Recovering zeroes of polynomials modulo a prime

Domingo Gomez
Faculty of Science, University of Cantabria
E-39071 Santander, Spain
gomezd@unican.es

Jaime Gutierrez
E.T.S. Industrial Engineering and Telecommunications, University of Cantabria
E-39071 Santander, Spain
jaime.gutierrez@unican.es

December 14, 2015

Abstract

Let p be a prime and $\mathbb{F}_p$ the finite field with p elements. We show how, when given an irreducible bivariate polynomial $F \in \mathbb{F}_p[X, Y]$ and an approximation to a zero, one can recover the root efficiently, if the approximation is good enough. The strategy can be generalized to polynomials in the variables $X_1, \ldots, X_m$ over the field $\mathbb{F}_p$. These results have 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 problem: given a bivariate polynomial $F(X,Y) \in \mathbb{F}_p[X,Y]$ and approximations to $(v_0, v_1) \in \mathbb{F}_p^2$ where $F(v_0, v_1) \equiv 0 \bmod p$, recover (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 $|w_i - v_i|$, $i = 0, 1$, is small.

The question 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 [2, 5, 6, 10, 13, 3, 16, 18]).

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 [7] (see also [4, 9, 8, 14, 15]). However, in the general case only heuristic results are known. Here, we are able to obtain rigorous results for absolute irreducible bivariate polynomials modulo a prime p. On the other hand, our result applies only when the modulus is a prime number, unlike previous algorithms.

The remainder of the paper is structured as follows. We start with a very short outline of some basis facts about the Closest Vector Problem (CVP) in Subsection 2.1 and the number of $\mathbb{F}_p$-rational points on algebraic curves in Subsection 2.2. In Section 3 we formulate the algorithm and our main result. Section 4 is dedicated to recovering roots for elliptic curve polynomials and, Section 5 we study the multivariate case.

We conclude with Section 6 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 [12]. For more details and more recent references, we recommend consulting [16, 20, 21, 22].

Let $\{\mathbf{b}_1, \dots, \mathbf{b}_s\}$ be a set of linearly independent vectors in $\mathbb{R}^r$. The set

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

is an *s-dimensional lattice* with *basis* $\{\mathbf{b}_1, \dots, \mathbf{b}_s\}$. 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 $\mathbf{t}$ in $\mathbb{R}^s$, the goal is finding a vector in the lattice $\mathcal{L}$ closest to the target vector $\mathbf{t}$. 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 [17], for example).

For a slightly weaker task of finding a sufficiently close vector, the celebrated *LLL algorithm* of Lenstra, Lenstra and Lovász [19] provides a desirable solution, as noticed by [1]. Here, we state this result as Lemma 1.

Lemma 1 *There exists a deterministic polynomial time algorithm which, when given an s-dimensional full rank lattice* $\mathcal{L}$ *and a shift vector* $\mathbf{t}$ *finds a lattice vector* $\mathbf{u} \in \mathcal{L}$ *satisfying the inequality*

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

Many other results on both exact and approximate finding of a closest vector in a lattice are discussed in [12, 16, 20, 21].

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 with coefficients in a finite field.

Given $F(X, Y) \in \mathbb{F}_p[X, Y]$, we denote by N the number of solutions of the equation $F(x, y) = 0$ in the finite field $\mathbb{F}_p$. We use the following well known result (see for instance in [23, 25]), adapted to the special case of $\mathbb{F}_p$.

Lemma 2 *Suppose that* F *is absolute irreducible polynomial of total degree* n*. Then the following equation,*

$$|N - p| = O_n(p^{1/2})$$

holds.

As a consequence, we have the following:

Lemma 3 *Suppose that F 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*

$$nM \geq p + O_n(p^{1/2})$$

holds.

Proof. By Lemma 2, a lower bound for the number of roots is

$$N \geq p + O_n(p^{1/2}).$$

For any $x = a \in \mathbb{F}_p$, we have that $F(a, Y) \in \mathbb{F}_p[Y]$ has at most n roots, because $F(X, Y)$ is irreducible of degree $n > 1$.

So, the following inequality holds,

$$nM \geq N \geq p + O_n(p^{1/2}),$$

and this finishes the proof. ∎

3 Main Result

In this section we give a probabilistic algorithm to recover the root of a bivariate polynomial from only an approximation of the root. The algorithms presented in [4, 7, 8, 9, 15] build a lattice, then find a short vector in the lattice and relate this vector with a polynomial. After that, they use resultants and find the roots of a univariate polynomial over the integers, whereas our algorithm requires to find a small root of an univariate polynomials modulo a prime.

3.1 Algorithm

Given a positive integer Δ with $p > \Delta \geq 1$, we say that a pair $(w_0, w_1) \in \mathbb{Z}^2$ is a Δ-approximation to another pair $(v_0, v_1) \in \mathbb{F}_p^2$ if there exist integers $\varepsilon_0, \varepsilon_1$ satisfying $|\varepsilon_i| \leq \Delta$ and $[w_i + \varepsilon_i]_p = v_i$.

For a bivariate polynomial over the finite field of p elements

$$H(X,Y) = \sum_{i=0}^{m_1} \sum_{j=0}^{m_2} a_{i,j} X^i Y^j \in \mathbb{F}_p[X,Y]$$

of degree $m_1 < p$ in the variable X and degree $m_2 < p$ in the variable Y, the *leading monomial of* H or $LM(H)$ is the unique monomial $X^{m_1}Y^{n_1}$ such that, $a_{m_1,j} = 0, \forall j > n_1$. The *leading coefficient of* H or $LC(H)$ is a_{m_1,n_1}.

