MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 194
APRIL 1991, PAGES 823–849

GENERATION OF ELEMENTS WITH SMALL MODULAR SQUARES AND PROVABLY FAST INTEGER FACTORING ALGORITHMS

BRIGITTE VALLÉE

ABSTRACT. Finding small modular squares, when the modulus is a large composite number of unknown factorization, is almost certainly a computationally hard problem. This problem arises in a natural way when factoring the modulus by the use of congruences of squares. We study here, with the help of lattices, the set of elements whose squares $\bmod n$ are small enough, less than $O(n^{2/3})$. We obtain a precise description of the gaps between such elements, and we develop two polynomial-time algorithms that find elements with small modular squares. The first is a randomized algorithm that generates such elements in a near uniform way. We use it to derive a class of integer factorization algorithms, the fastest of which provides the best rigorously established probabilistic complexity bound for integer factorization algorithms. The second algorithm is deterministic and often finds, amongst the neighbors of a given point, the nearest one that has a small modular square.

INTRODUCTION

At present, two of the most efficient factorization algorithms are the polynomial sieve algorithm and the continued fraction algorithm, which are based on congruences of squares. In order to factor n by using such algorithms, one has to find x, y such that $x^2 \equiv y^2 \bmod n$ and $x \not\equiv \pm y \bmod n$. The problem reduces to obtaining many *smooth* quadratic residues modulo n, a smooth number being a number which is composed solely of small prime factors. It is intuitively clear that smaller numbers are more likely to be smooth. One can precisely quantify this correlation with the help of the function $L(n) = \exp\sqrt{\log n \log\log n}$, and this function plays a central role in the complexity of integer factorization.

There are two different approaches: one is heuristic and leads to fast practical algorithms; the other is rigorous (appealing to no unproven assumption) but leads to less efficient algorithms.

(A) In the most practical factorization algorithms due to Morrison and Brillhart [4] or Pomerance [5, 7], one uses quadratic residues modulo n, of absolute value less than $n^{1/2+o(1)}$, that are produced in a deterministic way. Since these algorithms use small quadratic residues, they are efficient in practice. However,

Received April 1, 1989; revised September 25, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y05, 11Y16; Secondary 11B57, 11Hxx.

the analysis of their complexity cannot be done, unless one appeals to ad hoc *heuristic hypotheses* asserting that the numbers used are "pseudorandom" with respect to smoothness. One obtains in this way [5] a class of algorithms with nonrigorously proved complexity bounds in the range $L(n)^{\sqrt{2}}$ to $L(n)$.

(B) On the other hand, Dixon [3] uses purely random quadratic residues, so that one can *prove* the complexity of the corresponding class of probabilistic algorithms. However, since the quadratic residues used are only bounded by n, the algorithms are not as efficient in practice and their run times range from $L(n)^2$ to $L(n)^{\sqrt{2}}$ [6].

Here, we show that some of the good aspects of both worlds can be combined: We consider the set B of the elements whose squares modulo n are less than $4n^{2/3}$, and, by a detailed study of their distribution, we are able to produce a polynomial-time algorithm that generates the elements of this set in an almost uniform way. We apply this result to integer factorization and obtain a class of probabilistic algorithms whose time-complexity bounds are proved to be in the range $L(n)^{\sqrt{8/3}}$ to $L(n)^{\sqrt{4/3}}$. More precisely, the main result of this paper is a description of a rigorous, random factoring algorithm of time complexity $L(n)^{\sqrt{4/3}+o(1)}$ on input of the integer n. This last bound, with exponent near $\sqrt{4/3} = 1.1547$, is the best rigorous complexity bound established so far for integer factoring algorithms.[1]

In order to study the set B, we construct a particular covering of the integers $\bmod n$ for which the distribution of B is globally uniform: This covering is made with *Farey intervals* [1] which each contain almost exactly the number of elements of B that one should expect if the distribution of B were actually uniform. Locally, in each of these subsets, we build on methods we developed earlier for "guessing" lth roots $\bmod n$ [8]. We transfer our problem to lattices and use very natural properties in the geometry of numbers to solve an integer programming problem: *Describe, in an algorithmic way, points of a two-dimensional lattice which lie between two parabolas.* From there, we obtain a precise description of this set B, and we derive two polynomial-time algorithms which allow one to generate locally the elements of B. The first realizes a random drawing from B in an almost uniform way, while the second determines the two neighbors of an element of B.

Our paper is organized as follows: In §1, we describe a general framework for integer factorization algorithms, which covers most classical methods. We obtain general conditions (Theorem 2) under which a rigorous time-complexity bound can be derived. Amongst these conditions, a natural one emerges, namely the ability to describe precisely the set $B(\alpha)$ of the numbers whose square $\bmod n$ is less than n^{α}, with $0 < \alpha \leq 1$. First, we give a sharper estimate of the cardinality of this set when $\alpha > 1/2$ (Theorem 3).

---

[1]Note added May 1, 1990. Since this work was completed, H. W. Lenstra, Jr. and C. Pomerance have announced a rigorous complexity bound of $L(n)^{1+o(1)}$ for integer factorization.

In the sequel of the paper, we show how to study this set when α is near $2/3$. We consider the set B of numbers whose squares mod n are less than $4n^{2/3}$, and, by a *local use of lattices*, we obtain a description of this set that proves the facts that we observed in our numerical experiments (Theorems 4 and 7): We explain the occurrence of a regular pattern in the gaps between successive elements of B (Theorem 7) and we prove that there is a global balance in the variations of these gaps (Theorem 4).

This description is efficient enough to give rise to two polynomial-time algorithms: With Theorem 5, we show how to draw random elements of B both in polynomial time and in an almost uniform way. We thus obtain a condition, namely the *Uniformity Condition*, from which we deduce Theorem 6, which provides our complexity bound for integer factoring. In Theorem 8, we adopt a deterministic point of view. We determine in polynomial time the two elements of B which surround a given point.

We finish by comparing our results to the previously known ones, from the two points of view of theoretical number theory and computational number theory.

A preliminary presentation of some of these results appears in [9].

1. The α-Dixon method

Complexity bounds for the class of factorization algorithms that we describe here can be expressed mainly in terms of the function

$$L(n) = \exp\sqrt{\log n \log\log n}.$$

(Henceforth, $\log x = \log_e x$.) L^α is a shorthand notation for the class of functions $L(n)^{\alpha+o(1)}$, and we call *exponent* of f the number α defined by the relation $f \in L^\alpha$. Let $Z(n)$ denote the ring of the integers modulo n that we identify with the integers in the interval of length n centered at 0; we denote by Q the squaring operation in $Z(n)$:

$$Q(x) = x^2 \text{ modulo } n.$$

For two reals α and β, with $0 \leq \alpha \leq 1$, we shall deal with the two related sets:

$$B(\alpha) = \{x \in Z(n) \mid |Q(x)| \leq n^\alpha\},$$

$$F(\alpha, \beta) = \{x \in B(\alpha) \mid |Q(x)| \text{ is composed solely of primes } p \leq L(n)^\beta\}.$$

1.1. **The α-Dixon algorithm.** It is natural to consider a generalization of Dixon's factorization method [3] which operates with elements of $B(\alpha)$ in order to find elements of $F(\alpha, \beta)$, and we call it Dixon's α-method, or $D[\alpha]$ for short. It reduces to the standard Dixon's method when taking $\alpha = 1$, and we recover the general framework of both the continued fractions algorithm and the quadratic sieve method when taking α near $1/2$. The algorithm $D[\alpha]$ involves four main steps and two parameters β and γ that will be adjusted later. Its description is as follows.

(1) Look for all prime factors of n less than $L(n)$, and remove them.

(2) Consider the set P of the prime numbers less than $L(n)^{\beta}$; perform $L(n)^{\gamma}$ draws from $B(\alpha)$ in order to obtain $L(n)^{\beta}$ elements x_j of $F(\alpha, \beta)$ (i.e., completely factored in P).

$$\text{For all } j \leq L(n)^{\beta}, \text{ one has: } Q(x_j) = \prod_{\{i|p_i \in P\}} p_i^{m_{ij}}.$$

(3) Consider the matrix M formed with the coefficients $m_{ij} \bmod 2$. By means of Gaussian elimination on M in the field $GF(2)$, look for a subset J such that $\prod_{j\in J} Q(x_j)$ is a square, denoted by y^2. Then, $x^2 = \prod_{j\in J} x_j^2$ is congruent to y^2 modulo n.

(4) If the congruence $x^2 \equiv y^2$ $[n]$ is nontrivial, it provides a nontrivial factorization of n.

The main problem that we encounter in analyzing the complexity of such an algorithm is the determination of γ from the values of α and β. This can be done if the following two conditions are fulfilled:

Counting Condition. We can determine the probability that an element of $B(\alpha)$ belongs to the set $F(\alpha, \beta)$.

Uniformity Condition. We can draw from the set $B(\alpha)$ in polynomial time and in an almost uniform way.

Under these conditions, we know how to choose γ as a function of α and β. Next, we determine the optimal value of β as a function of α, and we obtain the complexity bound for the algorithm $D[\alpha]$.

