Advances in Mathematics of Communications doi:10.3934/amc.2022022

RECONSTRUCTING POINTS OF SUPERELLIPTIC CURVES OVER A PRIME FINITE FIELD

Jaime Gutierrez

University of Cantabria
Santander, E-39071, Spain

(Communicated by Ferruh Özbudak)

Abstract. Let p be a prime and $\mathbb{F}_p$ the finite field with p elements. We show how, when given an superelliptic curve $Y^n + f(X) \in \mathbb{F}_p[X, Y]$ and an approximation to $(v_0, v_1) \in \mathbb{F}_p^2$ such that $v_1^n = -f(v_0)$, one can recover (v_0, v_1) efficiently, if the approximation is good enough. As consequence we provide an upper bound on the number of roots of such bivariate polynomials where the roots have certain restrictions. The results has been motivated by the predictability problem for non-linear pseudorandom number generators and, other potential applications to cryptography.

1. Introduction

For a prime p, we denote by $\mathbb{F}_p$ the field of p elements and assume that it is represented by the set $\{0, 1, \ldots, p-1\}$. Sometimes, where obvious, we treat elements of $\mathbb{F}_p$ as integers in the above range.

Here we consider the following computational problem: given the polynomial $Y^n + f(X) \in \mathbb{F}_p[X, Y]$ and approximations to $(v_0, v_1) \in \mathbb{F}_p^2$ where $v_1^n + f(v_0) \equiv 0 \bmod p$, reconstruct (v_0, v_1). By an approximation to an integer point (v_0, v_1), we mean an integer point (w_0, w_1) such that $|w_i - v_i|$ is small.

This question was presented and studied in [14] for general bivariate polynomials $F(X, Y) \in \mathbb{F}_p[X, Y]$. Its has applications to, and has been motivated by, the predictability problem for non-linear pseudorandom number generators and the linear congruential generator on elliptic curves (see [3, 6, 7, 13, 16, 19, 21]).

This problem is a particular case of the problem of finding small solutions of multivariate polynomial congruences. For polynomial congruences in one variable, an algorithm has been given by Coppersmith in [10].

For multivariate case the existing approach [5, 9, 11, 17, 18] depends on linearization. It gives at least one equation over the integers, satisfied by (v_0, v_1). Heuristically, we can hope to find two or more such equations, and solve them simultaneously via a resultant. The existence or independence of the second equation is not guaranteed, such that all created polynomials define an algebraic variety of dimension 0, so the effectiveness of the method is just heuristic. On the other hand, the usually the performance of the so called Coppersmith's methods is not suitable, because of large dimensión of the constructed lattice.

2020 *Mathematics Subject Classification:* Primary: 11H06, 11Y16, 12Y05; Secondary: 11K16.
Key words and phrases: Superelliptic curves, lattice techniques, prime finite fields, cryptography.
Author is partially supported by grant PID2019-110633GB-I00 funded by MCIN/AEI/10.13039/ 501100011033.

As in [14], this paper attempts to replace the heuristic nature by a probabilistic statement. Given an approximation to an unknown solution (v_0, v_1), we construct a lattice with a small solution. The components of this vector are bounded in terms of the quality of the approximation, and for each choice of these components, we construct a polynomial $G(X, Y)$ such that (v_0, v_1) simultaneously solves $G(v_0, v_1) \equiv v_1^n + f(v_0) \equiv 0 \bmod p$. Now the probabilistic argument follows taking v_0 randomly and there are a bounded number of "bad" v_0 for which we can not recover the solution. If our true v_0 is not among these, the linearization will find only the correct (v_0, v_1). Finally, we are able to obtain a much better tolerance than in [14] since the superelliptic curve polynomials involve a linear number of monomials instead of a quadratic ones for arbitrary bivariate polynomials, then the associated lattice dimension grows linearly instead of quadratic and the norm of the shortest vector grows linearly. We also want to remark that the dimension of the lattices involved is relatively small comparing with the approach via Coppersmith's methods for the same bound of tolerance.

On the other hand, this problem is also a special case of obtaining which is the number of roots where the roots have certain restrictions, sometimes these kind of question has been called additive energy, the subject has been studied quite recently in [2, 12, 23]

The remainder of the paper is structured as follows. We start with a very short outline of some basic facts about the Closest Vector Problem (CVP), and the number of $\mathbb{F}_p$-rational points on algebraic curves in Section 2. In Section 3 we formulate our main result and give outline the plan of the proof Subsection 3.1 which the proof is given in Subsection 3.2. The study of the error tolerance and comparison with known results is provide in Subsection 3.3. Then, in Section 4 we discus the results of numerical tests of our approaches. Finally, we conclude with Section 5 which makes some final comments and poses open questions.

