RECOVERING ZEROS OF POLYNOMIALS MODULO A PRIME

DOMINGO GÓMEZ AND JAIME GUTIERREZ

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 nonlinear 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 \( F(v_0, v_1) \equiv 0 \mod p \), 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 nonlinear pseudorandom number generators and the linear congruential generator on elliptic curves (see [2, 3, 5, 6, 10, 13, 16]).

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].

For the multivariate case the existing approach \([4, 8, 9, 14, 15]\) 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, so the effectiveness of the method is just heuristic.

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 \(d\). 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 \( G(v_0, v_1) \equiv F(v_0, v_1) \equiv 0 \mod p \). For any nonzero approximation errors, \( \text{Resultant}(G, F; Y) \) has a bounded number of solutions. Now the probabilistic argument follows by taking \( v_0 \) randomly and there are a bounded number of “bad” \( v_0 \) for which we
cannot recover the solution. If our true \( v_0 \) is not among these, the linearization will find only the correct \((v_0, v_1)\).

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 the algorithm and our main result. Section 4 is dedicated to recovering roots for elliptic curve polynomials, and in 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 \( O \). As symbol without a subscript indicates an 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 [16,20–22].

Let \( \{b_1, \ldots, b_s\} \) be a set of linearly independent vectors in \( \mathbb{R}^r \). The set \( \mathcal{L} = \{c_1 b_1 + \cdots + c_s b_s \mid c_1, \ldots, c_s \in \mathbb{Z}\} \) is an \( s \)-dimensional lattice with basis \( \{b_1, \ldots, b_s\} \). 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 \( t \) in \( \mathbb{R}^s \), the goal is to find a vector in the lattice \( \mathcal{L} \) closest to the target vector \( t \). It is well known that this problem is \( \text{NP} \)-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 \( t \), finds a lattice vector \( u \in \mathcal{L} \) satisfying the inequality

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

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 [23,24]), adapted to the special case of \( \mathbb{F}_p \).

**Lemma 2.** If \( F \) is an absolutely irreducible polynomial of total degree \( n \), then

\[
|N - p| = O_n(p^{1/2})
\]

holds.
As a consequence, we have the following:

**Lemma 3.** Suppose that $F$ is an 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. \(\square\)

### 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 [4,7,9,1] build a lattice, then find a basis of short vectors in the lattice and relate the vectors with a polynomial equation. After that, they use resultants that we find the roots of a univariate polynomial over the integers, whereas our algorithm requires finding a small root of a univariate polynomial 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 $\epsilon_0, \epsilon_1$ satisfying $|\epsilon_i| \leq \Delta$ and $[w_i + \epsilon_i]_p = v_i$.

For a bivariate polynomial over the finite field of $p$ elements 

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

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 1) for recovering the root. The parameter $\Delta$ 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 $\epsilon_i = v_i - w_i$ for the approximation errors, we have

$$F(w_0 + \epsilon_0, w_1 + \epsilon_1) \equiv 0 \mod p,$$

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

$$\sum_{i=0}^{m_1} \sum_{j=0}^{m_2} \frac{F(i,j)(w_0, w_1)}{i!j!} \epsilon_0^i \epsilon_1^j \equiv 0 \mod p.$$
Our algorithm seeks a vector
\[
  \mathbf{e} = \left( \Delta^{m_1 + m_2 - i - j} \varepsilon_0^i \varepsilon_1^j \mid 0 \leq i \leq m_1, \ 0 \leq j \leq m_2, \ i + j > 0 \right),
\]
which is a solution of the following linear system of congruences in \((m_1 + 1)(m_2 + 1) - 1\) variables:
\[
  \begin{align*}
    \sum_{0 \leq i \leq m_1, 0 \leq j \leq m_2} \Delta^{i+j} F(i,j)(w_0, w_1) & \equiv -\Delta^{m_1 + m_2} F(w_0, w_1) \mod p, \\
    X_{i,j} & \equiv 0 \mod \Delta^{m_1 + m_2 - i - j}.
  \end{align*}
\]

