PREDICTING
NONLINEAR PSEUDORANDOM NUMBER GENERATORS

SIMON R. BLACKBURN, DOMINGO GOMEZ-PEREZ, JAIME GUTIERREZ,
AND IGOR E. SHPARLINSKI

ABSTRACT. Let p be a prime and let a and b be elements of the finite field $\mathbb{F}_p$ of p elements. The inversive congruential generator (ICG) is a sequence (u_n) of pseudorandom numbers defined by the relation $u_{n+1} \equiv au_n^{-1} + b \bmod p$. We show that if sufficiently many of the most significant bits of several consecutive values u_n of the ICG are given, one can recover the initial value u_0 (even in the case where the coefficients a and b are not known). We also obtain similar results for the quadratic congruential generator (QCG), $v_{n+1} \equiv f(v_n) \bmod p$, where $f \in \mathbb{F}_p[X]$. This suggests that for cryptographic applications ICG and QCG should be used with great care. Our results are somewhat similar to those known for the linear congruential generator (LCG), $x_{n+1} \equiv ax_n + b \bmod p$, but they apply only to much longer bit strings. We also estimate limits of some heuristic approaches, which still remain much weaker than those known for LCG.

1. INTRODUCTION

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

For fixed $a, b \in \mathbb{F}_p^*$, let $\psi_{a,b}$ be the permutation of $\mathbb{F}_p$ defined by

$$\psi_{a,b}(w) = \begin{cases} aw^{-1} + b, & \text{if } w \neq 0, \\ b, & \text{if } w = 0. \end{cases}$$

We refer to the coefficients a and b as the *multiplier* and *shift*, respectively.

We define the *inversive congruential generator* (u_n) of elements of $\mathbb{F}_p$ by the recurrence relation

$$(1) \qquad u_{n+1} = \psi_{a,b}(u_n), \qquad n = 0, 1, \ldots,$$

where u_0 is the *initial value*.

It is obvious that the sequence (1) is purely periodic with some least period $t \leq p$. It is known when such sequences achieve the largest possible period $t = p$; see [9], [12].

This generator has proved to be extremely useful for quasi–Monte Carlo type applications, and in particular it exhibits very attractive uniformity of distribution and nonlinearity properties; see [30], [31], [32], [33] for surveys or recent results. It is certainly natural to study its cryptographic properties as well.

In the cryptographic setting, the initial value u_0 and the constants a and b are assumed to be the secret key, and we want to use the output of the generator as a stream cipher. Of course, if several consecutive values u_n are revealed, it is easy to find u_0, a and b. So, we output only the most significant bits of each u_n in the hope that this makes the resulting output sequence difficult to predict. The main result of this paper is that not too many bits can be output at each stage: the inversive generator is unfortunately polynomial time predictable if sufficiently many bits of its consecutive elements are revealed.

Assume that the sequence (u_n) is not known, but for some n approximations w_j of k consecutive values u_{n+j}, $j = 0, \ldots, k-1$, are given. We show that the values u_{n+j}, a and b can be recovered from this information if the approximations w_j are sufficiently good.

We also consider this problem for the *quadratic congruential generator*, (v_n) of elements of $\mathbb{F}_p$ given by the recurrence relation

$$(2) \qquad v_{n+1} \equiv f(v_n) \bmod p, \qquad n = 0, 1, \ldots,$$

where v_0 is the *initial value* and $f(X) \in \mathbb{F}_p[X]$ is a quadratic polynomial. In fact we consider only polynomials of the form $f(X) = aX^2 + c$ and as before we refer to the coefficients a and c as the *multiplier* and *shift*, respectively. The case $a = 1$ corresponds to the celebrated *Pollard generator*. The case of general quadratic $f(X) = aX^2 + bX + c$, or even higher degree, polynomials can be considered by our method as well; see [4] for more details (where such generators are considered over arbitrary residue rings too).

For the *linear congruential generator*

$$x_{n+1} \equiv ax_n + b \bmod p, \qquad n = 0, 1, \ldots,$$

similar problems have been introduced by Knuth [22] and then considered in [6], [7], [13], [19], [24]; see also surveys [8], [25]. We remark that some of these papers also consider predicting nonlinear generators, but only in the case when all terms are output in full. Thus the situation we consider here, where only some of the bits of each term are revealed, has not previously been studied for nonlinear generators.

The linear structure of the linear congruential generator lies in the background of the attacks designed in the aforementioned works. The inversive generator (1) has a very high linear complexity [16]. Nevertheless, we show that it still succumbs to a lattice basis reduction based attack, using a certain linearisation technique, somewhat modelled from that of [5]. On the other hand, our results are substantially weaker than those known for the linear congruential generator. We believe they may reflect some inherent difficulties in breaking nonlinear congruential generators.

In some sense the problem we solve can be considered as a special case of the problem of finding small solutions of multivariate polynomial congruences. For polynomial congruences in one variable such an algorithm has been given by Coppersmith [10]; see also [11], [18]. However in the general case only heuristic results are known. Here, due to the special structure of the polynomials involved, we are able to obtain rigorous results.

Throughout the paper the term polynomial time means polynomial in $\log p$. Our results involve another parameter Δ which measures how well the values w_j approximate the terms u_{n+j}. This parameter is assumed to vary independently of p subject to satisfying the inequality $\Delta < p$ (and is not involved in the complexity estimates of our algorithms).

More precisely, we say that w is a Δ-*approximation* to u if $|w - u| \leq \Delta$. In all of our results, the case where Δ grows like a fixed power p^δ where $0 < \delta < 1$ corresponds to the situation where a positive proportion δ of the least significant bits of terms of the output sequence remain hidden.

The remainder of the paper is structured as follows.

We start with a short outline of some basic facts about lattices in subsection 2.1 and rational functions in subsection 2.2.

Then we study the inversive generator. In subsection 3.1, to illustrate our techniques in a simple case, we consider the problem of recovering u_n from the approximations w_j in the case when a and b are both known. In subsection 3.2, we consider the most important case, where neither of a and b are known. It may be relevant to mention that the intermediate case, where only one coefficient is known, has recently been considered in [3].

Then we turn our attention to the quadratic generator. Namely, in subsection 4.1 and subsection 4.2 we consider the cases of quadratic generator with known and unknown multiplier and shift a and c, respectively. We also obtain a more precise result in the special case of the Pollard generator.

In Section 5 we discus the results of numerical tests and some heuristic approaches to the problem.

We conclude with Section 6 which makes some final comments and poses open questions.

2. Preparations

2.1. Background on lattices.

Here we collect several well-known facts about lattices which form the background to our algorithms.

We review several related results and definitions on lattices which can be found in [15]. For more details and more recent references, we also recommend consulting [1], [19], [20], [27], [28], [29].

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

$$\mathcal{L} = \{\mathbf{z} \; : \; \mathbf{z} = c_1\mathbf{b}_1 + \cdots + c_s\mathbf{b}_s, \quad c_1, \ldots, c_s \in \mathbb{Z}\}$$

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

To each lattice $\mathcal{L}$ one can naturally associate its *volume*

$$\mathrm{vol}\,(\mathcal{L}) = (\det(\langle \mathbf{b}_i, \mathbf{b}_j \rangle)^s_{i,j=1})^{1/2},$$

where $\langle \mathbf{a}, \mathbf{b} \rangle$ denotes the standard inner product. The volume of a lattice $\mathcal{L}$ does not depend on the choice of the basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$.

For a vector $\mathbf{u}$, let $\|\mathbf{u}\|$ denote its *Euclidean norm*. The famous Minkowski theorem (see Theorem 5.3.6 in subsection 5.3 of [15]) gives the upper bound

$$(3) \qquad \min\{\|\mathbf{z}\|: \ \mathbf{z} \in \mathcal{L} \setminus \{\mathbf{0}\}\} \le s^{1/2} \operatorname{vol}(\mathcal{L})^{1/s}$$

on the shortest nonzero vector in any s-dimensional lattice $\mathcal{L}$ via its volume. In fact $s^{1/2}$ can be replaced by the *Hermite constant* $\gamma_s^{1/2}$, for which we have

$$\frac{1}{2\pi e}s + o(s) \le \gamma_s \le \frac{1.744}{2\pi e}s + o(s), \qquad s \to \infty.$$

The Minkowski bound (3) motivates a natural question: how can the shortest vector in a lattice be found? Unfortunately, there are several indications that this problem is **NP**-complete (when the dimension grows). However, for a slightly weaker task of finding a short vector, the celebrated *LLL algorithm* of Lenstra, Lenstra and Lovász [26] provides a desirable solution.

On the other hand, if the dimension s of the lattice $\mathcal{L}$ is fixed, then the shortest vector problem can be solved in *deterministic polynomial time* (polynomial in the bit-size of the basis of $\mathcal{L}$). For example, such an algorithm can be found in Section 3 of [21]. This above fact underlies all our *theoretical* results.

For our *heuristic* approach we need to consider lattices of growing dimension. Thus we need to use an approximate algorithm which is related to the celebrated algorithm of Lenstra, Lenstra and Lovász [26]. Many other results on both the exact and approximate finding of a shortest vector in a lattice are discussed in [15], [19], [20], [27], [28], [29]; see also [1] for the most recent developments. In particular, for any constant $\alpha > 0$, the algorithm of [1] finds, in *probabilistic polynomial time*, a nonzero vector $\mathbf{r} \in \mathcal{L}$ with

$$(4) \qquad \|\mathbf{r}\| \le \exp(\alpha\frac{s(\log\log s)^2}{\log s}) \min_{\mathbf{z}\in\mathcal{L}\setminus\{\mathbf{0}\}} \|\mathbf{z}\|.$$

This is slightly stronger than the best known deterministic algorithm for the shortest vector problem. We stress however that we use such approximate algorithms only for heuristic arguments, and it is also known that in practical calculations the above algorithms behave much better than their theoretic prediction. These, more recent achievements, do not however affect our results.

In fact, in this paper we consider only very special lattices. Namely we consider lattices which consist of integer solutions $\mathbf{x} = (x_0, \ldots, x_{s-1}) \in \mathbb{Z}^s$ to the system of congruences

$$\sum_{i=0}^{s-1} a_{ij}x_i \equiv 0 \bmod q_i, \qquad j = 1, \ldots, m,$$

modulo some integers $q_1, \ldots, q_m$. Typically (although not always) the volume of such a lattice is the product $Q = q_1 \cdots q_m$. Moreover all the aforementioned algorithms, when applied to such a lattice, become polynomial in $\log Q$.

2.2. **Zeros of rational functions.** Our second basic tool is essentially the *Lagrange theorem* which asserts that a nonzero polynomial of degree N over any field has no more than N zeros in this field. In fact we apply it to rational functions which require only obvious adjustments.

The rational functions we consider typically belong to a certain family of functions parametrised by small vectors in a certain lattice; thus the size of the family

can be kept under control. Zeros of these rational functions correspond to potentially "bad" initial values of the inversive (1) and quadratic (2) generators. Thus, if we can show that all rational functions in this family are not identical to zero modulo p, then we have an upper bound on the number of such "bad" initial values. Hence, the most crucial part of our approach is to study the possible vanishing of functions in the above family and to show that this may happen only for very few values of the coefficients of the generators (1) and (2). To establish this property, we repeatedly use the fact that nontrivial linear combinations of rational functions with pairwise distinct poles do not vanish.