Now, given $F \in \mathbb{F}_p[X,Y]$ with an unknown root $(v_0, v_1) \in \mathbb{F}_p^2$ for which we have a Δ-approximation $(w_0, w_1) \in \mathbb{Z}^2$, we derive a probabilistic algorithm (Algorithm 3.1) for recovering the root. The parameter Δ measures how well the value (w_0, w_1) approximates the root (v_0, v_1) and it is assumed to vary independently of p subject to satisfying the inequality $\Delta < p$. Moreover, it is not involved in the complexity estimate of the algorithm.

Using the notation $\varepsilon_i = v_i - w_i$ for the approximation errors, we have

$$F(w_0 + \varepsilon_0, w_1 + \varepsilon_1) \equiv 0 \bmod p,$$

and the Taylor expansion of F at (w_0, w_1) gives:

$$\sum_{i=0}^{m_1} \sum_{j=0}^{m_2} \frac{F^{(i,j)}(w_0, w_1)}{i!j!} \varepsilon_0^i \varepsilon_1^j \equiv 0 \bmod p.$$

Our algorithm seeks a vector

$$\mathbf{e} = \left(\Delta^{m_1+m_2-i-j} \varepsilon_0^i \varepsilon_1^j \mid 0 \le i \le m_1,\ 0 \le j \le m_2,\ i+j > 0\right), \qquad (1)$$

which is a solution of the following linear system of congruences in $(m_1 + 1)(m_2 + 1) - 1$ variables:

$$\begin{cases} \displaystyle\sum_{\substack{0 \le i \le m_1, 0 \le j \le m_2 \\ 0 < i+j}} \Delta^{i+j} \frac{F^{(i,j)}(w_0, w_1)}{i!j!} X_{i,j} \equiv -\Delta^{m_1+m_2} F(w_0, w_1) \bmod p, \\ X_{i,j} \equiv 0 \bmod \Delta^{m_1+m_2-i-j}. \end{cases} \qquad (2)$$

The computation of a small solution of an inhomogeneous system of congruences is equivalent to approximate finding CVP.

3.2 Correctness

In this subsection, we prove in which cases Algorithm 3.1 returns the correct solution. After proving the result, we will show rigorously that if Δ is sufficiently small, then Algorithm 3.1 returns the root with high probability and also we comment on other interesting consequences.

Algorithm 1: Recovering algorithm

Input: (F, Δ, w_0, w_1) such that (w_0, w_1) is a Δ-approximation to a root (v_0, v_1) of F.

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

Compute an approximate solution $\mathbf{f}$ of (2) using algorithm in [1];
$\gamma_0', \gamma_1' \leftarrow f_{1,0}/\Delta^{m_1+m_2-1}, f_{0,1}/\Delta^{m_1+m_2-1}$;
if $LM(F^{(1,0)})! = LM(F^{(0,1)})$ **then**
  $v_0' \leftarrow w_0 + \gamma_0'$;
  $v_1' \leftarrow w_1 + \gamma_1'$;
  Take ε_1 any value s. t. $F(v_0', w_1 + \varepsilon_1) = 0$ with $|\varepsilon_1| \leq \Delta$.;
  if ε_1 *exists* **then**
    (**return** $(v_0', w_1 + \varepsilon_1)$;
  end
  Take ε_0 any value s. t. $F(w_0 + \varepsilon_0, v_1') = 0$ with $|\varepsilon_0| \leq \Delta$.;
  if ε_0 *exists* **then**
    (**return** $(w_0 + \varepsilon_0, v_1')$;
  end
else
  $a \leftarrow LC\left(F^{(1,0)}\right)$;
  $b \leftarrow LC\left(F^{(0,1)}\right)$;
  Take ε_0, $F(w_0 + \varepsilon_0, w_1 + (b\gamma_1' + a\gamma_0' - a\varepsilon_0)/b) = 0$ with $|\varepsilon_0| \leq \Delta$.;
  if ε_0 *exists* **then**
    return $(w_0 + \varepsilon_0, w_1 + (b\gamma_1' + a\gamma_0' - a\varepsilon_0)/b)$;
  else
    return *(0,0)*
  end
end
return *(0,0)*;

Theorem 1 *Given $F(X,Y) \in \mathbb{F}_p[X,Y]$ an irreducible polynomial with degree m_1 in X, m_2 in Y and $m_1 m_2 > 1$, then Algorithm 3.1 recovers (v_0, v_1) in polynomial time in m_1, m_2 and $\log p$ provided that v_0 does not lie in a certain set $\mathcal{V}(\Delta; F) \subseteq \mathbb{F}_p$ of cardinality*

$$\begin{aligned} \#\mathcal{V}(\Delta; F) &= O\left((m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2}\Delta^{\omega_{m_1,m_2}}\right), \\ \omega_{m_1,m_2} &= 2 + \frac{m_1^2}{2}(2m_2+1) + \frac{m_2^2}{2}(2m_1+1) + m_1 m_2. \end{aligned}$$

Proof. The theorem is trivial when $O\left((m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2}\Delta^{\omega_{m_1,m_2}}\right) \geq p$, and so we assume that $O\left((m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2}\Delta^{\omega_{m_1,m_2}}\right) < p$. The proof goes as follows, first fix the polynomial F and we assume that $v_0 \in \mathbb{F}_p$ is chosen so as not to lie in certain subsets $\mathcal{U}_1(\Delta; F)$, $\mathcal{U}_2(\Delta; F)$, $\mathcal{U}_3(\Delta; F)$, $\mathcal{V}'(\Delta; F)$, which will be defined gradually as we move through the proof. The last step will be consider $\mathcal{V}(\Delta; F)$ the union of these subsets and then calculate the cardinality.