Throughout the paper, we use the convention that the parameters on which the implied constant in a Landau symbol O are written in the subscript of O. A symbol O without a subscript indicates and absolute implied constant.

2. Preliminaries

2.1. Closest vector problem in lattices. Here we review some results and definitions concerning the Closest Vector Problem, all of which can be found in [15]. Let $\{\vec{b}_1, \ldots, \vec{b}_s\}$ be a set of linearly independent vectors in $\mathbb{R}^r$. The set

$$\mathcal{L} = \{c_1\vec{b}_1 + \cdots + c_s\vec{b}_s \mid c_1, \ldots, c_s \in \mathbb{Z}\}$$

is an *s-dimensional lattice* with *basis* $\{\vec{b}_1, \ldots, \vec{b}_s\}$. If $s = r$, the lattice $\mathcal{L}$ is of *full rank*.

One basic lattice problem is the *Closest Vector Problem (CVP)*: given a basis of a lattice $\mathcal{L}$ in $\mathbb{R}^s$ and a shift vector $\vec{t}$ in $\mathbb{R}^s$, the goal is finding a vector in the lattice $\mathcal{L}$ closest to the target vector $\vec{t}$. It is well known that this problem is **NP**-hard when the dimension grows. However, it is solvable in deterministic polynomial time provided that the dimension of $\mathcal{L}$ is fixed (see [20], for example).

For a slightly weaker task of finding a sufficiently close vector, the celebrated *LLL algorithm* of Lenstra, Lenstra and Lovász [22] provides a desirable solution, as noticed by [1]. Here, we state this result as Lemma 2.1.

Lemma 2.1. *There exists a deterministic polynomial time algorithm which, when given an s-dimensional full rank lattice $\mathcal{L}$ and a shift vector $\vec{t}$, finds a lattice vector $\vec{u} \in \mathcal{L}$ satisfying the inequality*

$$\|\vec{t} - \vec{u}\| \le 2^{s/2} \min\{\|\vec{t} - \vec{v}\| : \ \vec{v} \in \mathcal{L}\}.$$

Many other results on both exact and approximate finding of a closest vector in a lattice are discussed in [15, 19, 24, 25].

2.2. THE NUMBER OF $\mathbb{F}_p$-RATIONAL POINTS ON PLANE ALGEBRAIC CURVES. Our second basic result is an upper bound on the number of roots of a bivariate polynomial $F(X, Y) \in \mathbb{F}_p[X, Y]$. More concretely, we use the following result of [14]:

Lemma 2.2. *Suppose that $F(X, Y)$ is absolutely irreducible bivariate polynomial of total degree $n > 1$. Then for $M = \#\{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p, F(x, y) = 0\}$, the inequality*

$$nM \ge p + \emptyset_n(p^{1/2})$$

holds.

3. MAIN RESULT

In this section we formulate and prove our main result providing a probabilistic algorithm to recover a point of a superelliptic curve.

3.1. FORMULATION AND PLAN OF PROOF. Given a prime p and a positive integer Δ with $p > \Delta \ge 1$, we say that an integer pair $(w_0, w_1) \in \mathbb{Z}^2$ is a $\Delta-$approximation to $(v_0, v_1) \in \mathbb{F}_p^2$ if there exist integers $\varepsilon_0, \varepsilon_1$ satisfying:

$$|\varepsilon_0|, |\varepsilon_1| \le \Delta, \ w_0 + \varepsilon_0 = v_0, \ w_1 + \varepsilon_1 = v_1.$$

We are considering irreducible bivariate polynomials $H_{(n,m,f)}(X, Y) \in \mathbb{F}_p[X, Y]$ of the form $Y^n + f(X)$ and the equation:

$$H_{(n,m,f)}(X, Y) = 0 \tag{1}$$

where n, m are positive integers such that $nm > 1$, and $f = f(X) \in \mathbb{F}_p[X]$ is a monic univariate polynomial of degree m, i.e.,

$$f = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0.$$

Theorem 3.1. *With the above notations and definitions, there exists a set $\mathcal{V}(\Delta; f) \subseteq \mathbb{F}_p$ of cardinality*

$$\#\mathcal{V}(\Delta; f) = O(A(n, m)\Delta^{\lambda_{n,m}})$$

where

- *If $m \ge n$*

$$A(n, m) = m^2(2m + 2n)^{(m+n-1)/2}$$

and

$$\lambda_{n,m} = \frac{m(m + 1) + n(n - 1)}{2}$$

- *If $n \ge m$*

$$A(n, m) = n^2(2m + 2n)^{(m+n-1)/2}$$

and

$$\lambda_{n,m} = \frac{n(n + 1) + m(m - 1)}{2}$$

with the following property: whenever $v_0 \notin \mathcal{V}(\Delta; f)$ *then, given a* $\Delta-$*approximation* (w_0, w_1) *to a point* (v_0, v_1) *of the polynomial* $H_{(n,m,f)}(X, Y)$ *one can recovers* (v_0, v_1) *in deterministic polynomial time in* m, n *and* $\log p$.

