomery's method. Coxon considered the idea of finding a GP from a given NFS polynomial pair. For a given polynomial pair f_1, f_2 with $2 \le \deg f_2 \le t \le \deg f_1$, define the matrix of size $(\deg f_1 + t - 2) \times (\deg f_1 + t - 1)$ by

$$S_t(f_1, f_2) = \begin{pmatrix} \operatorname{coeff}(x^{t-2} f_1) \\ \vdots \\ \operatorname{coeff}(f_1) \\ \operatorname{coeff}(x^{\deg f_1 - 2} f_2) \\ \vdots \\ \operatorname{coeff}(f_2) \end{pmatrix},$$

where $\text{coeff}\left(\sum_{i=0}^{\deg f_1+t-2} a_i x^i\right) = (a^{\deg f_1+t-2}, \ldots, a_0)$.

By defining $M_{t,i}$ be $(-1)^{i+1}$ times the determinant of the submatrix of $S_t(f_1, f_2)$ obtained by removing its ith column, and letting

$$c_t(f_1, f_2) = (M_{t,1}(f_1, f_2), \ldots, M_{t,\deg f_1+t-1}(f_1, f_2)),$$

Coxon showed that $c_t(f_1, f_2)$ is a GP which can be used to find NFS polynomial pair for each $\deg f_2 \leq t \leq \deg f_1$. Also, for a given polynomial pair f_1 and f_2, Coxon obtained an upper bound and a lower bound for the skewed 2-norm of f_1 and f_2. For detail results and proofs, refer Section 5 of [5].

3. Polynomial selections from GP of length $d + k$

To find a pair of nonlinear sieving polynomials, Montgomery [12] considers GP (mod N) $\vec{c} = [c_0, c_1, \ldots, c_{2d-2}]$ with length $2d-1$ and size $c_i = O(N^{1-1/d})$. On the other hand, Prest and Zimmermann [15] consider $\vec{c} = [c_0, c_1, \ldots, c_d]$ with length $d+1$ and size $c_i = O(N^{1-1/d})$. Finding GP (mod N) with length $d+1$ and size $c_i = O(N^{1-1/d})$ is relatively easy because, letting $c_0 = \lfloor N^{1/d} \rfloor + j$ for small j and $c_i \equiv c_0^i \pmod N$, one gets $c_i = O(N^{1-1/d})$. However it is not clear how one can find a GP (mod N) with bounded size for general length $d + k$

$$\vec{c} = [c_0, c_1, \ldots, c_{d+k-1}].$$

The most desirable case is $k = d-1$ so that we have a GP of length $2d-1$ and can find two independent polynomials of degree d having common root (mod N).

It should be mentioned that finding GP even in the cases $k = 2, 3, \ldots, d-2$ satisfying suitable size property is supposed to be a difficult problem. Moreover, for given GP of length $d + k$, we may find more than two polynomials having common roots (mod N), and the size of the coefficients of such polynomials are determined by the size of $\vec{c}$. Our aim is to generalize the idea of Montgomery to the case of GP $\vec{c}$ (mod N) of arbitrary length $d + k$ and also to provide an unified approach for the polynomials of degree d having common roots (mod N) arising from a GP $\vec{c}$ of variable length such as $d + 1$ [15, 17] and $2d - 1$ [12]. Moreover we will clarify the relations between the polynomials of different degree d having common root (mod N) for given GP $\vec{c}$ of fixed length. As an example, we will show that, for given 5-term GP of size $O(N^{2/3})$, we may generate 2 cubic polynomials and 4 polynomials of degree 4, all having coefficients of size $O(N^{1/6})$ and the same common root (mod N). To summarize the raised questions;

- *How many independent polynomials we may generate for given GP of fixed length*?
- *What are the possible degrees of such polynomials*?

• *How the size of the coefficients of such polynomials is related to the size of the given GP*?

We will answer all the above questions in the following theorem below. For given polynomial $f(x) = \sum a_i x^i$, let us define the norm of f as $||f|| = \sqrt{\sum a_i^2}$.

Theorem 1. *Let d and k be integers with $d \geq 2$ and $1 \leq k \leq d-1$. Suppose that $\vec{c} = [c_0, c_1, \ldots, c_{d+k-1}]$ is a GP (mod N) with ratio r and length $d+k$ such that the k vectors $[c_0, \ldots, c_d]$, $[c_1, \ldots, c_{d+1}], \ldots, [c_{k-1}, \ldots, c_{d+k-1}] \in \mathbb{Z}^{d+1}$ are linearly independent over $\mathbb{Q}$. Then we may generate $d-k+1$ polynomials f_i of degree at most d having common root r (mod N) satisfying*

$$||f_1|| \cdot ||f_2|| \cdots ||f_{d-k+1}|| = O\left(\frac{||\vec{c}||^k}{N^{k-1}}\right). \tag{3}$$

Proof. Let Λ be the lattice in $\mathbb{Z}^{d+1}$ spanned by the following k independent vectors

$$\vec{v}_0 = [c_0, \ldots, c_d], \ \ \vec{v}_1 = [c_1, \ldots, c_{d+1}], \ldots, \ \ \vec{v}_{k-1} = [c_{k-1}, \ldots, c_{d+k-1}], \tag{4}$$

obtained from $d+1$ consecutive terms of $\vec{c}$. Define Ω to be the lattice in $\mathbb{Z}^{d+k+1}$ spanned by the column vectors of the following $(d+k+1)\times(d+1)$ matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ Kc_0 & Kc_1 & \cdots & Kc_d \\ Kc_1 & Kc_2 & \cdots & Kc_{d+1} \\ \vdots & \vdots & \ddots & \vdots \\ Kc_{k-1} & Kc_k & \cdots & Kc_{d+k-1} \end{pmatrix}, \tag{5}$$