1.2. **Formalizing the Uniformity Condition.** Let us first make the Uniformity Condition precise:

Definition 1. Let $l = (l_1, l_2)$ be a pair of positive constants. A drawing algorithm C, defined over a finite set U with the uniform probability P, and with values in a subset X of $Z(n)$, is said to be l-uniform if for all $x \in X$, one has

$$\frac{l_1}{|X|} \leq P(u \in U | C(u) = x) \leq \frac{l_2}{|X|}.$$

We consider now a family of such drawing algorithms obtained when the index n varies. Then U, P, X, etc. *may depend on the integer* n. We will say that this family is quasi-uniform if one can find a pair l *independent of* n for which all the drawing algorithms are l-uniform. For short, any element of this family will be said to be quasi-uniform. Generally speaking,

> Quasi = Proportional up to absolute strictly positive multiplicative constants.

Now, we can precisely state the Uniformity Condition: *There exists a polynomial-time algorithm which draws elements from* $B(\alpha)$ *in a quasi-uniform way.*

1.3. **The complexity bound for the** $D[\alpha]$ **algorithm.** The first result describes a sufficient condition under which the Counting Condition is fulfilled.

Theorem 1. *If n is solely composed of prime factors greater than $L(n)$, the probability that an element x drawn by a quasi-uniform algorithm from $B(\alpha)$ belongs to $F(\alpha, \beta)$ is in $L^{-\alpha/(2\beta)}$.*

Note that the first step of the $D[\alpha]$ algorithm fulfills this hypothesis, and thus the Counting Condition. So it remains to show how the Uniformity Condition leads to time-complexity bounds for the $D[\alpha]$ algorithm.

Theorem 2. *Assume the following condition: there exists a polynomial-time algorithm which draws elements from $B(\alpha)$ in a quasi-uniform way. Then the probabilistic factoring algorithm, obtained by the α-Dixon method, with the optimum choice of auxiliary parameters $\beta = \sqrt{\alpha/2}$ and $\gamma = \sqrt{2\alpha}$, has time-complexity exponent equal to $\sqrt{2\alpha}$.*

Proof of Theorem 1. We use directly two results of Pomerance [5]:

The cardinality of $B(\alpha)$ is equal to $2n^{\alpha}L(n)^{o(1)}$.

The cardinality of $F(\alpha, \beta)$ is equal to $2n^{\alpha}L(n)^{-\alpha/(2\beta)+o(1)}$.

Thus, we deduce: The exponent of the probability that an element of $B(\alpha)$ belongs to $F(\alpha, \beta)$ is equal to $-\alpha/(2\beta)$. This exponent will not change if we replace a uniform drawing from $B(\alpha)$ by a quasi-uniform one. Thus, if we can choose x in $B(\alpha)$ in a quasi-uniform way, the probability that $Q(x)$ could be factored in the base P is equal to $L(n)^{-\alpha/(2\beta)+o(1)}$. □

Proof of Theorem 2. If we want to obtain L^{β} different quantities $Q(x)$ that are totally factored in P, we expect to perform L^{γ} draws from $B(\alpha)$ with the following relation between the parameters:

$$\gamma - \frac{\alpha}{2\beta} = \beta.$$

We adapt now to $D[\alpha]$ the improvements that Pomerance [6] gave to Dixon's standard method. He uses, in Step 2, the Elliptic Curves Factoring Method in order to find small factors of the $Q(x)$, and, in Step 3, the Wiedemann elimination method which works well on a sparse matrix with entries in a finite field.

Proceeding in this way, one can prove, as in [6], that the cost of each iteration of Step 2 is equal to $L(n)^{o(1)}$, so that the exponent of the total cost of this step is equal to

$$\gamma = \beta + \frac{\alpha}{2\beta}, \quad \text{which is minimal for } \beta = \sqrt{\frac{\alpha}{2}}.$$

The best exponent of Step 2 is thus $\sqrt{2\alpha}$.

In Step 3, one can successfully apply the Wiedemann method because the matrix M contains less than $O((\log n/\log\log n)^{1/2})$ nonzero elements in each row. This number has an exponent equal to 0, and thus the exponent of the elimination cost is equal to $2\beta = \sqrt{2\alpha}$. □

It remains now to obtain the Uniformity Condition under our particular choice of α. We will choose α near $2/3$, and we will complete this task in the

next sections, after a detailed study of the subset B associated with this choice of α.

1.4. **A sharper estimate of the cardinality of $B(\alpha)$.** We begin this study with providing a sharper estimate of the cardinality of the subset $B(\alpha)$, under specific hypotheses about the parameter α.

Theorem 3. *If n is solely composed of prime factors greater than $L(n)$, and if α is greater than $\alpha_0 = 1/2 + (\log\log n/\log n)^{1/2}$, one has*

$$||B(\alpha)| - 2n^{\alpha}| \leq n^{\alpha} L(n)^{-1+o(1)}.$$

For the proof of Theorem 3, we start with an odd integer n, with its prime factor decomposition

$$n = \prod_{i=1}^{h} p_i^{e_i},$$

where the p_i's are distinct primes in increasing order, and the exponents e_i are at least 1. Throughout the proof, small letters are for cardinalities of the sets denoted by the corresponding capital letters. Given any subset T of $Z(n)$ formed with t consecutive integers, we let

$$T^* = \{x \in T | (x, n) = 1\},$$
$$S = \{x \in Z(n) | Q(x) \in T\}, \qquad S^* = \{x \in Z(n) | (x, n) = 1 \text{ and } Q(x) \in T\}.$$

We must evaluate the cardinality of the subset S in the particular case when the corresponding set T is the subset $[-n^{\alpha}, +n^{\alpha}] \cap Z(n)$. The proof of Theorem 3 consists in three lemmas; in the first two lemmas, we consider a general subset T and we come back to our particular hypotheses in Lemma 3. We seek an upper bound for the expression $|s - t|$. Lemma 1 links s and the cardinality u of the subset U of T defined by

$$U = \{x \in T^* | x \text{ is a square modulo } n\}.$$

Lemma 1. *The cardinalities of S, S^*, T, T^* are related by*

$$(1) \qquad s^* = 2^h u, \quad s^* \leq s \leq s^* + 2^h(t - t^*), \quad t - t^* \leq h(t/p_1 + 1).$$

The proof of Lemma 1 is straightforward and is omitted. From the relations of Lemma 1 one easily deduces

$$(2) \qquad 0 \leq s - 2^h u \leq 2^h h(t/p_1 + 1).$$

In order to link t and u, Lemma 2 uses the Jacobi symbol and a particular case of the Pólya-Vinogradov inequality using this symbol; this provides an upper bound for $|t - 2^h u|$.

Lemma 2. *We have*

$$(3) \qquad |t - 2^h u| \leq 2^h[\sqrt{n}\log n + h(t/p_1 + 1)].$$

Proof. The Jacobi symbol $(\frac{\cdot}{n})$ relative to an odd integer n is defined from Legendre symbols:

$$\left(\frac{x}{n}\right) = \prod_{i=1}^{h} \left(\frac{x}{p_i}\right)^{e_i}.$$

The Legendre symbol relative to an odd prime p is defined by the three properties:

(i) $(\frac{x}{p}) = \pm 1$ for all x coprime with p.
(ii) $(\frac{x}{p}) = +1$ if and only if x is coprime with p and is square modulo p.
(iii) $(\frac{x}{p}) = 0$ if x is a multiple of p.

Moreover, an element x of T is a square modulo n if and only if it is a square modulo each p_i. We deduce the following expression for u:

$$u = \frac{1}{2^h} \sum_{x \in T^*} \prod_{i=1}^{h} \left(1 + \left(\frac{x}{p_i}\right)\right). \tag{4}$$

We work with the squarefree divisors of n. For a nonempty subset I of $H = \{1, 2, \ldots, h\}$, we let $q_I = \prod_{i \in I} p_i$. Equality (4) can be written

$$u - \frac{t^*}{2^h} = \frac{1}{2^h} \sum_{\varnothing \neq I \subset H} \sum_{x \in T^*} \left(\frac{x}{q_I}\right). \tag{5}$$

The Pólya-Vinogradov inequality [2] will give an upper bound for this expression; it asserts that: *For any odd squarefree integer m and for any interval T of $\mathbf{Z}$, one has*

$$\left|\sum_{x \in T} \left(\frac{x}{m}\right)\right| \leq \sqrt{m} \log m.$$

We use now all the Pólya-Vinogradov inequalities associated with the q_I's. Considering the subsets of T,

$$T_I = \{x \in T | (x, q_I) = 1\},$$

we obtain

$$\left|\sum_{x \in T_I} \left(\frac{x}{q_I}\right)\right| \leq \sqrt{q_I} \log q_I.$$

Using inequality (1) and the fact that T_I contains T^*, we deduce

$$\left|\sum_{x \in T^*} \left(\frac{x}{q_I}\right)\right| \leq \sqrt{q_I} \log q_I + h\left(\frac{t}{p_1} + 1\right).$$

We use these inequalities in (5), and obtain

$$|2^h u - t^*| \leq 2^h \sqrt{n} \log n + (2^h - 1)h\left(\frac{t}{p_1} + 1\right).$$

Using relation (1), we get the upper bound of Lemma 2. □

The previous two lemmas provide an upper bound for the quantity $|s - t|$; from inequalities (2) and (3), we obtain

$$|s - t| \leq 2^h \sqrt{n} \log n + 2^{h+1} h \left(\frac{t}{p_1} + 1 \right). \tag{6}$$

Now, under the specific hypotheses of Theorem 3, we can evaluate this upper bound and complete the proof of the theorem.