An outline of the algorithm given in the proof of this Theorem goes as follows. The algorithm is divided into two stages.

- **Stage 1**: We construct a certain linear of system of congruences $\mathcal{LS}_{(n,m,f)}$ (see (4) below) and the associated lattice $\mathcal{L}_{(n,m,f)}$ (see (6) below) of dimension $m + n - 1$; this lattice depends on the approximation (w_0, w_1). We also show that a certain vector $\vec{E}$ directly related to missing information about (v_0, v_1) is a very short vector. Now, we compute a solution $\vec{T}$ of the system of congruences $\mathcal{LS}_{(n,m,f)}$ in polynomial time using linear diophantine methods. Then apply the algorithm of Lemma 2.1 to the vector $\vec{T}$ and lattice $\mathcal{L}_{(n,m,f)}$, obtaining a vector $\vec{u}$ of the lattice $\mathcal{L}_{(n,m,f)}$.
- **Stage 2**: We show that $\vec{F} = \vec{T} - \vec{u}$ provides the required information about $\vec{E}$ for all (v_0, v_1) except when v_0 lies in a certain exceptional set $\mathcal{V}(\Delta; f) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; f) = O(A(n, m)\Delta^{\lambda_{n,m}})$ (which is defined as set of zeroes of a certain parametric family of 0-dimension bivariate polynomial ideals).

Algorithm 1: Recovering algorithm

Input: $(f(X), \Delta, w_0, w_1)$ such that (w_0, w_1) is a Δ-approximation to a root (v_0, v_1) of $Y^n + f(X)$.

Output: (v_0, v_1) or $(0, 0)$

Compute a solution $\vec{T}$ of the system of congruences (4) ;
Compute $\vec{u}$ a closest vector to $\vec{T}$ and lattice (6) using the algorithm in [1];
$\vec{F} \leftarrow \vec{T}$ - $\vec{u} = (f_1, \ldots, f_m, \ldots, f_{m+n-1})$
$\varepsilon_0, \varepsilon_1 \leftarrow f_1/\Delta^m, f_m/\Delta^m$;
if $|\varepsilon_0| \leq \Delta \quad \& \quad |\varepsilon_1| \leq \Delta$ **then**
  return $(w_0 + \varepsilon_0, w_1 + \varepsilon_1)$
else
  return $(0, 0)$
end

3.2. *Proof.* We assume that $v_0 \in \mathbb{F}_p$ is chosen so as not to lie in a certain subset $\mathcal{V}(\Delta; f)$ of $\mathbb{F}_p$. The cardinality of this set is bounded by $O(A(m, n)\Delta^{\lambda_{m,n}})$. It consists of the solutions of a certain $0-$dimensional bivariate polynomial ideal. It is explained through the proof.

Since (v_0, v_1) is a point of the superelliptic curve defined by the polynomial $H_{(n,m,f)}(X, Y) \in \mathbb{F}_p[X, Y]$, we have

$$v_1^n + v_0^m + a_{m-1}v_0^{m-1} + a_1 v_0 + a_0 \equiv 0 \bmod p \tag{2}$$

We assume $m \geq n$, (the other case the proof is identical). Using the equalities $v_0 = w_0 + \varepsilon_0$ and $v_1 = w_1 + \varepsilon_1$, Eq. (2) become:

$$(w_0 + \varepsilon_0)^m + \sum_{i=1}^{m} a_{m-i}(w_0 + \varepsilon_0)^{m-i} + (w_1 + \varepsilon_1)^n \equiv 0 \bmod p$$

$$= \sum_{i=1}^{m-1} \frac{f^{(i)}(w_0)}{i!}\varepsilon_0^i + \sum_{i=1}^{n-1} \binom{n}{i} w_1^{n-i}\varepsilon_1^i + \varepsilon_0^m + \varepsilon_1^n + w_1^n + f(w_0) \equiv 0 \bmod p,$$

where $f^{(i)}$ denotes the i-th order derivative of the univariate polynomial f. Now, we linearize this polynomial system. Writing:

$$\begin{aligned} A_i &\equiv \frac{f^{(i)}(w_0)}{i!} \bmod p, \qquad i = 1, \ldots, m-1, \\ B_i &\equiv \binom{n}{i} w_1^{n-i} \bmod p, \qquad i = 1, \ldots, n-1, \\ C &\equiv (-w_1^n - f(w_0)) \bmod p. \end{aligned} \tag{3}$$