Let $\mathcal{L}$ be the lattice associated to linear system of congruences (2), that is, $\mathcal{L}$ is the set of integer solutions $\mathbf{x} = (X_{i,j} \mid 0 \leq i \leq m_1,\ 0 \leq j \leq m_2,\ i+j > 0)$ satisfying,

$$\begin{cases} \displaystyle\sum_{\substack{0\leq i\leq m_1, 0\leq j\leq m_2 \\ 0<i+j}} \Delta^{i+j}\frac{F^{(i,j)}(w_0,w_1)}{i!j!}X_{i,j} \equiv 0 \bmod p \\ X_{i,j} \equiv 0 \bmod \Delta^{m_1+m_2-i-j}. \end{cases} \qquad (3)$$

We compute a solution $\mathbf{t}$ of the linear system of congruences (2), then algorithm of Lemma 1 applied to the vector $\mathbf{t}$ and lattice $\mathcal{L}$ returns a vector $\mathbf{u}$. We aim to show that $\mathbf{f} = \mathbf{t} - \mathbf{u}$ contains sufficient information about $\mathbf{e}$, provided that v_0 does not lie in the "bad" set $\mathcal{V}(\Delta; F)$ which we define below.

The vector

$$\mathbf{d} = \mathbf{e} - \mathbf{f} = \left(\Delta^{m_1+m_2-i-j}d_{i,j} \mid 0 \leq i \leq m_1,\ 0 \leq j \leq m_2,\ i+j > 0\right)$$

lies in $\mathcal{L}$, and so using the first congruence in (3) we obtain

$$\sum_{\substack{0\leq i\leq m_1, 0\leq j\leq m_2 \\ 0<i+j}} \frac{F^{(i,j)}(w_0,w_1)}{i!j!}d_{i,j} \equiv 0 \bmod p. \qquad (4)$$

On the other hand, the norm of vector $\mathbf{d}$ satisfies:

$$\|\mathbf{d}\| \leq \|\mathbf{f}\| + \|\mathbf{e}\| \leq (2^{(m_1+1)(m_2+1)/2} + 1)\|\mathbf{e}\|,$$

where the last inequality comes from the application of Lemma 1. Recalling the definition of $\mathbf{e}$ in Equation (1), it is easy bound to the norm of $\mathbf{e}$ by $(m_1+1)(m_2+1)\Delta^{m_1+m_2}$. Hence

$$\begin{aligned} |d_{i,j}| \leq 2^{(m_1+1)(m_2+1)/2+1}(m_1+1)(m_2+1)\Delta^{m_1+m_2-i-j}, \\ 0 \leq i \leq m_1,\ 0 \leq j \leq m_2,\ i+j > 0. \end{aligned} \tag{5}$$

We remark that if $d_{1,0} \equiv d_{0,1} \equiv 0 \bmod p$, then we have $f_{1,0} = \varepsilon_0$, $f_{0,1} = \varepsilon_1$. It implies we can recover (v_0, v_1). Hence, we may assume that $d_{1,0}$ is non-zero modulo p or $d_{0,1}$ is non-zero modulo p. In the following two cases, we assume that one value is zero modulo p and not the other. We see how to recover the root in these two special cases.

- Case 1. If $d_{1,0} \equiv 0 \bmod p$, then by bounds (5) we have $d_{1,0} = 0$ and $f_{1,0} = \varepsilon_0$. Computing in polynomial time the roots of the nonzero univariate polynomial $F(w_0 + \varepsilon_0, Y) = F(v_0, Y)$ in $\mathbb{F}_p$. We will show that there exist only one v_1 such that (w_0, w_1) is a Δ-approximation to (v_0, v_1) except for v_0 from a exceptional set $\mathcal{U}_1(\Delta; F) \subset \mathbb{F}_p$ of cardinality $O(m_1 m_2 \Delta)$. In fact, assuming $v_1' = w_1 + \varepsilon_1'$ with $|\varepsilon_1'| \leq \Delta$. Let $R(X) \in \mathbb{F}_p[X]$ the resultant of the polynomials $F(X, Y)$ and $F(X, Y - \varepsilon_1 + \varepsilon_1')$ with respect the variable Y. Since $|\varepsilon_1' - \varepsilon_1| \leq 2\Delta$, the number of such polynomials $R(X)$ are bounded by 2Δ. Again, since F is irreducible $R(X)$ is the zero polynomial if and only if $v_1 = v_1'$. Otherwise, $R(X)$ has degree at most $2m_1m_2$ and $R(v_0) = 0$ because (v_0, v_1) is a common zero of $F(X, Y)$ and $F(X, Y - \varepsilon_1 + \varepsilon_1')$. We place these $O(m_1 m_2 \Delta)$ values of v_0 in $\mathcal{U}_1(\Delta; F)$.