**Algorithm 1: Recovering algorithm**

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

**Output:** \((v_0, v_1)\) or \((0, 0)\)

1. Compute an approximate solution \(f\) of (2) using the algorithm in [1];
2. \(\gamma_0', \gamma_1' \leftarrow f_1, 0/\Delta^{m_1 + m_2 - 1}, f_0, 1/\Delta^{m_1 + m_2 - 1};\)
3. if \(LM(F(1,0))! = LM(F(0,1))\) then
   4. \(v_0' \leftarrow w_0 + \gamma_0';\)
   5. \(v_1' \leftarrow w_1 + \gamma_1';\)
   6. Take \(\varepsilon_1\) any value s.t. \(F(v_0', w_1 + \varepsilon_1) = 0\) with \(|\varepsilon_1| \leq \Delta;\)
   7. if \(\varepsilon_1\) exists then
      8. (return \((v_0', w_1 + \varepsilon_1);\)
   9. end
   10. Take \(\varepsilon_0\) any value s.t. \(F(w_0 + \varepsilon_0, v_1') = 0\) with \(|\varepsilon_0| \leq \Delta;\)
   11. if \(\varepsilon_0\) exists then
      12. (return \((w_0 + \varepsilon_0, v_1');\)
   13. end
   14. else
   15. \(a \leftarrow LC\ (F(1,0));\)
   16. \(b \leftarrow LC\ (F(0,1));\)
   17. Take \(\varepsilon_0, f(w_0 + \varepsilon_0, w_1 + (b\gamma_1' + a\gamma_0' - a\varepsilon_0)/b) = 0\) with \(|\varepsilon_0| \leq \Delta;\)
   18. if \(\varepsilon_0\) exists then
      19. (return \((w_0 + \varepsilon_0, w_1 + (b\gamma_1' + a\gamma_0' - a\varepsilon_0)/b);\)
   20. else
      21. (return \((0, 0);\)
   22. end
   23. end
   24. return \((0, 0);\)

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

### 3.2. Correctness

In this subsection, we prove in which cases Algorithm [II] returns the correct solution. After proving the result, we will show rigorously that if \(\Delta\) is sufficiently small, then Algorithm [III] returns the root with high probability and we also comment on other interesting consequences.
Theorem 1. Given an irreducible polynomial $F(X,Y) \in \mathbb{F}_p[X,Y]$ with degree $m_1$ in $X$, $m_2$ in $Y$ with $m_1 m_2 > 1$, then Algorithm 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
\[
\#\mathcal{V}(\Delta; F) = O\left( (m_1 + 1)(m_2 + 1)2^{(m_1 + 1)(m_2 + 1)/2} \Delta^{m_1 + m_2} \right),
\]
where
\[
\omega_{m_1, m_2} = 2 + \frac{m_1^2}{2}(2m_2 + 1) + \frac{m_2^2}{2}(2m_1 + 1) + m_1 m_2.
\]

Proof. The theorem is trivial when $O\left( (m_1 + 1)(m_2 + 1)2^{(m_1 + 1)(m_2 + 1)/2} \Delta^{m_1 + m_2} \right) \geq p$, and so we assume that $O\left( (m_1 + 1)(m_2 + 1)2^{(m_1 + 1)(m_2 + 1)/2} \Delta^{m_1 + m_2} \right) < p$. The proof goes as follows. First, fix the polynomial $F$ and assume that $v_0 \in \mathbb{F}_p$ is chosen so as not to lie in certain subsets $U_1(\Delta; F)$, $U_2(\Delta; F)$, $U_3(\Delta; F)$, $\mathcal{V}(\Delta; F)$, which will be defined gradually as we move through the proof. The last step will be to consider $\mathcal{V}(\Delta; F)$, the union of these subsets, and then calculate the cardinality.

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

\[
\sum_{0 \leq i \leq m_1, 0 \leq j \leq m_2} \Delta^{i+j} \frac{F(i,j,w_0,w_1)}{i!j!} X_{i,j} \equiv 0 \mod p,
\]

\[
X_{i,j} \equiv 0 \mod \Delta^{m_1 + m_2 - i - j}.
\]

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

The vector
\[
d = e - f = (\Delta^{m_1 + m_2 - i - j} d_{i,j} \mid 0 \leq i \leq m_1, 0 \leq j \leq m_2, i + j > 0)
\]
lies in $\mathcal{L}$, and so using the first congruence in (3) we obtain
\[
\sum_{0 \leq i \leq m_1, 0 \leq j \leq m_2} \Delta^{i+j} \frac{F(i,j,w_0,w_1)}{i!j!} d_{i,j} \equiv 0 \mod p.
\]