We obtain that vector

$$\begin{aligned} \vec{E} &= (\Delta^{m-1}\varepsilon_0, \Delta^{m-2}\varepsilon_0^2, \ldots, \Delta\varepsilon_0^{m-1}, \Delta^{m-1}\varepsilon_1, \Delta^{m-2}\varepsilon_1^2, \ldots, \Delta^{m-n+1}\varepsilon_1^{n-1}, \varepsilon_0^m + \varepsilon_1^n) \\ &= (\Delta^{m-1}\alpha_1, \Delta^{m-2}\alpha_2, \ldots, \Delta\alpha_{m-1}, \Delta^{m-1}\beta_1, \Delta^{m-2}\beta_2, \ldots, \Delta^{m-n+1}\beta_{n-1}, \gamma) \end{aligned}$$

is a solution to the following linear system of congruences $\mathcal{LS}_{(n,m,f)}$:

$$\begin{aligned} \sum_{i=1}^{m-1} \Delta^{i-1} A_i X_i + \sum_{i=1}^{n-1} \Delta^{i-1} B_i Y_i + \Delta^{m-1} Z &\equiv \Delta^{m-1} C \bmod p, \\ X_i &\equiv 0 \bmod \Delta^{m-i}, \quad i = 1, \ldots, m-1, \\ Y_i &\equiv 0 \bmod \Delta^{m-i}, \quad i = 1, \ldots, n-1. \end{aligned} \tag{4}$$

Moreover, $\vec{E}$ is a relatively short vector. We have:

$$\begin{aligned} |\alpha_i| &\leq \Delta^i, \quad i = 1, \ldots, m-1, \\ |\beta_i| &\leq \Delta^i, \quad i = 1, \ldots, n-1, \\ \|\vec{E}\| &\leq \sqrt{m+n+2}\Delta^m. \end{aligned} \tag{5}$$

Let $\mathcal{L}_{(n,m,f)}$ be the lattice consisting of integer solutions $(X_1, X_2, \ldots, X_{m-1}, Y_1, Y_2, \ldots, Y_{n-1}, Z) \in \mathbb{Z}^{n+m-1}$ of the homogeneous system of congruences:

$$\begin{aligned} \sum_{i=1}^{m-1} \Delta^{i-1} A_i X_i + \sum_{i=1}^{n-1} \Delta^{i-1} B_i Y_i + \Delta^{m-1} Z &\equiv 0 \bmod p, \\ X_i &\equiv 0 \bmod \Delta^{m-i}, \quad i = 1, \ldots, m-1, \\ Y_i &\equiv 0 \bmod \Delta^{m-i}, \quad i = 1, \ldots, n-1. \end{aligned} \tag{6}$$

We compute a solution $\vec{T}$ of the system of congruences (4), using linear diophantine equations methods. Applying the algorithm of Lemma 2.1 for the shift vector $\vec{T}$ and the lattice $\mathcal{L}_{(n,m,f)}$ we obtain a vector

$$\vec{F} = (\Delta^{m-1}\pi_1, \Delta^{m-2}\pi_2, \ldots, \Delta\pi_{m-1}, \Delta^{m-1}\rho_1, \Delta^{m-2}\rho_2, \ldots, \Delta^{m-n+1}\rho_{n-1}, \tau)$$

We have $\vec{F} = \vec{T} - \vec{u}$ (where $\vec{u}$ is the lattice vector returned by Lemma 2.1), is a vector of relatively *small* norm satisfying Eq. (4). From the algorithmic point of view, it is important to remark that we can compute $\vec{F}$ in polynomial time from the information we are given. We might hope that $\vec{E}$ and $\vec{F}$ are the same, or at least,

that we can recover the approximation errors from $\vec{F}$. If not, we will show that v_0 belongs to a subset $\mathcal{V}(\Delta; f) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; f) = O(A(m,n)\Delta^{\lambda_{m,n}})$.

The vector $\vec{D} = \vec{E} - \vec{F}$ lies in $\mathcal{L}_{(n,m,f)}$:

$$\vec{D} = (\Delta^{m-1}\delta_1, \Delta^{m-2}\delta_2, \ldots, \Delta\delta_{m-1}, \Delta^{m-1}\sigma_1, \Delta^{m-2}\sigma_2, \ldots, \Delta^{m-n+1}\sigma_{n-1}, \phi)$$

$$\delta_i = \alpha_i - \pi_i, \ (i = 1, \ldots, m-1); \quad \sigma_i = \beta_i - \rho_i, \ (i = 1, \ldots, n-1); \quad \phi = \gamma - \tau.$$