Having a field structure is important for our arguments as it allows us to use the *Lagrange theorem*. We however remark that with some modifications and adjustments one should be able to obtain similar, albeit weaker, results for nonlinear generators in residue rings. For example, there are several upper bounds on the number of zeros of modular polynomials which can be used instead of the Lagrange theorem; see [23].

3. Predicting the inversive generator

3.1. The inversive generator with known multiplier and shift.
As we have remarked, the most important case for cryptography is when the coefficients a and b of the recurrence relation (1) are unknown. However, this subsection considers the case when a and b are given, partly because this case is probably of independent interest and also because it gives an opportunity to demonstrate our approach in an easier setting. Certainly in this case the result is stronger.

In fact, in this case our method works with only two consecutive values u_0 and u_1. Set $v_0 = u_0$ and $v_1 = u_1 - b$. Then when $u_n \neq 0$, the congruence (1) implies that $v_0 v_1 \equiv a \bmod p$, and the approximations we know for u_0 and u_1 give rise to approximations for v_0 and v_1. So the following theorem proves the result we require.

Theorem 1. *Let p be a prime number and let Δ be an integer such that $p > \Delta \geq 1$. Let $a \in \mathbb{F}_p^*$. There exists a set $\mathcal{V}(\Delta; a) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; a) = O(\Delta^4)$ with the following property. There exists an algorithm which, when given a and Δ-approximations w_0, w_1 to $v_0, v_1 \in \mathbb{F}_p$ such that $v_0 \notin \mathcal{V}(\Delta; a)$ and $v_1 \equiv a/v_0 \bmod p$, returns v_0 and v_1 in deterministic polynomial time.*

Proof. The theorem is trivial when $\Delta^4 \geq p$, and so we assume that $\Delta^4 < p$. We may also assume that $\Delta \geq 2$.

The set $\mathcal{V}(\Delta; a)$ of values v_0 that we are going to exclude consists of $v_0 = 0$ together with those values v_0 satisfying a congruence of the form $d_1 v_0 + a d_2 v_0^{-1} \equiv E \bmod p$ where $|d_1|, |d_2| \leq 4\Delta$, where $|E| \leq 12\Delta^2$ and where at least one of d_1 and d_2 is nonzero modulo p. Note that there are at most $O(\Delta^4)$ choices for d_1, d_2 and E. Once these parameters are chosen, there can be at most two choices for v_0 such that $d_1 v_0 + a d_2 v_0^{-1} \equiv E \bmod p$ (since multiplying both sides of this congruence by v_0 gives a nontrivial quadratic or linear congruence satisfied by v_0). Hence $\#\mathcal{V}(\Delta; a) = O(\Delta^4)$.

Suppose that $v_0 \notin \mathcal{V}(\Delta; a)$.

For $j \in \{0, 1\}$, define $\varepsilon_j = v_j - w_j$. So $|\varepsilon_j| \leq \Delta$. An outline of our proof goes as follows. We aim to show that the integers ε_j occur as certain components of a short vector in a lattice; this lattice can be constructed from the information w_0, w_1 and a that we are given. We find ε_0 and ε_1 by using well-known techniques for finding

short vectors in lattices, and then we use the equality $v_j = w_j + \varepsilon_j$ to recover v_0 and v_1.

We have that

$$(w_0 + \varepsilon_0)(w_1 + \varepsilon_1) \equiv a \bmod p.$$

Writing

$$A \equiv (w_0 w_1 - a)\Delta^{-2} \bmod p, \qquad B_0 \equiv w_0 \Delta^{-1} \bmod p,$$
$$B_1 \equiv w_1 \Delta^{-1} \bmod p, \qquad C \equiv 1 \bmod p,$$

we obtain

$$A\Delta^2 + B_0 \Delta \varepsilon_1 + B_1 \Delta \varepsilon_0 + C\varepsilon_0 \varepsilon_1 \equiv 0 \bmod p.$$

Therefore the lattice $\mathcal{L}$ consisting of integer solutions $\mathbf{x} = (x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ of the system of congruences

$$Ax_0 + B_0 x_1 + B_1 x_2 + Cx_3 \equiv 0 \bmod p,$$
(5)
$$x_0 \equiv 0 \bmod \Delta^2,$$
$$x_1 \equiv x_2 \equiv 0 \bmod \Delta$$

contains a vector

$$\mathbf{e} = (\Delta^2 e_0, \Delta e_1, \Delta e_2, e_3) = (\Delta^2, \Delta \varepsilon_1, \Delta \varepsilon_0, \varepsilon_0 \varepsilon_1).$$

We aim to show that $\mathbf{e}$ is a small vector in the lattice $\mathcal{L}$. We have

$$e_0 = 1, \qquad |e_1|, |e_2| \leq \Delta, \qquad |e_3| \leq \Delta^2;$$

thus the Euclidean norm of $\mathbf{e}$ satisfies the inequality

$$\|\mathbf{e}\| \leq (\Delta^4 + \Delta^4 + \Delta^4 + \Delta^4)^{1/2} = 2\Delta^2.$$

Assume that there is another vector $\mathbf{f} = (\Delta^2 f_0, \Delta f_1, \Delta f_2, f_3) \in \mathcal{L}$ with $\|\mathbf{f}\| \leq \|\mathbf{e}\| \leq 2\Delta^2$ which is not parallel to $\mathbf{e}$. In particular,

$$|f_0| \leq \|\mathbf{f}\| \Delta^{-2} \leq 2, \qquad |f_1|, |f_2| \leq \|\mathbf{f}\| \Delta^{-1} \leq 2\Delta, \qquad |f_3| \leq \|\mathbf{f}\| \leq 2\Delta^2.$$

Define the vector $\mathbf{d}$ by $\mathbf{d} = f_0 \mathbf{e} - e_0 \mathbf{f}$. The first component of the vector $\mathbf{d}$ is zero, and since $\mathbf{d}$ lies in $\mathcal{L}$ the first congruence in (5) implies that

$$B_0 \Delta d_1 + B_1 \Delta d_2 + Cd_3 \equiv 0 \bmod p$$

or

(6)
$$w_0 d_1 + w_1 d_2 \equiv -d_3 \bmod p,$$

where $d_i = e_i f_0 - f_i e_0 = e_i f_0 - f_i$. Note that $|d_i| \leq 2|e_i| + |f_i|$ for $i = 1, 2, 3$ and so our bounds on $|e_i|$ and $|f_i|$ imply that

(7)
$$|d_1|, |d_2| \leq 4\Delta \qquad \text{and} \qquad |d_3| \leq 4\Delta^2.$$

Now, d_1 and d_2 cannot both be 0 modulo p. To see this, suppose for a contradiction that $d_1 \equiv d_2 \equiv 0 \bmod p$. The congruence (6) shows that $d_3 \equiv 0 \bmod p$. But $d_1 \equiv d_2 \equiv d_3 \equiv 0 \bmod p$ implies $d_1 = d_2 = d_3 = 0$, by our upper bounds (7) absolute values of d_1, d_2 and d_3 (because by our assumptions $4\Delta \leq 4\Delta^2 \leq \Delta^4 < p$). But this implies that $\mathbf{d} = 0$ and so $f_0 \mathbf{e} = e_0 \mathbf{f}$. This contradicts the fact that $\mathbf{f}$ and $\mathbf{e}$ are not parallel.

Making the substitutions $w_j = v_j - \varepsilon_j$ in (6), and using the fact that $v_1 \equiv a v_0^{-1} \bmod p$, we find that

(8)
$$d_1 v_0 + a d_2 v_0^{-1} \equiv E \bmod p,$$

where
$$E = -d_3 + \varepsilon_0 d_1 + \varepsilon_1 d_2.$$
The bounds (7) imply that $|E| \leq 12\Delta^2$. But then (8) implies that $v_0 \in \mathcal{V}(\Delta; a)$, and so we have a contradiction. This contradiction shows that there exists no small vector $\mathbf{f}$ in $\mathcal{L}$ other than vectors parallel to $\mathbf{e}$.

To finish the proof, we note that $\mathcal{L}$ is defined using information we are given, and we recall that the shortest vector problem can be solved in deterministic polynomial (in the bit size of a given basis of the lattice) time in any fixed dimension; see [21]. This certainly applies to the lattice $\mathcal{L}$. Once we have found a short vector $\mathbf{f}$ in $\mathcal{L}$, we know that $\mathbf{e} = \mathbf{f}/f_0$ since $\mathbf{f}$ is parallel to $\mathbf{e}$ and since $e_0 = 1$. Obviously, given the third component $\Delta \varepsilon_0$ of $\mathbf{e}$ we can find v_0. This completes the proof. $\qquad \square$

3.2. **The inversive generator with unknown multiplier and shift.** Here we consider probably the most interesting case when both the multiplier a and the shift b are unknown. Our results involve a reasonably small set of exceptional pairs (a, b) for which the algorithm may fail. However it has a complicated structure (thus its definition is given only in the proof of Theorem 2 below).

Theorem 2. *Let p be a prime number and let Δ be an integer such that $p > \Delta \geq 1$. There is a set $\mathcal{C}(\Delta) \subset \mathbb{F}_p^2$ of cardinality $\#\mathcal{C}(\Delta) = O(\Delta^3 p)$ such that for any $a, b \in \mathbb{F}_p^*$ with $(a, b) \notin \mathcal{C}(\Delta)$ there exists a set $\mathcal{U}(\Delta; a, b) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{U}(\Delta; a, b) = O(\Delta^{15})$ having the following property. There exists an algorithm which, when given Δ-approximations w_j, $j = 0, 1, 2, 3$, to four consecutive elements u_0, u_1, u_2, u_3 produced by the inversive generator (1) where $u_0 \notin \mathcal{U}(\Delta; a, b)$, returns u_0, a and b in deterministic polynomial time.*

Proof. We may assume that $\Delta^{15} < p$ (for otherwise the theorem is trivial). Fix $a, b \in \mathbb{F}_p^*$. We assume that $(a, b) \notin \mathcal{C}(\Delta)$, where $\mathcal{C}(\Delta)$ is a set of cardinality $O(\Delta^3 p)$ that we specify below.

We assume that $u_0 \notin \mathcal{U}(\Delta; a, b)$, where $\mathcal{U}(\Delta; a, b)$ is a certain set of cardinality $O(\Delta^{15})$; again, we specify this set below.