On the other hand, the norm of vector $d$ satisfies
\[
\|d\| \leq \|f\| + \|e\| \leq (2^{(m_1 + 1)(m_2 + 1)/2} + 1)\|e\|,
\]
where the last inequality comes from the application of Lemma 1. Recalling the definition of $e$ in Equation (1), it is an easy bound to the norm of $e$ by $(m_1 + 1)(m_2 + 1)\Delta^{m_1 + m_2}$. Hence
\[
|d_{i,j}| \leq 2^{(m_1 + 1)(m_2 + 1)/2 + 1}(m_1 + 1)(m_2 + 1)\Delta^{m_1 + m_2 - i - j},
\]
\[
0 \leq i \leq m_1, 0 \leq j \leq m_2, i + j > 0.
\]

We remark that if $d_{1,0} \equiv d_{0,1} \equiv 0 \mod p$, then we have $f_{1,0} = \varepsilon_0$, $f_{0,1} = \varepsilon_1$. This implies that we can recover $(v_0, v_1)$. Hence, we may assume that $d_{1,0}$ is nonzero modulo $p$ or $d_{0,1}$ is nonzero 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.
Notice that this polynomial is nonzero, otherwise the polynomial \( F \) has a unique solution unless \( v_0 \) belongs to an exceptional set \( \mathcal{U}_3(\Delta; F) \subset \mathbb{F}_p \) of cardinality \( O(m_1m_2\Delta) \). Assume that \( \varepsilon'_0 \) is another root of Equation (1), and let \( R(X) \in \mathbb{F}_p[X] \) be the resultant of the polynomials \( F(X,Y) \) and \( F(X + \varepsilon'_0 - \varepsilon_0, Y + a(-\varepsilon_0 + \varepsilon'_0)) \) with respect to the variable \( Y \). Since \( |\varepsilon'_0 - \varepsilon_0| \leq 2\Delta \), the number of such polynomials \( R(X) \) is bounded by \( 2\Delta \). 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 \( O(m_1m_2\Delta) \) values of \( v_0 \) in \( \mathcal{U}_3(\Delta; F) \).

**Case 2.** If \( d_{0,1} \equiv 0 \mod p \), then in the same way as the prior case, we place \( O(m_1m_2\Delta) \) values of \( v_0 \) in \( \mathcal{U}_2(\Delta; F) \).

Now, we consider \( d_{1,0}d_{0,1} \neq 0 \mod p \) and substitute \( w_0 = X - \varepsilon_0, w_1 = Y - \varepsilon_1 \) in the congruence (3), to 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 \( b_{i,j} \) depend on \( \varepsilon_0, \varepsilon_1, d_{1,0}, \ldots, d_{m_1m_2} \). It satisfies

\[
G(v_0, v_1) \equiv 0 \mod p.
\]

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

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

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

\[
F(w_0 + x, w_1 + ax + b) \equiv 0 \mod p, \quad \text{with } |x| \leq \Delta.
\]

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 (4) has a unique solution unless \( v_0 \) belongs to an exceptional set \( \mathcal{U}_3(\Delta; F) \subset \mathbb{F}_p \) of cardinality \( O(m_1m_2\Delta) \). Assume that \( \varepsilon'_0 \) is another root of Equation (4), and let \( R(X) \in \mathbb{F}_p[X] \) be the resultant of the polynomials \( F(X,Y) \) and \( F(X + \varepsilon'_0 - \varepsilon_0, Y + a(-\varepsilon_0 + \varepsilon'_0)) \) with respect to the variable \( Y \). Since \( |\varepsilon'_0 - \varepsilon_0| \leq 2\Delta \), the number of such polynomials \( R(X) \) is bounded by \( 2\Delta \). 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 \( F(X + \varepsilon'_0 - \varepsilon_0, Y + a(-\varepsilon_0 + \varepsilon'_0)) \). 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 \( \mathbb{F}_p \):

\[
\begin{align*}
G(X,Y) &\equiv 0 \mod p, \\
F(X,Y) &\equiv 0 \mod p.
\end{align*}
\]
Then, for every choice of \( \varepsilon_0, \varepsilon_1 \) and vector \( \mathbf{d} \) where \( d_{1,0}d_{0,1} \) 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

\[
\Delta^2 + \prod_{0 \leq i \leq m_1, 0 \leq j \leq m_2} \left( 2(m_1 + 1)(m_2 + 1)2^{(m_1+1)(m_2+1)/2}\Delta^{m_1+m_2-i-j} \right)
= O\left( ((m_1 + 1)(m_2 + 1)2^{(m_1+1)(m_2+1)/2}(m_1+1)(m_2+1)\Delta^{\omega_{m_1,m_2}}) \right),
\]