On the other hand, since the dimension of the lattice $\mathcal{L}_{(n,m,f)}$ is $m+n-1$ by Lemma 2.1 we obtain that the norm of $\vec{D}$ satisfies:

$$\|\vec{D}\| \leq \|\vec{E}\| + \|\vec{F}\| \leq (2^{(m+n-1)/2} + 1)\|\vec{E}\| \tag{7}$$

where the last inequality comes from the application of Lemma 2.1. Eq. (5) and Eq. (7) imply:

$$\begin{aligned} |\delta_i| &\leq (2^{(m+n-1)/2} + 1)\sqrt{m+n+2}\Delta^i, \quad i = 1, \ldots, m-1, \\ |\sigma_i| &\leq (2^{(m+n-1)/2} + 1)\sqrt{m+n+2}\Delta^i, \quad i = 1, \ldots, n-1, \\ |\phi| &\leq (2^{(m+n-1)/2} + 1)\sqrt{m+n+2}\Delta^m. \end{aligned} \tag{8}$$

If $\delta_1 \equiv 0 \bmod p$ and $\sigma_1 \equiv 0 \bmod p$, then $(v_0, v_1) = (w_0 + \pi_1, w_1 + \rho_1) \in \mathbb{F}_p^2$ and we can recover the original point (v_0, v_1). So, we can assume $\delta_1 \not\equiv 0 \bmod p$ or $\sigma_1 \not\equiv 0 \bmod p$.

Substituting $w_0 = X - \varepsilon_0, w_1 = Y - \varepsilon_1$ in the first equation of lattice (6) $\mathcal{L}_{(n,m,f)}$ we obtain a bivariate polynomial:

$$\begin{aligned} G(X,Y) &= \sum_{i=1}^{m-1} \frac{f^{(i)}(X-\varepsilon_0)}{i!}\delta_i + \sum_{i=1}^{n-1} \binom{n}{i}(Y-\varepsilon_1)^{n-i}\sigma_i + \phi \\ &= f^{(1)}(X-\varepsilon_0)\delta_1 + \sum_{i=2}^{m-1} \frac{f^{(i)}(X-\varepsilon_0)}{i!}\delta_i + n(Y-\varepsilon_1)^{n-1}\sigma_1 \\ &\quad + \sum_{i=2}^{n-1} \binom{n}{i}(Y-\varepsilon_1)^{n-i}\sigma_i + \phi. \end{aligned}$$

Since we are assuming that $\delta_1 \not\equiv 0 \bmod p$ or $\sigma_1 \not\equiv 0 \bmod p$ then $G(X,Y)$ is a non-zero bivariate polynomial of total degree at most $m-1$ whose coefficients are in $\mathbb{Z}[\varepsilon_1, \varepsilon_0, \delta_1, \ldots, \delta_{m-1}, \sigma_1, \ldots, \sigma_{n-1}, \phi]$. We consider the polynomial system in $\mathbb{F}_p[X,Y]$:

$$\begin{aligned} G(X,Y) &\equiv 0 \bmod p, \\ Y^n + f(X) &\equiv 0 \bmod p. \end{aligned} \tag{9}$$

Since the polynomial $Y^n + f(X) \in \mathbb{F}_p[X,Y]$ is irreducible, then by the classical Bezout's theorem: for every choice of $\varepsilon_1, \varepsilon_0, \delta_1, \ldots, \delta_{m-1}, \sigma_1, \ldots, \sigma_{n-1}, \phi$ with $\delta_1 + \sigma_1 \neq 0$ the number of values v_0 satisfying the above polynomial system (9) is at most $(m-1)m$. We place any solution v_0 into the set $\mathcal{V}(\Delta; f)$. We have to show that the cardinality of $\mathcal{V}(\Delta; f)$ is a claimed in the statement theorem. In order to do that, we count the total number of polynomials $G(X,Y)$. We observe that $G(X,Y)$ is writing as Taylor expression at point $(\varepsilon_0, \varepsilon_1) \in \mathbb{Z}^2$, so it is enough to count the number of choices for $\delta_1, \ldots, \delta_{m-1}, \sigma_1, \ldots, \sigma_{n-1}, \phi$. Now, using bounds

(8) we obtain:

$$\phi \prod_{i=1}^{m-1} \delta_i \prod_{i=1}^{n-1} \sigma_i = (m+n+2)^{(m+n-1)/2}(2^{(m+n-1)/2}+1)\Delta^{(m(m+1)+n(n-1))/2}$$

which finishes the proof. □

3.3. THE ERROR TOLERANCE $\lambda_{n,m}$ FOR Δ. The quality of the approximation (w_0, w_1) is the measure used to characterize when the method returns the expected root (v_0, v_1).