Lemma 3. *If n is solely composed of prime factors greater than $L(n)$, and if one sets $t = 2n^\alpha$ with α greater than $\alpha_0 = 1/2 + (\log\log n / \log n)^{1/2}$, one has*

$$|s - 2n^\alpha| \leq n^\alpha L(n)^{-1+o(1)}.$$

Proof. Since n has all its prime divisors larger than $L(n)$, one has

$$h \leq (\log n / \log\log n)^{1/2} \quad \text{and also} \quad 2^h \leq L(n)^{o(1)}.$$

Furthermore, our hypotheses allow us to bound from above each term on the right of (6) by

$$n^\alpha L(n)^{-1+o(1)},$$

which completes the proof of Lemma 3. □

We can come back now to the subset $B(\alpha)$, which is exactly the subset S associated with $T = [-n^\alpha, +n^\alpha] \cap Z(n)$. Thus, Lemma 3 finally completes the proof of Theorem 3.

2. A STUDY OF THE SUBSET B USING FAREY COVERING AND GEOMETRY OF NUMBERS

The purpose of this section is to introduce basic notions and tools that we use for studying the set B of elements x of $Z(n)$ whose squares $x^2 \bmod n$ are in absolute value at most $4n^{2/3}$. Starting with two experimental facts, we are led to a covering of $Z(n)$ related to Farey sequences, as well as to a special class of integer lattices linked to B. The results relative to random generation of elements of B that are of use for the complexity of integer factorization are stated in this section (Theorems 4, 5, 6) and proved in §3, using the main tools of this section. But here, the structure of B appears to be curious enough to deserve detailed analysis. In particular, we wish to precisely explain all the experimental facts that we observe, and use them to generate locally the elements of B in a deterministic way. This will be done in Theorems 7 and 8 of §4.

In the sequel, we adopt the shorthand notation:

$$B = B\left(\frac{2}{3} + \frac{\log 4}{\log n} \right), \quad h = 4n^{2/3}, \quad \text{and} \quad k = \frac{n}{h} = \frac{1}{4} n^{1/3}.$$

We assume here that our problem is not trivial, i.e., we have $2h < n$ or equivalently $n > 2^9$.

2.1. **Experimental observations.** In order to study the subset B, we need to describe the distribution of gaps between successive elements of B. We observed in numerical experiments two important facts:

Pattern Occurrence. The gaps between successive elements of B may have large variations near the rationals $pn/(2q)$ of small denominator q, but their distribution appears to follow a definite pattern inside a *sufficiently small interval* around $pn/(2q)$.

> If q is very small, there appear sequences of gaps all equal to q, separated by much larger gaps.
>
> If q is moderately small, an element of B may appear in the midst of a gap of length q (which then splits into two gaps of sum q). At the same time, much larger gaps disappear.

This pattern seems to disappear when going away from $pn/(2q)$.

Balance Phenomenon. There is a balance between these gaps, so that the total number of B's elements inside a *sufficiently large interval* around $pn/(2q)$ is almost the same as if the distribution of B in the whole $Z(n)$ were actually uniform.

It appears that *the length of a suitable interval to express these phenomena is inversely proportional to* q.

Let us give a numerical example of these facts: For $n = 46961$, we observe the situation near three rationals: $n/4$, $n/12$, and $n/18$. We use the notation x^y for a y-fold repetition of a gap sequence x.

Near $n/18$, the sequence of gaps starting at 2601 is:

$$(8\,1)^{10}\,(7\,1)\,(8\,1)^2\,(7\,1)\,(8\,1)^2\,(7\,1)\,(8\,1)\,(7\,1)\,(8\,1)\,(7\,1)\,(8\,1) \text{ etc.}$$

Near $n/12$, we find the following sequence of gaps starting at 3895:

$$6^6\,(5\,1)^5\,5\,6^5\,(5\,1)^2\,5\,6^3\,(5\,1)^2\,5 \text{ etc.}$$

Note that the point $n/12$ lies in the middle of the first sequence of gaps equal to 6, which is also the longest one in this neighborhood.

Near $n/4$, the sequence of gaps starting at 11103 is:

$$2^4\ 13\ 2^4\ 13\ 2^4\ 13\ 2^4\ 13\ 2^5\ 13\ 2^5\ 2^6\ 17\ 2^7\ 23\ 2^8\ 25\ 2^{10}\ 27\ 2^{12}\ 35\ 2^{16}\ 59\ 2^{90}\ 57 \text{ etc.}$$

Note that the point $n/4$ lies close to the middle of the sequence of gaps 2^{90}, which is also the longest one in the neighborhood.

It remains to prove these facts, which we now set out to do.

2.2. **Farey covering.** In order to prove the above observations, we construct a particular covering of $Z(n)$, based on Farey sequences (see, e.g., [1]), that we call the Farey covering of order k. By definition, this covering is made of intervals $I(p, q)$ with center $pn/(2q)$ and radius $n/(2kq) = h/(2q)$, where $|p| \leq q \leq k$ and $(p, q) = 1$.

We are going to prove that these intervals are convenient for our purpose: They are sufficiently large to realize a balance between the variations of the gaps in B, and sufficiently small to preserve the pattern of these gaps.

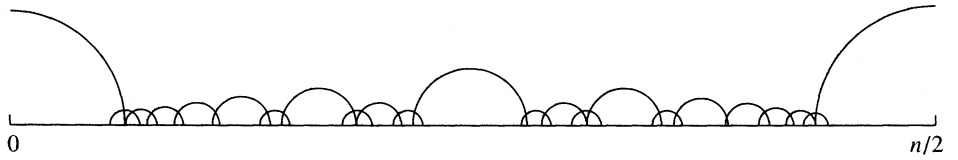

FIGURE 1
Farey intervals for $k = 8$

We compare intervals $I(p, q)$ with closely related intervals $J(p, q)$. Given three consecutive Farey fractions with denominators less than k:

$$\frac{p_1'}{q_1'}, \frac{p}{q}, \text{ and } \frac{p_2'}{q_2'},$$

which thus satisfy $p_2'q - q_2'p = +1$ and $p_1'q - q_1'p = -1$, we define the interval $J(p, q)$ of so-called "mediants" by

$$J(p, q) = \left(\frac{(p + p_1')n}{2(q + q_1')}, \frac{(p + p_2')n}{2(q + q_2')} \right).$$

It is clear that the intervals $J(p, q)$ form a partition that is not too different from our Farey covering.

Lemma 4. *An interval* $I(p, q)$ *can only meet its two next neighbors* $I(p_1', q_1')$ *and* $I(p_2', q_2')$. *Moreover, the interval* $J(p, q)$ *is included in* $I(p, q)$, *and the length of* $I(p, q)$ *is less than twice the length of* $J(p, q)$.

We omit the easy proof of this lemma, which can be found in [1].

So the Farey covering is almost a partition in the following [precise] sense:

Definition 2. Let l be an integer. A covering $\mathcal{Y} = \{Y_j | j \in J\}$ of $Z(n)$ is said to be an l-partition if, for all x of $Z(n)$, the number of elements Y_j that contain x is at most l.

So we have proved that the Farey covering made of the $I(p, q)$'s is actually a 2-partition and also a quasi-partition—with "quasi" being used in accordance with the principles of §1.2.

2.3. **Formalizing the Balance Phenomenon.** We first need to extend our definition of uniformity to coverings, in order to formalize the Balance Phenomenon.

Definition 3. Let $l = (l_1, l_2)$ be a pair of two strictly positive constants. Two subsets X and Y of $Z(n)$ are l-independent (with respect to P, the uniform probability measure over $Z(n)$) if

$$l_1 \leq \frac{P(X \cap Y)}{P(X)P(Y)} \leq l_2.$$

A pair made of a subset X of $Z(n)$ and a covering $\mathcal{Y} = \{Y_j | j \in J\}$ of $Z(n)$ is l-independent if, for all j of J, the sets X and Y_j are l-independent.

We consider now, as in §1.2, a family of pairs $(X, \mathcal{Y})$ obtained when the index n varies. We will say that this family is quasi-independent if one can find an $l = (l_1, l_2)$ *that does not depend on* n for which all the pairs $(X, \mathcal{Y})$ are l-independent. For short, any pair $(X, \mathcal{Y})$ of this family will be said to be quasi-independent. Alternatively, we shall say that the distribution of X is quasi-uniform with respect to the covering $\mathcal{Y}$.

The first result in this section formalizes a version of the Balance Phenomenon: Up to absolute multiplicative constants, each subset $B \cap I(p, q)$ contains as many elements as if the distribution of B were actually uniform.