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 an approximation to the Closest Vector Problem can be found in deterministic polynomial time in the bit size of a given basis lattice and in the lattice dimension \((m_1 + 1)(m_2 + 1) - 1\). \( \square \)

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, provided 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 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 \( \Delta \)-approximation, there is only one possible root if \( \Delta \) is small enough. We believe that the roots are spread in many families of irreducible, not necessarily absolutely irreducible polynomials, i.e., given \( F \) and for most \((w_0, w_1)\) and \( \Delta \) sufficiently small, \( F \) has \( O_{m_1,m_2}(1) \) zeros at distance \( \Delta \).

However, several aspects must be taken into account before considering the threshold for \( \Delta \) as the error tolerance upon which the algorithm fails. First, there are 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 necessarily fails. 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, maybe, for such a special 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 $E(F_p)$ be an elliptic curve defined over $F_p$ given by an affine Weierstrass equation, which for $\gcd(p,6) = 1$ takes the form

$$Y^2 = X^3 + aX + b,$$

for some $a, b \in F_p$ with $4a^3 + 27b^2 \neq 0$.

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

**Proof.** Apply Theorem 1 with $m_1 = 3$ and $m_2 = 2$. □

However, we can obtain a better result for the sparse polynomial $\mathbf{8}$.

**Theorem 2.** With the above notation and definitions, there exists a set $\mathcal{V}(\Delta; a) \subseteq F_p$ of cardinality $\#\mathcal{V}(\Delta; a) = O(\Delta^2)$ with the following property. There exists an algorithm which, when given the polynomial $\mathbf{8}$ and $(w_0, w_1) \in \mathbb{Z}^2$, a $\Delta$-approximation to a zero $(v_0, v_1) \in F_p$ of the polynomial $\mathbf{8}$, returns $(v_0, v_1)$ in polynomial time, provided that $v_0$ does not lie in $\mathcal{V}(\Delta; a; b) \subseteq F_p$.

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

$$e := (\Delta^2 \varepsilon_0, \Delta^2 \varepsilon_1, \Delta \varepsilon_2, -\varepsilon_1^2 + \varepsilon_0^2),$$

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

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

Since $\|e\| < 3\Delta^3$, 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 verify

\[
G(v_0, v_1) \equiv 0 \pmod{p},
\]

\[
v_1^2 - v_0^3 - av_0 - b \equiv 0 \pmod{p}
\]

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 \( V(\Delta; a) \). We need to show that the cardinality of \( V(\Delta; a) \) 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 \( A \equiv -3\varepsilon_0^2d_1 + 2\varepsilon_1d_2 - 3\varepsilon_0d_3 + d_4 \pmod{p} \).

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. \( \square \)

It is well known that the elliptic curve polynomial is an absolutely irreducible polynomial, so Lemma 3 applies. Obviously this result is nontrivial only for \( \Delta < p^{1/8} \). Thus increasing the size of the admissible values of \( \Delta \) 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 no 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 \( \Delta \) a positive integer such that \( p > \Delta \geq 1 \). Let

\[
F(X, Y, Z) = Z^2 + aXY + bY + c \in \mathbb{F}_p[X, Y, Z].
\]

There exists an algorithm with the following property: 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 \( F(v_1, v_2, v_3) \equiv 0 \pmod{p} \), it 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 the two previous sections. We consider \( \varepsilon_i = v_i - w_i, \ i = 1, 2, 3, \) with \( |\varepsilon_i| < \Delta. \) Substituting in the polynomial equation

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

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

\[
e := (\Delta \varepsilon_1, \Delta \varepsilon_2, \Delta \varepsilon_3, \varepsilon_1^2 + \varepsilon_1 \varepsilon_2),
\]

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

\[
C_1 \Delta X_1 + C_2 \Delta X_2 + C_3 \Delta X_3 + C_4 \Delta^2 X_4 \equiv -\Delta^2 C \mod p,
\]

\[
\begin{cases}
X_1 \equiv 0 \mod \Delta, \\
X_2 \equiv 0 \mod \Delta, \\
X_3 \equiv 0 \mod \Delta,
\end{cases}
\]