where K is a constant. Then Theorem 4 of [14] says that, if $\{\vec{x}_1, \ldots, \vec{x}_{d+1}\}$ is an LLL-reduced basis of Ω and if one chooses K sufficiently large, then $\{\vec{x}'_1, \ldots, \vec{x}'_{d-k+1}\}$ is an LLL-reduced basis for $\Lambda^\perp$, where $\vec{x}'_i \in \mathbb{Z}^{d+1}$ is the vector obtained by taking the first $(d+1)$-terms of $\vec{x}_i$ and $\Lambda^\perp$ is the orthogonal lattice of Λ. In [14], one may choose $K > 2^{\frac{d}{2}+\frac{(d+1-k)(d-k)}{4}}\mathrm{vol}(\overline{\Lambda})$, where $\overline{\Lambda} = \mathrm{span}_{\mathbb{Q}}(\Lambda) \cap \mathbb{Z}^{d+1}$ is the complete lattice of Λ. Since one has $2^{d+(d-k)^2}\mathrm{vol}(\Lambda) \geq 2^{\frac{d}{2}+\frac{(d+1-k)(d-k)}{4}}\mathrm{vol}(\overline{\Lambda})$, one can also choose $K > 2^{d+(d-k)^2}\mathrm{vol}(\Lambda)$.

Therefore $\vec{x}'_i = (a_0, a_1, \ldots, a_d) \in \Lambda^\perp$ satisfies

$$0 = a_0c_0 + a_1c_1 + \cdots + a_dc_d \equiv a_0 + a_1r + a_2r^2 + \cdots a_dr^d \pmod{N},$$

where $r \equiv c_0^{-1}c_1 \pmod{N}$, which implies that $\vec{x}'_i$ corresponds to a polynomial $f_i(x) = a_0 + a_1x + \cdots + a_dx^d$ with degree at most d. Hence we may consider $\{f_1, f_2, \ldots, f_{d-k+1}\}$ is a basis for $\Lambda^\perp$ over $\mathbb{Q}$ of dimension $d+1-k$. A standard

result of LLL-reduced basis says that

$$\mathrm{vol}(\Lambda^{\perp}) \leq \prod_{i=1}^{d-k+1} ||f_i|| \leq 2^{\frac{(d-k+1)(d-k)}{4}} \mathrm{vol}(\Lambda^{\perp}),$$

where $\mathrm{vol}(\Lambda^{\perp}) = \mathrm{vol}(\overline{\Lambda})$. Therefore, to estimate the size of f_i, we need to estimate the volume of $\Lambda^{\perp}$. Observe that $\vec{y} \in \mathbb{Z}^{d+1}$ is orthogonal to the vectors $\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{k-1}$ defined in (4) if and only if it is orthogonal to the lattice Λ' spanned by

$$\vec{v}_0, \frac{\vec{v}_1 - r\vec{v}_0}{N}, \frac{\vec{v}_2 - r\vec{v}_1}{N}, \ldots, \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N},$$

where r is the geometric ratio of GP $\vec{c}$. Since

$$\mathrm{vol}(\Lambda^{\perp}) = \mathrm{vol}((\Lambda')^{\perp}) = \mathrm{vol}(\overline{\Lambda'}) \leq \mathrm{vol}(\Lambda'),$$

to estimate the volume of $\Lambda^{\perp}$, we need to compute $\mathrm{vol}(\Lambda') = \sqrt{\det(A^T A)}$ where A is the $k \times k$ matrix with each column written as

$$\vec{v}_0, \frac{\vec{v}_1 - r\vec{v}_0}{N}, \frac{\vec{v}_2 - r\vec{v}_1}{N}, \ldots, \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N}.$$

Now

$$\begin{aligned}
&\det(A^T A) \\
&= \left| \begin{pmatrix} \vec{v}_0 \\ \frac{\vec{v}_1 - r\vec{v}_0}{N} \\ \vdots \\ \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \end{pmatrix} \begin{pmatrix} \vec{v}_0 & \frac{\vec{v}_1 - r\vec{v}_0}{N} & \cdots & \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \end{pmatrix} \right| \\
&= \begin{vmatrix} \vec{v}_0 \cdot \vec{v}_0 & \vec{v}_0 \cdot \frac{\vec{v}_1 - r\vec{v}_0}{N} & \cdots & \vec{v}_0 \cdot \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \\ \frac{\vec{v}_1 - r\vec{v}_0}{N} \cdot \vec{v}_0 & \frac{\vec{v}_1 - r\vec{v}_0}{N} \cdot \frac{\vec{v}_1 - r\vec{v}_0}{N} & \cdots & \frac{\vec{v}_1 - r\vec{v}_0}{N} \cdot \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \cdot \vec{v}_0 & \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \cdot \frac{\vec{v}_1 - r\vec{v}_0}{N} & \cdots & \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \cdot \frac{\vec{v}_{k-1} - r\vec{v}_{k-2}}{N} \end{vmatrix} \\
&= \frac{1}{N^{2(k-1)}} \begin{vmatrix} \vec{v}_0 \cdot \vec{v}_0 & \vec{v}_0 \cdot (\vec{v}_1 - r\vec{v}_0) & \cdots & \vec{v}_0 \cdot (\vec{v}_{k-1} - r\vec{v}_{k-2}) \\ (\vec{v}_1 - r\vec{v}_0) \cdot \vec{v}_0 & (\vec{v}_1 - r\vec{v}_0) \cdot (\vec{v}_1 - r\vec{v}_0) & \cdots & (\vec{v}_1 - r\vec{v}_0) \cdot (\vec{v}_{k-1} - r\vec{v}_{k-2}) \\ \vdots & \vdots & \ddots & \vdots \\ (\vec{v}_{k-1} - r\vec{v}_{k-2}) \cdot \vec{v}_0 & (\vec{v}_{k-1} - r\vec{v}_{k-2}) \cdot (\vec{v}_1 - r\vec{v}_0) & \cdots & (\vec{v}_{k-1} - r\vec{v}_{k-2}) \cdot (\vec{v}_{k-1} - r\vec{v}_{k-2}) \end{vmatrix} \\
&= \frac{1}{N^{2(k-1)}} \det(B^T B),
\end{aligned}$$

where B is the matrix with each column vector written as $\vec{v}_0$, $\vec{v}_1 - r\vec{v}_0$, $\vec{v}_2 - r\vec{v}_1, \ldots, \vec{v}_{k-1} - r\vec{v}_{k-2}$. Since the base change matrix between the following two bases for $\mathbb{Q}^{d+1}$,

