MATHEMATICS OF COMPUTATION
Volume 83, Number 290, November 2014, Pages 2953–2965
S 0025-5718(2014)02808-1
Article electronically published on February 7, 2014

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

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 $\mathbf{d}$. 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 $G(v_0, v_1) \equiv F(v_0, v_1) \equiv 0 \bmod p$. For any nonzero approximation errors, $Resultant(G, F; Y)$ 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

Received by the editor October 29, 2012 and, in revised form, January 16, 2013 and February 6, 2013.

2010 *Mathematics Subject Classification.* Primary 11H06, 11Y16, 12Y05; Secondary 11K16, 11T71.

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

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

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 to find 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*

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

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. *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. □

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, 15] 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 $\varepsilon_0, \varepsilon_1$ 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 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

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

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

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

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 f of (2) using the algorithm in [1];
γ'_0, γ'_1 ← f_{1,0}/Δ^{m_1+m_2-1}, f_{0,1}/Δ^{m_1+m_2-1};
if LM(F^{(1,0)})! = LM(F^{(0,1)}) then
    v'_0 ← w_0 + γ'_0;
    v'_1 ← w_1 + γ'_1;
    Take ε_1 any value s.t. F(v'_0, w_1 + ε_1) = 0 with |ε_1| ≤ Δ.;
    if ε_1 exists then
        (return (v'_0, w_1 + ε_1);
    end
    Take ε_0 any value s.t. F(w_0 + ε_0, v'_1) = 0 with |ε_0| ≤ Δ.;
    if ε_0 exists then
        (return (w_0 + ε_0, v'_1);
    end
else
    a ← LC(F^{(1,0)});
    b ← LC(F^{(0,1)});
    Take ε_0, F(w_0 + ε_0, w_1 + (bγ'_1 + aγ'_0 − aε_0)/b) = 0 with |ε_0| ≤ Δ.;
    if ε_0 exists then
        return (w_0 + ε_0, w_1 + (bγ'_1 + aγ'_0 − aε_0)/b);
    else
        return (0,0)
    end
end
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 1 returns the correct solution. After proving the result, we will show rigorously that if Δ is sufficiently small, then Algorithm 1 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*

$$\#\mathcal{V}(\Delta; F) \quad = \quad O\left((m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2}\Delta^{\omega_{m_1,m_2}}\right),$$

where

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

Proof. The theorem is trivial when $O\left((m_1+1)(m_2+1)2^{(m_1+1)(m_2+1)/2}\Delta^{\omega_{m_1,m_2}}\right) \geq p$, 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 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 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 $\mathbf{x} = (X_{i,j} \mid 0 \leq i \leq m_1,\ 0 \leq j \leq m_2,\ i+j > 0)$ satisfying

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

We compute a solution $\mathbf{t}$ of the linear system of congruences (2), then apply the algorithm of Lemma 1 applied to the vector $\mathbf{t}$ and lattice $\mathcal{L}$ to obtain 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

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

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 an easy bound to the norm of $\mathbf{e}$ by $(m_1+1)(m_2+1)\Delta^{m_1+m_2}$. Hence

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

We remark that if $d_{1,0} \equiv d_{0,1} \equiv 0 \bmod p$, then we have $f_{1,0} = \varepsilon_0, f_{0,1} = \varepsilon_1$. 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.

- Case 1. If $d_{1,0} \equiv 0 \bmod p$, then by bounds (5) we have $d_{1,0} = 0$ and $f_{1,0} = \varepsilon_0$. Compute 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 exists only one v_1 such that (w_0, w_1) is a Δ-approximation to (v_0, v_1) except for v_0 from an exceptional set $\mathcal{U}_1(\Delta; F) \subset \mathbb{F}_p$ of cardinality $O(m_1 m_2 \Delta)$. In fact, to assume $v_1' = w_1 + \varepsilon_1'$ with $|\varepsilon_1'| \le \Delta$, let $R(X) \in \mathbb{F}_p[X]$ be the resultant of the polynomials $F(X, Y)$ and $F(X, Y - \varepsilon_1 + \varepsilon_1')$ with respect the variable Y. Since $|\varepsilon_1' - \varepsilon_1| \le 2\Delta$, the number of such polynomials $R(X)$ is 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 in the same way as the prior case, we place $O(m_1 m_2 \Delta)$ 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), 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 $\varepsilon_0, \varepsilon_1, d_{1,0}, \ldots, d_{m_1,m_2}$. 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 lying in a certain set $\mathcal{U}_3(\Delta; F)$. First, we claim

