Prime Number Generation Without Factorization: A Hyperbola-Based Algorithm

Jayme Mendes[1].

Abstract. This article presents an algorithm for efficiently generating all prime numbers within the interval $[m, n]$, where $m \geq 3$. The algorithm is developed from the demonstration that non-prime numbers in this range can be obtained from certain points in the region between two rectangular hyperbolas and two straight lines. The method does not perform factorization tests and does not require prior knowledge of any prime number, which makes it easier to obtain large primes for $n - m = q = constant$, when the time and memory complexities become equal to $\mathcal{O}(\log n)$ and $\mathcal{O}(1)$, respectively.

Keywords: prime numbers, sieve algorithm, rectangular hyperbolas, computational complexity, number theory.

0.1 Introduction

This article introduces a algorithm that leverages the geometric properties of rectangular hyperbolas to generate all prime numbers within a specified interval $[m, n]$, where $m \geq 3$ and m and n are odd integers. Unlike traditional sieves that rely on sequential divisibility tests or precomputed prime lists, our method operates by systematically excluding composite numbers identified within a specific region defined by these hyperbolas. This approach distinguishes itself by its independence from prior prime knowledge and the absence of factorization tests, thereby offering a unique perspective on prime number generation [1, 2].

The algorithm begins by constructing set A, comprising all odd numbers within the interval $[m, n]$, which serves as the candidate set for primes. The set S, containing all composite odd numbers in the same interval, is then derived. The prime number set $\mathbb{P}$ is obtained through the set difference $\mathbb{P} = A \setminus S$. The core contribution of this work lies in the geometric characterization of S, demonstrating that its elements correspond to points within a region bounded by two rectangular hyperbolas and two straight lines in the Cartesian plane. This geometric insight enables a highly efficient method for identifying and excluding composite numbers.

Furthermore, we analyze the algorithmic complexity of our method, revealing that it achieves a time complexity of $\mathcal{O}(n \log n)$ in general cases and a remarkable $\mathcal{O}(\log n)$ when the interval size $n - m$ is held constant. This efficiency, particularly for large intervals, positions our algorithm as a promising tool for generating large prime numbers, a critical requirement in modern cryptographic applications [3, 4].

This article is structured as follows: it presents the geometric framework, the formal definitions and the main theorem, outlining the construction of the set of composite numbers of S; details the proof of the theorem, elucidating the geometric foundations of the approach; provides pseudocode and an illustrative example, demonstrating the practical application of the algorithm; investigates algorithmic complexity analysis, highlighting the efficiency of the method; and concludes with a summary of the results and possible paths for future research.

[1] *jayme@ime.eb.br; ime.eb.mil.br/en/;*
github.com/Mergener/prime-hyperbola

0.2 Geometric Framework and Conceptual Overview

The presented sieving algorithm is based on a set-theoretic framework that unites number theory and geometric principles, as formalized by the theorem in the next section. By mapping prime number identification onto the Cartesian plane, we leverage the inherent symmetries and properties of rectangular hyperbolas to isolate composite numbers. This geometric perspective offers both a visual intuition for prime distribution and a computationally efficient mechanism for their identification [1].

The fundamental point of this approach is that composite numbers within a given interval $[m, n]$ correspond to points (x, y) situated within a region limited by the rectangular hyperbolas $xy = m$ and $xy = n$, and by the lines $x = 3$ and $y = 3$. These boundaries ensure the consideration of only relevant composite candidates, allowing the algorithm to systematically exclude non-primes without resorting to traditional divisibility tests or precomputed prime lists [3, 4].

Capitalizing on this geometric characterization of composite numbers, the algorithm efficiently filters out non-prime elements by exploiting the properties of hyperbolas. This method proves particularly advantageous for large intervals, mitigating the computational overhead inherent in conventional sieving techniques [5]. The subsequent formal definitions and theorem provide a rigorous mathematical foundation for this approach, demonstrating how the geometric properties of hyperbolas can be harnessed for prime number generation. The theorem not only validates the algorithm's correctness but also underscores its efficiency, paving the way for practical applications in cryptography and computational number theory [6].