$$\begin{aligned}
&\{\vec{v}_0, \quad \vec{v}_1, \quad \vec{v}_2, \quad \ldots, \quad \vec{v}_{k-1}\}, \\
&\{\vec{v}_0, \quad \vec{v}_1 - r\vec{v}_0, \quad \vec{v}_2 - r\vec{v}_1, \quad \ldots, \quad \vec{v}_{k-1} - r\vec{v}_{k-2}\},
\end{aligned}$$

is triangular and having 1 in all diagonal entries (in particular unimodular), they span the same lattice and thus we get $\det(B^TB) = \det((\vec{v}_i \cdot \vec{v}_j)) = O(||\vec{c}||^{2k})$. Consequently one gets

$$\mathrm{vol}(\Lambda^{\perp}) \leq \mathrm{vol}(\Lambda') = O\left(\frac{||\vec{c}||^k}{N^{k-1}}\right)$$

which completes the proof. □

Corollary 1. *With the same conditions in Theorem 1, suppose that k vectors $[c_0, c_1, \ldots, c_{d-1}]$, $[c_1, c_2, \ldots, c_d], \ldots, [c_{k-1}, c_k, \ldots, c_{k+d-2}]$ of consecutive d terms are linearly independent over $\mathbb{Q}$. Then we get at least one polynomial of degree d having r as a zero* (mod N). *Moreover if all f_i are*

$$O\left(\left(\frac{||\vec{c}||^k}{N^{k-1}}\right)^{1/(d-k+1)}\right),$$

then we may choose all such polynomials having degree d.

Proof. On the contrary, assume that all f_i found in Theorem 1 have degree $< d$. This happens when the basis vectors $\vec{x}'_1, \ldots, \vec{x}'_{d-k+1}$ for $\Lambda^{\perp}$ have last coordinate 0 (i.e., $\vec{x}'_i = (a_0, a_1, \ldots, a_{d-1}, 0)$). Then we may view $\{\vec{x}'_1, \ldots, \vec{x}'_{d-k+1}\} \subset \mathbb{Z}^d$ which spans $(d-k+1)$-dimensional orthogonal subspace to k independent vectors $[c_i, c_{i+1}, \ldots, c_{i+d-1}]$ $(0 \leq i \leq k-1)$ in $\mathbb{Z}^d$, which is absurd. For the second assertion, let $f \in \{f_1, f_2, \ldots, f_{d-k+1}\}$ be a polynomial of degree d. Then for any f_i with deg $f_i < d$, we may replace f_i by $f_i + f$ so that the resulting polynomial has common root r (mod N) and the coefficients are of $O\left(\left(\frac{||\vec{c}||^k}{N^{k-1}}\right)^{1/(d-k+1)}\right)$. □

One can also think of the converse of Theorem 1 and it can be phrased as follows.

Theorem 2. *Suppose $1 \leq k \leq d-1$ and $j = \lceil \frac{d-1}{k} \rceil + 1$. Assume that there exist degree d polynomials $g_1(x), \ldots, g_j(x) \in \mathbb{Z}[x]$ having common root r* (mod N) *such that $g_1, \ldots, g_j$ are linearly independent over $\mathbb{Q}$. Then one can find GP $\vec{c} = [c_0, \ldots, c_{d+k-1}]$* (mod N) *of length $d+k$ and $||\vec{c}|| = O(||g||^{d+k-1})$ where $||g|| = \max||g_i||$.*

Proof. The condition $j = \lceil \frac{d-1}{k} \rceil + 1$ implies $(j-1)k < d+k-1 \leq jk$. One may consider $(2d+2k-1) \times (d+k)$ matrix

$$\mathcal{M} = \begin{pmatrix} I_{d+k} \\ KG_1 \\ \vdots \\ KG_{j-1} \\ KG_j \end{pmatrix}, \tag{6}$$

where I_{d+k} is the identity matrix of dimension $d+k$ and $KG_i (1 \le i \le j-1)$ is $k \times (d+k)$ submatrix spanned by the k row vectors in $\mathbb{Z}^{d+k}$

$$[\overbrace{Kg_i}^{d+1}, \overbrace{0, \ldots, 0}^{k-1}], [0, \overbrace{Kg_i}^{d+1}, \overbrace{0, \ldots, 0}^{k-2}], \ldots, [\overbrace{0, \ldots, 0}^{k-1}, \overbrace{Kg_i}^{d+1}].$$

The submatrix KG_j is defined similarly but the number of cyclic shifts (i.e., the number of rows) is $d+k-1-(j-1)k$. Now as in the case of the matrix in (5), one may think of LLL reduced basis of $d+k$ column vectors of $\mathcal{M}$. Theorem 4 in [14] again says that, if K is sufficiently large, we have one dimensional orthogonal lattice $\vec{c} = [c_0, c_1, \ldots, c_{d+k-1}] \subset \mathbb{Z}^{d+k}$ to the lattice of dimension $d+k-1$ spanned by the row vectors of $KG_1, \ldots, KG_j$. Since $[1, r, r^2, \ldots, r^{d+k-1}]$ is also orthogonal to all the row vectors of $KG_1, \ldots, KG_j \pmod N$, one finds that $\vec{c}$ and $[1, r, r^2, \ldots, r^{d+k-1}]$ spans the same space (mod N), and therefore the ratio of $\vec{c} \pmod N$ is r. Finally the volume of the lattice $\vec{c}$ is bounded by the volume of the lattice spanned by the $d+k-1$ row vectors of $KG_1, \ldots, KG_j$ and is of $O(||g||^{d+k-1})$. □

Remark 1. From Theorems 1 and 2, it is natural to expect $j \le d-k+1$. Indeed, if $j > d-k+1$, then from $d-k+2 \le j < \frac{d+2k-1}{k}$, we get $(k-1)d < k^2-1 = (k-1)(k+1)$ and thus $d < k+1$ which is a contradiction.