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 \( f \) be a vector with smallest Euclidean norm satisfying the above linear system of congruences \([13]\). We may hope that \( e \) and \( f \) are the same, or at least, that we can recover the approximation errors from \( f. \) 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 \( d = e - f = (\Delta d_1, \Delta d_2, \Delta d_3, d_4) \) lies in the lattice associated to \([13]\):

\[
\begin{cases}
C_1 \Delta X_1 + C_2 \Delta X_2 + C_3 \Delta X_3 + C_4 \Delta^2 X_4 \equiv 0 \mod p, \\
X_1 \equiv 0 \mod \Delta, \\
X_2 \equiv 0 \mod \Delta, \\
X_3 \equiv 0 \mod \Delta.
\end{cases}
\]

Since \( ||e|| = O(\Delta^2) \), we have that

\[
d_1 = O(\Delta), \ d_2 = O(\Delta), \ d_3 = O(\Delta), \ d_4 = O(\Delta^2).
\]

If \( d_1 \equiv d_2 \equiv d_3 \equiv 0 \mod p, \) 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

\[
G(v_1, v_2, v_3) \equiv 0 \mod p.
\]

Then, we have the following ideal \( I: \)

\[
\begin{cases}
G(v_1, v_2, v_3) \equiv 0 \mod p, \\
F(v_1, v_2, v_3) \equiv 0 \mod p.
\end{cases}
\]

Now, we take the resultant \( R(X, Y) \) of \( G \) and \( F \) with respect to the variable \( Z; \) then \( I \cap \mathbb{F}_p[X, Y] \) 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 \( \varepsilon_1 \) and \( d_1 \) the number values of \((v_1, v_2)\) 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 \(A \equiv -\varepsilon_2d_1 - \varepsilon_1d_2 - 2\varepsilon_3d_3 + d_4 \mod p\).

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 \(O(p\Delta^3)\) values of \((v_1, v_2)\) that satisfy the system of congruences in (16).

The result is only interesting if \(p\Delta^5 < p^2\), that is, if \(\Delta < p^{1/5}\). Because \(F\) is absolutely 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 1 can be slightly modified to consider different bounds for the approximations errors, i.e., let \(w_0\) be a \(\Delta_1\)-approximation to \(v_0\) and \(w_1\) be a \(\Delta_2\)-approximation to \(v_1\), for positive integers \(\Delta_1\) and \(\Delta_2\). Instead of using (2), the following system is introduced:

\[
\sum_{0 \leq i \leq m_1, 0 \leq j \leq m_2} \Delta_i \Delta_j \frac{F(i,j)(w_0, w_1)}{i!j!} X_{i,j} \equiv -\Delta_1^{m_1} \Delta_2^{m_2} F(w_0, w_1) \mod p,
\]

\[
X_{i,j} \equiv 0 \mod \Delta_1^{m_1-1} \Delta_2^{m_2-j}.
\]

We present the following theorem, the proof of which follows the same strategy as in Theorem 1 but now deals with the system of congruences in (17).

**Theorem 4.** With the above notations and definitions, if \(F(X, Y) \in \mathbb{F}_p[X, Y]\) is an irreducible polynomial with \(m_1m_2 > 1\), then 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

\[
\#\mathcal{V}(\Delta_1, \Delta_2; F) = O(((m_1 + 1)(m_2 + 1))^{2(m_1+1)(m_2+1)/2} (m_1+1)(m_2+1) \Delta_1^{\omega_{m_1, m_2}^1} \Delta_2^{\omega_{m_1, m_2}^2}),
\]

where

\[
\omega_{m_1, m_2}^1 = \frac{1}{2} (m_2 + 1)(m_1^2 + m_1), \quad \omega_{m_1, m_2}^2 = \frac{1}{2} (m_1 + 1)(m_2^2 + m_2).
\]

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 result.

**Acknowledgement**

This research was partially supported by the Spanish Government project MTM2011-24678.
References


Faculty of Science, University of Cantabria, E-39071 Santander, Spain

E-mail address: gomezd@unican.es

E.T.S. Industrial Engineering and Telecommunications, University of Cantabria, E-39071 Santander, Spain

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