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

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 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

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

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 an exceptional set $\mathcal{U}_3(\Delta; F) \subset \mathbb{F}_p$ of cardinality $O(m_1 m_2 \Delta)$. Assume that ε_0' is another root of Equation (6), 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 $|\varepsilon_0' - \varepsilon_0| \le 2\Delta$, the number of such polynomials $R(X)$ is 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 $O(m_1 m_2 \Delta)$ 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 $\mathbf{d}$ 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

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

where

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

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 $(m_1+1)(m_2+1)-1$. □

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 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 F and for most (w_0, w_1) and Δ sufficiently small, F has $O_{m_1,m_2}(1)$ zeros at distance Δ.

However, several aspects must be taken into account before considering the threshold for Δ 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 $E(\mathbb{F}_p)$ be an elliptic curve defined over $\mathbb{F}_p$ given by an *affine Weierstrass equation*, which for $\gcd(p,6)=1$ takes the form

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

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

Corollary 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 Theorem 1 with $m_1 = 3$ and $m_2 = 2$. □

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

Theorem 2. *With the above notation and definitions, there exists 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)*, returns* (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 $[w_i + \varepsilon_i]_p = v_i$. 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 $\mathbf{f}$ 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 approximation errors from $\mathbf{f}$. If not, we will show that v_0 belongs to the 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 verify

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

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

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

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

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:

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

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):

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

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:

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

Now, we take the resultant $R(X, Y)$ of G and F with respect to 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 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 $A \equiv -\varepsilon_2 d_1 - \varepsilon_1 d_2 - 2\varepsilon_3 d_3 + d_4 \bmod p$.

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 in (16). $\square$

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 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. Instead of using (2), the following system is introduced:

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

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 $m_1 m_2 > 1$, 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*

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

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 result.

Acknowledgement

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

References

[1] L. Babai, *On Lovász' lattice reduction and the nearest lattice point problem*, Combinatorica **6** (1986), no. 1, 1–13, DOI 10.1007/BF02579403. MR856638 (88a:68049)

[2] Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski, *Predicting nonlinear pseudorandom number generators*, Math. Comp. **74** (2005), no. 251, 1471–1494, DOI 10.1090/S0025-5718-04-01698-9. MR2137013 (2005m:11142)

[3] Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski, *Reconstructing noisy polynomial evaluation in residue rings*, J. Algorithms **61** (2006), no. 2, 47–59, DOI 10.1016/j.jalgor.2004.07.002. MR2281416 (2007j:11168)

[4] Johannes Blömer and Alexander May, *A tool kit for finding small roots of bivariate polynomials over the integers*, Advances in cryptology—EUROCRYPT 2005, Lecture Notes in Comput. Sci., vol. 3494, Springer, Berlin, 2005, pp. 251–267, DOI 10.1007/11426639_15. MR2352192 (2008h:94046)

[5] Dan Boneh, Shai Halevi, and Nick Howgrave-Graham, *The modular inversion hidden number problem*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 36–51, DOI 10.1007/3-540-45682-1_3. MR1934514 (2003h:94022)

[6] Joan Boyar, *Inferring sequences produced by pseudo-random number generators*, J. Assoc. Comput. Mach. **36** (1989), no. 1, 129–141, DOI 10.1145/58562.59305. MR1072416 (91g:68035)

[7] Don Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10** (1997), no. 4, 233–260, DOI 10.1007/s001459900030. MR1476612 (99b:94027)

[8] Don Coppersmith, *Finding small solutions to small degree polynomials*, Cryptography and lattices (Providence, RI, 2001), Lecture Notes in Comput. Sci., vol. 2146, Springer, Berlin, 2001, pp. 20–31, DOI 10.1007/3-540-44670-2_3. MR1903884 (2003f:11034)