The following corollary shows that, for given GP of fixed length l, one can obtain several polynomials with similar size having common root (mod N) for various degrees d with $\frac{l}{2} < d < l$, which implies the size of the coefficients depends on the length of GP not on the degree.

Corollary 2. *Let $\vec{c}$ be a GP* (mod N) *of l-term of size $O(N^{\epsilon\frac{l-1}{l+1}})$ with $d < l < 2d$ and $0 < \epsilon < \frac{l+1}{l-1}$. Then we may generate $2d-l+1$ polynomials f_i with degree at most d such that*

$$\prod_{i=1}^{2d-l+1} ||f_i|| = O(N^{\epsilon\frac{2d-l+1}{l+1}} \cdot N^{(\epsilon-1)(l-d-1)}).$$

Proof. From Theorem 1, by letting $l = d+k$,

$$\begin{aligned} ||f_1|| \cdot ||f_2|| \cdots ||f_{2d-l+1}|| &= O\left(\frac{||\vec{c}||^{l-d}}{N^{l-d-1}}\right) = O\left(\frac{N^{\epsilon\frac{(l-1)}{l+1}(l-d)}}{N^{\epsilon(l-d-1)}} \cdot \frac{N^{\epsilon(l-d-1)}}{N^{l-d-1}}\right) \\ &= O\left(N^{\epsilon\frac{(l-d)(l-1)}{l+1} - \epsilon(l-d-1)} \cdot N^{(\epsilon-1)(l-d-1)}\right) \\ &= O\left(N^{\epsilon\frac{2d-l+1}{l+1}} \cdot N^{(\epsilon-1)(l-d-1)}\right). \end{aligned}$$

□

Remark 2. Letting $\epsilon = 1$, one has

$$\prod_{i=1}^{2d-l+1} ||f_i|| = O(N^{\frac{2d-l+1}{l+1}}).$$

Moreover, if all f_i have roughly the same size, we get $||f_i|| = O(N^{\frac{1}{l+1}})$. For example, if $l = 2d-1$, we get two polynomials of degree at most d of size $O(N^{\frac{1}{2d}})$ as expected in [12, 13]. The condition $||f_i|| = O(N^{\frac{1}{l+1}})$ implies that the size of f_i does not depend on the degree $\frac{l}{2} < d < l$ for fixed l. For example, if we have a 5-term GP of $O(N^{2/3})$, then we may generate 2 polynomials of degree 3 for $(d,k) = (3,2)$, and also 4 polynomials of degree 4 for $(d,k) = (4,1)$, where all the coefficients are of $O(N^{1/6})$.

Corollary 3. *With the same conditions in Theorem 1, suppose that $r^{2d+2}-1$ is relatively prime to N. Let $h(x) \in \mathbb{Z}[x]$ be a polynomial of degree at most d such that $h(r) \equiv 0 \pmod N$. Then there exist integers $s_1, s_2, \ldots, s_{d-k+1}$ such that $h(x) \equiv \sum_{i=1}^{d-k+1} s_i f_i(x) \pmod N$.*

Proof. For any polynomial $f(x) = \sum_{i=0}^{d} a_i x^i$ of degree at most d, define a vector $\vec{f} = [a_0, \ldots, a_d]$ in $\mathbb{Z}^{d+1}$. Since $\mathbb{Q}^{d+1}$ is spanned by the basis vectors, $\vec{f_1}, \vec{f_2}, \ldots, \vec{f}_{d-k+1}, \vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{k-1}$ where $\vec{v}_i$ are defined in (4), we have

$$\vec{h} = \sum_{i=1}^{d-k+1} s_i \vec{f_i} + \sum_{j=0}^{k-1} t_j \vec{v}_j$$

for some s_i, t_j in $\mathbb{Q}$. Now letting $\vec{r} = [1, r, \ldots, r^d]$ and noticing the ratio of the GP $\vec{c} = [c_0, \ldots, c_{d+k-1}] \pmod N$ is r, we get

$$\vec{v_j} = [c_j, c_{j+1}, \ldots, c_{d+j}] \equiv c_j \vec{r} \pmod N.$$

Therefore

$$\begin{aligned} 0 \equiv h(r) &\equiv \vec{h} \cdot \vec{r} \\ &\equiv \sum s_i f_i(r) + \sum t_j (\vec{v}_j \cdot \vec{r}) \equiv \sum t_j c_j (\vec{r} \cdot \vec{r}) \\ &\equiv \sum t_j c_j (1 + r^2 + r^4 + \cdots + r^{2d}) \equiv \frac{r^{2d+2}-1}{r^2-1} \sum t_j c_j \pmod N. \end{aligned}$$

Since $r^{2d+2} - 1$ is relatively prime to N, we get $\sum_{j=0}^{k-1} t_j c_j \equiv 0 \pmod N$. Consequently

$$\begin{aligned} \vec{h} &= \sum_{i=1}^{d-k+1} s_i \vec{f_i} + \sum_{j=0}^{k-1} t_j \vec{v}_j \equiv \sum_{i=1}^{d-k+1} s_i \vec{f_i} + \sum_{j=0}^{k-1} t_j c_j \vec{r} \\ &\equiv \sum_{i=1}^{d-k+1} s_i \vec{f_i} + \vec{r}(\sum_{j=0}^{k-1} t_j c_j) \equiv \sum_{i=1}^{d-k+1} s_i \vec{f_i} \pmod N. \end{aligned}$$

□

4. Constructing GP (mod N)

4.1. GP (mod N) with length $d+1$

As is mentioned in Section 2.1.1, one finds such GP by the base-m method with $m = \lfloor N^{1/d} \rfloor + j$ for small j so that the base-m expansion of N, $N =$

$\sum_{i=0}^{d} a_i m^i$, gives a polynomial $f(x) = \sum_{i=0}^{d} a_i x^i$ with $f(m) \equiv 0 \pmod N$ and coefficients $a_i = O(N^{\frac{1}{d}})$. On the other hand, Theorem 1 says that we can find d such polynomials of degree d with coefficients $O(N^{\frac{d-1}{d^2}})$ having m as a common zero (mod N). It should be mentioned that d polynomials in Theorem 1 are obtained via LLL algorithm [11] not from the base-m method. Also since there are d polynomials, we have much freedom in manipulating those polynomials via rotations and translations to find optimal polynomials having good root property. By extending the idea of GP in (2) of Montgomery, we may generate GP (mod N) with length $d+1$ as follows.