0.3 Definitions

Let x be a real number. We define[2]:

$$\lceil x \rceil^* := \min\{q \in \{2\mathbb{N}+1\} \mid q \geq x\} \quad \text{and} \quad \lfloor x \rfloor^* := \max\{q \in \{2\mathbb{N}+1\} \mid q \leq x\}.$$

0.4 Theorem

Let m and n be odd natural numbers such that $3 \leq m \leq n$. Define the set A as:

$$A = \{i \mid i \text{ is odd}, m \leq i \leq n\}.$$

Let $S = B \cup C$ be the set of all composite odd numbers in A, where:

$$B = \left\{ i \cdot (\lceil m/i \rceil^* + j) \mid i \in \{3, 5, \ldots, \lfloor \sqrt{m} \rfloor^*\}, j \in \{0, 2, \ldots, (\lfloor n/i \rfloor^* - \lceil m/i \rceil^*)\} \right\},$$

and

$$C = \{(\lfloor \sqrt{m} \rfloor^* + i) \cdot (\lfloor \sqrt{m} \rfloor^* + i + j) \mid i \in \{2, 4, \ldots, (\lfloor \sqrt{n} \rfloor^* - \lfloor \sqrt{m} \rfloor^*)\},$$
$$j \in \{0, 2, ..., (\lfloor n/(\lfloor \sqrt{m} \rfloor^* + i) \rfloor^* - \lfloor \sqrt{m} \rfloor^* - i)\}$$

Then, $\mathbb{P} = A \setminus S$ is the set of prime numbers in A.

---

[2]It is not difficult to demonstrate that $\lfloor x \rfloor^* = 2\lfloor x/2 \rfloor - (-1)^{\lfloor x \rfloor}$ and $\lceil x \rceil^* = 2\lceil x/2 \rceil + (-1)^{\lceil x \rceil}$.

0.5 Proof of the theorem

As mentioned above, the set A is defined as $A = \{m, m+2, m+4, ..., n\}$, where n and m are odd numbers. Therefore, it remains to demonstrate that the set S is precisely as stated in the theorem: "Let $S = B \cup C$ be the set of all non-prime odd numbers in A".

In the first quadrant of the xy plane, the coordinates of the points (x, y) whose products satisfy the condition $m \leq x \cdot y \leq n$ are delimited by the rectangular hyperbolas $y = m/x$ and $y = n/x$ [7], respectively; i.e. $m/x \leq y \leq n/x$. Furthermore, since the set S must contain only non-prime odd numbers given by $x \cdot y$, x and y must both be odd numbers greater than or equal to 3. Therefore, the elements of S are in the region delimited by: $y \geq 3$, $x \geq 3$, $m/x \leq y \leq m/x$. However, for the sake of symmetry, the same values of $x \cdot y$ in this quadrant are found for both $y \geq x$ and $y \leq x$. We can then choose the region bounded by $x \geq 3$, $y \geq x$ and $m/x \leq y \leq n/x$ to obtain the elements $x \cdot y$ of S (fig.[1]).