Theorem 4. *The pair made with subset* B *and the Farey covering of order* $k = (1/4)n^{1/3}$ *is quasi-independent.*

2.4. **Obtaining the Uniformity Condition when α is near $2/3$.** In a subset X that has a quasi-uniform distribution with respect to a quasi-partition $\mathcal{Y}$, we can work locally and we propose to construct quasi-uniform drawings from $X \cap Y_j$. This can help in obtaining a quasi-uniform drawing from X, and this principle will be used now for getting the uniformity condition when α is near $2/3$.

So we will work in each subset $B \cap I(p, q)$. There, we will prove a weak version of the Pattern Occurrence (Lemma 6) and use the exhibited pattern to construct locally quasi-uniform drawings that we will assemble together to obtain the Two-Thirds Algorithm, which provides the Uniformity Condition when α is near $2/3$.

First we give an informal description of this algorithm: Imagine that points of B are balls that are contained in a chest of drawers. Each drawer represents a Farey interval.

(1) The balls are not necessarily all distinct. Perhaps, there are two incarnations of the same ball in two distinct drawers [*according to the 2-partition*].

(2) The number of balls in each drawer is almost proportional to the size of the drawer [*according to the Balance Phenomenon*].

(3) In each drawer, the balls are collected in numbered boxes. The first two boxes are perhaps empty, but one knows exactly the number of balls that they contain. The other ones contain a number of balls that almost follows a law depending on the numbering of the box [*according to the Pattern Occurrence*].

It is clear that one can choose "easily" a ball in this chest of drawers in an "almost" uniform way. This is expressed in the following result:

Theorem 5. *There exists a polynomial-time algorithm, called the Two-Thirds Algorithm, which draws elements from* B *in a quasi-uniform way.*

This last theorem, together with our general Theorem 2, gives the main result of the paper.

Theorem 6. *There exists an integer factoring probabilistic algorithm, associated with the α-Dixon method with $\alpha = 2/3$, whose time-complexity exponent is equal to $\sqrt{4/3}$.*

2.5. **Using lattices for a local study of the subset B.** We now introduce our main local tool, lattices.

Inside each of the intervals $I(p, q)$, some simple facts of geometry of numbers can explain and prove our observations about gaps between successive elements of B. We make a local use of lattices of $\mathbf{Z}^2$ and, thus, the elements of B near a point x_0 give rise to points of a lattice $L(x_0)$ between two parabolas. Furthermore, if $x_0 \in I(p, q)$ is sufficiently close to the rational number $pn/(2q)$, this lattice has a geometry which is "compatible" with the geometry of the parabolas, and we can easily describe, in an algorithmic way, the points of the lattice between the two parabolas and count them. We now will develop these arguments.

We consider the lattice $L(x_0)$ which is generated by the two vectors $(1, 2x_0)$ and $(0, n)$, and the elements of B near point x_0 give rise to points of $L(x_0)$ between two parabolas. If $x = x_0 + u$ is an element of $Z(n)$, we have

$$Q(x) \equiv x_0^2 + 2x_0u + u^2 \ [n].$$

Thus, if we let $w = Q(x) - u^2 - x_0^2$, we have the equivalence between the two conditions:

(i) $x = x_0 + u$ belongs to B,

(ii) there exists w such that the point $m(x) = (u, w)$ belongs to $L(x_0)$ and lies between the two parabolas with respective equations

$$w + u^2 + x_0^2 = h \quad \text{and} \quad w + u^2 + x_0^2 = -h.$$

If now x_0 is the integer nearest to the rational $pn/(2q)$ with a small denominator q,

$$x_0 - \frac{pn}{2q} = u_0 \quad \text{with } |u_0| \leq \frac{1}{2},$$

we introduce the domain $P(p, q)$ formed with the points $m(x)$ of $L(x_0)$ arising from the points x of $B \cap I(p, q)$. In other words, for two integers p and q satisfying $|p| \leq q \leq k$, and $(p, q) = 1$, we propose to describe the domain of lattice points

$$P(p, q) = \{(u, w) \in L(x_0) \mid |u + u_0| \leq h/2q \text{ and } |w + u^2 + x_0^2| \leq h\}.$$

There exists a primitive vector of $L(x_0)$ which makes this task easy. The vector

$$\vec{r} = q(1, 2x_0) - p(0, n) = (q, 2qu_0)$$

has a slope equal to $2u_0$, which is in absolute value at most 1, and has a horizontal component equal to q. If $I(p', q')$ is a Farey interval adjacent to x_0, we can use the vector

$$\vec{s} = q'(1, 2x_0) - p'(0, n) = (q', 2q'u_0 + n/q)$$

to complete $\vec{r}$ into a basis of $L(x_0)$. Finally, we have shown the following result:

Lemma 5. *The points of the lattice $L(x_0)$ lie on quasi-horizontal lines which cut on the vertical axis segments of length equal to n/q; moreover, on each line, the points of $L(x_0)$ have horizontal gaps equal to q. From one line to the next, the points of $L(x_0)$ are shifted with a horizontal spacing equal to q' in absolute value.*

3. Generating random elements of B in a quasi-uniform way

Now, our main tools—Farey covering, lattices, parabola—are defined. We are going to use them to explain our experimental observations. In this section, we are interested in the random generation of B, and we will, in particular, establish Theorems 4 and 5.

3.1. **The boxes of the drawer.** We now explain how to define the boxes of the drawer $I(p, q)$ that we mentioned in our informal description of the Two-Thirds Algorithm in §2.4.

We consider the lines of the lattice, parallel to the vector $\vec{r}$, which intersect the domain $P(p, q)$ associated with $I(p, q)$. The two extremal positions of these lines are easy to determine (Figure 2).

The first one is the tangent to the parabola of equation $w = -u^2 - x_0^2 + h$, with a slope equal to $2u_0$. This line satisfies the equation

$$w - (-u_0^2 - x_0^2 + h) = 2u_0(u + u_0).$$

The second joins the two limit points of $P(p, q)$ whose respective coordinates are

$$\left(-u_0 + \frac{h}{2q}, -\left(u_0 - \frac{h}{2q}\right)^2 - h - x_0^2\right)$$

and

$$\left(-u_0 - \frac{h}{2q}, -\left(u_0 + \frac{h}{2q}\right)^2 - h - x_0^2\right).$$

This line has actually a slope equal to $2u_0$ and satisfies the equation

$$w + \left(u_0 + \frac{h}{2q}\right)^2 + h + x_0^2 = 2u_0\left(u + u_0 + \frac{h}{2q}\right).$$

These two lines intersect the vertical axis at the respective points

$$w_0 = h - x_0^2 + u_0^2 \quad \text{and} \quad w_1 = -h - x_0^2 + u_0^2 - \frac{h^2}{4q^2},$$

so that all the lines parallel to $\vec{r}$ that intersect $P(p, q)$ are the ones that intersect the segment $[w_0, w_1]$ whose length is equal to $2h + h^2/4q^2$.

One numbers these lines from top to bottom; a real ν is called an index if there exists a line of $L(x_0)$ parallel to $\vec{r}$ which intersects the vertical axis at the point with ordinate equal to $w_0 - \nu n/q$; this quasi-horizontal line is denoted by $D(\nu)$; and, if x is a point of $B \cap I(p, q)$, we call index of x the index ν of the line $D(\nu)$ which contains the point $m(x)$.

We use two particular lines, parallel to $\vec{r}$, which cut the vertical axis at $w = w_0 - 4h$ and $w = w_0 - h^2/4q^2$ in order to divide $P(p, q)$ into three domains: the *chest*, the *legs*, and the *feet* (Figure 2). So, we define our boxes:

The first two boxes are the chest and the feet, while the other ones are all the lines $D(\nu)$ of the legs.

Then, we define four particular indices: ν_0 is the first index of the domain, ν_1 is the first index of the legs, ν_2 is the last index of the legs, and ν_3 is the last index of the domain. The index ν_1 is defined to be the least index greater than or equal to $4hq/n$, while the index ν_2 is the greatest index less than $h^2/4qn$. Since the total height of $P(p, q)$ is equal to $w_0 - w_1 = h^2/4q^2 + 2h$, the index ν_3 is the greatest index less than $h^2/4qn + 2hq/n$.