Proposition 1. *Suppose p is a prime such that*

$$\text{(i) } p < N^{1/d}, \qquad \text{(ii) } x^d \equiv N \pmod p \text{ is solvable.}$$

Let r be a solution of $x^d \equiv N \pmod p$ with $|r - N^{1/d}| \le \frac{p}{2}$. Then

$$\vec{c} = [c_0, c_1, c_2, \dots, c_d] = \left[p^{d-1}, p^{d-2}r, \dots, r^{d-1}, \frac{r^d - N}{p}\right] \tag{7}$$

is a $(d+1)$-term GP (mod N) of size $O(N^{1-1/d})$ with geometric ratio rp^{-1} (mod N).

Remark 3. Heuristic argument tells that, for randomly chosen prime p with $p \equiv 1 \pmod d$, the probability that N is a d-th power residue (mod p) is $\frac{1}{d}$. Therefore we may generate plenty of p and r satisfying the conditions of the Proposition 1.

Remark 4. Letting $p = 1$, we get $\vec{c} = [1, r, r^2, \dots, r^d - N]$ which is exactly the base-m method. Thus the proposed method is a generalization of the base-m method and has more flexibility. Note that p in the proposition need not necessarily be a prime as long as the solutions of $x^d \equiv N \pmod p$ are efficiently computable. One possible direction of this idea is to think of the solutions of $x^d \equiv N \pmod{\prod p_i}$ using Chinese Remainder Theorem from the solutions of $x^d \equiv N \pmod{p_i}$.

Remark 5. Another generalization of Proposition 1 is using kN in place of N, where k is small and a product of small primes. Therefore if r is a solution of $x^d \equiv kN \pmod p$, then the GP

$$\vec{c} = \left[p^{d-1}, p^{d-2}r, \dots, r^{d-1}, \frac{r^d - kN}{p}\right] \tag{8}$$

produces polynomials $f_i(x)$ such that $f_i(p^{-1}r) \equiv 0 \pmod{kN}$, which implies that $f_i(x) \equiv 0 \pmod q$ has a solution for all primes q dividing k. In this way, one may find polynomials with good root properties. (See Example 2.)

Applying LLL algorithm on the $(d+2) \times (d+1)$ matrix in (5) with the GP in (7) or (8) gives d polynomials of degree d with coefficients size $O(N^{(d-1)/d^2})$ under the assumption of Corollary 1. All generated polynomials have $p^{-1}r$ as a

common root (mod N) and the linear polynomial $px-r$ also has $p^{-1}r \pmod N$ as a root. We can also extend our idea to select skewed polynomials following the method in [15]. For given skewness s and GP $\vec{c}$, applying LLL algorithm on the column vectors of

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & s & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & s^d \\ Kc_0 & Kc_1 & \cdots & Kc_d \end{pmatrix} \tag{9}$$

gives d skewed polynomials.

Example 1. Let

$$\begin{aligned} N &= C59 \\ &= 71641520761751435455133616475667090434063332228247871795429 \end{aligned}$$

and $d = 3$ as in [15]. We choose prime $p = 41532518328905334671$ near $N^{1/3}$. Then $x^3 - N \equiv 0 \pmod p$ has solution $r = 25417166874734771107$. Running LLL algorithm with the GP $\vec{c} = [p^2, pr, r^2, \frac{r^3-N}{p}]$ gives 3 polynomials of degree 3 having common root $p^{-1}r \pmod N$:

$$\begin{aligned} f_1(x) &= 2294658610753x^3 + 9597429436365x^2 - 1723025618025x \\ &\quad - 771270274282, \\ f_2(x) &= 11446806849070x^3 - 244248671393x^2 + 4093360192946x \\ &\quad + 6409599094515, \\ f_3(x) &= 5816639714842x^3 + 718509494635x^2 - 13763827243329x \\ &\quad + 12637580760070. \end{aligned}$$

Since $l(x) = px - r$ has the common root $p^{-1}r \pmod N$ also, using Corollary 3, we may express $l(x)$ as a linear combination

$$l(x) \equiv -232236f_1(x) + 1304425f_2(x) + 2658649f_3(x) \pmod N.$$

Example 2. Let N, d be the same as in Example 1. We choose prime $p = 15712338827$ near $(210N)^{1/6}$. Then $x^3 \equiv 210N \pmod p$ has solution $r = 246864077935052193511$. Let $s = 5000 \approx N^{\frac{1}{12}}$ be the skewness parameter. Running LLL algorithm on the matrix (9) with $\vec{c} = [p^2, pr, r^2, \frac{r^3-210N}{p}]$ gives 3 skewed polynomials of degree 3 having common root $p^{-1}r \pmod N$:

$$\begin{aligned} f_1(x) &= 115x^3 + 43124977x^2 + 1893281131859157x \\ &\quad + 4083363045384283521, \\ f_2(x) &= 100x^3 + 37499980x^2 + 1646332102153129x \\ &\quad - 7182470305537674917, \\ f_3(x) &= 2998982x^3 + 1127760117969x^2 + 374107139392334x \end{aligned}$$

$$- 2209056969433053257.$$

The above polynomials have $\alpha(f_1) = -1.50$, $\alpha(f_2) = -1.96$, $\alpha(f_3) = -0.09$, of which two polynomials f_1 and f_2 have better α-values than $\alpha(f) = -0.41$, $\alpha(g) = -0.65$ in page 9 of [15], where

$$f(x) = 42044x^3 - 58243x^2 + 216589713956652x + 309824665860518028,$$
$$g(x) = 189599x^3 - 262649x^2 - 11115144906243x - 3123165185295940301.$$

Moreover our resultant $\mathrm{Res}(f_1, f_2) = -26250N = N^{1.075}$ is just 64-digits while $\mathrm{Res}(f, g) = N^{1.22}$ in [15] is of 73 digits. Our resultant is 9-digits less than [15] and only 5-digits more than N.