We may assume that
$$u_0 u_1 u_2 (u_0 - u_1) \not\equiv 0 \bmod p$$
for we may place the five (or fewer) values of u_0 for which this does not hold into our set $\mathcal{U}(\Delta; a, b)$. From
$$u_1 \equiv a u_0^{-1} + b \bmod p \qquad \text{and} \qquad u_2 \equiv a u_1^{-1} + b \bmod p$$
we derive
$$u_1 u_0 \equiv a + b u_0 \bmod p \qquad \text{and} \qquad u_1 u_2 \equiv a + b u_1 \bmod p.$$
Therefore,
$$(9) \qquad u_1(u_2 - u_0) \equiv b(u_1 - u_0) \bmod p.$$
Similarly
$$u_2(u_3 - u_1) \equiv b(u_2 - u_1) \bmod p.$$
Multiplying the first congruence by $(u_2 - u_1)$ and the second congruence by $(u_1 - u_0)$ and subtracting, we derive
$$(10) \qquad u_1(u_2 - u_0)(u_2 - u_1) - u_2(u_3 - u_1)(u_1 - u_0) \equiv 0 \bmod p.$$

We write $H(u_0, u_1, u_2, u_3)$ for the left-hand side of (10), so

$$H(u_0, u_1, u_2, u_3) = u_0 u_1^2 - 2u_0 u_1 u_2 + u_1 u_2^2 + u_0 u_2 u_3 - u_1 u_2 u_3.$$

For $i \in \{0, 1, 2, 3\}$, we define

$$H_i(u_0, u_1, u_2, u_3) = \frac{\partial}{\partial u_i} H(u_0, u_1, u_2, u_3).$$

Thus,

$$
\begin{aligned}
(11) \qquad
& H_0(u_0, u_1, u_2, u_3) = u_1^2 - 2u_1 u_2 + u_2 u_3, \\
& H_1(u_0, u_1, u_2, u_3) = 2u_0 u_1 - 2u_0 u_2 + u_2^2 - u_2 u_3, \\
& H_2(u_0, u_1, u_2, u_3) = -2u_0 u_1 + 2u_1 u_2 + u_0 u_3 - u_1 u_3, \\
& H_3(u_0, u_1, u_2, u_3) = u_0 u_2 - u_1 u_2.
\end{aligned}
$$

Defining $\varepsilon_j = u_j - w_j$ for $j \in \{0, 1, 2, 3\}$, we obtain

$$
\begin{aligned}
H(u_0, u_1, u_2, u_3) \quad = \quad & H(w_0, w_1, w_2, w_3) + \sum_{i=0}^{3} H_i(w_0, w_1, w_2, w_3)\varepsilon_i \\
& + \sum_{i=0}^{3} w_i G_i(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3) + F(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3),
\end{aligned}
$$

where G_0, G_1, G_2, G_3 are homogeneous polynomials of degree 2 and F is a homogeneous polynomial of degree 3; these polynomials all have constant coefficients (which could be easily evaluated explicitly). We now define

$$A \equiv H(w_0, w_1, w_2, w_3)\Delta^{-3} \bmod p, \qquad B_i \equiv H_i(w_0, w_1, w_2, w_3)\Delta^{-2} \bmod p,$$

$$C_i \equiv w_i \Delta^{-1} \bmod p, \qquad D \equiv 1 \bmod p,$$

for $i = 0, 1, 2, 3$. Therefore the lattice $\mathcal{L}$ consisting of integer solutions $\mathbf{x} = (x_0, \ldots, x_9) \in \mathbb{Z}^{10}$ of the system of congruences

$$
\begin{aligned}
(12) \qquad
& Ax_0 + \sum_{i=0}^{3} B_i x_{i+1} + \sum_{i=0}^{3} C_i x_{i+5} + Dx_9 \equiv 0 \bmod p, \\
& x_0 \equiv 0 \bmod \Delta^3, \\
& x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \bmod \Delta^2, \\
& x_5 \equiv x_6 \equiv x_7 \equiv x_8 \equiv 0 \bmod \Delta
\end{aligned}
$$

contains a vector

$$
\begin{aligned}
\mathbf{e} \quad = \quad & (\Delta^3 e_0, \Delta^2 e_1, \Delta^2 e_2, \Delta^2 e_3, \Delta^2 e_4, \Delta e_5, \Delta e_6, \Delta e_7, \Delta e_8, e_9) \\
= \quad & (\Delta^3, \Delta^2 \varepsilon_0, \Delta^2 \varepsilon_1, \Delta^2 \varepsilon_2, \Delta^2 \varepsilon_3, \Delta G_0(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3), \Delta G_1(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3), \\
& \quad \Delta G_2(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3), \Delta G_3(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3), F(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)).
\end{aligned}
$$

Obviously $\|\mathbf{e}\| = O(\Delta^3)$. Suppose, for a contradiction, that there is another vector

$$\mathbf{f} = (\Delta^3 f_0, \Delta^2 f_1, \Delta^2 f_2, \Delta^2 f_3, \Delta^2 f_4, \Delta f_5, \Delta f_6, \Delta f_7, \Delta f_8, f_9) \in \mathcal{L}$$

with $\|\mathbf{f}\| \leq \|\mathbf{e}\|$ which is not parallel to $\mathbf{e}$. We have,

$$|f_0| \leq \|\mathbf{f}\|\Delta^{-3} = O(1), \qquad |f_1|, |f_2|, |f_3|, |f_4| \leq \|\mathbf{f}\|\Delta^{-2} = O(\Delta),$$

$$|f_5|, |f_6|, |f_7|, |f_8| \leq \|\mathbf{f}\|\Delta^{-1} = O(\Delta^2), \qquad |f_9| \leq \|\mathbf{f}\| = O(\Delta^3).$$

The first component of the vector $\mathbf{d} = f_0\mathbf{e} - e_0\mathbf{f} \in \mathcal{L}$ is zero. Therefore, using the first congruence in (12), we obtain

$$(13) \qquad \sum_{i=0}^{3} B_i d_{i+1} + \sum_{i=0}^{3} C_i d_{i+5} + D d_9 \equiv 0 \bmod p,$$

where $d_i = e_i f_0 - f_i e_0 = e_i f_0 - f_i$, for $i = 1, \ldots, 9$. Hence

$$|d_1|, |d_2|, |d_3|, |d_4| = O(\Delta), \quad |d_5|, |d_6|, |d_7|, |d_8| = O(\Delta^2), \quad |d_9| = O(\Delta^3).$$

Using the definition of B_i, C_i and D, and substituting $w_i = u_i - \varepsilon_i$, we derive from (13) the relation

$$(14) \qquad \sum_{i=0}^{3} H_i(u_0, u_1, u_2, u_3)\widetilde{d}_{i+1} + \sum_{i=0}^{3} u_i \widetilde{d}_{i+5} + \widetilde{d}_9 \equiv 0 \bmod p,$$

where $\widetilde{d}_1, \widetilde{d}_2, \ldots, \widetilde{d}_9$ depend only on $d_1, d_2, \ldots, d_9$ and $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$. It is easy to find explicit expressions for the components of $\widetilde{\mathbf{d}} = (\widetilde{d}_1, \ldots, \widetilde{d}_9)$. However we only need to observe that

$$\widetilde{d}_i = d_i + \delta_i, \qquad i = 1, \ldots, 9,$$

where

- $\delta_1 = \delta_2 = \delta_3 = \delta_4 = 0$;
- $\delta_5, \delta_6, \delta_7, \delta_8$ are linear combinations with constant coefficients of products of one of d_1, d_2, d_3, d_4 with one of $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$;
- δ_9 is a linear combination with constant coefficients of the products $d_5\varepsilon_0$, $d_6\varepsilon_1, d_7\varepsilon_2, d_8\varepsilon_3$ together with the products of one of d_1, d_2, d_3, d_4 with two of $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$.

Therefore, there is an absolute constant κ (which can be easily evaluated explicitly) such that

$$(15) \qquad |\widetilde{d}_1|, |\widetilde{d}_2|, |\widetilde{d}_3|, |\widetilde{d}_4| \leq \kappa\Delta, \quad |\widetilde{d}_5|, |\widetilde{d}_6|, |\widetilde{d}_7|, |\widetilde{d}_8| \leq \kappa\Delta^2, \quad |\widetilde{d}_9| \leq \kappa\Delta^3.$$

Moreover, it is clear from the above form that if $\widetilde{d}_1 = \widetilde{d}_2 = \cdots = \widetilde{d}_9 = 0$, then $d_1 = d_2 = \cdots = d_9 = 0$. Indeed, $\widetilde{d}_1 = \widetilde{d}_2 = \widetilde{d}_3 = \widetilde{d}_4 = 0$ is equivalent to $d_1 = d_2 = d_3 = d_4 = 0$. Then $\delta_5 = \delta_6 = \delta_7 = \delta_8 = \delta_9 = 0$, and thus $\widetilde{d}_5 = \widetilde{d}_6 = \widetilde{d}_7 = \widetilde{d}_8 = \widetilde{d}_9 = 0$ implies that $d_5 = d_6 = d_7 = d_8 = d_9 = 0$.

Let us consider the rational functions

$$\Psi_0(u) = u, \qquad \Psi_1(u) = \frac{bu + a}{u},$$

$$\Psi_2(u) = \frac{(a + b^2)u + ab}{a + bu}, \qquad \Psi_3(u) = \frac{(2ab + b^3)u + a^2 + ab^2}{(a + b^2)u + ab}.$$

We have $u_i = \Psi_i(u_0)$, $i = 0, 1, 2, 3$. We remark that $\Psi_i(u)$ is never a constant function (when $i \neq 0$, this is because $a \not\equiv 0 \bmod p$). We may assume that $a + b^2 \not\equiv 0 \bmod p$, since we may add the $O(p)$ pairs (a, b) such that $a + b^2 \equiv 0 \bmod p$ to our set $\mathcal{C}(\Delta)$. This assumption, together with the fact that $b \not\equiv 0 \bmod p$, implies that none of $\Psi_1(u), \Psi_2(u), \Psi_3(u)$ are linear in u. So each of $\Psi_1(u), \Psi_2(u), \Psi_3(u)$ has a pole, at 0, $-a/b$ and $-ab/(a + b^2)$, respectively. Note that 0, $-a/b$ and $-ab/(a + b^2)$ are distinct elements of $\mathbb{F}_p$.

We may use the functions $\Psi_i(u)$ to eliminate u_1, u_2 and u_3 from (14). For $i \in \{0, 1, 2, 3\}$, define

$$h_i(u) = H_i(\Psi_0(u), \Psi_1(u), \Psi_2(u), \Psi_3(u)).$$

Then (14) can be written as

(16)
$$\sum_{i=0}^{3} h_i(u_0)\widetilde{d}_{i+1} + \sum_{i=0}^{3} \Psi_i(u_0)\widetilde{d}_{i+5} + \widetilde{d}_9 \equiv 0 \bmod p.$$

Let us consider the rational function

$$\Phi_{\widetilde{\mathbf{d}}}(u) = \sum_{i=0}^{3} h_i(u)\widetilde{d}_{i+1} + \sum_{i=0}^{3} \Psi_i(u)\widetilde{d}_{i+5} + \widetilde{d}_9$$

corresponding to the left-hand side of (16).

We aim to show that $\Phi_{\widetilde{\mathbf{d}}}(u)$ can never be a constant function of u_0, but in order for us to do this, we must exclude more pairs (a, b). Indeed, we add to $\mathcal{C}(\Delta)$ those pairs (a, b) that satisfy the following property for $x \equiv -a/b \bmod p$ or $x \equiv -ab/(a + b^2) \bmod p$:

(17)
$$\Psi_0(x) - \Psi_1(x) \equiv r/s \bmod p$$

where s is nonzero and $|r| \leq \kappa\Delta^2$, $|s| \leq \kappa\Delta$ (where κ is as in (15)). In the case when $x \equiv -a/b \bmod p$, the condition (17) is equivalent to the condition $-a \equiv (r/s)b \bmod p$ (to see this, use the fact that $\Psi_1(-a/b) \equiv 0 \bmod p$). For each of the $O(\Delta^3)$ choices of r and s, there are clearly at most p pairs (a, b) satisfying this condition and so we have added at most $O(\Delta^3 p)$ pairs (a, b) to $\mathcal{C}(\Delta)$ in this case. When $x \equiv -ab/(a + b^2) \bmod p$, it is easy to show that the condition (17) is equivalent to

$$-ab^3 + (a + b^2)^2 \equiv (1 + (r/s))(a + b^2)b^2 \bmod p.$$

This is a nontrivial restriction on the pair (a, b), whatever the values of r and s, since the monomial ab^3 always appears. So for each of the $O(\Delta^3)$ choices for r and s, at most $O(p)$ pairs (a, b) satisfy (17). So we have added $O(\Delta^3 p)$ pairs to $\mathcal{C}(\Delta)$ in this case also.