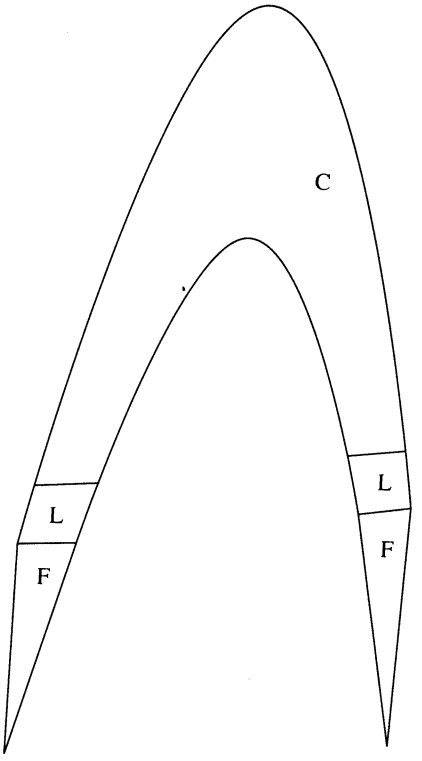

FIGURE 2
The three parts of $P(p, q)$
C: *the chest*, L: *the legs*, F: *the feet*

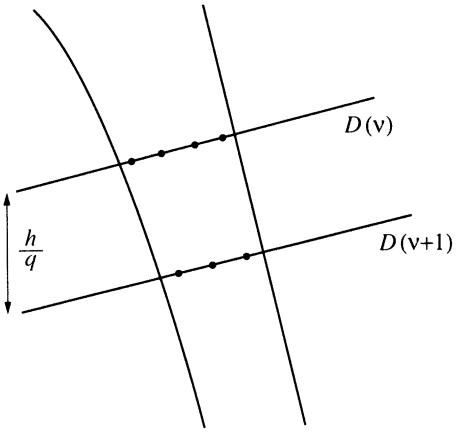

FIGURE 3
The segments $T(\nu)$

Note that Figure 2 is not to scale: Our choice of h makes the legs very long, while the chest and the feet are very small and each contains at most four indices. Observe the relations: $0 \le \nu_0 < 1$ and

$$\nu_2 + 1 \ge \frac{h^2}{4qn} \ge \frac{h^2}{4kn} = 16 = 16\frac{hk}{n} \ge 16\frac{hq}{n} \ge 4(\nu_1 - 1). \tag{7}$$

3.2. **Estimate of the number of balls in each box; a weak version of the Pattern Occurrence.** We show that the number $N(\nu)$ of points of $P(p, q)$ on each line $D(\nu)$ of the legs follows the approximate law

$$N(\nu) \approx 2\frac{h}{\sqrt{\nu qn}}. \tag{8}$$

More precisely, we show the following.

Lemma 6. *The number $N(\nu)$ of points of $P(p, q)$ on line $D(\nu)$ of the legs satisfies*

$$\frac{h}{\sqrt{\nu qn}} \le N(\nu) \le \frac{7}{2}\frac{h}{\sqrt{\nu qn}}.$$

Proof. In the legs, we consider the two segments $T^-(\nu)$ and $T^+(\nu)$ cut on the line $D(\nu)$ by the two parabolas. Their horizontal projections are the two segments $S^-(\nu)$ and $S^+(\nu)$,

$$S^-(\nu) = [-b(\nu) - u_0, -a(\nu) - u_0], \qquad S^+(\nu) = [a(\nu) - u_0, b(\nu) - u_0],$$

with $a(\nu) = \sqrt{\nu n/q - 2h}$ and $b(\nu) = \sqrt{\nu n/q}$. Each of them has a length $s(\nu)$ equal to (cf. Figure 3)

$$s(\nu) = b(\nu) - a(\nu) = \sqrt{\frac{\nu n}{q}}\left(1 - \sqrt{1 - \frac{2hq}{\nu n}}\right).$$

A series expansion is legitimate in the legs because we have there $\nu \ge 4hq/n$; we use the fact that, for all $x \le 1/2$,

$$\frac{x}{2} \le 1 - \sqrt{1-x} \le \frac{x}{2}\left[1 + \frac{x}{4}\left(\frac{1}{1-x}\right)\right] \le \frac{5}{4}\frac{x}{2}$$

and obtain

$$h\sqrt{\frac{q}{\nu n}} \le s(\nu) \le \frac{5}{4}h\sqrt{\frac{q}{\nu n}}.$$

Furthermore, on each of these segments, the lattice $L(x_0)$ has points with a horizontal spacing equal to q, and since we have

$$\frac{s(\nu)}{q} \ge \frac{h}{\sqrt{\nu qn}} \ge 2 \quad \text{for all } \nu \le \nu_2, \tag{9}$$

it is clear that each segment $T(\nu)$ contains at least two points of $L(x_0)$. More precisely, we can evaluate the number $N(\nu)$ of lattice points on the union of

the two segments of $T(\nu)$:

$$(10)\qquad \begin{aligned} N(\nu) &\geq 2\left(\frac{h}{\sqrt{\nu q n}} - 1\right) \geq \frac{h}{\sqrt{\nu q n}}, \\ N(\nu) &\leq 2\left[\frac{5}{4}\frac{h}{\sqrt{\nu q n}} + 1\right] \leq \frac{7}{2}\frac{h}{\sqrt{\nu q n}}. \end{aligned}$$

Thus, up to absolute multiplicative constants, $N(\nu)$ follows the claimed law. □

3.3. **The number of points in $P(p, q)$; proof of Theorem 4 and the Balance Phenomenon.** In order to prove Theorem 4, we are going to evaluate the above number N in comparison with the number

$$N_e = \frac{h}{q} \times \frac{2h}{n} = \frac{2h^2}{qn}$$

that we should expect if the distribution of B were exactly uniform.

In order to calculate the number N_l of points in the legs, we use quasi-law (10) and comparisons with integrals:

$$(11)\qquad \begin{aligned} \sum_{\nu=\nu_1}^{\nu_2} \frac{1}{\sqrt{\nu}} &\geq \int_{\nu_1}^{\nu_2+1} \frac{d\nu}{\sqrt{\nu}} = 2(\sqrt{\nu_2+1} - \sqrt{\nu_1}), \\ \sum_{\nu=\nu_1}^{\nu_2} \frac{1}{\sqrt{\nu}} &\leq \frac{1}{\sqrt{\nu_1}} + \int_{\nu_1+1}^{\nu_2} \frac{d\nu}{\sqrt{\nu}} \leq \frac{1}{\sqrt{\nu_1}} + 2\sqrt{\nu_2}, \end{aligned}$$

and with the relations (7), and the quasi-law (10), we get

$$(12)\qquad \frac{1}{2}\left(1 - \frac{\sqrt{5}}{4}\right) N_e \leq N_l \leq \frac{7}{4}\left(1 + \frac{1}{16}\right) N_e.$$

In the chest and in the feet, one obtains also upper bounds in a straightforward manner, but *no nontrivial lower bounds.*

There are at most four lines in the chest, and, on each line, the number of points is less than $(2/q)\sqrt{(\nu_1 - 1)n/q} + 1 \leq 4\sqrt{h}/q + 1 \leq 0.251N_e$. Thus, the number N_c of points in the chest satisfies $N_c \leq 1.004N_e$.

There are at most two lines in the feet, and on each line, the number of points is less than 8. Thus, the number N_f of points in the feet satisfies $N_f \leq 16 \leq 0.125N_e$.

Finally, we obtain

$$\tfrac{1}{5}N_e \leq N \leq 4N_e.$$

So the pair B and the Farey covering of order $k = (1/4)n^{1/3}$ are l-independent. More precisely, one can take $l_1 = 1/5$ and $l_2 = 4$. This provides an explicit proof of Theorem 4.

3.4. **The Two-Thirds Algorithm.** We can give now a more formal description of this algorithm and prove its properties.

Input. A random point x of $Z(n)$.

Output. A point z of B which lies in the same Farey interval as x.

(1) *Choice of the Farey interval—the drawer.* Randomly choose an x in $Z(n)$, and, with the last two best approximations of $2x/n$ with denominators

less than k, which are called p_1/q_1 and p_2/q_2, determine a Farey interval $I(p, q)$ which contains x:

> Consider the mediant p_3/q_3 of the rationals p_1/q_1 and p_2/q_2, defined by the relations: $p_3 = p_1 + p_2$ and $q_3 = q_1 + q_2$. It belongs to the segment $[p_1/q_1, p_2/q_2]$. If $2x/n$ belongs to $[p_1/q_1, p_3/q_3]$, then choose $(p, q) = (p_1, q_1)$, else choose $(p, q) = (p_2, q_2)$.

Then determine the domain $P(p, q)$ relative to this Farey interval, its four main indices $\nu_0, \nu_1, \nu_2, \nu_3$ defined in §3.1, as well as the point x_0 nearest to the rational $pn/(2q)$.

(2) *Evaluation of the number of points in the Farey interval.* Determine the points of $L(x_0)$ inside the domain $P(p, q)$. [For this, we operate *in a different way in the chest or in the feet, as in the legs.*] [In the chest and in the feet, we do not have lower bounds for the number of points, but we can perform an exact calculation, because the number of lines is at most four in each case. In the legs, we use the quasi-law (8) of $N(\nu)$ and approximate $N(\nu)$ by $2h/\sqrt{q\nu n}$.]

(2a) First, determine exactly the points in the chest and the feet, and *exactly calculate* their numbers, which are denoted N_c and N_f.

(2b) Then, with the help of an integral, *evaluate* the number N_l of the points in the legs. Let $N = N_c + N_l + N_f$ be the total number of lattice points inside $P(p, q)$.

(3) *Choice of the line—the box.* Randomly choose an integer t in $[1, N]$.