Since we may try many possible candidates of p, r and k satisfying $r^d \equiv kN \pmod{p}$, it is a more flexible method than that of the base-m method, so it is expected to get polynomials of better yields when combined with other techniques. In our implementations, we could generate plenty of examples of polynomial pairs with resultant of 65,66-digit range.

Example 3. Let N=RSA-768 [9, 16], a 232-digit integer. When we apply the method of [15], we could not get a pair of polynomials having resultant of size less than 289-digits in reasonable amount of time. However, using the GP in (7), one very often finds polynomial pairs having resultant in 282,283 digit range. For example, letting $p = 32733705462716307256112435063084197039 3$ and $r = 10714954733198634148690454723380273838963973618831054709981043058017 1279354053$ with $s = 4 \times 10^{18}$, LLL algorithm produces

$$\begin{aligned} f_1(x) = {} & 178655088759073666x^3 \\ & + 969692933834622148120387568720241589 2x^2 \\ & + 3252861381469571959984877544904580973969779093081174675563x \\ & + 158775985060009566775100511324375720183149609994785843081132012976428812737 3, \end{aligned}$$

$$\begin{aligned} f_2(x) = {} & 89327544379536833x^3 \\ & + 484846466917311074060193784360120794 6x^2 \\ & + 162643069073478598015610729976587202326545172185600832297 8x \\ & - 527808937406931229095767710602794905939041200441813443344995552252034956133 40, \end{aligned}$$

where the resultant of the two polynomials is of 282-digits.

To summarize, even if we cannot improve the asymptotic complexity of Prest and Zimermann, we have more diverse output polynomials by using the GP in (7) or in (8).

4.2. GP (mod N) with length $d+2$

We introduce a form of $(d+2)$-term GP (mod N) of size $O(N^{1-1/d})$ which improves a GP introduced in Proposition 1.

Proposition 2. *With the same conditions in Proposition 1, assume further $N^{1/d} = O(p)$ and suppose that*

$$dr^{d-1}x \equiv -\frac{r^d - N}{p} \pmod{p} \tag{10}$$

has a solution t with $t = O(1)$. Then we can find a GP (mod N) *with length $d+2$ and size $O(N^{1-1/d})$.*

Proof. Write $r^* = r + tp$ where t is a solution of (10). By Hensel's Lemma, r^* is a solution of $x^d \equiv N \pmod{p^2}$ with $|r^* - N^{1/d}| = O(p)$. Therefore the first $d+1$ terms of the following GP

$$\begin{aligned} \vec{c^*} &= [c_0^*, c_1^*, \ldots, c_{d-1}^*, c_d^*, c_{d+1}^*] \\ &= \left[p^{d-1}, p^{d-2}r^*, \ldots, r^{*d-1}, \frac{r^{*d} - N}{p}, \frac{r^*(r^{*d} - N)}{p^2}\right], \end{aligned} \tag{11}$$

are of $O(N^{1-1/d})$, i.e., $c_0^*, c_1^*, \ldots, c_d^* = O(N^{1-1/d})$. Also the assumption $N^{1/d} = O(p)$ implies $r = O(p)$. Therefore $\frac{r^*}{p} = \frac{r}{p} + t = O(1)$ and we get $c_{d+1} = c_d^* \cdot \frac{r^*}{p} = O(N^{1-1/d})$. □

Remark 6. An equivalent condition of Proposition 2 is that there exists a prime p with $p \approx N^{1/d}$ such that $x^d \equiv N \pmod{p^2}$ has a solution r^* with $r^* \approx p$.

Next corollary shows that the GP introduced above gives polynomials with special properties.

Corollary 4. *Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial of degree d obtained by applying $(d+2)$-term GP in* (11)*. Then we get $a_{d-1} = 0$.*

Proof. From the orthogonality condition

$$[a_0, a_1, \ldots, a_d] \ \perp \ [c_0^*, \ldots, c_{d-1}^*, c_d^*], [c_1^*, \ldots, c_d^*, c_{d+1}^*],$$

we obtain two equations

$$\begin{aligned} c_0^* a_0 + \cdots + c_{d-1}^* a_{d-1} + c_d^* a_d &= 0, \\ c_1^* a_0 + \cdots + c_d^* a_{d-1} + c_{d+1}^* a_d &= 0. \end{aligned}$$

By cancelling a_d from the above two equations,

$$\begin{aligned} 0 &= (c_1^* c_d^* - c_0^* c_{d+1}^*)a_0 + \cdots + (c_{d-1}^* c_d^* - c_{d-2}^* c_{d+1}^*)a_{d-2} + (c_d^{*2} - c_{d+1}^* c_{d-1}^*)a_{d-1} \\ &= (c_d^{*2} - c_{d+1}^* c_{d-1}^*)a_{d-1} + \sum_{i=0}^{d-2}(c_{i+1}^* c_d^* - c_i^* c_{d+1}^*)a_i \\ &= (c_d^{*2} - c_{d+1}^* c_{d-1}^*)a_{d-1} + \sum_{i=0}^{d-2}(c_{i+1}^* c_d^* - c_i^* \frac{r^*}{p} c_d^*)a_i = (c_d^{*2} - c_{d+1}^* c_{d-1}^*)a_{d-1} \end{aligned}$$

Since $c^*_{d+1}c^*_{d-1} - c^{*2}_d \neq 0$, we have $a_{d-1} = 0$. □

Therefore if we can find a GP introduced in (11), then we may generate polynomials whose second highest coefficient is zero. It may give some possible advantage in NFS algorithms. In particular, when $d = 3$, we can generate 2 cubic polynomials of coefficients size $O(N^{1/6})$ with coefficient of x^2 zero. Unfortunately, for large N, it is not easy to find such p and r.