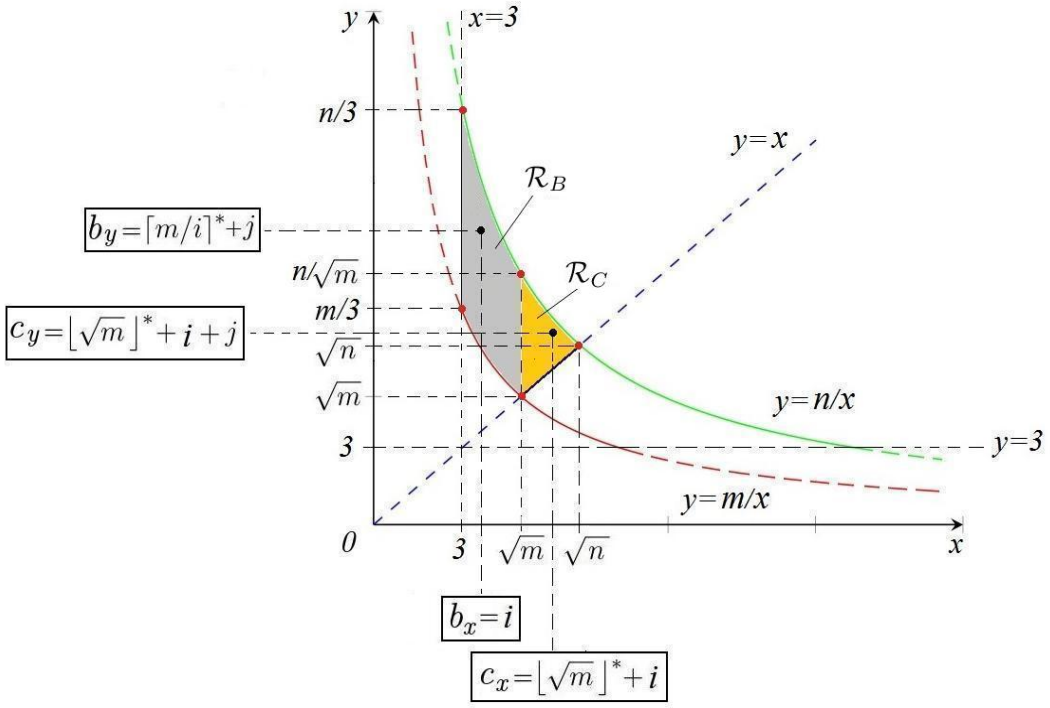

Figure 1: Points with coordinates x and y given by odd numbers that form all non-prime odd numbers $x \cdot y$ in the interval $[m, n]$ in regions B and C: $\mathcal{R}_B = \{(x, y) \mid 3 \leq x \leq \sqrt{m},\ m/x \leq y \leq n/x\}$; $\mathcal{R}_C = \{(x, y) \mid \sqrt{m} < x \leq \sqrt{n}\ ,\ x \leq y \leq n/x\}$.

To facilitate the construction of S as $S = B \cup C$, we define the sets B and C, whose associated regions are described below and illustrated in fig.[1].

The set B consists of non-prime odd numbers obtained as products $x \cdot y$, where x and y are odd coordinates within the following region:

$$\mathcal{R}_B = \{(x, y) \mid 3 \leq x \leq \sqrt{m},\ m/x \leq y \leq n/x\} \tag{1}$$

Thus, the set formed by the odd coordinates x in $\mathcal{R}_B$ is given by

$$\{b_x\} = \{3, 5, 7, \ldots, \lfloor \sqrt{m} \rfloor^*\} = \{i \mid i = 3, 5, 7, \ldots, \lfloor \sqrt{m} \rfloor^*\}$$

and the set formed by the odd coordinates y in $\mathcal{R}_B$ is given by

$$\{b_y\} = \{\lceil m/i \rceil^*, \lceil m/i \rceil^* + 2, \ldots, \lfloor n/i \rfloor^*\} = \{\lceil m/i \rceil^* + j \mid j = 0, 2, \ldots, (\lfloor n/i \rfloor^* - \lceil m/i \rceil^*)\},$$

Finally, the set $B = \{b_x\} \odot \{b_y\}$, defined as an ordered distributive product of sets[3], is given by

$$B = \{b_x\} \odot \{b_y\} = \{i \cdot (\lceil m/i \rceil^* + j) \,|\, i = 3, 5, \ldots, \lfloor \sqrt{m} \rfloor^*, j = 0, 2, \ldots, (\lfloor n/i \rfloor^* - \lceil m/i \rceil^*)\} \quad (2)$$

The elements of the set C are non-prime odd numbers given by the products $x \cdot y$, where x and y are odd numbers in the region delimited by

$$\mathcal{R}_C = \{(x, y) \mid \sqrt{m} < x \leq \sqrt{n} \ , \ x \leq y \leq n/x\} \quad (3)$$

Thus, the set formed by the odd coordinates x in $\mathcal{R}_C$ is given by

$$\{c_x\} = \{\lfloor \sqrt{m} \rfloor^* + 2, \lfloor \sqrt{m} \rfloor^* + 4, ..., \lfloor \sqrt{n} \rfloor^*\} = \{\lfloor \sqrt{m} \rfloor^* + i \,|\, i = 2, 4, 6, ..., \left(\lfloor \sqrt{n} \rfloor^* - \lfloor \sqrt{m} \rfloor^*\right)\}$$

and the set formed by the odd coordinates y in $\mathcal{R}_C$ is given by

$$\{c_y\} = \{\lfloor \sqrt{m} \rfloor^* + i, \lfloor \sqrt{m} \rfloor^* + i + 2, ..., \lfloor n/(\lfloor \sqrt{m} \rfloor^* + i) \rfloor^*\} =$$

$$= \{\lfloor \sqrt{m} \rfloor^* + i + j \,|\, j = 0, 2, ..., (\lfloor n/(\lfloor \sqrt{m} \rfloor^* + i) \rfloor^* - \lfloor \sqrt{m} \rfloor^* - i)\}$$