(3a) If $t \leq N_c + N_f$, determine the point y of the chest or the feet which corresponds to this number. The abscissa u of this point gives the output $z = x_0 + u$.

(3b) If not, from the number $t - (N_c + N_f)$, first determine the index ν of the line $D(\nu)$: Use the estimate (8) and the comparison between the series with general term $1/\sqrt{\nu}$ and an integral. Then, calculate exactly the number of lattice points on this line, and randomly choose a lattice point y on this line. The abscissa u of this point gives the output $z = x_0 + u$.

3.5. **Properties of the Two-Thirds Algorithm.** The polynomial-time complexity of this algorithm is clear. Furthermore, we see that it uses only $O(\log n)$ arithmetic operations on numbers of order n.

The constants of quasi-uniformity arise in our algorithm from each of the three steps and make precise the informal description that we gave in §2.4.

(1) There are some x's that belong to two Farey intervals, and others that belong to only one such interval. We choose $I(p, q)$ in the first step if and only if $2x/n$ lies inside $J(p, q)$. According to Lemma 4, this interval $J(p, q)$ has length proportional to $I(p, q)$ up to absolute multiplicative constants. So we can choose the $I(p, q)$'s quasi-proportionally to their length.

(2) Use Theorem 4 (Balance Phenomenon).

(3) Use Lemma 6 (weak version of the Pattern Occurrence).

This completes the proof of Theorem 5. From this, we deduce finally Theorem 6, which provides the best rigorously established probabilistic complexity bound for integer factorization algorithms.

4. More about the Pattern Occurrence

So far, we have been interested in the random generation of elements of B. Now we adopt a more deterministic point of view. We propose to describe the gaps around a given element of B in order to explain the Pattern Occurrence and determine in polynomial-time the two closest neighbors in B of a point of $Z(n)$.

We still use lattices and consider the local transfer of points of $B \cap I(p, q)$ into $P(p, q)$. This transfer is compatible with the topology of these two subsets: two neighbors in $B \cap I(p, q)$ lead to two sufficiently close points of $P(p, q)$.

In §3, we used transfer from $B \cap I(p, q)$ to $P(p, q)$, but we stayed in $P(p, q)$. Now, we come back to $B \cap I(p, q)$ by using horizontal projections. Using this double transfer, we, most of all, obtain two results: the first (Theorem 7) gives a theoretical description of gaps around a point of B, while the second (Theorem 8) is an algorithm, called the Neighbors Algorithm, which "often" finds the two neighbors in B of a given point.

4.1. **An informal explanation of the main arguments.** Our study is based on some remarks that we state first in an informal way.

Comparison between two notions of neighborhood. We define two notions of neighborhood: Two points of $B \cap I(p, q)$ are B-neighbors if no point of B lies between them. Two points of $P(p, q)$ are P-neighbors if they belong to the same segment $T(\nu)$ and, if, on this segment, no point of $P(p, q)$ lies between them.

The comparison between the two notions of neighborhood depends on the denominator q of the Farey interval $I(p, q)$, and we must distinguish two cases, according to the sign of the quantity $t = 1 - 2hq/n = 1 - 2q/k$. If t is negative, the segments $S(\nu)$ are disjoint and the order on $B \cap I(p, q)$ is compatible with the natural order on $P(p, q)$. Otherwise, if t is positive, the segments $S(\nu)$ overlap each other, and there is a mixing between the horizontal projections $S(\nu)$ of successive segments of $T(\nu)$ (cf. Figures 4 and 5).

Low degree of overlapping. The degree of overlapping is never too large, so that we can consider only a small number of lines to determine the B-neighbors of a point. This is ultimately the reason why we obtain a polynomial-time algorithm.

Regularity around ordinary points. Our method works for points of $Z(n)$ that are only moderately well approximated by rationals $pn/(2q)$. Such points

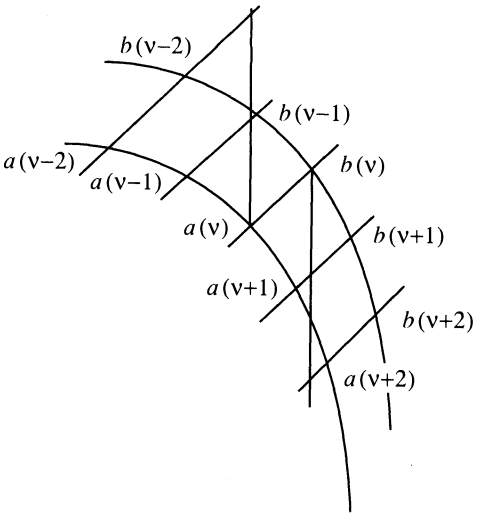

FIGURE 4
Case when $q \geq k/2$

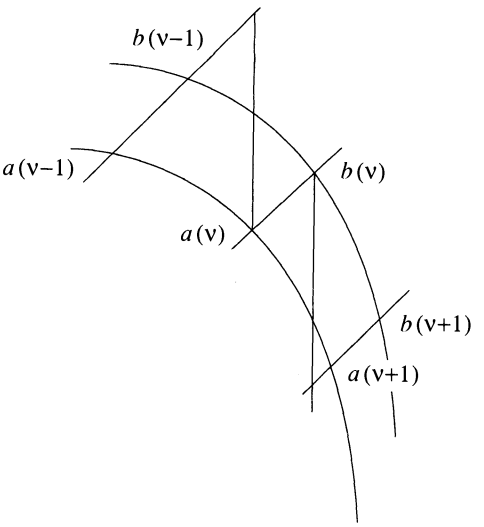

FIGURE 5
Case when $q < k/2$

are called ordinary and give rise to points of $P(p, q)$ which lie neither too high in the chest, nor too low in the feet. Around such a point, the pattern of the domain $P(p, q)$ is sufficiently clear to easily determine the P-neighbors of this point.

4.2. **Gaps around ordinary points.** We first formalize the notion of an ordinary point.

Definition 4. A point x_1 of $I(p, q)$ is called *ordinary* if its distance u_1 from $pn/(2q)$ satisfies the following inequalities:

$$\sqrt{\frac{2n}{q}} \leq u_1 \leq \frac{\sqrt{3}h}{4q}. \tag{13}$$

The subset of these points is denoted by $O(p, q)$.

The following lemma gives an estimate of the density of this ordinary subset and makes precise the indices of ordinary points (indices are to be taken in the sense of 3.1).

Lemma 7. *The index of an ordinary point satisfies the inequality* $2 \leq \nu \leq \nu_2 - 1$, *and the ordinary subset has a density greater than* $5/8$.

Theorem 7 below takes advantage of the three remarks that we previously stated.

Theorem 7. *Let* x_1 *be a point of* $B \cap O(p, q)$ *at a distance* u_1 *from* $pn/(2q)$, *and let* p'/q' *be the best approximation of* p/q *with a denominator* $q' < q$.

We set $t = 1 - 2hq/n$. *Then the following hold*:

(1) *There exists a point* x_2 *of* B *at a distance exactly equal to* q *from* x_1.

(2) *If* $q \geq k/2$, *the two gaps around* x_1 *belong to the set*

$$G = \{g | 1 \leq g \leq q,\ g \equiv \alpha q'[q] \text{ with } \alpha \in \mathbf{Z} \text{ and } |\alpha| \leq 2\}.$$

(3) *If* $q < k/2$, *at least one of the two gaps around* x_1 *is exactly equal to* q. *The other one satisfies*

$$\frac{1}{3}\frac{tn}{qu_1} \leq g \leq \frac{2}{3}\frac{tn}{qu_1} + 2q \quad \text{and} \quad g \equiv \pm q'[q].$$

We now prove these results: we begin by proving Lemma 7, then each part of Theorem 7. We use the notations of §§2.5 and 3.2, and we shall assume throughout the proof, without loss of generality, that x_1 is greater than $pn/2q$. So, the point $m(x_1)$ belongs to the positive part $T^+(\nu)$ of a segment $T(\nu)$. We consider successive segments $T(\nu)$ of the legs and the positive parts $S^+(\nu)$ of their horizontal projections:

$$[a(\nu) - u_0, b(\nu) - u_0]$$

with

$$a(\nu) = \sqrt{\frac{\nu n}{q} - 2h} = \sqrt{(\nu + t - 1)\frac{n}{q}} \quad \text{and} \quad b(\nu) - \sqrt{\frac{\nu n}{q}}.$$

We wish to compare the position of these abscissae for successive values of ν. It is clear that this comparison depends on the sign of t, where t is always less than 1 in absolute value.

4.3. **Properties of ordinary points. Proof of Lemma 7.** The first inequality for the index ν, namely $\nu \geq 2$, is clear. As to the assertion $\nu \leq \nu_2 - 1$, we obtain by equations (7) and (13)

$$u_1^2 \leq \frac{3h^2}{16q^2} \leq \left[\frac{h^2}{4qn} - 4\right]\frac{n}{q} \leq (\nu_2 - 3)\frac{n}{q} \leq a(\nu_2 - 1)^2,$$

so that the index ν of x_1 is less than $\nu_2 - 1$.