Example 4. Let

$$\begin{aligned} N = {} & 42304196922091749899425810572641313100785712232032845201868564718324398920706756285412652631922499612541193795676176096098273078826778123746044315 91, \\ p = {} & 867803115298087219317219920374307471978389794888 43. \end{aligned}$$

Then we find that

$$r = 29603635990292704794807646350860921932096349571925$$

is a root of $x^3 \equiv N \pmod{p^2}$. We get a 5-term GP (mod N) as $\vec{c} = [p^2, pr, r^2, \frac{r^3-N}{p}, \frac{r(r^3-N)}{p^2}]$. With this GP as an input, running LLL algorithm on the lattice in (5) produces 2 cubic polynomials

$$\begin{aligned} f_1(x) = {} & -81169500497977807111875 19x^3 \\ & -16882603980128238644837 75x \\ & +84560760268939108662310 3, \\ f_2(x) = {} & 46519400932385985058355 98x^3 \\ & -97236800537453385369870 47x \\ & +31625080754111664388691 49 \end{aligned}$$

for the case $d = 3, k = 2$. If we let $d = 4, k = 1$, then we obtain 4 polynomials of degree 4 as follows:

$$\begin{aligned} f_1(x) = {} & -16624470838844689974x^4 - 12938092473604980037x^3 \\ & +30640947335461408697x^2 - 49074330569257104938x \\ & +13793429687479158462, \\ f_2(x) = {} & 51774904293910722379x^4 + 50132776966516924 75x^3 \\ & -26435016679243240057x^2 - 17960790855546870693x \\ & +8449918455213426306, \\ f_3(x) = {} & 56975869172891318371x^4 - 78804912313470526585x^3 \\ & +29417741697300821984x^2 - 74672196812934981 72x \\ & +1096444195584483276, \\ f_4(x) = {} & -65193201182400829 35x^4 - 64290644589732753918x^3 \end{aligned}$$

$$- 72206567262569865997x^2 - 22589152230759774686x + 18318665834905661971.$$

All 6 generated polynomials have a common root $p^{-1}r \pmod N$. Therefore we obtain 1 polynomial pair of degree (3,3), 8 polynomial pairs of degree (3,4), 6 polynomial pairs of degree (4,4).

Remark 7. Similarly as in Section 4.1, we may extend the idea in Proposition 2 to more general case when $x^d \equiv kN \pmod{p^2}$ with small k has a solution $r^* \approx p$ so that

$$\left[p^{d-1}, p^{d-2}r^*, \ldots, r^{*d-1}, \frac{r^{*d} - kN}{p}, \frac{r^*(r^{*d} - kN)}{p^2}\right] \tag{12}$$

is a $(d+2)$-term GP $\pmod N$ of $O(N^{1-1/d})$.

Example 5. Let

$$\begin{aligned} N = {} & 16883459020876298444631914839678933912679050383997017432286924927358594079070128713116772352361686949218607383329500280934457485822542406312052073 9, \\ p = {} & 20786403171775734254530527129787360981315034315689. \end{aligned}$$

Then we find that

$$r = 109870829235056655534505175588331267929189879271 23$$

is a root of $x^3 \equiv 2N \pmod{p^2}$. From a 5-term GP $\pmod N$ as $\vec{c} = [p^2, pr, r^2, \frac{r^3-2N}{p}, \frac{r(r^3-2N)}{p^2}]$, we get 2 cubic polynomials

$$\begin{aligned} f_1(x) = {} & -44521848631644169357090 1x^3 + 32181799250628910087622 89x \\ & - 16520264150308528349364 42, \\ f_2(x) = {} & 63266109424647158230454 83x^3 + 95735207803034197201330 2x \\ & - 12024535040312982465423 37 \end{aligned}$$

for the case $d = 3, k = 2$. If we let $d = 4, k = 1$, then we obtain 4 polynomials of degree 4 as follows:

$$\begin{aligned} f_1(x) = {} & 407256045356420449 69x^4 - 110225194518255025 52x^3 \\ & - 406696899322406112 8x^2 - 172381768023255975 30x \\ & + 88914669487528458 0, \\ f_2(x) = {} & 365265703294450498 5x^4 + 896329174924350873 4x^3 \\ & + 376672185657316746 33x^2 + 602087300016172132 3x \\ & - 15110171934817525190, \\ f_3(x) = {} & 211998330435745180 00x^4 + 154650811090284490 02x^3 \\ & - 111884224575116547 94x^2 - 366065649241686480 47x \end{aligned}$$

$$
\begin{aligned}
&+ 19037810592983267379,\\
f_4(x) = {} & 161002688894870991 42x^4 + 245453369061318493 97x^3\\
&- 438553582462476473 66x^2 + 248793904171228471 69x\\
&- 51579984448780331 15,
\end{aligned}
$$

where all 6 polynomials have common root $p^{-1}r \pmod N$.

Using $x^d \equiv kN \pmod{p^2}$ for many small k increases the probability that the equation is solvable. In practice, the GP in (12) is much easier to find than the GP with $k = 1$. For instance, in Example 4 with $k = 1$, there are 3 pairs (p, r^*) such that $r^{*3} \equiv N \pmod{p^2}$ with $|r^*| \le 10p$ and $\frac{m}{10} < p < m$. If we extend our search range to $1 \le k \le 10$, then have 27 of (p, r^*) such that $r^{*3} \equiv kN \pmod{p^2}$ with $|r^*| \le 10p$ and $\frac{m}{10} < p < m$, which is not so cost effective because we get less than three times of (p, r^*) even if we increased the range of k ten times. On the other hand, reducing the search range of p from $\frac{m}{10} < p < m$ to $\frac{m}{10} < p < \frac{19m}{100}$ produces 9 pairs of (p, r^*) with $1 \le k \le 10$. That is, we still find more GP by reducing the range of p and increasing the range of k, which seems more effective since we consider congruence equations (mod p^2) for smaller values of p.