Finally, the set C is given by ordered distributive product $C = \{c_x\} \odot \{c_y\}$:

$$C = \{c_x\} \odot \{c_y\} = \{(\lfloor \sqrt{m} \rfloor^* + i) \cdot (\lfloor \sqrt{m} \rfloor^* + i + j) \,|$$

$$i = 2, 4, ..., \left(\lfloor \sqrt{n} \rfloor^* - \lfloor \sqrt{m} \rfloor^*\right) \ , \ j = 0, 2, ..., (\lfloor n/(\lfloor \sqrt{m} \rfloor^* + i) \rfloor^* - \lfloor \sqrt{m} \rfloor^* - i)\} \quad (4)$$

It is thus demonstrated that

$$S = B \cup C$$

contain all non-prime odd numbers in the range $[m, n]$ and therefore the set of prime numbers in the same range is equal to

$$\mathbb{P} = A \setminus S$$

End of proof

0.6 **Examples**

- $[m, n] = [25, 81]$

As an example of what was shown above, let us look at the example (fig.[2]) for $m = 25$ and $n = 81$ [9]. The first approach in this example relies on directly visualizing the geometry of the problem, as can be seen in figure [2].

The geometric locus in the xy plane where $x \cdot y = n = 81$ and $x \cdot y = n = 25$ are the rectangular hyperbolas $y = 81/x$ and $y = 25/x$, respectively, shown in fig.[2]; while the set of all non-prime odd numbers $x \cdot y$ in the interval $[25, 81]$ are located in the region bounded by $y \geq x$, $x \geq 3$ and $25/x \leq y \leq 81/x$ (hatched region in fig.[2]).

From fig.[2] we directly obtain the elements of the set S, given by $x \cdot y$ in the interval $25 \leq x \cdot y \leq 81$:

$$S = \{25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69, 75, 77, 81\}.$$

[3] Let $P = \{p_i | i = 1...m\}$ and $Q = \{q_{ij} | i = 1...m, j = 1...n\}$ be two ordered sets. We define the ordered distributive product of P and Q, denoted by $P \odot Q$, as the set: $P \odot Q = \{p_i \cdot q_{ij} \mid i = 1...m, j = 1...n\}$ where each element of P is multiplied by all elements of Q, preserving the order of P as the primary factor.