We now derive an upper bound for the cardinality of the complementary subset, which we call exceptional and denote by E. We have

$$|E| \leq \sum 2\sqrt{\frac{2n}{q}} + \sum\left(1 - \frac{\sqrt{3}}{2}\frac{h}{q}\right),$$

where the sums are taken over the integers (p, q) satisfying the two conditions $|p| \leq q \leq k$ and $(p, q) = 1$. The first sum is at most $n\sqrt{2}/6$, while the second is at most $n(1 - \sqrt{3}/2)$, and finally an upper bound for $|E|$ is $3n/8$.

4.4. **Part of Theorem 7. Part 1.** Consider the index ν of an ordinary point x_1. By Lemma 7, the point $m(x_1)$ associated with x_1 by means of our usual transfer belongs to a segment $T^+(\nu)$ that lies in the legs or in the lowest part

of the chest. If the segment lies in the legs, the length $s(\nu)$ of its horizontal projection is greater than $2q$ by relation (9) and it surely contains at least two points of the lattice. If it lies in the chest, our hypothesis says that it cannot be too high in this chest, so that it is sufficiently long and also contains two points of the lattice.

4.5. **Proof of Theorem 7. Case when** $q \geq k/2$. If t is negative (i.e., $q \geq k/2$ and $-1 \leq t \leq 0$), the horizontal projections $S^+(\nu)$ of the segments $T^+(\nu)$ are not disjoint (cf. Figure 4). We must determine how they overlap each other. We consider an ordinary point x_1 of $B \cap I(p, q)$ with an index equal to ν. Thus, the two quantities $b(\nu+1) - b(\nu)$ and $a(\nu) - a(\nu-1)$ measure the degree of this overlapping around this point x_1, and we get a lower bound for them.

On the right of $T(\nu)$, we obtain

$$b(\nu+1) - b(\nu) = \sqrt{(\nu+1)\frac{n}{q}} - \sqrt{\nu\frac{n}{q}} \geq \frac{n}{2q}\,\frac{1}{b(\nu+1)},$$

and we deduce from Lemma 7 that

$$b(\nu+1) - b(\nu) \geq \frac{1}{2}\sqrt{\frac{n}{\nu_2 q}} \geq k \geq q.$$

Thus, there is a point of $L(x_0)$ which lies in $T(\nu+1)$, to the right of $m(x_1)$, such that the gap between x_1 and its right neighbor is at most q.

On the left of $T(\nu)$, we use a lower bound for $a(\nu) - a(\nu-1)$. Since the sequence of the $s(\nu)$ is decreasing, we obtain

$$a(\nu) - a(\nu-1) = b(\nu) - b(\nu-1) + s(\nu-1) - s(\nu) \geq q,$$

so that there is a point of $L(x_0)$ which lies in $T(\nu-1)$ and to the left of $m(x_1)$. We conclude that the gap between x_1 and its left neighbor is at most q.

Finally, the two gaps around an ordinary point are at most q.

We remark also that, since $t \geq -1$, the abscissa $a(\nu+3)$ is greater than $b(\nu+1)$, so that the two segments $S(\nu)$ and $S(\nu+3)$ are at a distance greater than q. So, if the point $m(x_1)$ belongs to a line $D(\nu)$, a point $m(x)$ associated with a next neighbor x of x_1 can only belong to the five lines $D(\nu+\alpha)$, with α an integer at most 2 in absolute value. According to Lemma 5, the horizontal shift between points of $L(x_0) \cap D(\nu)$ and those of $L(x_0) \cap D(\nu+1)$ is equal to q' in absolute value. This proves Part 2 of Theorem 7.

4.6. **Proof of Theorem 7. Case when** $q < k/2$. If t is positive (i.e., $q < k/2$ and $0 < t < 1$), the segments $S(\nu)$ are disjoint (cf. Figure 5). So the natural order on $I(p, q)$ is induced by the natural order on $P(p, q)$. Thus, in this case, since the point $m(x_1)$ has at least one P-neighbor $m(x)$ in the segment $T(\nu)$ at a distance exactly equal to q, the two points x_1 and x are B-neighbors, with a spacing equal to q between them.

The same fact may hold true for the other B-neighbor x' of x_1, if the point $m(x_1)$ has another P-neighbor in the segment $T(\nu)$. But, we must consider also the case when $m(x_1)$ is at the end of the segment $T(\nu)$.

First consider the case when $m(x_1)$ is the last point on the right of $T(\nu)$. Thus, the gap between x_1 and its right neighbor is at most $a(\nu+1)-b(\nu)+2q$ and at least $a(\nu+1)-b(\nu)$. We get estimates for $a(\nu+1)-b(\nu)$:

$$a(\nu+1)-b(\nu)=b(\nu)\left[\sqrt{1+\frac{t}{\nu}}-1\right]$$

and

$$\frac{7tn}{16q}\frac{1}{b(\nu)}\le a(\nu+1)-b(\nu)\le\frac{tn}{2q}\frac{1}{b(\nu)},$$

since the index ν of the ordinary point x_1 is at least 2. Now, if $m(x_1)$ is the last point of $L(x_0)$ on the right of $T(\nu)$, we have

$$b(\nu)-q\le u_1\le b(\nu).$$

But, by hypothesis, we also have from (13)

$$u_1^2\ge\frac{2n}{q}\ge\frac{4n}{k}=4h=2^8k^2\ge 2^{10}q^2,\quad\text{so that } u_1\ge 32q, \tag{14}$$

and

$$b(\nu)\le(u_1+q)\le\tfrac{33}{32}u_1.$$

We deduce that

$$\frac{tn}{3qu_1}\le a(\nu+1)-b(\nu)\le\frac{tn}{2qu_1}. \tag{15}$$

In the same vein, if $m(x_1)$ is the last point on the left of $T(\nu)$, the gap between x_1 and its left neighbor is at most $a(\nu)-b(\nu-1)+2q$ and at least $a(\nu)-b(\nu-1)$. We get estimates for $a(\nu)-b(\nu-1)$:

$$\frac{tn}{2q}\frac{1}{a(\nu)}\le a(\nu)-b(\nu-1)\le\frac{5tn}{8q}\frac{1}{a(\nu)},$$

since the index ν of the ordinary point x_1 is greater than 2. Now, if $m(x_1)$ is the last point of $L(x_0)$ on the left of $T(\nu)$, we have

$$a(\nu)\le u_1\le a(\nu)+q$$

and, by (14),

$$\tfrac{8}{5}a(\nu)\ge\tfrac{8}{5}(u_1-q)\ge\tfrac{3}{2}u_1.$$

We deduce that

$$\frac{tn}{2qu_1}\le a(\nu)-b(\nu-1)\le\frac{2tn}{3qu_1}. \tag{16}$$

Finally, comparing relations (15) and (16) that summarize the two cases, we obtain the announced bound. We use the horizontal shift of Lemma 5 to complete the proof of Part 3 of Theorem 7, and also the proof of the whole theorem.

4.7. **A precise description of the pattern of B near an ordinary point.** The right half $O^+(p, q)$ of the ordinary part $O(p, q)$ of the Farey interval $I(p, q)$ may be written as the disjoint union of segments

$$\Pi(j) = \left[\frac{pn}{2q} + b(\nu_0 + j + 1), \frac{pn}{2q} + b(\nu_0 + j + 2)\right),$$

where the integer j varies from 1 to $\nu_2 - \nu_0$. (The indices ν_0 and ν_2 are defined in §3.1.)

We use these intervals to define the pattern that we observed in §2.1. More precisely, we can easily describe gaps between successive elements of $B \cap \Pi(j)$: they form what we call the jth pattern of B inside $O^+(p, q)$. The jth pattern has length $\pi(j)$ which follows the approximate law

$$\pi(j) \approx \frac{1}{2}\sqrt{\frac{n}{(\nu_0 + j + 1)q}}.$$

If $q < k/2$, the jth pattern begins by a first gap g—a big one—, approximately equal to

$$g \approx t\pi(j);$$

then, there is a sequence of gaps, all equal to q. The number $N_1(j)$ of terms of this sequence is approximately equal to $N(\nu_0 + j + 1)/2$, where N denotes the function defined in §3.2. We have

$$N_1(j) \approx (1 - t)\frac{\pi(j)}{q}.$$

If $q \geq k/2$, the jth pattern is divided between two subpatterns separated by gaps:

- a first subpattern which is a sequence of $N_2(j)$ gaps all equal to q,
- then a gap g,
- after this, a sequence of $N_3(j)$ pairs of gaps $(q', q - q')$,
- and finally another gap g'.

The two numbers $N_2(j)$ and $N_3(j)$ are approximately equal to

$$N_2(j) \approx (1 - |t|)\frac{\pi(j)}{q} \quad \text{and} \quad N_3(j) \approx |t|\frac{\pi(j)}{q}.$$

Note that the gaps g and g' may depend on the integer j, but they must belong to the set G defined in Theorem 7, possibly associated with an α equal to 2 in absolute value.

We have thus obtained an approximate description, where all the approximations are given up to strictly positive absolute multiplicative constants. Here, "absolute" means independent of the index ν, of the pair (p, q), and the modulus n. We provide a quasi(!)-description of the Pattern Occurrence, and we can verify that it explains well our experimental facts of §2.1.