Table 1 show a small numerical data for the number of the pair (r^*, p) satisfying $r^{*3} \equiv kN \pmod{p^2}$ for all N which is a product of two primes $q_1 \ne q_2$ with $10^4 < q_1, q_2 < 10^5$. Note that each pair (r^*, p) corresponds to a GP of length 5 which is either the form of (11) or (12). This result suggests that 5-term GP (11) and (12) exist with high probability, even though the number of GP is relatively small for each N. Moreover it says that one is more likely to find solution of $x^3 \equiv kN \pmod{p^2}$ by increasing the range of k rather than that of p. It should be mentioned that it also saves the time for the following reason. If we increase the range of k from $k = 1$ to $1 \le k \le 10$, the number of equations $x^3 \equiv kN \pmod{p^2}$ we need to consider is increased by the factor of 10. However if we increase the range of p from $\frac{m}{10} < p < m$ to $\frac{m}{10} < p < 10m$, the number of equations $x^3 \equiv kN \pmod{p^2}$ we need to consider is increased by the factor of $\pi(\frac{99}{10}m)/\pi(\frac{9}{10}m) \approx 11$ but the catch in this case is that we have to solve the congruence equation $x^3 \equiv kN \pmod{p^2}$ for ten times larger size of p which inevitably slow down the implementation time on PARI-GP, as is shown in the table.

5. Conclusions

We presented a method of constructing nonlinear polynomials of degree d for all $\frac{l}{2} < d < l$ having common roots (mod N) given GP (mod N) of fixed length l. We also give the estimation of the size of the coefficients of the nonlinear polynomials in terms of the size of the given GP, which generalizes Montgomery's method. We showed that the GP of length $d + 1$ can be constructed in more flexible way than the usual base-m method and we find corresponding

TABLE 1. Existence of GP (11) and (12)

	$k=1$ $\frac{m}{10} < p < m$	$k=1$ $\frac{m}{10} < p < 10m$	$1 \le k \le 10$ $\frac{m}{10} < p < \frac{19m}{100}$
Average number of (r^*, p) with $\lvert r^*\rvert \le 5p$ for each N	2.29	3.94	7.46
The number of N such that $x^3 \equiv kN \pmod{p^2}$ has a solution $\lvert r^*\rvert \le 5p$	89.79%	98.04%	99.91%
Average number of (r^*, p) with $\lvert r^*\rvert \le 10p$ for each N	3.81	6.57	12.44
The number of N such that $x^3 \equiv kN \pmod{p^2}$ has a solution $\lvert r^*\rvert \le 10p$	97.75%	99.85%	100%
PARI-GP time estimation on Intel U7300 1.30GHz CPU laptop	2 days	18 days	2days

polynomials of various degrees having common root (mod N). We also stated the conditions when a special GP of length $d+2$ exists.

Acknowledgements. The authors would like to thank the referee for the valuable comments on this paper and to P. L. Montgomery for his helpful suggestions regarding a few questions related to this paper. Also, the authors would like to mention that Nicholas Coxon has improved and extended our result in http://arxiv.org/abs/1109.6398 [4]. This research was supported by the National Research Foundation of Korea funded by the Ministry of Science, ICT & Future Planning (NRF-2013R1A1A2060698).

The work of G. H. Cho was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2009-0093827). The work of N. Koo was supported by the research project (B21503-1) of the National Institute for Mathematical Sciences, Republic of Korea.

References

[1] K. Aoki, J. Franke, T. Kleinjung, A. K. Lenstra, and D. A. Osvik, *A Kilobit special number field sieve factorization*, Advances in cryptology-ASIACRYPT 2007, pp. 1–12, Lecture Notes in Comput. Sci., 4833, Springer, Berlin, 2007.

[2] S. Bai, C. Bouvier, A. Kruppa, and P. Zimmermann, *Better Polynomials for GNFS*, To appear in Mathematics of Computation.

[3] S. Bai, R. P. Brent, and E. Thomé, *Root optimization of polynomials in the number field sieve*, Math. Comp. **84** (2015), no. 295, 2447–2457.

[4] N. Coxon, *On nonlinear polynomial selection for the number field sieve*, preprint, 2011.

[5] ———, *Montgomery's method of polynomial selection for the number field sieve*, preprent, 2014.

[6] R. Crandall and C. Pomerance, *Prime Numbers*: *A Computational Perspective 2ed*, Springer, 2005.

[7] J. Gower, *Rotations and translations of number field sieve polynomials*, Proceeding of Asiacrypt 2003, LNCS 2894, pp. 302–310, 2003.

[8] T. Kleinjung, *On polynomial selection for the general number field sieve*, Math. Comp. **75** (2006), no. 256, 2037–2047.

[9] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thome, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, *Factorization*

of a 768-bit RSA modulus, Advances in cryptology-EUROCRYPTO 2010, pp. 333–350, Lecture Notes in Comput. Sci., 6223, Springer, Berlin, 2010.
[10] A. K. Lenstra and H. W. Lenstra, Jr, *The Development of the Number Field Sieve*, LNM 1554, Springer, 1993.
[11] A. K. Lenstra, H. W. Lenstra, Jr, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 513–534.
[12] P. Montgomery, *Small geometric progressions modulo n*, Unpublished note of 2 pages, December 1993, revised 1995 and 2005.
[13] B. Murphy, *Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm*, PhD thesis, Australian National University, July 1999.
[14] P. Nguyen and J. Stern, *Merkle-Hellman revisited: A cryptoanalysis of the Qu-Vanstone cryptosystem based on group factorizations*, Advances in cryptology-EUROCRYPTO '97 (Santa Barbara, CA, 1997), pp. 198–212, Lecture Notes in Comput. Sci., 1294, Springer, Berlin, 1997.
[15] T. Prest and P. Zimmermann, *Non-linear polynomial selection for the number field sieve*, J. Symbolic Comput. **47** (2012), no. 4, 401–409.
[16] RSA challenge; available at http://www.rsa.com/rsalabs/html/challenges.html=
[17] R. S. Williams, *Cubic Polynomials in the Number Field Sieve*, MSc Thesis, Texas Tech University, 2010.

Gook Hwa Cho
Institute for Mathematical Sciences
Ewha Womans University
Seoul 03765, Korea
E-mail address: ghcho@ewha.ac.kr

Namhun Koo
Division of Mathematical Models
National Institute for Mathematical Sciences
Daejeon 34047, Korea
E-mail address: nhkoo@nims.re.kr

Soonhak Kwon
Department of Mathematics
Sungkyunkwan University
Suwon 16419, Korea
E-mail address: shkwon@skku.edu