Factor function and factorization

Moisej Plistiev

Faculty of Mathematics, University of Vienna

July 12, 2024

Objective

- Encode factorization and some other number theoretic problems in analytic functions
- Present an approach to root finding of analytic functions suitable for encoding

Computational Model I

Oracle Turing machine

An oracle TM which uses function oracles is an ordinary multi-tape TM:

- equipped with an additional tape, called the query tape, and
- an additional state, called the answering state.

computation

When an oracle TM M_ϕ, working with a functional oracle ϕ, enters the query state, the "oracle" ϕ replaces the current string y on the query tape by the new string $\phi(y)$, moves the read/write head of the query tape to the cell of the first symbol of $\phi(y)$, and places the machine M in the answering state. This action of the oracle ϕ counts only one unit of time.

Computational Model II

Let D denote the set of all dyadic rational numbers, i.e., rational numbers which have finite representations in binary expansion. Real numbers are represented by Cauchy sequences of dyadic rational numbers. More specifically, for any real number x, let CS_x be the set of all functions $\phi : \mathbb{N} \to D$ such that for all $n \in \mathbb{N}$, $|\phi(n) - x| \leq 2^{-n}$.

Computational Model III

Definition (Computable Real number)

A sequence $\{x_n\}$ of real numbers is polynomial-time computable if there exist a TM M and a polynomial p such that on input (n, k), M outputs a dyadic rational e satisfying $|e - x_n| \leq 2^{-k}$ in $p(n+k)$ moves.

Definition (Computable function)

A real function $f : [a, b] \to \mathbb{R}$ is computable if there is an oracle TM M such that for any $x \in [a, b]$, and $\phi \in CS_x$ and any $n > 0$, the machine M_ϕ, with input n and oracle ϕ, outputs a dyadic rational $e \in D$ such that $|e - f(x)| \leq 2^{-n}$. f is said to be polynomial-time computable if there also exists a polynomial p such that the machine M_ϕ, on input n, always halts in $p(n)$ moves (regardless of what the oracle function is).

Factor function

Now, let us introduce the function

$$f(x) := \sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)$$

where t is a natural number. The function has an interesting property:

Theorem

On the interval $[1, t]$ the function $f(x)$ equals zero if and only if $x \mid t$

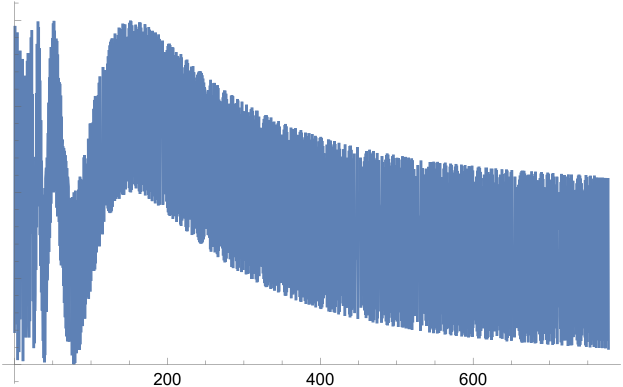
Proof.

Proof is based on 3 simple facts:

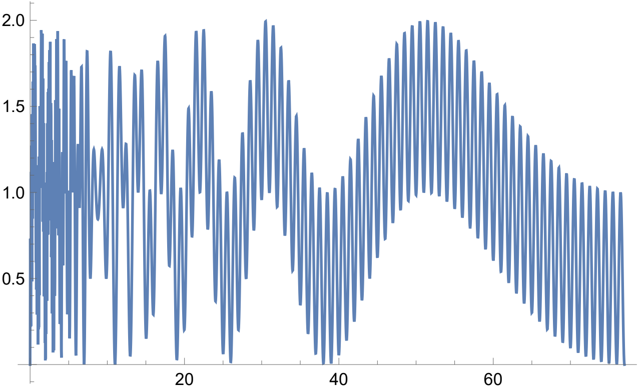
- The function is nonegative
- $\sin^2(\frac{\pi t}{x}) = 0$ if and only if $\frac{t}{x}$ is a natural number
- $\sin^2(\pi x) = 0$ if and only if x is a natural number