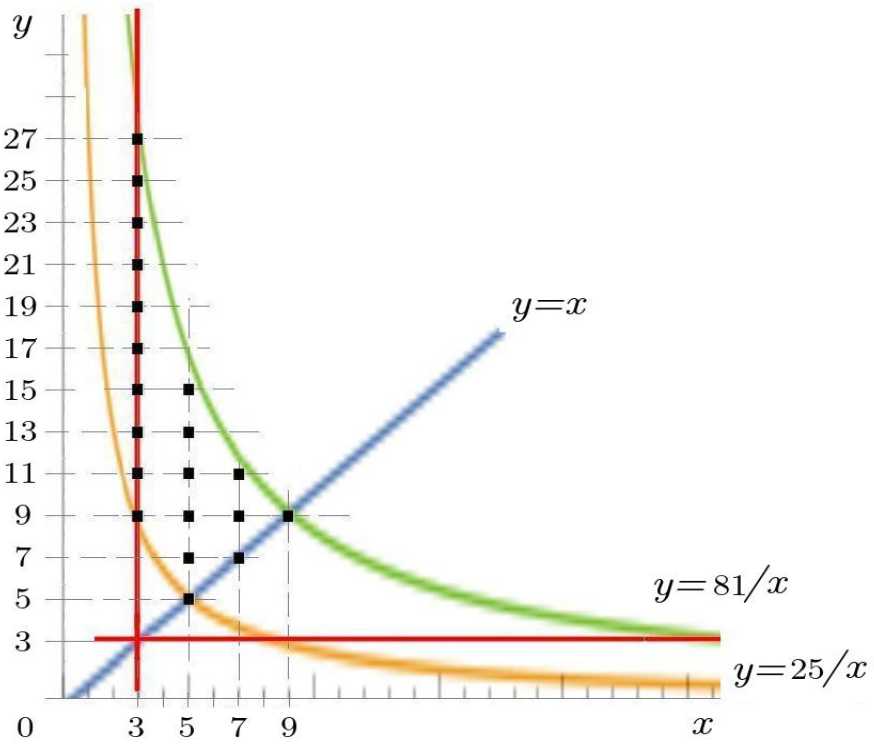

Figure 2: Points with coordinates x and y given by odd numbers representing all non-prime odd numbers in the interval $[m, n] = [25, 81]$ are located in the region $y \geq x$, $x \geq 3$ and $25/x \leq y \leq 81/x$.

On the other hand, the set of all odd numbers in the interval $[25, 81]$ is given by an arithmetic progression with a common difference of 2:

$$A = \{25,27,29,31,33,35,37,39,41,43,45,47,49,51,53,55,57,59,61,63,65,67,69,71,73,75,77,79,81\}.$$

Obviously, subtracting the above sets directly gives the set of prime numbers in the interval $[25, 81]$:

$$\mathbb{P} = A \setminus S = \{29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79\}$$

We will obtain below the set $\mathbb{P}$ for the interval $[25, 81]$ from the direct application of the theorem.

$$A = \{25,27,29,31,33,35,37,39,41,43,45,47,49,51,53,55,57,59,61,63,65,67,69,71,73,75,77,79,81\}$$

$$\begin{aligned}
B &= \{i \cdot (\lceil 25/i \rceil^* + j) \mid i \in \{3, 5, \ldots, \lfloor \sqrt{25} \rfloor^*\}, j \in \{0, 2, \ldots, (\lfloor 81/i \rfloor^* - \lceil 25/i \rceil^*)\}\} \\
&= \{i \cdot (\lceil 25/i \rceil^* + j) \mid i \in \{3, 5\}, j \in \{0, 2, \ldots, (\lfloor 81/i \rfloor^* - \lceil 25/i \rceil^*)\}\} = \\
&= \{3 \cdot (9 + j) \mid j \in \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}\} \cup \{5 \cdot (5 + j) \mid j \in \{0, 2, 4, 6, 8, 10\}\} \\
&= \{27, 33, 39, 45, 51, 57, 63, 69, 75, 81\} \cup \{25, 35, 45, 55, 65, 75\} \\
&= \{25, 27, 33, 35, 39, 45, 51, 55, 57, 63, 65, 69, 75, 81\}
\end{aligned}$$

and

$$C = \{(\lfloor \sqrt{25} \rfloor^* + i) \cdot (\lfloor \sqrt{25} \rfloor^* + i + j) \mid i \in \{2, 4, ..., (\lfloor \sqrt{81} \rfloor^* - \lfloor \sqrt{25} \rfloor^*)\},$$

$j \in \{0, 2, ..., (\lfloor 81/(\lfloor\sqrt{25}\rfloor^* + i)\rfloor^* - \lfloor\sqrt{25}\rfloor^* - i)\}\} =$

$= \{(5+i)\cdot(5+i+j) \mid i \in \{2,4\}, j \in \{0, 2, ..., (\lfloor 81/(5+i)\rfloor^* - 5 - i)\}\}$

$= \{7\cdot(7+j) \mid j \in \{0,2,4\}\} \cup \{9\cdot(9+j) \mid j \in \{0\}\} =$

$= \{49, 63, 77\} \cup \{81\} = \{49, 63, 77, 81\}$

then

$$S = B \cup C = \{25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69, 75, 77, 81\}$$

and

$$\mathbb{P} = A \setminus S =$$

$= \{25,27,29,31,33,35,37,39,41,43,45,47,49,51,53,55,57,59,61,63,65,67,69,71,73,75,77,79,81\} -$