Assume, for a contradiction, that $\Phi_{\widetilde{\mathbf{d}}}(u)$ is a constant function of u. Now, we observe $h_0(u)$ has a double pole at 0, but the other functions $h_1(u), h_2(u), h_3(u), \Psi_0(u), \Psi_1(u), \Psi_2(u)$ and $\Psi_3(u)$ have at most a single pole at 0. So for $\Phi_{\widetilde{\mathbf{d}}}(u)$ to be a constant function, we must have that $\widetilde{d}_1 \equiv 0 \bmod p$. A similar argument involving the double pole at $-a/b$ of $h_1(u)$ shows that $\widetilde{d}_2 \equiv 0 \bmod p$.

We may now write $\Phi_{\widetilde{\mathbf{d}}}(u)$ as the sum of a rational function with no poles at $-ab/(a + b^2)$ and the function

$$\Omega_{\widetilde{\mathbf{d}}}(u) = (\widetilde{d}_3(\Psi_0(u) - \Psi_1(u)) + \widetilde{d}_8)\Psi_3(u).$$

Our assumption that $\Phi_{\widetilde{\mathbf{d}}}(u)$ is a constant function implies that $\Omega_{\widetilde{\mathbf{d}}}(u)$ cannot have a pole at $-ab/(a + b^2)$ and so $\widetilde{d}_3(\Psi_0(u) - \Psi_1(u)) + \widetilde{d}_8$ must have a root at $-ab/(a + b^2)$. If $\widetilde{d}_3 \not\equiv 0 \bmod p$, this would imply that (17) is satisfied when $x \equiv -ab/(a + b^2) \bmod p$, contradicting the fact that $(a, b) \notin \mathcal{C}(\Delta)$. Hence $\widetilde{d}_3 \equiv 0 \bmod p$. We may now argue similarly that $\widetilde{d}_4 \equiv 0 \bmod p$, by writing $\Phi_{\widetilde{\mathbf{d}}}(u)$ as the sum of a function with no poles at $-a/b$ and the rational function

$$\Xi_{\widetilde{\mathbf{d}}}(u) = (\widetilde{d}_4(\Psi_0(u) - \Psi_1(u)) + \widetilde{d}_7)\Psi_2(u)$$

and then using the fact that (17) is not satisfied when $x \equiv -a/b \bmod p$ to prove that $\Xi_{\widetilde{\mathbf{d}}}(u)$ has a pole at $-a/b$ unless $\widetilde{d}_4 \equiv 0 \bmod p$.

It is now easy to see that $\widetilde{d}_5 \equiv \widetilde{d}_6 \equiv \widetilde{d}_7 \equiv \widetilde{d}_8 \equiv 0 \bmod p$ by considering the poles at ∞, 0, $-a/b$ and $-ab/(a+b^2)$, respectively. The congruence (16) then shows that $\widetilde{d}_9 \equiv 0 \bmod p$. Our bounds on the absolute value of the integers $\widetilde{d}_i$ then show that $\widetilde{d}_i = 0$ for all i. But this means that $\mathbf{d} = 0$, which contradicts our assumption that $\mathbf{e}$ and $\mathbf{f}$ are not parallel.

We have shown that if there exists a short vector $\mathbf{f}$ in $\mathcal{L}$ that is not parallel to $\mathbf{e}$, then u_0 must satisfy a congruence of the form (16) for some choice of coefficients $\widetilde{d}_i$. We have also shown that the left-hand side of (16) is nonconstant, and so there are only a bounded number of possibilities for u_0 once the $\widetilde{d}_i$ are chosen. There are at most $O(\Delta^{15})$ choices for the vector $\widetilde{\mathbf{d}}$, and so we may assure ourselves that a congruence (16) is never satisfied by excluding $O(\Delta^{15})$ values of u_0. Once these values are excluded, we see that all short vectors $\mathbf{f}$ in $\mathcal{L}$ are parallel to $\mathbf{e}$. The rest of the proof is identical to the proof of Theorem 1. We also remark that because $u_0 \not\equiv u_1 \bmod p$ for $u_0 \notin \mathcal{U}(\Delta; a, b)$, from the congruence (9) we can determine b (and then a). $\qquad\square$

4. Predicting the quadratic generator

4.1. The quadratic generator with known multiplier and shift.
For a given integer $\Delta > 0$, let $\mathcal{A}(\Delta)$ be the set of $a \in \mathbb{F}_p$ that can be represented as $a \equiv rs^{-1} \bmod p$ with $|r| \leq 4\Delta$, $|s| \leq 4\Delta^2$; thus $\#\mathcal{A}(\Delta) = O(\Delta^3)$.

Theorem 3. *Let p be a prime number and let Δ be an integer such that $p > \Delta \geq 1$. For any $a \in \mathbb{F}_p^*$ and $c \in \mathbb{F}_p$ such that $a \notin \mathcal{A}(\Delta)$, there exists a set $\mathcal{V}(\Delta; a, c) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; a, c) = O(\Delta^4)$ with the following property. There exists an algorithm which, when given a, c and Δ-approximations w_0, w_1 to two consecutive values v_0, v_1 produced by the quadratic generator (2) with $f(X) = aX^2 + c$ where $v_0 \notin \mathcal{V}(\Delta; a, c)$, returns the value of v_0 in deterministic polynomial time.*

Proof. We may assume that $\Delta^4 < p$, for otherwise the theorem is trivially true.

Let $\varepsilon_j = v_j - w_j$, $j = 0, 1$. From

$$v_1 \equiv av_0^2 + c \bmod p,$$

we obtain

$$w_1 + \varepsilon_1 - a(w_0 + \varepsilon_0)^2 - c \equiv 0 \bmod p.$$

Writing

$$A \equiv (w_1 - aw_0^2 - c)\Delta^{-2} \bmod p, \qquad B_1 \equiv -2aw_0\Delta^{-1} \bmod p,$$
$$B_2 \equiv \Delta^{-1} \bmod p, \qquad C \equiv -a \bmod p,$$

we obtain

$$A\Delta^2 + B_1\Delta\varepsilon_0 + B_2\Delta\varepsilon_1 + C\varepsilon_0^2 \equiv 0 \bmod p.$$

Therefore the lattice $\mathcal{L}$ consisting of integer solutions

$$\mathbf{x} = (x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$$

of the system of congruences

$$Ax_0 + B_1 x_1 + B_2 x_2 + C x_3 \equiv 0 \bmod p,$$
$$x_0 \equiv 0 \bmod \Delta^2,$$
$$x_1 \equiv x_2 \equiv 0 \bmod \Delta$$

contains a vector

$$\mathbf{e} = (\Delta^2 e_0, \Delta e_1, \Delta e_2, e_3) = (\Delta^2, \Delta \varepsilon_0, \Delta \varepsilon_1, \varepsilon_0^2).$$

We have

$$e_0 = 1, \qquad |e_1|, |e_2| \leq \Delta, \qquad |e_3| \leq \Delta^2;$$

thus

$$\|\mathbf{e}\| \leq (4\Delta^4)^{1/2} = 2\Delta^2.$$

Assume that there is another vector $\mathbf{f} = (\Delta^2 f_0, \Delta f_1, \Delta f_2, f_3) \in \mathcal{L}$ with $\|\mathbf{f}\| \leq \|\mathbf{e}\| \leq 2\Delta^2$ which is not parallel to $\mathbf{e}$. We have

$$|f_0| \leq 2, \qquad |f_1|, |f_2| \leq 2\Delta, \qquad |f_3| \leq 2\Delta^2.$$

The first component of the vector $f_0 \mathbf{e} - e_0 \mathbf{f} \in \mathcal{L}$ is zero, and hence

$$B_1 \Delta d_1 + B_2 \Delta d_2 + C d_3 \equiv 0 \bmod p,$$

or

(18) $$-2a w_0 d_1 + d_2 - a d_3 \equiv 0 \bmod p,$$

where $d_i = e_i f_0 - f_i$, and thus $|d_i| \leq 2|e_i| + |f_i|$ for $i = 1, 2, 3$. Hence

(19) $$|d_1|, |d_2| \leq 4\Delta, \qquad |d_3| \leq 4\Delta^2.$$

Using the above congruences, we have that if $d_1 \equiv 0 \bmod p$, then $d_2 - a d_3 \equiv 0 \bmod p$. Now, if $d_2 \equiv 0 \bmod p$, then we get a contradiction to the fact that $\mathbf{f}$ and $\mathbf{e}$ are not parallel. Otherwise, we also get a contradiction because $a \notin \mathcal{A}(\Delta)$. So we may assume that $d_1 \not\equiv 0 \bmod p$.

Substituting $w_i = v_i - \varepsilon_i$, $i = 0, 1$, into the congruence (18), we find the congruence

$$-2a d_1 v_0 \equiv E \bmod p,$$

where

$$E = a(-2d_1 \varepsilon_0 + d_3) - d_2.$$

The bound (19) implies that d_1 can take only $O(\Delta)$ distinct values. Moreover, E can take $O(\Delta^3)$ distinct values (because $2d_1 \varepsilon_0 - d_3 = O(\Delta^2)$ and $d_2 = O(\Delta)$). Since $d_1 \not\equiv 0 \bmod p$, this means that there are only $O(\Delta^4)$ values of v_0 that satisfy some congruence of the form (18). We place these values in the set $\mathcal{V}(\Delta; a, c)$. For other values of v_0, the shortest vector $\mathbf{f}$ of the lattice $\mathcal{L}$ is parallel to $\mathbf{e}$. The rest of the proof is identical to the proof of Theorem 1. $\qquad \square$

It is clear that $1 \in \mathcal{A}(\Delta)$; thus Theorem 3 does not apply to the Pollard generator. Hence, now we consider this case separately and in fact obtain a stronger result.

Theorem 4. *Let p be a prime number and let Δ be an integer such that $p > \Delta \geq 1$. For any $c \in \mathbb{F}_p^*$, there exists a set $\mathcal{V}(\Delta; c) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; c) = O(\Delta^3)$ with the following property. There exists an algorithm which, when given Δ-approximations w_j, $j = 0, 1$, to two consecutive values v_0, v_1 produced by the quadratic generator (2) with $f(X) = X^2 + c$ where $v_0 \notin \mathcal{V}(\Delta; c)$, returns the value of v_0 in deterministic polynomial time.*

Proof. We may assume that $\Delta^3 < p$, since otherwise the theorem is trivially true.