[9] Jean-Sébastien Coron, *Finding small roots of bivariate integer polynomial equations: a direct approach*, Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., vol. 4622, Springer, Berlin, 2007, pp. 379–394, DOI 10.1007/978-3-540-74143-5_21. MR2423860 (2009f:12001)

[10] Alan M. Frieze, Johan Håstad, Ravi Kannan, Jeffrey C. Lagarias, and Adi Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, SIAM J. Comput. **17** (1988), no. 2, 262–280, DOI 10.1137/0217016. Special issue on cryptography. MR935340 (89d:11115)

[11] Domingo Gómez, Jaime Gutierrez, and Álvar Ibeas, *Attacking the Pollard generator*, IEEE Trans. Inform. Theory **52** (2006), no. 12, 5518–5523, DOI 10.1109/TIT.2006.885451. MR2300710 (2007m:94160)

[12] Martin Grötschel, László Lovász, and Alexander Schrijver, *Geometric algorithms and combinatorial optimization*, Algorithms and Combinatorics: Study and Research Texts, vol. 2, Springer-Verlag, Berlin, 1988. MR936633 (89m:90135)

[13] Jaime Gutierrez and Álvar Ibeas, *Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits*, Des. Codes Cryptogr. **45** (2007), no. 2, 199–212, DOI 10.1007/s10623-007-9112-3. MR2341883 (2008g:11204)

[14] Nicholas Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, Cryptography and coding (Cirencester, 1997), Lecture Notes in Comput. Sci., vol. 1355, Springer, Berlin, 1997, pp. 131–142, DOI 10.1007/BFb0024458. MR1660500 (99j:94049)

[15] Ellen Jochemsz and Alexander May, *A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 267–282, DOI 10.1007/11935230_18. MR2444641 (2009h:94128)

[16] Antoine Joux and Jacques Stern, *Lattice reduction: a toolbox for the cryptanalyst*, J. Cryptology **11** (1998), no. 3, 161–185, DOI 10.1007/s001459900042. MR1633944 (99c:94031)

[17] Ravi Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res. **12** (1987), no. 3, 415–440, DOI 10.1287/moor.12.3.415. MR906415 (89c:90078)

[18] Hugo Krawczyk, *How to predict congruential generators*, J. Algorithms **13** (1992), no. 4, 527–545, DOI 10.1016/0196-6774(92)90054-G. MR1187200 (93g:65013)

[19] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534, DOI 10.1007/BF01457454. MR682664 (84a:12002)

[20] Daniele Micciancio and Shafi Goldwasser, *Complexity of lattice problems*, The Kluwer International Series in Engineering and Computer Science, 671, Kluwer Academic Publishers, Boston, MA, 2002. A cryptographic perspective. MR2042139 (2004m:94067)

[21] Phong Q. Nguyen and Jacques Stern, *Lattice reduction in cryptology: an update*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 85–112, DOI 10.1007/10722028_4. MR1850600 (2002h:94064)

[22] Phong Q. Nguyen and Jacques Stern, *The two faces of lattices in cryptology*, Cryptography and lattices (Providence, RI, 2001), Lecture Notes in Comput. Sci., vol. 2146, Springer, Berlin, 2001, pp. 146–180, DOI 10.1007/3-540-44670-2_12. MR1903893 (2003d:94082)

[23] Igor Shparlinski, *Cryptographic applications of analytic number theory*, Progress in Computer Science and Applied Logic, vol. 22, Birkhäuser Verlag, Basel, 2003. Complexity lower bounds and pseudorandomness. MR1954519 (2004h:94049)

[24] Joseph H. Silverman (ed.), *Cryptography and lattices*, Lecture Notes in Computer Science, vol. 2146, Springer-Verlag, Berlin, 2001. MR1903881 (2002m:11002)

[25] Serguei A. Stepanov, *Arithmetic of algebraic curves*, Monographs in Contemporary Mathematics, Consultants Bureau, New York, 1994. Translated from the Russian by Irene Aleksanova. MR1321599 (95j:11055)

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