$\{25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69, 75, 77, 81\}$

$$\mathbb{P} = \{29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79\}$$

- $[m, n] = [3, 11]$

$$A = \{3, 5, 7, 9, 11\}$$

$$B = \{i \cdot (\lceil 3/i\rceil^* + j) \mid i \in \{3, 5, \ldots, \lfloor\sqrt{3}\rfloor^*\}, j \in \{0, 2, \ldots, (\lfloor 11/i\rfloor^* - \lceil 3/i\rceil^*)\}\}$$

Since the last value of i ($i = \sqrt{3}$) is smaller than the first one ($i = 3$), the set B is empty:

$$B = \varnothing$$

And the set C will be constructed as shown below:

$C = \{(\lfloor\sqrt{3}\rfloor^* + i)\cdot(\lfloor\sqrt{3}\rfloor^* + i + j) \mid i \in \{2\}, j \in \{0, 2, ..., (\lfloor 11/(\lfloor\sqrt{3}\rfloor^* + i)\rfloor^* - \lfloor\sqrt{3}\rfloor^* - i)\}\}$

$= \{(\lfloor\sqrt{3}\rfloor^* + 2)\cdot(\lfloor\sqrt{3}\rfloor^* + 2 + j) \mid j \in \{0\}\} = \{9\}$

then

$$S = B \cup C = \varnothing \cup \{9\} = \{9\}$$

and

$$\mathbb{P} = A \setminus S = \{3, 5, 7, 9, 11\} - \{9\} = \{3, 5, 7, 11\}$$

0.7 Pseudocode

The pseudocode[10] below allows one to calculate prime numbers in the range $[m, n]$, according to what is described in the theorem.

```
// Assume:
//       n >= m
//       m >= 3
//       m and n are odd integers.
//       floor(x)* is x if x is odd or is an odd number closest to x
and below it if x is non-integer or even integer number
//       ceil(x)* is x if x is odd or is an odd number closest to x
and above it if x is non-integer or even integer number
//       isqrt(x) returns the highest integer y that satisfies y*y <= x
//
function Primes(m, n, f):
S <- Zero-initialized boolean array of size (n - m) / 2 + 1
P <- Set of primes, empty-initialized

// Compute set B.
for int i from 3 to floor(isqrt(m))* with step 2 do
for int j from 0 to floor(n / i)* - ceil(m / i)* with step 2 do
bij <- i * (ceil(m / i)* + j)
Mark S[(bij - m) / 2] as true

// Compute set C.
for int i from 2 to floor(isqrt(n))* - floor(isqrt(m))* with step 2 do
for int j from 0 to floor(n / (floor(isqrt(m))* + i))* - floor(isqrt(m))* -
i with step 2:
cij <- (floor(isqrt(m))* + i) * (floor(isqrt(m))* + i + j)
Mark S[(cij - m) / 2] as true

// All odd numbers between m and n that are not in S are primes.
for each Integer i from m to n with step 2 do
if S[(i - m) / 2] is false then
Add i to P

return P
```

0.8 Algorithmic complexity

0.8.1 Time complexity

The time complexity of iterating over set A is $\mathcal{O}(m-n)$, as the set contains $(n-m)/2+1$ elements. However, for $n - m = q = constant$, the complexity becomes $\mathcal{O}(1)$. The same argument above leads us to conclude that the time complexity to construct the set $\mathbb{P}$ is also given by $\mathcal{O}(n - m)$ in a general case and $\mathcal{O}(1)$ if $n - m = q = constant$.

The time complexity of the sieve developed in this article will be governed by the number of products $x \cdot y$ calculated to obtain the set S [3], according to the theorem presented (see fig.[1] and fig.[2]).

The calculation of the number of products $x \cdot y$ will be performed in two ways; the first, done by the exact count of the number of products using the functions $\lfloor x \rfloor^*$ e $\lceil x \rceil^*$, and the second uses the density of points on the plane and on the line, giving an approximate value, but easier to apply.