Let $\varepsilon_j = v_j - w_j$, $j = 0, 1$. From

$$v_1 \equiv av_0^2 + c \bmod p,$$

we obtain

$$w_1 + \varepsilon_1 - (w_0 + \varepsilon_0)^2 - c \equiv 0 \bmod p.$$

Writing

$$A \equiv (w_1 - w_0^2 - c)\Delta^{-2} \bmod p, \quad B \equiv -2w_0\Delta^{-1} \bmod p, \quad C \equiv 1 \bmod p,$$

we obtain

$$A\Delta^2 + B\Delta\varepsilon_0 + C(\varepsilon_1 - \varepsilon_0^2) \equiv 0 \bmod p.$$

Therefore the lattice $\mathcal{L}$ consisting of integer solutions

$$\mathbf{x} = (x_0, x_1, x_2) \in \mathbb{Z}^3$$

of the system of congruences

$$Ax_0 + Bx_1 + Cx_2 \equiv 0 \bmod p,$$
$$x_0 \equiv 0 \bmod \Delta^2,$$
$$x_1 \equiv 0 \bmod \Delta$$

contains a vector

$$\mathbf{e} = (\Delta^2 e_0, \Delta e_1, e_2) = (\Delta^2, \Delta\varepsilon_0, \varepsilon_1 - \varepsilon_0^2).$$

We have

$$e_0 = 1, \qquad |e_1| \le \Delta, \qquad |e_2| \le 2\Delta^2;$$

thus

$$\|\mathbf{e}\| \le (6\Delta^4)^{1/2} \le 3\Delta^2.$$

Assume that there is another vector $\mathbf{f} = (\Delta^2 f_0, \Delta f_1, f_2) \in \mathcal{L}$ with $\|\mathbf{f}\| \le \|\mathbf{e}\| \le 3\Delta^2$ which is not parallel to $\mathbf{e}$. We have

$$|f_0| \le 3, \qquad |f_1| \le 3\Delta, \qquad |f_2| \le 3\Delta^2.$$

The first component of the vector $f_0\mathbf{e} - e_0\mathbf{f} \in \mathcal{L}$ is zero, and hence

$$B\Delta d_1 + Cd_2 \equiv 0 \bmod p,$$

or

(20) $$-2w_0 d_1 + d_2 \equiv 0 \bmod p,$$

where $d_i = e_i f_0 - f_i$, and thus $|d_i| \le 3|e_i| + |f_i|$ for $i = 1, 2$. Hence

(21) $$|d_1| \le 6\Delta, \qquad |d_2| \le 9\Delta^2.$$

Using the above congruences, we have that if $d_1 \equiv 0 \bmod p$, then $d_2 \equiv 0 \bmod p$ and we get a contradiction to the fact that $\mathbf{f}$ and $\mathbf{e}$ are not parallel.

Substituting $w_0 = v_0 - \varepsilon_0$ into the congruence (20), we find the congruence

$$2d_1 v_0 \equiv E \bmod p,$$

where

$$E = 2d_1\varepsilon_0 + d_2.$$

The bound (21) implies that d_1 can take only $O(\Delta)$ distinct values and $E = O(\Delta^2)$ can take only $O(\Delta^2)$ distinct values. Hence there are only $O(\Delta^3)$ values of v_0 that satisfy some congruence of the form (20). We place these values of v_0 in the set

$\mathcal{V}(\Delta; c)$. For other values of v_0, the shortest vector $\mathbf{f}$ of the lattice $\mathcal{L}$ is parallel to $\mathbf{e}$. The rest of the proof is identical to the proof of Theorem 1. $\square$

4.2. **The quadratic generator with unknown multiplier and shift.** We analyze the general case first, before considering the Pollard generator. Our results require some restrictions on the multiplier. For a given integer $\Delta > 0$, let $\mathcal{A}(\Delta)$ be the set of $a \in \mathbb{F}_p$ that can be represented as $a \equiv rs^{-1} \bmod p$ with $|r| \le 33\Delta$, $|s| \le 77\Delta^2$. Note that $\#\mathcal{A}(\Delta) = O(\Delta^3)$.

Theorem 5. *Let p be a prime number and let Δ be an integer such that $p > \Delta \ge 1$. For any $a \in \mathbb{F}_p^*$ and $c \in \mathbb{F}_p$ with $a \notin \mathcal{A}(\Delta)$, there exists a set $\mathcal{V}(\Delta; a, c) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; a, c) = O(\Delta^{19})$ with the following property. There exists an algorithm which, when given Δ-approximations w_j, $j = 0, 1, 2, 3$, to four consecutive values v_0, v_1, v_2, v_3 produced by the quadratic generator (2) with $f(X) = aX^2 + c$ where $v_0 \notin \mathcal{V}(\Delta; a, c)$, recovers v_0, a and c in deterministic polynomial time.*

Proof. We may assume that $\Delta^{19} < p$, since otherwise the theorem is trivially true.

Moreover, we assume that $v_0^2 - v_1^2 \not\equiv 0 \bmod p$. Clearly there are at most four values of v_0 for which this does not hold. From

$$(22) \qquad v_1 \equiv av_0^2 + c \bmod p, \qquad v_2 \equiv av_1^2 + c \bmod p, \qquad v_3 \equiv av_2^2 + c \bmod p$$

we derive

$$v_0^2 v_2 - v_1^3 + v_1 v_2^2 - v_0^2 v_3 - v_2^3 + v_1^2 v_3 \equiv 0 \bmod p.$$

Let $\varepsilon_j = v_j - w_j$, $j = 0, 1, 2, 3$. Making the substitutions $v_j = w_j + \varepsilon_j$ in the congruence above, we find that

$$A\Delta^3 + B_1\Delta^2\varepsilon_0 + B_2\Delta^2\varepsilon_1 + B_3\Delta^2\varepsilon_2 + B_4\Delta^2\varepsilon_3 + C_1\Delta(\varepsilon_0^2 - \varepsilon_1^2) +$$
$$C_2\Delta(\varepsilon_2\varepsilon_0 - \varepsilon_0\varepsilon_3) + C_3\Delta(\varepsilon_1^2 - 3\varepsilon_2^2 + 2\varepsilon_1\varepsilon_2) +$$
$$C_4\Delta(\varepsilon_2^2 - 3\varepsilon_1^2 + 2\varepsilon_1\varepsilon_3) + D\varepsilon \equiv 0 \bmod p,$$

where

$$(23) \qquad \varepsilon = \varepsilon_2^2\varepsilon_1 - \varepsilon_1^3 + \varepsilon_1^2\varepsilon_3 - \varepsilon_2^3 - \varepsilon_0^2\varepsilon_3 + \varepsilon_0^2\varepsilon_2$$

and

$$A \equiv (w_0^2 w_2 - w_1^3 - w_2^3 + w_2^2 w_1 - w_0^2 w_3 + w_1^2 w_3)\Delta^{-3} \bmod p,$$
$$B_1 \equiv (2w_0 w_2 - 2w_0 w_3)\Delta^{-2} \bmod p,$$
$$B_2 \equiv (w_2^2 - 3w_1^2 + 2w_1 w_3)\Delta^{-2} \bmod p,$$
$$B_3 \equiv (2w_2 w_1 + w_0^2 - 3w_2^2)\Delta^{-2} \bmod p,$$
$$B_4 \equiv (w_1^2 - w_0^2)\Delta^{-2} \bmod p,$$
$$C_1 \equiv (-w_3 + w_2)\Delta^{-1} \bmod p,$$
$$C_2 \equiv 2w_0\Delta^{-1} \bmod p,$$
$$C_3 \equiv w_2\Delta^{-1} \bmod p,$$
$$C_4 \equiv w_1\Delta^{-1} \bmod p,$$
$$D \equiv 1 \bmod p.$$

Therefore the lattice $\mathcal{L}$ consisting of integer solutions $\mathbf{x} = (x_0, x_1, \ldots, x_9) \in \mathbb{Z}^{10}$ of the system of congruences

$$Ax_0 + \sum_{i=1}^{4} B_i x_i + \sum_{i=1}^{4} C_i x_{4+i} + Dx_9 \equiv 0 \bmod p,$$

$$x_0 \equiv 0 \bmod \Delta^3,$$

$$x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \bmod \Delta^2,$$

$$x_5 \equiv x_6 \equiv x_7 \equiv x_8 \equiv 0 \bmod \Delta$$

contains a vector

$$\begin{aligned}
\mathbf{e} &= (\Delta^3 e_0, \Delta^2 e_1, \Delta^2 e_2, \Delta^2 e_3, \Delta^2 e_4, \Delta e_5, \Delta e_6, \Delta e_7, \Delta e_8, e_9) \\
&= (\Delta^3, \Delta^2 \varepsilon_0, \Delta^2 \varepsilon_1, \Delta^2 \varepsilon_2, \Delta^2 \varepsilon_3, \Delta(\varepsilon_0^2 - \varepsilon_1^2), \Delta(\varepsilon_2 \varepsilon_0 - \varepsilon_0 \varepsilon_3), \\
&\qquad \Delta(\varepsilon_1^2 - 3\varepsilon_2^2 + 2\varepsilon_1 \varepsilon_2), \Delta(\varepsilon_2^2 - 3\varepsilon_1^2 + 2\varepsilon_1 \varepsilon_3), \varepsilon),
\end{aligned}$$

where ε is given by (23). We have

$$e_0 = 1, \qquad |e_1|, |e_2|, |e_3|, |e_4| \leq \Delta,$$

$$|e_5|, |e_6| \leq 2\Delta^2, \qquad |e_7|, |e_8| \leq 6\Delta^2, \qquad |e_9| \leq 6\Delta^3;$$

thus

$$\|\mathbf{e}\| \leq (121\Delta^6)^{1/2} = 11\Delta^3.$$

Assume that there is another vector

$$\mathbf{f} = (\Delta^3 f_0, \Delta^2 f_1, \Delta^2 f_2, \Delta^2 f_3, \Delta^2 f_4, \Delta f_5, \Delta f_6, \Delta f_7, \Delta f_8, f_9) \in \mathcal{L}$$

with $\|\mathbf{f}\| \leq \|\mathbf{e}\| \leq 11\Delta^3$ which is not parallel to $\mathbf{e}$. We have

$$|f_0| \leq 11, \qquad |f_1|, |f_2|, |f_3|, f_4| \leq 11\Delta,$$

$$|f_5|, |f_6|, |f_7|, f_8| \leq 11\Delta^2, \qquad |f_9| \leq 11\Delta^3.$$

The first component of the vector $f_0 \mathbf{e} - e_0 \mathbf{f} \in \mathcal{L}$ is zero, and so we obtain

(24) $$\sum_{i=1}^{4} B_i \Delta^2 d_i + \sum_{i=1}^{4} C_i \Delta d_{4+i} + Dd_9 \equiv 0 \bmod p$$

where $d_i = e_i f_0 - f_i e_0 = e_i f_0 - f_i$, and thus $|d_i| \leq 11|e_i| + |f_i|$ for $i = 1, \ldots, 9$. Hence

(25) $$\begin{aligned}
|d_1|, |d_2|, |d_3|, |d_4| &\leq 22\Delta, \qquad |d_5|, |d_6| \leq 33\Delta^2, \\
|d_7|, |d_8| &\leq 77\Delta^2, \qquad |d_9| \leq 77\Delta^3.
\end{aligned}$$

Using the definition of A, B_i, C_i, D and after the substitutions $w_i = v_i - \varepsilon_i$, $i = 0, 1, 2, 3$, and v_i, $i = 1, 2, 3$, in terms of v_0 in the congruence (24), we find