- Case 2. If $d_{0,1} \equiv 0 \bmod p$, then by bounds (5) we have $d_{0,1} = 0$ and $f_{0,1} = \varepsilon_1$. Computing in polynomial time the roots of the nonzero univariate polynomial $F(X, w_1 + \varepsilon_1) = F(X, v_1)$ in $\mathbb{F}_p$. We will show that there exists only one v_0 such that (w_0, w_1) is a Δ-approximation to (v_0, v_1) unless v_0 belongs in a set $\mathcal{U}_2(\Delta; F) \subset \mathbb{F}_p$ of cardinality $O(2m_1 m_2 \Delta)$. In fact, assuming $v_0' = w_0 + \varepsilon_0'$ with $|\varepsilon_0'| \leq \Delta$. Let $R(X) \in \mathbb{F}_p[X]$ the resultant of the polynomials $f(X - \varepsilon_0' + \varepsilon_0, Y)$ and $f(X, Y)$ with respect the variable Y. Since $|\varepsilon_0' - \varepsilon_0| \leq 2\Delta$, the number of such polynomials $R(X)$ are bounded by 2Δ. And, $R(X)$ is the zero polynomial if and only if $v_0 = v_0'$. Otherwise, $R(X)$ has degree at most $2m_1m_2$ and $R(v_0) = 0$ because (v_0, v_1) is a common zero of $F(X,Y)$ and $F(X - \varepsilon_0' + \varepsilon_0, Y)$. We place these $O(m_1m_2\Delta)$ values of v_0 in $\mathcal{U}_2(\Delta; F)$.

Now, we consider $d_{1,0}d_{0,1} \not\equiv 0 \bmod p$ and substitute $w_0 = X - \varepsilon_0, w_1 = Y - \varepsilon_1$ in the congruence (3), we obtain the bivariate polynomial

$$G(X,Y) = \sum_{i=0}^{m_1} \sum_{j=0}^{m_2} b_{i,j} X^i Y^j,$$

where $b_{i,j} \in \mathbb{Z}[\varepsilon_0, \varepsilon_1, d_{1,0}, \ldots, d_{m_1,m_2}]$ and it satisfies,

$$G(v_0, v_1) \equiv 0 \bmod p.$$

Now, we will show that for every choice of $\varepsilon_0, \varepsilon_1$ and vector $\mathbf{d}$ with $d_{1,0}d_{0,1}$ not equivalent to zero modulo p, then $G(X,Y)$ is a nonzero polynomial except for v_0 lies in a certain set $\mathcal{U}_3(\Delta; F)$. First, we claim

$$G(X,Y) = 0 \implies d_{1,0}LT(F^{(1,0)}) + d_{0,1}LT(F^{(0,1)}) \equiv 0 \bmod p.$$

In fact, $d_{1,0}LC(F^{(1,0)}) + d_{0,1}LC(F^{(0,1)}) \equiv 0 \bmod p$, where $LT(H)$ (resp. $LC(H)$) is the leading term (resp. the leading coefficient) of a polynomial H with respect a monomial ordering.

This relationship between the leading terms allows us to compute $a, b \in \mathbb{Z}$ such that $\varepsilon_1 = a\varepsilon_0 + b$ and solve

$$F(w_0 + x, w_1 + ax + b) \equiv 0 \bmod p, \quad \text{with } |x| \leq \Delta. \tag{6}$$

Notice that this polynomial is nonzero, otherwise the polynomial $F(X,Y)$ will be reducible. As in the above Case 1, we can show that Equation (6) has a unique solution unless v_0 belongs to a exceptional set $\mathcal{U}_3(\Delta; F) \subset \mathbb{F}_p$ of cardinality $O(m_1m_2\Delta)$. Assuming ε_0' another root of the Equation (6) and let $R(X) \in \mathbb{F}_p[X]$ the resultant of the polynomials $F(X,Y)$ and $F(X + \varepsilon_0' - \varepsilon_0, Y + a(-\varepsilon_0 + \varepsilon_0'))$ with respect the variable Y. Since $|\varepsilon_0' - \varepsilon_0| \leq 2\Delta$, the number of such polynomials $R(X)$ are bounded by 2Δ. Again, since F is irreducible $R(X)$ is the zero polynomial if and only if $\varepsilon_0 = \varepsilon_0'$. Otherwise, $R(X)$ has degree at most $2m_1m_2$ and $R(v_0) = 0$ because (v_0, v_1)

is a common zero of $F(X,Y)$ and $F(X+\varepsilon_0'-\varepsilon_0, Y+a(-\varepsilon_0+\varepsilon_0'))$. We place these $O(m_1m_2\Delta)$ values of v_0 in $\mathcal{U}_3(\Delta;F)$. Finally, we consider the polynomial system in $\mathbb{F}_p$:

$$\begin{aligned} G(X,Y) &\equiv 0 \bmod p, \\ F(X,Y) &\equiv 0 \bmod p. \end{aligned} \tag{7}$$

Then, for every choice of $\varepsilon_0, \varepsilon_1$ and vector $\mathbf{d}$ with $d_{1,0}d_{0,1}$ is nonzero modulo p, only a constant number of values v_0 are possible. This is because the classical Bezout Theorem for algebraic curves applies, so because $F(X,Y)$ is an irreducible polynomial and $G(X,Y)$ is not a multiple of F, then the number of the points of system (7) is at most $(m_1+m_2-1)^2$. We place any solution v_0 to (7) for any possible values of $d_{i,j}$ and $\varepsilon_0, \varepsilon_1$ into a new exceptional set $\mathcal{V}'(\Delta;F)$. We need to provide a bound for its cardinality.