Exact calculation

Initially, we will calculate the number of points (x, y) with $9 \leq x \cdot y \leq n$ in the region $x \geq 3$, $y \geq 3$ and $y \leq n/x$ (fig.[3]). It can be observed that for each $y = j = 3, 5, 7, ..., \lfloor n/i \rfloor^*$, there are $x = i = 3, 5, 7, ..., \lfloor n/3 \rfloor^*$ values of x. Therefore, the number of points in this region will be given by the double sum below:

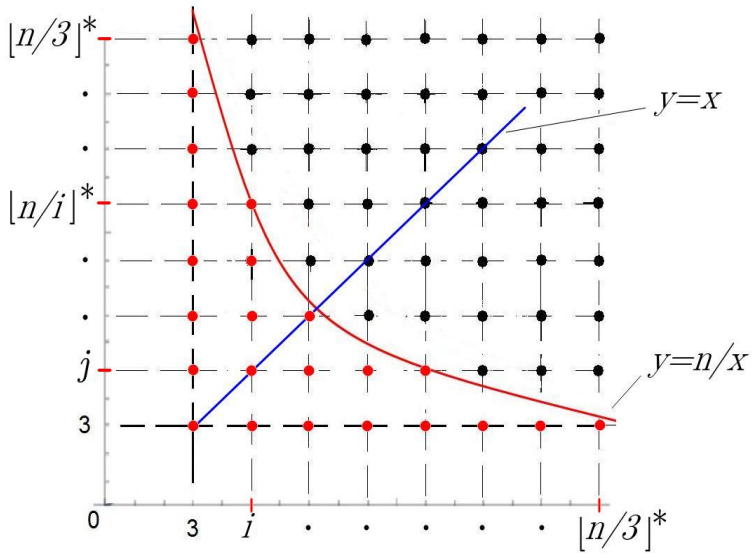

Figure 3: Points with coordinates x and y given by odd numbers representing all non-prime odd numbers in the interval $[9, n]$ are located in the region $y \geq x$, $x \geq 3$ and $9/x \leq y \leq n/x$.

- **Approximate calculation**

Considering (fig.[1], fig.[3]) that each square with side 2 and area 4 in the plane xy can be associated with 1 product $x \cdot y$, that the lines $x = 3$ and $y = x$ can be associated with $1/2$ product $x \cdot y$ at each interval $\Delta y = 2$ and $\Delta x = 2$, respectively, we can calculate the approximate total number of computed values as follows.

N_1 is the number of points inside the surface delimited by the hyperbolas $y = m/x$ and $y = n/x$ and the lines $x = 3$ and $y = x$ (fig.[1]):

$$N_1 \approx \frac{1}{4}\int_3^{\sqrt{m}} \left(\frac{n}{x} - \frac{m}{x}\right) dx + \frac{1}{4}\int_{\sqrt{m}}^{\sqrt{n}} \left(\frac{n}{x} - x\right) dx = \frac{n}{8}\log(n/9) - \frac{m}{8}\log(m/9) - \frac{1}{8}(n-m)$$

On the straight line $x = 3$, the length to be considered is equal to $n/3 - m/3$, therefore, we will have $((n/3 - m/3)/2 + 1)$ points separated by 2 units of length on this straight line segment. Considering that we must associate $(1/2)$ point to each interval (fig.[1]):

$$N_2 \approx \frac{n-m}{12} + \frac{1}{2}$$

The abscissa of interest on the line $y = x$ goes from $\sqrt{m}$ to $\sqrt{n}$, resulting in $(\sqrt{n} - \sqrt{m})/2 + 1$ points along the line (fig.[1]), then:

$$N_3 \approx \frac{\sqrt{n} - \sqrt{m}}{4} + \frac{1}{2}$$

The sum of N_1, N_2 and N_3 gives the total number of computed values:

$$N \approx \frac{n}{8}\log(n/9) - \frac{m}{8}\log(m/9) + \frac{1}{4}(\sqrt{n} - \sqrt{m}) - \frac{1}{24}(n-m) + 1 \tag{5}$$

From the above equation it can be concluded that the time complexity is given by $\mathcal{O}(n \log n)$ when the difference $n - m$ is not fixed.

Writing m as $m = n - q$, we have:

$$N \approx \frac{q}{8}\log((n-q)/9) - \frac{n}{8}\log(1 - q/n) + \frac{1}{4}\frac{q}{\sqrt{n} + \sqrt{n-q}} - \frac{q}{24} + 1 \tag{6}$$

Consequently, when $n - m = q$ is a constant, the time complexity reduces to $\mathcal{O}(\log n)$.