(26) $$F(v_0) \equiv 0 \bmod p$$

for some polynomial

$$F(X) = \sum_{k=0}^{10} \alpha_k X^k \in \mathbb{F}_p[X]$$

where the coefficients α_k, $k = 0, \ldots, 10$, are polynomials in ε_j, $j = 0, \ldots, 3$, and d_i, $i = 1, \ldots, 9$. Using MAPLE, we have computed the coefficients α_i explicitly, and we present some of these explicit expressions below. We claim that F is a nonconstant

polynomial in v_0 of degree at most 10. If we suppose the contrary, then from the explicit formulas

$$\alpha_{10} = 2a^8 d_2 \qquad \text{and} \qquad \alpha_9 = -2a^7 d_1$$

we conclude that if F is a constant polynomial, then

(27) $$d_1 \equiv d_2 \equiv 0 \bmod p.$$

Under the condition (27), the explicit formulas for α_8 and α_6 take the form (note that we do not use α_7)

$$\alpha_8 = -3a^6 d_3 - a^7 d_5 \qquad \text{and} \qquad \alpha_6 = -(12a^5 c - 2a^4)d_3 - 4a^6 c d_5.$$

Thus if $\alpha_8 \equiv \alpha_6 \equiv 0 \bmod p$, then

(28) $$d_3 \equiv d_5 \equiv 0 \bmod p.$$

Under the conditions (27) and (28), the explicit formulas for α_4, α_2 and α_1 take the form (note that we do not use α_5 and α_3)

$$\alpha_4 = a^3 d_7 - a^2 d_4, \quad \alpha_2 = a d_8 + 2a^2 c d_7 + (2ac - 2a\varepsilon_1 - 1)d_4, \quad \alpha_1 = 2d_6 + 2d_4 \varepsilon_0.$$

Then the condition $\alpha_4 \equiv \alpha_2 \equiv \alpha_1 \equiv 0 \bmod p$ leads to

(29) $$d_4 \equiv d_7 a \bmod p, \qquad d_6 \equiv -d_4 \varepsilon_0 \bmod p, \qquad d_8 \equiv -(2\varepsilon_1 a + 1)d_7.$$

If $d_4 \not\equiv 0 \bmod p$, then $d_7 \not\equiv 0 \bmod p$ since $d_4 \equiv d_7 a \bmod p$. But then $d_4 \equiv d_7 a \bmod p$ contradicts the fact that $a \notin \mathcal{A}(\Delta)$. So we may assume that $d_4 \equiv 0 \bmod p$. But then (27), (28) and (29) show that $d_i \equiv 0 \bmod p$, for $i = 1, \dots, 8$, and by (24) it implies that $d_9 \equiv 0 \bmod p$. Again our bounds (25) on $|d_i|$ imply that $d_i = 0$, $i = 1, \dots, 9$, and that $\mathbf{d} = 0$ and so $\mathbf{e}$ and $\mathbf{f}$ are parallel. This contradicts our choice of $\mathbf{f}$.

Since F is a nonconstant polynomial in v_0 of degree at most 10, the congruence (26) can be satisfied for at most ten values of v_0 once d_i, $i = 1, \dots, 9$, and ε_i, $i = 0, \dots, 3$, have been chosen. By (25) the total number of possible vectors $\mathbf{d}$ is $O(\Delta^{15})$. There are also $O(\Delta^4)$ choices for $(\varepsilon_0, \dots, \varepsilon_3)$. Hence there are only $O(\Delta^{19})$ values of v_0 that satisfy some congruence of the form (26). For other values of v_0, the shortest vector $\mathbf{f}$ of the lattice $\mathcal{L}$ is parallel to $\mathbf{e}$. Thus, once again, the rest of the proof is identical to the proof of Theorem 1. We also remark that because $v_0^2 \not\equiv v_1^2 \bmod p$ for $v_0 \notin \mathcal{V}(\Delta; a, c)$, we can find a and c from the congruence (22). $\square$

As before, in the case of the Pollard generator we have a stronger result (which does not involve any exceptional set of parameters).

Theorem 6. *Let p be a prime number and let Δ be an integer such that $p > \Delta \geq 1$. For any $c \in \mathbb{F}_p^*$, there exists a set $\mathcal{V}(\Delta; c) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{V}(\Delta; c) = O(\Delta^4)$ with the following property. There exists an algorithm which, when given Δ-approximations w_j $j = 0, 1, 2$, to three consecutive values v_0, v_1, v_2 produced by the quadratic generator (2) with $f(X) = X^2 + c$ where $v_0 \notin \mathcal{V}(\Delta; c)$, recovers v_0 and c in deterministic polynomial time.*

Proof. We assume that $\Delta^4 < p$, since otherwise the theorem is trivial.
From

$$v_1 \equiv v_0^2 + c \bmod p \qquad \text{and} \qquad v_2 \equiv v_1^2 + c \bmod p,$$

we derive

$$-v_1 + v_0^2 + v_2 - v_1^2 \equiv 0 \bmod p.$$

Let $\varepsilon_j = v_j - w_j$, $j = 0, 1, 2$. Substituting $v_j = w_j + \varepsilon_j$ into the last congruence, we obtain

$$-w_1 - \varepsilon_1 + w_0^2 + 2w_0\varepsilon_0 + \varepsilon_0^2 + w_2 + \varepsilon_2 - w_1^2 - 2w_1\varepsilon_1 - \varepsilon_1^2 \equiv 0 \bmod p.$$

Writing

$$A \equiv (-w_1 + w_0^2 + w_2 - w_1^2)\Delta^{-2} \bmod p, \qquad B_1 \equiv 2w_0\Delta^{-1} \bmod p,$$
$$B_2 \equiv (-1 - 2w_1)\Delta^{-1} \bmod p, \qquad C \equiv 1 \bmod p,$$

we obtain

$$A\Delta^2 + B_1\Delta\varepsilon_0 + B_2\Delta\varepsilon_1 + C(\varepsilon_2 + \varepsilon_0^2 - \varepsilon_1^2) \equiv 0 \bmod p.$$

Therefore the lattice $\mathcal{L}$ consisting of integer solutions

$$\mathbf{x} = (x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$$

of the system of congruences

$$Ax_0 + B_1x_1 + B_2x_2 + Cx_3 \equiv 0 \bmod p,$$
$$x_0 \equiv 0 \bmod \Delta^2,$$
$$x_1 \equiv x_2 \equiv 0 \bmod \Delta$$

contains a vector

$$\mathbf{e} = (\Delta^2 e_0, \Delta e_1, \Delta e_2, e_3) = (\Delta^2, \Delta\varepsilon_0, \Delta\varepsilon_1, \varepsilon_2 + \varepsilon_0^2 - \varepsilon_1^2).$$

We have

$$e_0 = 1, \qquad |e_1|, |e_2| \leq \Delta, \qquad |e_3| \leq 3\Delta^2;$$

thus

$$\|\mathbf{e}\| \leq (12\Delta^4)^{1/2} \leq 4\Delta^2.$$

Assume that there is another vector $\mathbf{f} = (\Delta^2 f_0, \Delta f_1, \Delta f_2, f_3) \in \mathcal{L}$ with $\|\mathbf{f}\| \leq \|\mathbf{e}\| \leq 4\Delta^2$ which is not parallel to $\mathbf{e}$. We have,

$$|f_0| \leq 4, \qquad |f_1|, |f_2| \leq 4\Delta, \qquad |f_3| \leq 4\Delta^2.$$

The first component of the vector $f_0\mathbf{e} - e_0\mathbf{f} \in \mathcal{L}$ is zero, and so we find

$$B_1\Delta d_1 + B_2\Delta d_2 + Cd_3 \equiv 0 \bmod p,$$

or

(30) $$2w_0d_1 + (-1 - 2w_1)d_2 + d_3 \equiv 0 \bmod p,$$

where $d_i = e_if_0 - f_i$, and thus $|d_i| \leq 4|e_i| + |f_i|$ for $i = 1, \ldots, 9$. Hence

(31) $$|d_1|, |d_2| \leq 8\Delta, \qquad |d_3| \leq 16\Delta^2.$$

Using the above congruences, we have that d_1 and d_2 cannot both be 0 modulo p; otherwise we get a contradiction to the fact that $\mathbf{f}$ and $\mathbf{e}$ are not parallel.

Substituting $w_0 = v_0 - \varepsilon_0$, $w_1 = v_0^2 + c - \varepsilon_1$ into congruence (30), we find

$$-2d_2v_0^2 + 2d_1v_0 \equiv E \bmod p,$$

where

$$E = 2\varepsilon_0d_1 - 2\varepsilon_1d_2 + d_2 + 2cd_2 - d_3.$$

The bound (31) implies that d_1 can take only $O(\Delta)$ distinct values and that E can take $O(\Delta^3)$ distinct values (because $d_2 = O(\Delta)$; thus $2cd_2$ can take $O(\Delta)$ distinct values, and $2\varepsilon_0d_1 - 2\varepsilon_1d_2 + d_2 - d_3 = O(\Delta^2)$). Hence there are only $O(\Delta^4)$ values of v_0 that satisfy some congruence of the form (30); we place these values in the

set $\mathcal{V}(\Delta; c)$. For other values of v_0, the shortest vector $\mathbf{f}$ of the lattice $\mathcal{L}$ is parallel to $\mathbf{e}$. The rest of the proof is identical to the proof of Theorem 1.   □

5. Numerical tests and heuristic arguments

5.1. **The inversive generator.** We have implemented the algorithm of Theorem 1 in a **C++** program using the **NTL** library; see [34]. For each level of precision, Δ, we have tested the algorithm for 1000 random examples with 500-bit primes p. For $\Delta = p^{0.24}$ the algorithm was successful in 100% of the cases. In the borderline case $\Delta = p^{0.25}$ the algorithm was successful in about 58% of the cases. For larger values of Δ, namely for $\Delta = p^{0.26}$, the algorithm was successful in only about 2% of the cases (and for $\Delta = p^{0.27}$ it was successful only once, that is, in 0.1% of the cases). This confirms that $\Delta = p^{1/4}$ is indeed the natural threshold for the algorithm of Theorem 1.

The algorithm of Theorem 2 has also been tested 1000 times with 500-bit primes p. For $\Delta = p^{0.065}$ the algorithm was successful in 100% of the cases. Moreover, for $\Delta = p^{0.07}$ it was successful in about 20% of the cases, which indicates that the threshold value $\Delta = p^{1/15}$ of Theorem 2 can probably be improved.

In fact, there is a clear reason for why the result of Theorem 1 is tight while the result of Theorem 2 is not. To estimate the size of the set of exceptional values in the proof of Theorem 1, we find that any exceptional value v_0 must satisfy a congruence of the form (8), where d_1, d_2 and E are small. We then count the number of congruences (8) which can arise by bounding the number of choices for d_1, d_2 and E. However, the corresponding congruence (16) in the proof of Theorem 2 has various coefficients $\widehat{d}_i$ that we have not computed explicitly, and this might well have affected our counting arguments adversely. Moreover, in this case, due to the much higher dimension of the lattice, the influence of the implied constants hidden in the 'O'-symbols is also more substantial.