A "bad" set of values for the component v_0 is described, provided that whenever that value lies outside the set, the algorithm works correctly. The size of the set is asymptotically $O_{n,m}(\Delta^{\lambda_{n,m}})$. This means that if

$$\Delta < p^{1/\lambda_{n,m}}$$

and p is large enough the method is unlikely to fail, providing that the root (v_0, v_1) is taken at random in the set of all roots of $H_{(n,m,f)}(X, Y)$. The result in Lemma 2.2 shows a uniform distribution of the first coordinate of the root for absolutely irreducible polynomials. Our theorem shows also that, for most zeros of a polynomial, the zeros are determined if the most significant bits are fixed. This means that, given a Δ-approximation, there is only one possible root if Δ is small enough. We believe that the roots are spread in many families of irreducible, not necessarily absolutely irreducible polynomials, i. e., given $H_{(n,m,f)}(X, Y)$ and for most (w_0, w_1) and Δ sufficiently small, $H_{(n,m,f)}(X, Y)$ has $O_{n,m}(1)$ zeros at distance Δ.

On the other hand, as we mentioned in the introduction section, in paper [14] presented a similar algorithm for recovering points of any irreducible bivariate polynomials modulo a prime:

Theorem 3.2 ([14])**.** *Given an irreducible polynomial $F(X, Y) \in \mathbb{F}_p[X, Y]$ of degree m in X, n in Y with $nm > 1$ and, a $\Delta-$approximation $(w_0, w_1) \in \mathbb{Z}^2$ to $(v_0, v_1) \in \mathbb{F}_p^2$ such that $F(v_0, v_1) = 0$, then one can recovers (v_0, v_1) in polynomial time in m, n and $\log p$ provided that v_0 does not lie in a certain set $\mathcal{V}(\Delta; F) \subseteq \mathbb{F}_p$ of cardinality,*

$$\#\mathcal{V}(\Delta; F) = O(A(n, m)\Delta^{\omega_{n,m}})$$

where

$$A(n, m) = (m+1)(n+1)2^{(m+1)(n+1)/2}$$

and

$$\omega_{n,m} = 2 + \frac{m^2}{2}(2n+1) + \frac{n^2}{2}(2m+1) + mn.$$

Now, we have $\omega_{n,m}$ is cubic polynomial in variables m and n, but $\lambda_{n,m}$ is quadratic. Of course, it is something expected because of the especial structure of superelliptic curve polynomial $H_{(n,m,f)}(X, Y)$.

However, several aspects must be taken into account before considering $\lambda_{n,m}$ the threshold for Δ as the error tolerance upon which the algorithm fails. First, the are constants hidden in the asymptotic reasoning. For instance, we can apply the exact CVP instead of Lemma 2.1. In this case, the vector $\vec{F}$ returned by the CVP to vector $\vec{T}$ and lattice $\mathcal{L}_{(n,m,f)}$ is the vector of minimal norm satisfying the $\mathcal{LS}_{(n,m,f)}$ ((4)), at most equal to the norm of the solution $\vec{E}$, using the bounds (5):

$$
\begin{aligned}
|\pi_i| &\leq \sqrt{m+n+2}\Delta^i, \quad i = 1, \ldots, m-1, \\
|\rho_i| &\leq \sqrt{m+n+2}\Delta^i, \quad i = 1, \ldots, n-1, \\
|\tau| &\leq \sqrt{m+n+2}\Delta^m.
\end{aligned} \tag{10}
$$

Then, bounds (5) and (10) imply that $\|\vec{D}\| = \|\vec{E} - \vec{F}\| \leq 2\sqrt{m+n+2}\Delta^m$ and the norm $\vec{D} = \vec{E} - \vec{F}$ verifies:

$$
\begin{aligned}
|\delta_i| &\leq 2\sqrt{m+n+2}\Delta^i, \quad i = 1, \ldots, m-1, \\
|\sigma_i| &\leq 2\sqrt{m+n+2}\Delta^i, \quad i = 1, \ldots, n-1, \\
|\phi| &\leq 2\sqrt{m+n+2}\Delta^m.
\end{aligned} \tag{11}
$$

Then the cardinality of the set $\mathcal{V}(\Delta; f) \subseteq \mathbb{F}_p$ is

$$m(m-1)(m+n+2)^{(m+n-1)/2}2^{(m+n-1)/2}\Delta^{\lambda_{n,m}}),$$

which is, obviously, smaller than the stated in the theorem.

Finally, the threshold could be higher, as the "bad" set does not guarantee that the method necessarily fails.

3.4. HYPERELLIPTIC CURVE POLYNOMIALS. For the lattice techniques and practical applications is very important the lattice dimension. In general the performance of Coppersmith's method is bad because of large dimension of the constructed lattice. The lattices in this paper are of fixed and low dimension, one time that n and m are fixed.