In comparison, the Sieve of Eratosthenes [11] and the Sieve of Atkin [4] have time complexities of $\mathcal{O}(n \log\log n)$ and $\mathcal{O}(n/\log\log n)$, respectively, which makes the sieve presented in this article promising for finding large prime numbers.

0.8.2 Memory complexity

The sieve uses a Boolean matrix [12] S to mark the composite numbers [13]. Knowing that $|S| \leq |A| = ((n-m)/2 + 1)$, where n and m are the limits of the range, the memory complexity of the sieve is $\mathcal{O}(n - m)$. If $(n - m) = q = constant$, the memory complexity becomes $\mathcal{O}(1)$.

0.9 Conclusion

This article presented a novel algorithm for the efficient generation of prime numbers within an interval $[m, n]$ based on the geometric properties of rectangular hyperbolas. The method stands out for not performing factorization tests and for not requiring prior knowledge of prime numbers, which differentiates it from traditional sieves. The proof of the theorem demonstrated the correctness of the algorithm by establishing a correspondence between composite numbers in the interval and points in specific regions bounded by hyperbolas and straight lines in the Cartesian plane.

The analysis of the algorithmic complexity revealed that the algorithm has a time complexity of $\mathcal{O}(n \log n)$ in the general case. More significantly, when the interval size $n - m$ is constant, the time complexity is reduced to $\mathcal{O}(\log n)$, and the memory complexity to $\mathcal{O}(1)$. This efficiency for constant-size intervals makes the algorithm particularly promising for the generation of large prime numbers, relevant in cryptographic applications.

Future research may explore additional optimizations in the implementation of the algorithm, as well as its adaptation for the generation of primes in even larger intervals or with specific characteristics. The investigation of possible parallelizations of the algorithm could also be an interesting path to further improve its performance.

Acknowledgements

I would like to express my deepest gratitude to Thomas Mergener (Pontifical Catholic University of Rio de Janeiro; https://www.puc-rio.br/english/) for his invaluable contributions to this work, including the implementation of the pseudocode and C++ code.

I would also like to extend my sincere appreciation to Sergio Vellozo (Military Institute of Engineering; https://www.ime.eb.mil.br/en/) for his meticulous review and insightful comments on the article.

References

[1] G.H. Hardy, E.M. Wright. *An Introduction to the Theory of Numbers*. 6th edition, Oxford University Press, 2008.

[2] H. Davenport. *Multiplicative Number Theory*. 3rd edition, Springer, 2000.

[3] R. Crandall, C. Pomerance. *Prime Numbers: A Computational Perspective*. 2nd edition, Springer, 2005.

[4] A.O.L. Atkin, D.J. Bernstein. *Prime sieves using binary quadratic forms*. Mathematics of Computation, 73(246), 2004.

[5] A. Granville. *Smooth numbers: computational number theory and beyond*. Algorithmic Number Theory, MSRI Publications, 44, 2008.

[6] D. Bressoud. *Factorization and Primality Testing*. Springer-Verlag, 1989.

[7] A. Baker. *A Concise Introduction to the Theory of Numbers*. Cambridge University Press, 1984.

[8] J. Sorenson. *The pseudosquares prime sieve*. Proceedings of the 7th International Symposium on Algorithmic Number Theory, 2006.

[9] J. Sorenson. *Two fast parallel prime number sieves*. Mathematics of Computation, 1998.

[10] T. Mergener. C++ *implementation at https://github.com/Mergener/prime-hyperbola*. 2025.

[11] M. O'Neill. *The Genuine Sieve of Eratosthenes*. Journal of Functional Programming, 2009.

[12] K. Kim & F. Roush.*Abstract Algebra*. https://www.sciencedirect.com/science/ article/abs/pii/B0122274105000193, 2001.

[13] T. Cormen, C. Leiserson, R. Rivest, & C. Stein. *Introduction to Algorithms* (3rd ed.). MIT Press. https://mitpress.mit.edu/9780262533058/introduction-to-algorithms/, 2009.

[14] D. Koukoulopoulos *Distribution of prime numbers*. American Mathematical Society, 2020.