We now present some heuristic arguments showing that Theorem 1 could possibly be strengthened so that it becomes nontrivial when the precision Δ is of the order of $p^{1/3}$ rather than of order $p^{1/4}$ as currently. Suppose that we are given $k \geq 2$ consecutive Δ-approximations w_j. Denoting $\varepsilon_j = v_j - w_j$, $j = 0, \ldots, k-1$, as in the proof of Theorem 1, we calculate that the vector

$$\mathbf{e} = (\Delta^2, \Delta\varepsilon_0, \ldots, \Delta\varepsilon_{k-1}, \varepsilon_0\varepsilon_1, \ldots, \varepsilon_{k-2}\varepsilon_{k-1})$$

of dimension $s = 2k$ belongs to the lattice $\mathcal{L}$ consisting of integer solutions $\mathbf{x} = (x_0, \ldots, x_{2k-1}) \in \mathbb{Z}^{2k}$ of the system of congruences

$$A_j x_0 + B_{1,j} x_{j+1} + B_{2,j} x_{j+2} + C_j x_{k+j+1} \equiv 0 \bmod p, \qquad j = 0, \ldots, k-2,$$

$$x_0 \equiv 0 \bmod \Delta^2,$$

$$x_1 \equiv \cdots \equiv x_k \equiv 0 \bmod \Delta,$$

where the coefficients $A_j, B_{1,j}, B_{2,j}, C_j, j = 0, \ldots, k-1$, can be explicitly evaluated in terms of $w_0, \ldots, w_{k-1}$ (and, of course, a, b and Δ). The volume of the lattice $\mathcal{L}$ is

$$\mathrm{vol}\,(\mathcal{L}) = p^{k-1} \cdot \Delta^2 \cdot \Delta^k = p^{k-1}\Delta^{k+2}.$$

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

One easily verifies that for any $\varepsilon > 0$ there exists some $\eta > 0$ such that if $\Delta \leq p^{(k-1)/(3k-2)-\varepsilon}$, then

$$\|\mathbf{e}\| = O(\Delta^2) = O(p^{(k-1)/2k-\eta}\Delta^{(k+2)/2k}) = O(\operatorname{vol}(\mathcal{L})^{1/2k}p^{-\eta}).$$

In this case, $\|\mathbf{e}\|$ is substantially smaller than $\operatorname{vol}(\mathcal{L})^{1/2k}$. Therefore, $\mathbf{e}$ is likely to be the only vector (up to a scalar factor) of such a small norm in $\mathcal{L}$. Thus it can be found by one of the shortest vector problem algorithms.

For the case $k = 2$ this reduces to the inequality $\Delta \leq p^{1/4-\varepsilon}$ which corresponds to Theorem 1. However for large k this bound remains heuristic. We also note that when k grows slowly with p, it can be replaced by the bound $\Delta \leq p^{1/3-\varepsilon}$.

We have carried out some numerical testing for this approach too, although due to very high dimension of lattices involved we content ourselves with fewer tests and shorter primes. Here is a selection of our test results. For $\Delta = p^{0.3}$ we tested the algorithm 1000 times with 100-bit primes p and $k = 5$; the algorithm succeeded in about 89% of the cases. For $\Delta = p^{0.32}$ we tested the algorithm 200 times with 100-bit primes p and $k = 10$; the algorithm succeeded in 55% of the cases. These values of k are chosen according to the above heuristic arguments to guarantee that

$$0.3 < \frac{k-1}{3k-2} \qquad \text{and} \qquad 0.32 < \frac{k-1}{3k-2},$$

respectively.

Similar heuristic improvements can be made in the situation of subsection 3.2. Arguing as above in this situation, one verifies that using $k \geq 4$ consecutive Δ-approximations leads to a lattice $\mathcal{L}$ of dimension $s = 6k - 14$ consisting of integer solutions $\mathbf{x} = (x_0, \ldots, x_{6k-15}) \in \mathbb{Z}^{6k-14}$ of the system of congruences

$$A_j x_0 + \sum_{i=0}^{3} B_{i,j} x_{i+j+1} + \sum_{i=0}^{3} C_{i,j} x_{i+k+4j+1} + D_j x_{5k+j-11} \equiv 0 \bmod p,$$

$$j = 0, \ldots, k-4,$$

$$x_0 \equiv 0 \bmod \Delta^3,$$

$$x_1 \equiv \cdots \equiv x_k \equiv 0 \bmod \Delta^2,$$

$$x_{k+1} \equiv \cdots \equiv x_{5k-12} \equiv 0 \bmod \Delta$$

of volume

$$\operatorname{vol}(\mathcal{L}) = p^{k-3} \cdot \Delta^3 \cdot \Delta^{2k} \cdot \Delta^{4k-12} = p^{k-3}\Delta^{6k-9}$$

which contains a vector $\mathbf{e} \in \mathcal{L}$ of norm $\|\mathbf{e}\| = O(\Delta^3)$. One easily verifies that for any $\varepsilon > 0$ there exists some $\eta > 0$ such that if $\Delta \leq p^{(k-3)/(12k-33)-\varepsilon}$, then

$$\|\mathbf{e}\| = O(\Delta^3) = O(p^{(k-3)/(6k-14)-\eta}\Delta^{(6k-9)/(6k-14)}) = O(\operatorname{vol}(\mathcal{L})^{1/(6k-14)}p^{-\eta}).$$

Hence again, in this case, $\|\mathbf{e}\|$ is substantially smaller than $\operatorname{vol}(\mathcal{L})^{1/(6k-14)}$ and can probably be found by one of the shortest vector problem algorithms.

For the case $k = 4$ this reduces to the inequality $\Delta \leq p^{1/15-\varepsilon}$ which corresponds to Theorem 2. When k grows slowly with p, it can be replaced by the bound $\Delta \leq p^{1/12-\varepsilon}$.

It should be noted that in the case of growing k (and in many practical situations even for fixed values of k) one would rather use one of the approximate algorithms

for the shortest vector problem which we have outlined in subsection 2.1. In particular, by (4) we can find a vector $\mathbf{f} \in \mathcal{L}$ with

$$\|\mathbf{f}\| \leq \exp(\alpha \frac{k(\log\log k)^2}{\log k})\|\mathbf{e}\|$$

for some absolute constant $\alpha > 0$. Thus, if $k = O(\log p)$, we still have that, for the same values of Δ, $\|\mathbf{f}\|$ is much smaller than $\mathrm{vol}\,(\mathcal{L})^{1/s}$ for the above lattices $\mathcal{L}$. Thus this does not affect our heuristic arguments and it is very likely that such a vector $\mathbf{f}$ is a scalar multiple of $\|\mathbf{e}\|$.

Here is a brief summary of our test results (again with few and smaller primes). For $\Delta = p^{0.075}$ we tested the algorithm 1000 times with 100-bit primes p and $k = 6$; the algorithm succeeded in about 98% of the cases. For $\Delta = p^{0.08}$ we tested the algorithm 200 times with 100-bit primes p and $k = 10$; the algorithm succeeded in about 50% of the cases. These values of k are chosen according to the above heuristic arguments to guarantee that

$$0.075 < \frac{k-3}{12k-33} \qquad \text{and} \qquad 0.08 < \frac{k-3}{12k-33},$$

respectively.

Note that the algorithm had a relatively low success rate of just over 50% when $k = 10$, whether the parameters a, b are known or not. We believe that this is probably due to the fact that for $k = 10$ the right-hand sides of the corresponding inequalities $0.32142\cdots$ and $0.080459\cdots$ are only barely greater than the left-hand sides 0.32 and 0.08. Of course, the influence of the constants depending on the dimension s of the corresponding lattice, as well as of the fact that LLL finds only a short vector rather than a shortest one, is more significant in these cases (we have $s = 20$ and $s = 46$, respectively).

We have also carried out some selective testing with smaller values of k and discovered that the algorithm is occasionally successful. However, our testing has not been done in a systematic way and it is hard to give any estimates of the success rate in this situation.

5.2. **The quadratic generator.** We have not carried out any numerical tests for the case of the general quadratic generator (that is, for algorithms of Theorems 3 and 5) but rather concentrated on the special case of the Pollard generator. We remark that the lattice corresponding to Theorem 3 is very similar to that of Theorem 1. Moreover, the heuristic extension of the algorithm of Theorem 3 leads to a lattice of the same volume and dimension as that in the case of the inversive generator with known coefficients. We have no reason to suspect that these lattices behave substantially differently to those corresponding to the inversive generator. In particular, we believe that heuristically the quadratic generator with known coefficients a and c can be reconstructed up to the value $\Delta = p^{1/3-\varepsilon}$.

The algorithm of Theorem 4 has been implemented in a **C++** program using the **NTL** library; see [34]. As in the case of Theorem 1, for each level of precision Δ we have tested the algorithm for 1000 random examples with 500-bit primes p and in fact the numerical results are very similar to those for the inversive generator. For $\Delta = p^{0.32}$ the algorithm was successful in 100% of the cases, for $\Delta = p^{0.33}$ the algorithm was successful in about 99% of the cases and for $\Delta = p^{0.34}$ the algorithm was successful in less than 7% of the cases. Therefore, we believe that $\Delta = p^{1/3}$ is indeed the natural threshold for the algorithm of Theorem 4.

Similar tests (1000 trials with 500-bit primes p) for the algorithm of Theorem 6 have revealed that with $\Delta = p^{0.24}$ the algorithm was successful in 100% of the cases, and in the borderline case with $\Delta = p^{0.25}$ the algorithm was successful in about 56% of the cases. For larger values of Δ, namely for $\Delta = p^{0.26}$ it was successful in less than 2% of the cases (and for $\Delta = p^{0.27}$ it was never successful). Thus, these results confirm the sharpness of the threshold $\Delta = p^{1/4}$ for Theorem 6.

Naturally, we have also tried to use heuristic arguments for the Pollard generator. Surprisingly enough, when c is known, they do not seem to lead to any improvements of Theorem 4 leaving the upper bound on the admissible values of Δ at the same level $p^{1/3-\varepsilon}$. However, when c is unknown, heuristic arguments lead to a refinement of the algorithm of Theorem 6.

We now present these calculations showing that when more approximations to consecutive values of a sequence (v_n) given by the Pollard generator $f(X) = X^2 + c$ are available, then the precision Δ could be of order $p^{1/3}$ rather than of order $p^{1/4}$. We assume that we are given $k \geq 3$ consecutive Δ-approximations w_j. Denoting $\varepsilon_j = v_j - w_j$, $j = 0, \ldots, k-1$, as in the proof of Theorem 6 we derive that the vector

$$\mathbf{e} = (\Delta^2, \Delta\varepsilon_0, \ldots, \Delta\varepsilon_{k-2}, \varepsilon_2 + \varepsilon_0^2 - \varepsilon_1^2, \ldots, \varepsilon_{k-1} + \varepsilon_{k-3}^2 - \varepsilon_{k-2}^2)$$

of dimension $s = 2(k-1)$ belongs to the lattice $\mathcal{L}$ consisting of integer solutions $\mathbf{x} = (x_0, \ldots, x_{2k-3}) \in \mathbb{Z}^{2(k-1)}$ of the system of congruences

$$A_j x_0 + B_{1,j} x_{j+1} + B_{2,j} x_{j+2} + C_j x_{k+j} \equiv 0 \bmod p, \qquad j = 0, \ldots, k-3,$$
$$x_0 \equiv 0 \bmod \Delta^2,$$
$$x_1 \equiv \cdots \equiv x_{k-1} \equiv 0 \bmod \Delta,$$

where the coefficients $A_j, B_{1,j}, B_{2,j}, C_j, j = 0, \ldots, k-3$, can be explicitly evaluated in terms of $w_0, \ldots, w_{k-1}, c$ and Δ. The volume of the lattice $\mathcal{L}$ is

$$\mathrm{vol}\,(\mathcal{L}) = p^{k-2} \cdot \Delta^2 \cdot \Delta^{k-1} = p^{k-2}\Delta^{k+1}.$$

One easily verifies that for any $\varepsilon > 0$ there exists some $\eta > 0$ such that if $\Delta \leq p^{(k-2)/(3k-5)-\varepsilon}$, then

$$\|\mathbf{e}\| = O(\Delta^2) = O(p^{(k-2)/(2k-2)-\eta}\Delta^{(k+1)/(2k-2)}) = O(\mathrm{vol}\,(\mathcal{L})^{1/(2k-2)}p^{-\eta}).$$

Hence again, $\|\mathbf{e}\|$ is substantially smaller than $\mathrm{vol}\,(\mathcal{L})^{1/(2k-2)}$ and can probably be found by one of the shortest vector problem algorithms.