When $n = 1$ is the polynomial evaluation case, the theorem shows, basically, the same bound obtained in [4], here the considered univariate polynomial $f(X)$ is monic. The involved full lattice $\mathcal{L}_{(1,m,f)}$ has dimension m and the threshold is

$$\lambda_{1,m} = \frac{m(m+1)}{2}.$$

When $n = 2$ is the hyperelliptic curve polynomial, in this special case the involved full lattice $\mathcal{L}_{(2,m,f)}$ has dimension $m+1$ and the threshold is

$$\lambda_{2,m} = \frac{m(m+1)+2}{2}$$

Finally, the special case $n = 2$ and $m = 3$ corresponds to the elliptic curve case. Here, we have a lattice of dimension 4 and the cardinality for the bad set is Δ^7, which is an improvement of Theorem 2 in paper [14].

4. EMPIRICAL RESULTS

We have proposed an algorithm to recover points of superelliptic curve. The input required by the algorithm include approximations to the point.

In the first case, a "bad" set of values for the component x_0 is described, proving that whenever that value lies outside the set, the algorithm works correctly. Furthermore, the size of the set is asymptotically bounded with $\Delta^{\lambda_{n,m}}$.

We have performed some numerical tests with SageMath implementation of the main Theorem. Firstly, we fixed the integers n and m and generate a superelliptic curve $H_{(n,m,f)}(X, Y)$ over a prime finite field of a desired size by chosing ramdomly in $\mathbb{F}_p$ the parameters/coefficients of the univariate polynomial f to fix Eq. (1).

Then, we generate randomly a point in the curve by choosing their first coordinate and trying to solve Eq. (1). For several approximations to the point are given as input to our algorithms.

We summarize its results in the following tables. We have selected primes of several sizes, and note the obtained success threshold. As we can see, $1/\lambda_{n,m}$ appears as the correct threshold:

- $n = 1, m = 5$, $1/\lambda_{1,5} = 1/15 = 0.066666$

$\log_2(p)$	50	100	500	1000
$\log_p(\Delta)$	0.65	0.066	0.0664	0.0666

- $n = 2, m = 3$, $1/\lambda_{2,3} = 1/7 = 0.142857$

$\log_2(p)$	50	100	500	1000
$\log_p(\Delta)$	0.13	0.140	0.14	0.142

- $n = 2, m = 5$, $1/\lambda_{2,5} = 1/16 = 0.06250$

$\log_2(p)$	50	100	500	1000
$\log_p(\Delta)$	0.05	0.06	0.061	0.062

Another argument to show that the threshold is correct it is the so-called Gaussian heuristic. The so-called "Gaussian heuristic" suggests that and s-dimensional lattice $\mathcal{L}$ with volume $vol(\mathcal{L})$ is unlikely to have a nonzero vector which is substantially shorter than $vol(\mathcal{L})^{1/s}$. Moreover, if it is known that such a very short vector does exist, then up to a scalar factor it is likely to be the only vector with this property.

The involved lattice in this paper $\mathcal{L}_{(n,m,f)}$ ((6)) has volumen has volume the product of the modulo integers, that is,

$$vol(\mathcal{L}_{(n,m,f)}) = p\Delta^{\frac{m(m-1)+(n-1)(2m-n)}{2}}$$

Since the dimension of the lattice $\mathcal{L}_{(n,m,f)}$ is $m+n-1$. Then, vector $\vec{E}$ is likely to be the one founded whenever

$$\Delta^m < p^{1/(m+n-1)}\Delta^{\frac{m(m-1)+(n-1)(2m-n)}{2(m+n-1)}},$$

this is,

$$\Delta < p^{1/\lambda_{n,m}}.$$

Which it is exactly the same bound provided in the Theorem.

5. Remarks and open questions

So far, we have discussed the case where the quality is the same for approximations w_0, w_1 to v_0, v_1 respectively. Indeed, the presented theorem can be slightly modified consider different bounds for the approximations errors, i.e., let w_0 be a Δ_1-approximation to v_0 and w_1 be a Δ_2-approximation to v_1, for positive integers Δ_1 and Δ_2. On the other hand, the result can be also extended for arbitrary polynomial $f(X)$, in this case the cardinality of the set $\mathcal{V}(\Delta; f) \subseteq \mathbb{F}_p$ is $A(n,m)\Delta^{\lambda_{n,m}})$, where

$$\lambda_{n,m} = \frac{m(m+1)+n(n+1)}{2}.$$

Obviously our result is nontrivial only for $\Delta = O(p^{1/\lambda_{n,m}})$. Thus increasing the size of the admissible values of Δ is of prime importance.