4.8. **The Neighbors Algorithm.** As before, we consider an ordinary point x_1 of $O(p, q)$, at a distance u_1 from $pn/(2q)$. For an easier description of the algorithm, and without loss of generality, we shall suppose that x_1 is greater than $pn/(2q)$.

But, here, point x_1 need not belong to B, and we now explain how to find the two B-neighbors of the point x_1. We gather the results of previous subsections, and we obtain a description of the Neighbors Algorithm. This is a polynomial-time algorithm that succeeds on the ordinary subset.

Input. A random point x_1 of $Z(n)$.

Output. The two neighbors x_1^- and x_1^+ of x_1 in B.

(1) With the last best approximation of $2x_1/n$ with denominator less than k, denoted by p/q, determine the Farey interval $I(p, q)$ which contains x_1 and the integer x_0 nearest to the rational $pn/(2q)$.

Calculate the distance u_1 of x_1 to $pn/(2q)$ and check whether x_1 is ordinary. If not, the algorithm fails.

(2) Determine the index ν such that $u_1 \in [b(\nu), b(\nu+1))$.

If $q < k/2$, there are only three possibilities for the index μ of the next B-neighbors of x_1: it can only belong to the set $M = \{\nu, \nu+1, \nu+2\}$.

If $q \geq k/2$, there are only five possibilities for the index μ of the next B-neighbors of x_1: it can only belong to the set $M = \{\nu-1, \nu, \nu+1, \nu+2, \nu+3\}$.

(3) On each line $D(\mu)$ to be considered, determine the abscissae $u^-(\mu)$ and $u^+(\mu)$ of two points of $P(p, q)$ nearest to the line of equation $u + u_0 = u_1$, and finally the two next B-neighbors x_1^- and x_1^+ of x_1 by the relations

$$x_1^- = x_0 + \mathrm{Max}\{u^-(\mu) | \mu \in M\} \quad \text{and} \quad x_1^+ = x_0 + \mathrm{Min}\{u^+(\mu) | \mu \in M\}.$$

The analysis of the complexity of this algorithm is clear and gives the following result.

Theorem 8. *The Neighbors Algorithm is a polynomial-time algorithm which finds the two next B-neighbors of an ordinary point or fails. The subset where the algorithm succeeds has a density larger than* $5/8$.

5. Discussions and conclusion

We place here our method and our results in the context of previously known results, both within classical number theory and computational number theory.

5.1. **Discussion of the choice** $\alpha = 2/3$. A natural question to ask is: Why does our method work well for α near $2/3$? Can it be generalized for other values of the parameter α greater than α_0?

It is clear that the transfer of the problem to the lattice $L(x_0)$ works for all values of the parameter α: we use the auxiliary parameters $h = 4n^\alpha$ and $k = (1/4)n^{1-\alpha}$, and we define the domain $P(p, q)$. The quasi-uniform law of $N(\nu)$ in the legs remains true and the computations in the legs and in the feet

can be started in the same way. However, one cannot generalize our method in a straightforward way for values of the parameter α smaller than $2/3$: in these cases, the legs may be very short, and the chest very big! First, relation (7) no longer holds true, so that the lower bound (10) in the legs is no longer valid. Second, the behavior of the number of points in the chest may have large variations and can no longer be compared with the expected number N_e.

During the study of the set $B(\alpha)$, the area of the chest which is of order $n^{3\alpha/2}$ has to be compared with the determinant n of our lattice $L(x_0)$. This is why the value $2/3$ of the parameter α is a natural one. When $\alpha < 2/3$, one cannot predict the number of points of $L(x_0)$ in the chest. This is all the more true since all the lattices that we use are irregular [8]: they have a shortest vector that is very short, i.e., much shorter than $n^{1/2}$. *We thus see that* $\alpha = 2/3$ *is optimal for this class of methods.*

5.2. **Using the Two-Thirds Algorithm.** Using our algorithm, we have at our disposal a range of algorithms depending on the optimizations we elect to adopt in the $D[\alpha]$ algorithm for $\alpha = 2/3$ (in Step 2 for matrix formation, and Step 3 for elimination). We only discussed the best possible bound of $L^{\sqrt{4/3}}$, but it may be of interest to observe that a bound of $L^{\sqrt{2}}$, which was the previously known complexity record, is easily obtained by using Pollard-Strassen's factorization in Step 2. Some of the time-bound exponents associated with various optimizations are summarized below (compare with the corresponding table in [5]).

Basic	$\sqrt{8/3} = 1.632$
Pollard-Strassen	$\sqrt{2} = 1.414$
Early Abort	$\sqrt{7/3} = 1.527$
Pomerance [5]	$\sqrt{5/3} = 1.290$
Pomerance [6]	$\sqrt{4/3} = 1.154$

Also, on the practical side, we can transform the Two-Thirds Algorithm into a heuristic algorithm of $B(\alpha)$ with $\alpha < 2/3$: it is sufficient to always choose in Step 3 the point of $L(x_0)$ nearest to the middle of segment $S(\nu)$. In this way, we abandon a rigorously established quasi-uniformity property, but we expect a gain in obtaining quadratic residues smaller than $n^{2/3}$ whose square roots still retain some sort of randomness, since they are spread over the whole of the interval $Z(n)$. This approach contrasts with the particular set of quadratic residues obtained by the continued fraction algorithm [4].

5.3. **Coming back to the estimate of the cardinality of** B. Note that Theorem 4 also gives an evaluation of the global cardinality of B. Since the Farey covering is a 2-partition, we deduce from §3.3 that

$$\tfrac{1}{2}\sum |B \cap I(p, q)| \leq |B| \leq \sum |B \cap I(p, q)|,$$

where the sum is taken over the integers (p, q) satisfying the two conditions $|p| \leq q \leq k$ and $(p, q) = 1$; from this, we obtain

$$\frac{1}{10} \leq \frac{|B|}{2h} \leq 4.$$

These bounds are of course less sharp than the bounds of Theorem 3, but they do not involve any arithmetic property of the modulus n, while the proof of Theorem 3 is principally based on the prime decomposition of the modulus. Furthermore, our results of §2 are locally stronger, since the Pólya-Vinogradov inequality cannot give any local estimate. Note also that the local distribution of B is largely independent from arithmetic properties of the modulus n.

So, in the particular case when $\alpha = 2/3$, we have developed a geometric method which gives an alternative result about the cardinality of B. Our result is weaker from the global point of view, but much stronger from the local point of view.

5.4. **An explanation of experimental facts.** Our study of the subset B was motivated to a large extent, at least in the beginning, by the links that it has with the $D[\alpha]$ method. But the results of our numerical experiments were so curious that we guessed much more structure in this subset than we could hope for. We could actually explain these structural properties with simple tools—Farey intervals, lattices—that are well adapted to this problem. So, the subset B is interesting in itself, and also as a good example of Mathematics of Computation!

Acknowledgments

I wish to thank Philippe Flajolet for all the help he gave me in this work: the idea of using the Pólya-Vinogradov inequality, probabilistic clarifications, and many numerical experiments, not to speak of encouragement. I wish also to thank Claus Schnorr, who improved my previous bounds for Lemma 2, and Andrew Odlyzko, who helped me to simplify the proof of this lemma. An anonymous referee pointed out some errors and encouraged me to make precise all the notions of "quasi" in this paper. Many thanks to him/her!

This work was supported partly by PRC "Mathématiques et Informatique" and partly by a contract with SEPT.

Bibliography

1. T. M. Apostol, *Modular functions and Dirichlet series in number theory*, Springer, New York, 1976.
2. H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York, 1980.
3. J. D. Dixon, *Asymptotically fast factorization of integers*, Math. Comp. **36** (1981), 255–260.
4. M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of* F_7, Math. Comp. **29** (1975), 183–205.
5. C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational Methods in Number Theory: Part I, Math. Centre Tract, no. 154, 1982, pp. 89–139.

6. C. Pomerance, *Fast, rigorous factorization and discrete logarithm algorithms*, Proc. Japan–U.S. Joint Seminar, Discrete Algorithms and Complexity, Academic Press, 1987, pp. 119–143.
7. ——, *The quadratic sieve factoring algorithm*, Advances in Cryptology, Proc. Eurocrypt 84, Paris 1984 (T. Beth, N. Cot, and I. Ingemarsson, eds.), Lecture Notes in Comput. Sci., vol. 209, Springer, 1985, pp. 67–79.
8. B. Vallée, M. Girault, and Ph. Toffin, *How to guess l-th roots modulo n by reducing lattice bases*, Proc. AAECC-6, Roma 1988, Lecture Notes in Comput. Sci., vol. 357, Springer, 1989, pp. 427–442.
9. B. Vallée, *Provably fast integer factoring with quasi-uniform small quadratic residues*, Proc. 21st ACM Sympos. on Theory of Computing, Seattle, 1989, pp. 98–106.

DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ DE CAEN, F-14032 CAEN CEDEX, FRANCE
E-mail address: vallee@geocub.greco-prog.fr