For the case $k = 3$ this reduces to the inequality $\Delta \leq p^{1/4-\varepsilon}$ which corresponds to Theorem 6. When k grows slowly with p, it can be replaced by the bound $\Delta \leq p^{1/3-\varepsilon}$.

For $\Delta = p^{0.3}$ and for $\Delta = p^{0.32}$ we need that

$$0.3 < \frac{k-2}{3k-5} \qquad \text{and} \qquad 0.32 < \frac{k-2}{3k-5}$$

which imply $k \geq 6$ and $k \geq 11$, respectively. Accordingly, we have tested 1000 generators with 500-bit primes p for $\Delta = p^{0.3}$ and $k = 6$; the algorithm was successful in 99.7% of the cases. We have also tested 200 generators with 100-bit primes p for $\Delta = p^{0.32}$ and $k = 11$; the algorithm was successful in 99% of the cases.

6. Remarks and open questions

Some of our results exclude certain sets of exceptional parameters. Typically the parameters excluded involve elements $a \in \mathbb{F}_p$ which admit a representation of the form $a \equiv rs^{-1} \bmod p$ with some small integers r and s. First of all we remark that such elements a can easily be tested, and in fact the corresponding r and s can be found by the continued fraction algorithm. Indeed, one sees that if $as = r + kp$ for some integer k, then

$$\frac{a}{p} - \frac{k}{s} = \frac{r}{sp}.$$

Thus if r and s are small enough, k/s gives an anomalously good approximation to a/p which can be achieved only at one of the convergents of the continued fraction expression of a/p. On the other hand, it is natural to ask whether one can deliberately choose the generator coefficients from such exceptional sets in order to obtain cryptographically stronger sequences. We believe that this is not the case, and some modifications to our method can eliminate these exceptional sets completely. In the case of the inversive generator with only one unknown coefficient (that is, in the intermediate situation between Theorem 1 and Theorem 2) the appropriate modifications have been carried out in [3].

As we mentioned in subsection 5.1, the bound on the size of the set of exceptional values of u_0 given in Theorem 2 is probably not tight and might be improved by more careful examination of the structure of the coefficients of rational functions arising in the proof of Theorem 2. Probably this applies to Theorem 5 too. Giving rigorous proofs of our heuristic arguments in Section 5 is a challenging open question as well.

Finally, another "nonlinear" approach to attacking the generators considered here might be feasible. Here we multiply ℓ distinct congruences modulo p and obtain a congruence modulo p^ℓ, as in subsection 3.2 of [5]. However in our case the structure of the variables is more complicated than that of [5], and, after "linearisation" it leads to a lattice of very large dimension. Thus this approach does not seem to provide any advantages. It may be very hard to give any precise rigorous or even convincing heuristic analysis of this approach. For example, it is not clear how to evaluate the volume of the associated lattice (as some of the relations may be linearly dependent).

Our approach also works for congruential generators modulo composite numbers; see [4]. However, as we have mentioned, one of our basic tools, the Lagrange theorem, should be replaced with much weaker bounds which apply to zeros of polynomial congruences modulo composite numbers; see [23].

Unfortunately, we do not know how to predict the nonlinear generators when the modulus p is secret as well. We remark that in the case of the linear congruential generator a heuristic approach to this problem has been proposed in [19]. However it is not clear how to extend the arguments of [19] (even just heuristically) to the case of nonlinear generators.

Recently pseudorandom number generators on elliptic curves have been actively studied; see [2], [14], [17] and references therein. Studying predictability properties of these sequences is a very interesting and important question and is an area ripe for further study.

References

[1] M. Ajtai, R. Kumar and D. Sivakumar, 'A sieve algorithm for the shortest lattice vector problem', *Proc. 33rd ACM Symp. on Theory of Comput.*, ACM, 2001, 601–610.

[2] P. Beelen and J. Doumen, 'Pseudorandom sequences from elliptic curves', *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer-Verlag, Berlin, 2002, 37–52. MR 2004d:11066

[3] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting the inversive generator', *Proc. 9th IMA Intern. Conf on Cryptography and Coding*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **2898** (2003), 264–275.

[4] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Reconstructing noisy polynomial evaluation in residue rings', J. of Algorithms (to appear).

[5] D. Boneh, S. Halevi and N. A. Howgrave-Graham, 'The modular inversion hidden number problem', *Proc. Asiacrypt'2001*, Lect. Notes in Comp. Sci., vol. 2248, Springer-Verlag, Berlin, 2001, 36–51. MR 2003h:94022

[6] J. Boyar, 'Inferring sequences produced by pseudo-random number generators', *J. ACM*, **36** (1989), 129–141. MR 91g:68035

[7] J. Boyar, 'Inferring sequences produced by a linear congruential generator missing low–order bits', *J. Cryptology* **1** (1989) 177–184. MR 90g:94012

[8] E. F. Brickell and A. M. Odlyzko, 'Cryptanalysis: A survey of recent results', *Contemp. Cryptology*, IEEE Press, NY, 1992, 501–540. MR 93k:94009

[9] W.-S. Chou, 'The period lengths of inversive pseudorandom vector generations', *Finite Fields Appl.*, **1** (1995), 126–132. MR 96i:11087

[10] D. Coppersmith, 'Small solutions to polynomial equations, and low exponent RSA vulnerabilities', *J. Cryptology*, **10** (1997), 233–260. MR 99b:94027

[11] D. Coppersmith, 'Small solutions of small degree polynomials', *Proc. Intern. Conf. on Cryptography and Lattices*, Lect. Notes in Comp. Sci., vol. 2146, Springer-Verlag, Berlin, 2001, 20–31. MR 2003f:11034

[12] M. Flahive and H. Niederreiter, 'On inversive congruential generators for pseudorandom numbers', *Finite Fields, Coding Theory, and Advances in Communications and Computing*, Marcel Dekker, New York, 1993, 75–80. MR 94a:11117

[13] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias and A. Shamir, 'Reconstructing truncated integer variables satisfying linear congruences', *SIAM J. Comp.*, **17** (1988), 262–280. MR 89d:11115

[14] G. Gong, T. A. Berson and D. A. Stinson, 'Elliptic curve pseudorandom sequence generators', *Proc. 6th Workshop on Selected Areas in Cryptography*, Lect. Notes in Comp. Sci., vol. 1758, Springer-Verlag, Berlin, 2000, 34–49. MR 2001j:94032

[15] M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer-Verlag, Berlin, 1993. MR 95e:90001

[16] J. Gutierrez, I. E. Shparlinski and A. Winterhof, 'On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators', *IEEE Trans. on Information Theory*, **49** (2003), 60–64.

[17] F. Hess and I. E. Shparlinski, 'On the linear complexity and multidimensional distribution of congruential generators over elliptic curves', *Designs, Codes and Cryptography* (to appear).

[18] N. A. Howgrave-Graham, 'Finding small roots of univariate modular equations revisited', *Proc. 6th IMA Intern. Conf on Cryptography and Coding*, Lect. Notes in Comp. Sci., vol. 1355, Springer-Verlag, Berlin, 1997, 131–142. MR 99j:94049

[19] A. Joux and J. Stern, 'Lattice reduction: A toolbox for the cryptanalyst', *J. Cryptology*, **11** (1998), 161–185. MR 99c:94031

[20] R. Kannan, 'Algorithmic geometry of numbers', *Annual Review of Comp. Sci.*, **2** (1987), 231–267. MR 89a:11131

[21] R. Kannan, 'Minkowski's convex body theorem and integer programming', *Math. Oper. Res.*, **12** (1987), 415–440. MR 89c:90078

[22] D. E. Knuth, 'Deciphering a linear congruential encryption', *IEEE Trans. Inf. Theory* **31** (1985), 49–52. MR 87c:94040

[23] S. V. Konyagin, 'On the number of solutions of a univariate congruence of nth degree', *Matem. Sbornik*, **102** (1979), 171–187 (in Russian). MR 80k:10013a

[24] H. Krawczyk, 'How to predict congruential generators', *J. Algorithms*, **13** (1992), 527–545. MR 93g:65013

[25] J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143. MR 92f:11109

[26] A. K. Lenstra, H. W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', *Mathematische Annalen*, **261** (1982), 515–534. MR 84a:12002

[27] D. Micciancio and S. Goldwasser, *Complexity of lattice problems*, Kluwer Acad. Publ., 2002.

[28] P. Q. Nguyen and J. Stern, 'Lattice reduction in cryptology: An update', *Proc. 4th Intern. Symp. on Algorithmic Number Theory*, Lect. Notes in Comp. Sci., vol. 1838, Springer-Verlag, Berlin, 2000, 85–112. MR 2002h:94064

[29] P. Q. Nguyen and J. Stern, 'The two faces of lattices in cryptology', *Proc. Intern. Conf. on Cryptography and Lattices*, Lect. Notes in Comp. Sci., vol. 2146, Springer-Verlag, Berlin, 2001, 146–180. MR 2003d:94082

[30] H. Niederreiter, 'New developments in uniform pseudorandom number and vector generation', *Monte Carlo and Quasi–Monte Carlo Methods in Scientific Computing*, Lect. Notes in Statistics, vol. 106, Springer-Verlag, Berlin, 1995, 87–120. MR 97k:65019

[31] H. Niederreiter, 'Design and analysis of nonlinear pseudorandom number generators', *Monte Carlo Simulation*, A.A. Balkema Publishers, Rotterdam, 2001, 3–9.

[32] H. Niederreiter and I. E. Shparlinski, 'Recent advances in the theory of nonlinear pseudorandom number generators', *Proc. Conf. on Monte Carlo and Quasi–Monte Carlo Methods, 2000*, Springer-Verlag, Berlin, 2002, 86–102. MR 2003k:65005

[33] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Proc. the 15th Symp. on Appl. Algebra, Algebraic Algorithms, and Error-Correcting Codes*, Lect. Notes in Comp. Sci., vol. 2643, Springer-Verlag, Berlin, 2003, 6–17.

[34] V. Shoup, 'Number theory **C++** library (NTL)', version 5.3.1, available at `http://www.shoup.net/ntl/`.

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY, UNIVERSITY OF LONDON, EGHAM, SURREY, TW20 0EX, UNITED KINGDOM
    E-mail address: `s.blackburn@rhul.ac.uk`

FACULTY OF SCIENCE, UNIVERSITY OF CANTABRIA, E-39071 SANTANDER, SPAIN
    E-mail address: `gomezd@unican.es`

FACULTY OF SCIENCE, UNIVERSITY OF CANTABRIA, E-39071 SANTANDER, SPAIN
    E-mail address: `jaime.gutierrez@unican.es`

DEPARTMENT OF COMPUTING, MACQUARIE UNIVERSITY, SYDNEY, NSW 2109, AUSTRALIA
    E-mail address: `igor@comp.mq.edu.au`