On the other hand, as in [10], we can generate more non-linear equations by multiplication of several non-linear equations before the linearization step in order to improve attacks. However in our case the structure of the variables is more complicated than that of [10], and, after linearization it leads to a lattice of very large dimension. Thus this approach does not seem to provide any advantages. It may be very hard to give any precise rigorous or even convincing heuristic analysis of this approach.

Also, for future work we would like to investigate the applications of this result to study the cardinality of superelliptic curves points in small boxes, [8].

ACKNOWLEDGMENTS

The author would like to thank the reviewers for their careful reading of the paper and their valuable comments that improved the paper.

REFERENCES

[1] L. Babai, On Lovász' lattice reduction and the nearest lattice point problem, *Combinatorica*, **6** (1986), 1–13.

[2] R. C. Baker, M. Munsch and I. E. Shparlinski, Additive energy and a large sieve inequality for sparse sequences, preprint, arXiv:2103.12659.

[3] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, Predicting nonlinear pseudorandom number generators, *Math. Comp.*, **74** (2005), 1471–1494.

[4] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, Reconstructing noisy polynomial evaluation in residue rings, *J. Algorithms*, **61** (2006), 47–59.

[5] J. Blömer and A. May, A tool kit for finding small roots of bivariate polynomials over the integers, in *Advances in Cryptology–Eurocrypt 2005*, Lecture Notes in Comput. Sci., 3494, Springer, Berlin, 2005, 251–267.

[6] D. Boneh, S. Halevi and N. Howgrave-Graham, The modular inversion hidden number problem, in *Advances in Cryptology–ASIACRYPT 2001 (Gold Coast)*, Lecture Notes in Comput. Sci., 2248, Springer, Berlin, 2001, 36–51.

[7] J. Boyar, Inferring sequences produced by pseudo-random number generators, *J. Assoc. Comput. Mach.*, **36** (1989), 129–141.

[8] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, Points on curves in small boxes and applications, *Michigan Math. J*, **63** (2014), 503–534.

[9] D. Coppersmith, Finding small solutions to small degree polynomials, in *Cryptography and Lattices (Providence, RI, 2001)*, Lecture Notes in Comput. Sci., 2146, Springer, Berlin, 2001, 20–31.

[10] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *J. Cryptology*, **10** (1997), 233–260.

[11] J.-S. Coron, Finding small roots of bivariate integer polynomial equations: A direct approach, in *Advances in Cryptology–CRYPTO 2007*, Lecture Notes in Comput. Sci., 4622, Springer, Berlin, 2007, 379–394.

[12] A. Dunn, B. Kerr, I. E. Shparlinski and A. Zaharescu, Bilinear forms in Weyl sums for modular square roots and applications, *Adv. Math.*, **375** (2020), 58pp.

[13] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias and A. Shamir, Reconstructing truncated integer variables satisfying linear congruences, *SIAM J. Comput.*, **17** (1988), 262–280.

[14] D. Gómez and J. Gutierrez, Recovering zeros of polynomials modulo a prime, *Math. Comp.*, **83** (2014), 2953–2965.

[15] M. Grötschel, L. Lovász and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Algorithms and Combinatorics: Study and Research Texts, 2, Springer-Verlag, Berlin, 1988.

[16] J. Gutierrez and Á. Ibeas, Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits, *Des. Codes Cryptogr.*, **45** (2007), 199–212.

[17] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, in *Cryptography and Coding (Cirencester, 1997)*, Lecture Notes in Comput. Sci., 1355, Springer, Berlin, 1997, 131–142.
[18] E. Jochemsz and A. May, A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in *Advances in Cryptology–ASIACRYPT 2006*, Lecture Notes in Comput. Sci., 4284, Springer, Berlin, 2006, 267–282.
[19] A. Joux and J. Stern, Lattice reduction: A toolbox for the cryptanalyst, *J. Cryptology*, **11** (1998), 161–185.
[20] R. Kannan, Minkowski's convex body theorem and integer programming, *Math. Oper. Res.*, **12** (1987), 415–440.
[21] H. Krawczyk, How to predict congruential generators, *J. Algorithms*, **13** (1992), 527–545.
[22] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.*, **261** (1982), 515–534.
[23] L. Mérai and I. E. Shparlinski, Sparsity of curves and additive and multiplicative expansion of rational maps over finite fields, *Acta Arith.*, **188** (2019), 401–411.
[24] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems. A Cryptographic Perspective*, The Kluwer International Series in Engineering and Computer Science, 671, Kluwer Academic Publishers, Boston, MA, 2002.
[25] P. Q. Nguyen and J. Stern, Lattice reduction in cryptology: An update, in *Algorithmic Number Theory (Leiden, 2000)*, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000, 85–112.

Received April 2021; revised February 2022; early access March 2022.

E-mail address: jaime.gutierrez@unican.es