By the bounds obtained in (5) the total number of possible choices for the integers $\varepsilon_0, \varepsilon_1$ and $d_{i,j}, i=0,\ldots,m_1, j=0,\ldots,m_2$ is at most:

$$\begin{aligned} \Delta^2 + \prod_{\substack{0\le i\le m_1, 0\le j\le m_2 \\ 0<i+j}} &\left(2(m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2}\Delta^{m_1+m_2-i-j}\right) \\ &= O(((m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2})^{(m_1+1)(m_2+1)}\Delta^{\omega_{m_1,m_2}}), \end{aligned}$$

where

$$\omega_{m_1,m_2} = 2 + \frac{m_1^2}{2}(2m_2+1) + \frac{m_2^2}{2}(2m_1+1) + m_1m_2.$$

We define $\mathcal{V}(\Delta;F) = \mathcal{U}_1(\Delta;F)\cup\mathcal{U}_2(\Delta;F)\cup\mathcal{U}_3(\Delta;F)\cup\mathcal{V}'(\Delta;F)$. To finish the proof, we note that $\mathcal{L}$ is defined using information we are given, and recall that to find an approximation to the Closest Vector Problem can be solved in deterministic polynomial time in the bit size of a given basis lattice and in the lattice dimension $(m_1+1)(m_2+1)-1$. ■

The quality of the approximation (w_0, w_1) is the measure used to characterize when the algorithm returns the expected root (v_0, v_1). A "bad" set of values for the component v_0 is described, provied that whenever that value lies outside the set, the algorithm works correctly. The size of the set is asymptotically $O_{m_1,m_2}(\Delta^{\omega_{m_1,m_2}})$. This means that if

$$\Delta < p^{1/\omega_{m_1,m_2}}$$

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 F. The result in Lemma 3 shows a uniform distribution of the first coordinate of the root for absolute 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 this property is also valid for others families of irreducible, but not absolute irreducible polynomials have $O_{m_1,m_2}(1)$ zeros.

However, several aspects must be taken into account before considering the threshold for Δ as the error tolerance upon which the algorithm fails. Firstly, the constants hidden in the asymptotic reasoning (namely, the size of the prime p). Second, the threshold could be higher, as the "bad" set does not guarantee that the method needed fail. Finally, the most important fact: the proposed algorithm is for arbitrary (dense) bivariate polynomials, but in many applications we need to work with special bivariate polynomials and, may be, for this class of polynomials we can obtain a much better tolerance. The following section will illustrate this last remark for elliptic curve equations.

4 Elliptic curves

Let $E(\mathbb{F}_p)$ be an elliptic curve defined over $\mathbb{F}_p$ given by an *affine Weierstrass equation*, which for $\gcd(p, 6) = 1$ takes form

$$Y^2 = X^3 + aX + b, \tag{8}$$

for some $a, b \in \mathbb{F}_p$ with $4a^3 + 27b^2 \neq 0$.

Corolary 1 *With the above conditions and definitions. Algorithm 1, with input polynomial (8), recovers (v_0, v_1) in polynomial time in $\log p$ provided that v_0 does not lie in a certain set $\mathcal{V}(\Delta; a) \subseteq \mathbb{F}_p$ of cardinality, $\#\mathcal{V}(\Delta; a; b) = O(\Delta^{32})$.*

Proof. Apply the Theorem 4 with $m_1 = 3$ and $m_2 = 2$ ∎

However, we can obtain a better result for this sparse polynomial (8).

Theorem 2 *With the above notations and definitions. There exist a set $\mathcal{V}(\Delta; a) \subseteq \mathbb{F}_p$ of cardinality, $\#\mathcal{V}(\Delta; a) = O(\Delta^8)$ with the following property. There exists an algorithm which, when given the polynomial (8) and*

$(w_0, w_1) \in \mathbb{Z}^2$ *a* Δ*-approximation to a zero* $(v_0, v_1) \in \mathbb{F}_p^2$ *of the polynomial (8), return* (v_0, v_1) *in polynomial time, provided that* v_0 *does not lie in* $\mathcal{V}(\Delta; a; b) \subseteq \mathbb{F}_p$.

Proof. In this case, we are looking for the vector $\mathbf{e} \in \mathbb{Z}^4$ which is of the form

$$\mathbf{e} := \left(\Delta^2\varepsilon_0, \Delta^2\varepsilon_1, \Delta\varepsilon_0^2, -\varepsilon_1^2 + \varepsilon_0^3\right),$$

where $|\varepsilon_i| \leq \Delta$ and $[w_i + \varepsilon_i]_p = v_i$. And, it is a solution of the following linear system of congruences :

$$\begin{cases} C_1\Delta X_1 + C_2\Delta X_2 + C_3\Delta^2 X_3 + C_4\Delta^3 X_4 & \equiv & -\Delta^3 C \bmod p, \\ X_1 & \equiv & 0 \bmod \Delta^2, \\ X_2 & \equiv & 0 \bmod \Delta^2, \\ X_3 & \equiv & 0 \bmod \Delta; \end{cases} \tag{9}$$

where

$$C_1 \equiv_p 3w_0^2 + a,\ C_2 \equiv_p -2w_1, C_3 \equiv_p 3w_0, C_4 = 1, C = w_0^3 + aw_0 + b - w_1^2.$$

Let $\mathbf{f}$ be a vector with smallest Euclidean norm satisfying the above linear system of congruences (9). We might hope that $\mathbf{e}$ and $\mathbf{f}$ are the same, or at least, that we can recover the approximations errors from $\mathbf{f}$. If not, we will show that v_0 belongs to subset $\mathcal{V}(\Delta; a) \subseteq \mathbb{F}_p$. Let us bound the "bad" possibilities for which this process does not succeed. Vector $\mathbf{d} = \mathbf{e} - \mathbf{f} = (\Delta^2 d_1, \Delta^2 d_2, \Delta d_3, d_4)$ lies in the lattice associated to (9):

$$\begin{cases} C_1\Delta X_1 + C_2\Delta X_2 + C_3\Delta^2 X_3 + C_4\Delta^3 X_4 & \equiv & 0 \bmod p, \\ X_1 & \equiv & 0 \bmod \Delta^2, \\ X_2 & \equiv & 0 \bmod \Delta^2, \\ X_3 & \equiv & 0 \bmod \Delta; \end{cases} \tag{10}$$

Since $\|\mathbf{e}\| < 3\Delta^3$, we have that

$$|d_1| \leq 6\Delta, \quad |d_2| \leq 6\Delta, \quad |d_3| \leq 6\Delta^2, \quad |d_4| \leq 12\Delta^3. \tag{11}$$

If $d_1 \equiv d_2 \equiv 0 \bmod p$, then we can recover the root (v_0, v_1). Hence, we may assume that d_1 is nonzero or d_2 is nonzero.

Substituting $w_0 = X - \varepsilon_0, w_1 = Y - \varepsilon_1$ in the first equation of lattice (10), we obtain a nonzero bivariate polynomial of total degree at most 2:

$$G(X,Y) = (3(X-\varepsilon_0)^2 + a)d_1 - 2(Y-\varepsilon_1)d_2 + 3(X+\varepsilon_0)d_3 + d_4,$$

whose coefficients are in $\mathbb{Z}[d_1, d_2, d_3, d_4, \varepsilon_0, \varepsilon_1]$ and verifying :

$$\begin{aligned} G(v_0, v_1) &\equiv 0 \bmod p, \\ v_1^2 - v_0^3 - av_0 - b, &\equiv 0 \bmod p \end{aligned} \qquad (12)$$

Now, for every choice of $\varepsilon_0, \varepsilon_1$ and d_1, d_2, d_3, d_4 with $d_1 + d_2 \neq 0$, the number of values v_0 satisfying system (12) is at most 6.

We place any solution v_0 into the set $\mathcal{V}(\Delta; a)$. We need to show that the cardinality of $\mathcal{V}(\Delta; a)$ is as claimed in the statement of the theorem.

We write

$$G(X,Y) = (3X^2 - 6X\varepsilon_0 + a)d_1 - 2Yd_2 + 3Xd_3 + A,$$

where $A \equiv -3\varepsilon_0 d_1 + 2\varepsilon_1 d_2 - 3\varepsilon_0 d_3 + d_4 \bmod p$.

By (11) the total number of possible choices for $d_1, d_2, d_3, \varepsilon_0$ is $O(\Delta^5)$. On the other hand, A can take $O(\Delta^3)$ distinct values. Hence there are only $O(\Delta^8)$ values of v_0 that satisfy the system of congruences (12).

Again, to finish the proof we note that the lattice is defined using information we are given, and that the CVP can be solved in deterministic polynomial time in $\log p$ in any fixed dimension. ■

It is well known that the elliptic curve polynomial is absolute irreducible polynomial, then Lemma 3 applies. Obviously this result is non-trivial only for $\Delta < p^{1/8}$. Thus increasing the size of the admissible values of Δ is very interesting.

5 Multivariate polynomials

In this section we consider the natural extension for several variables. Given a multivariate polynomial $F(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1 \ldots, X_n]$ and a point $(w_1, \ldots, w_n)$ whose components approximate those of $(v_1, \ldots, v_n) \in \mathbb{F}_p^n$, where $F(v_1, \ldots, v_n) = 0$, the goal is to recover $(v_1, \ldots, v_n)$.

In many cases the problem has not interest at all. For instance, consider any polynomial $G(Z) \in \mathbb{F}_p[Z]$ and the absolutely irreducible polynomial

$$f(X,Y,Z) = X - Y + g(Z) \in \mathbb{F}_p[X,Y,Z].$$

Then, for each root (v_0, v_1, v_2) of $F(X, Y, Z)$ there is (v_0', v_1', v_2') such that $|v_i - v_i'| < \Delta$:

$$v_0' = v_0 + 1, \quad v_1' = v_1 + 1, \quad v_2' = v_2.$$

However, for other families of polynomials the method introduced in previous sections can be applied. We will illustrate this with the following example.

Theorem 3 *Let p be a prime number and Δ a positive integer such that $p > \Delta \geq 1$. Let*

$$F(X, Y, Z) = Z^2 + aXY + bY + c \in F_p[X, Y, Z].$$

There exists an algorithm with the following properties. When given f (in this case, given a, b and c) and approximations (w_1, w_2, w_3) to (v_1, v_2, v_3) with $|v_i - w_i| \leq \Delta$ and where $F(v_1, v_2, v_3) \equiv 0 \bmod p$, recovers (v_1, v_2, v_3) in polynomial time in $\log p$, provided that (v_1, v_2) does not lie in a certain set $V(\Delta, a, b, c) \subseteq \mathbb{F}_p^2$ of cardinality, $O(p\Delta^5)$.

Proof. The first step of the proof is the same as in two previous sections. We consider $\varepsilon_i = v_i - w_i$, $i = 1, 2, 3$, with $|\varepsilon_i| < \Delta$. Substituting in the polynomial equation

$$F(w_1+\varepsilon_1, w_2+\varepsilon_2, w_3+\varepsilon_3) = (w_3+\varepsilon_3)^2+a(w_1+\varepsilon_1)(w_2+\varepsilon_2)+b = F(v_1, v_2, v_3) \equiv 0 \bmod p.$$

Then, we are looking for the vector $\mathbf{e} \in \mathbb{Z}^4$ which is of the form

$$\mathbf{e} := \left(\Delta\varepsilon_1, \Delta\varepsilon_2, \Delta\varepsilon_3, \varepsilon_3^2 + \varepsilon_1\varepsilon_2\right),$$

and also a solution of the following linear system of congruences:

$$\left\{ \begin{array}{rcl} C_1\Delta X_1 + C_2\Delta X_2 + C_3\Delta X_3 + C_4\Delta^2 X_4 & \equiv & -\Delta^2 C \bmod p \\ X_1 & \equiv & 0 \bmod \Delta \\ X_2 & \equiv & 0 \bmod \Delta \\ X_3 & \equiv & 0 \bmod \Delta; \end{array} \right. \qquad (13)$$

where

$$C_1 = w_2,\ C_2 = b + w_1, C_3 = 2w_3, C_4 = 1, C = F(w_1, w_2, w_3).$$

(Note that the coefficients C_i are the corresponding partial derivatives of f).

Let $\mathbf{f}$ be a vector with smallest Euclidean norm satisfying the above linear system of congruences (13). We may hope that $\mathbf{e}$ and $\mathbf{f}$ are the same, or at least, that we can recover the approximation errors from $\mathbf{f}$. If not, we will show that (v_1, v_2) belongs to the subset $\mathcal{V}(\Delta, a, b, c) \subseteq \mathbb{F}_p^2$. Let us bound the "bad" possibilities for which this process does not succeed. Vector $\mathbf{d} = \mathbf{e} - \mathbf{f} = (\Delta d_1, \Delta d_2, \Delta d_3, d_4)$ lies in the lattice associated to (13):

$$\begin{cases} C_1\Delta X_1 + C_2\Delta X_2 + C_3\Delta X_3 + C_4\Delta^2 X_4 & \equiv & 0 \bmod p \\ X_1 & \equiv & 0 \bmod \Delta \\ X_2 & \equiv & 0 \bmod \Delta \\ X_3 & \equiv & 0 \bmod \Delta. \end{cases} \tag{14}$$

Since $\|\mathbf{e}\| = O(\Delta^2)$, we have that

$$d_1 = O(\Delta), \quad d_2 = O(\Delta), \quad d_3 = O(\Delta), \quad d_4 = O(\Delta^2). \tag{15}$$

If $d_1 \equiv d_2 \equiv d_3 \equiv 0 \bmod p$, then we can recover the root (v_1, v_2, v_3). Hence, we may assume that either d_1 or d_2 or d_3 is nonzero.

Substituting $w_1 = X - \varepsilon_1, w_2 = Y - \varepsilon_2, w_3 = Z - \varepsilon_3$ in the first equation of lattice (14), we obtain a nonzero polynomial modulo p:

$$G(X, Y, Z) = (Y - \varepsilon_2)d_1 + (b + X - \varepsilon_1)d_2 + 2(Z - \varepsilon_3)d_3 + d_4,$$

whose coefficients are in $\mathbb{Z}[d_1, d_2, d_3, d_4, \varepsilon_1, \varepsilon_2, \varepsilon_3]$ and such that

$$G(v_1, v_2, v_3) \equiv 0 \bmod p.$$

Then, we have the following ideal I:

$$\begin{cases} G(v_1, v_2, v_3) & \equiv & 0 \bmod p \\ F(v_1, v_2, v_3) & \equiv & 0 \bmod p. \end{cases} \tag{16}$$

Now, we take the resultant $R(X, Y)$ of G and F with respect the variable Z, then $I \bigcap \mathbb{F}_p[X, Y]$ is a subset of the zero set of $R(X, Y)$. A bound for the cardinality of the zero set of $R(X, Y)$ is $O(p)$.

Now, for every choice of ε_i and d_i the number values (v_1, v_2) satisfying system (16) is $O(p)$.

We place any such solution (v_1, v_2) into the set $\mathcal{V}(\Delta, a, b, c)$. We need to show that the cardinality of $\mathcal{V}(\Delta, a, b, c)$ is as claimed in the statement of the theorem.

We write

$$G(X, Y, Z) = Yd_1 + (b + X)d_2 + 2Zd_3 + A,$$

where $A \equiv -\varepsilon_2 d_1 - \varepsilon_1 d_2 - 2\varepsilon_3 d_3 + d_4 \bmod p$

By (15) , the total number of possible choices for d_i $(i = 1, 2, 3)$ is $O(\Delta^3)$. On the other hand, A can take $O(\Delta^2)$ distinct values. Hence there are only $O(p\Delta^5)$ values of (v_1, v_2) that satisfy the system of congruences (16).

■

The result is only interesting if $p\Delta^5 < p^2$, that is, if $\Delta < p^{1/5}$. Because, F is absolute irreducible we can derive a probabilistic algorithm.

6 Conclusions and Open Problems

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, Algorithm 3.1 can be slightly modified considering different bounds for the approximations errors, i.e. w_0 be a Δ_1-approximation to v_0 and w_1 be a Δ_2-approximation to v_1. Instead of using (2), the following system is introduced:

$$\left\{ \begin{array}{rcl} \displaystyle\sum_{\substack{0\le i\le m_1, 0\le j\le m_2\\ 0<i+j}} \Delta_1^i \Delta_2^j \frac{F^{(i,j)}(w_0, w_1)}{i!j!} X_{i,j} & \equiv & -\Delta_1^{m_1}\Delta_2^{m_2} F(w_0, w_1) \bmod p \\ X_{i,j} & \equiv & 0 \bmod \Delta_1^{m_1-i}\Delta_2^{m_2-j}. \end{array} \right. \tag{17}$$

We present the following theorem which the proof follows the same strategy as in the main one, but now dealing with the above system of congruences (17).

Theorem 4 *With the above notations and definitions; if $F(X, Y) \in \mathbb{F}_p[X, Y]$ is an irreducible polynomial with $m_1 m_2 > 1$, there exists an algorithm recovering (v_0, v_1) in polynomial time in m_1, m_2 and $\log p$ provided that v_0 does not lie in a certain set $\mathcal{V}(\Delta_1, \Delta_2; F) \subseteq \mathbb{F}_p$ of cardinality,*

$$\#\mathcal{V}(\Delta_1, \Delta_2; F) =$$
$$O(((m_1 + 1)(m_2 + 1)2^{(m_1+1)(m_2+1)/2})^{(m_1+1)(m_2+1)} \Delta_1^{\omega^1_{m_1,m_2}} \Delta_2^{\omega^2_{m_1,m_2}}),$$

where

$$\omega^1_{m_1,m_2} = \frac{1}{2}\,(m_2+1)(m_1^2+m_1), \quad \omega^2_{m_1,m_2} = \frac{1}{2}\,(m_1+1)(m_2^2+m_2)$$

As for open problems, we would like to extend the presented theorems for several variables. We think that there are only some special polynomials where the extension of this algorithm does not work.

Also we think that the idea of this method could lead to other improvements as presented in [11]. Although a similar strategy could be applied, it is not obvious how to prove a deterministic results.

References

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

[2] Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor Shparlinski. Predicting nonlinear pseudorandom number generators. *Math. Comput.*, 74(251):1471–1494, 2005.

[3] Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski. Reconstructing noisy polynomial evaluation in residue rings. *J. Algorithms*, 61(2):47–59, 2006.

[4] Johannes Blömer and Alexander May. A tool kit for finding small roots of bivariate polynomials over the integers. In *Advances in Cryptology (Eurocrypt 2005)*, pages 251–267. Springer-Verlag, 2005.

[5] Dan Boneh, Shai Halevi, and Nick Howgrave-Graham. The modular inversion hidden number problem. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 36–51. Springer, Berlin, 2001.

[6] Joan Boyar. Inferring sequences produced by pseudo-random number generators. *J. ACM*, 36(1):129–141, 1989.

[7] Don Coppersmith. Small solutions to polynomial equations, and low exponent rsa vulnerabilities. *J. Cryptology*, 10(4):233–260, 1997.

[8] Don Coppersmith. Finding small solutions to small degree polynomials. In Silverman [24], pages 20–31.

[9] Jean-Sébastien Coron. Finding small roots of bivariate integer polynomial equations: A direct approach. In Alfred, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 379–394. Springer, 2007.

[10] Alan M. Frieze, Johan Håstad, Ravi Kannan, J. C. Lagarias, and Adi Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM J. Comput.*, 17(2):262–280, 1988.

[11] Domingo Gómez, Jaime Gutierrez, and Álvar Ibeas. Attacking the Pollard generator. *IEEE Trans. Inform. Theory*, 52(12):5518–5523, 2006.

[12] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer Verlag, 1988.

[13] Jaime Gutierrez and Álvar Ibeas. Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits. *Des. Codes Cryptography*, 45(2):199–212, 2007.

[14] Nicholas Howgrave-Graham. Finding small roots of univariate modular equations revisited. In *Cryptography and coding (Cirencester, 1997)*, volume 1355 of *Lecture Notes in Comput. Sci.*, pages 131–142. Springer, Berlin, 1997.

[15] Ellen Jochemsz and Alexander May. A strategy for finding roots of multivariate polynomials with new applications in attacking rsa variants. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 267–282. Springer, 2006.

[16] Antoine Joux and Jacques Stern. Lattice reduction: A toolbox for the cryptanalyst. *J. Cryptology*, 11(3):161–185, 1998.

[17] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Math. Oper. Res.*, 12(3):415–440, August 1987.

[18] Hugo Krawczyk. How to predict congruential generators. *J. Algorithms*, 13(4):527–545, 1992.

[19] Arjen K Lenstra, Hendrik W Lenstra, and Lzl Lovsz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515534, 1982.

[20] Danielle Micciancio and Shafi Goldwasser. *Complexity of lattice problems*. Kluwer Academic Publications, 2002.

[21] Phong Q. Nguyen and Jacques Stern. Lattice reduction in cryptology: An update. In Wieb Bosma, editor, *ANTS*, volume 1838 of *Lecture Notes in Computer Science*, pages 85–112. Springer, 2000.

[22] Phong Q. Nguyen and Jacques Stern. The two faces of lattices in cryptology. In Silverman [24], pages 146–180.

[23] Igor E. Shparlinski. *Cryptographic applications of analytic number theory*. Birkhauser, 2003.

[24] Joseph H. Silverman, editor. *Cryptography and Lattices, International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001, Revised Papers*, volume 2146 of *Lecture Notes in Computer Science*. Springer, 2001.

[25] S. A. Stepanov. *Arithmetic of algebraic curves, Monographs in Contemporary Mathematics*. Consultants Bureau, 1994.