□

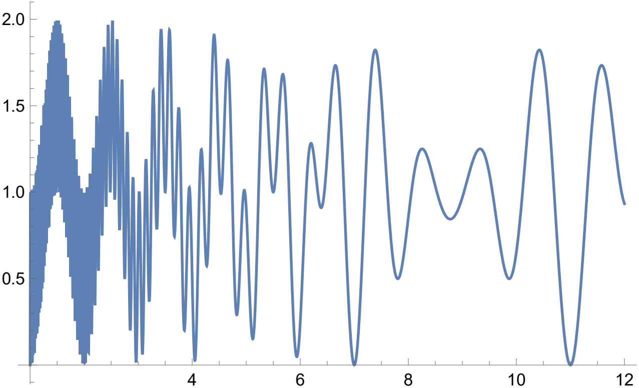
The function between 1 and 777



The function between 1 and 77



The function between 1 and 12



Modifications of factor function

Mentioned function has essential singularity in 0 and analytic everywhere else. It has conjugate complex zeros.We could transform $f(x)$ shifting on parameter v:

$$f_{shifted}(x) := \sin^2(\frac{\pi t}{x+v}) + \sin^2(\pi(x+v))$$

and compress on parameter v

$$f_{compressed}(x) := \sin^2(\frac{\pi t}{vx}) + \sin^2(\pi vx)$$

It can be also formulated as maxima version: the function, which has maxima iff x divides t:

$$f(x) := \cos^2(\frac{\pi t}{x}) + \cos^2(\pi x)$$

Other modifications

There is 2 - dimensional version:

$$f_(x, y) := \sin^2(\pi x) + \sin^2(\pi y) + (xy - t)^2$$

and

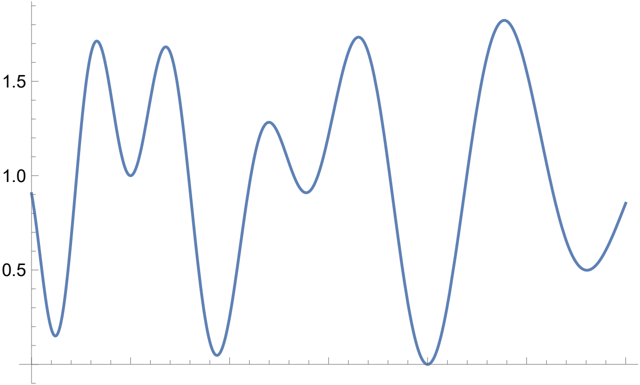
$$f_(x, y) := \sin^2(\pi x) + \sin^2(\pi y) + \sin^2(\pi xy/t)$$

For a Diophantine equation $= ax^2 + by = c$ there is a following property: The equation has zero if the function

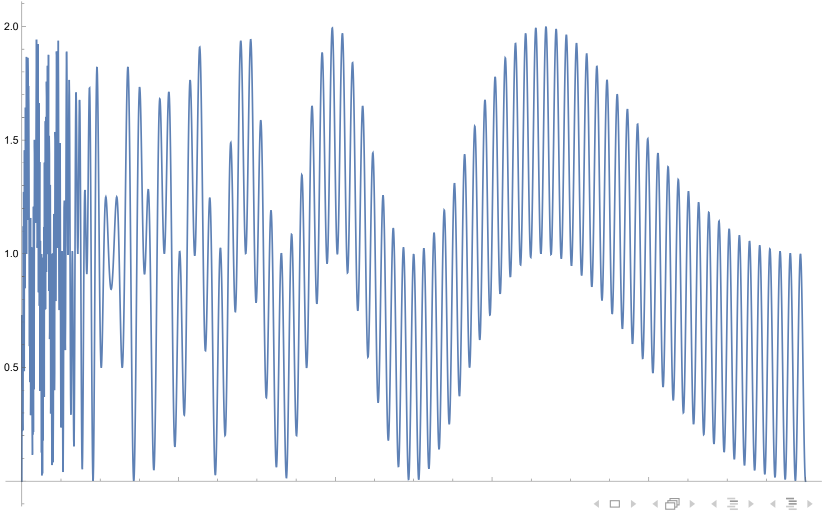
$$f_(x, y) := \sin^2(\pi x) + \sin^2(\pi y) + (ax^2 + by - c)^2$$

equals 0.

Shifted Version



Compressed version (0, 1)



Limitations

It is not effective to use standard methods as Newton - Rapson, since the function has a lot of maxima and needs a very close initial approximation. The probable approaches:

- Complex integration, then the complexity of root finding is equal to the complexity of the integration
- Real integration, we need to estimate the complexity and there appears a problem of 'false zeros"

Root - finding method: Basics

1. An analytic function is computable in polynomial time if and only if its Taylor series is a polynomial-time computable sequence.Müller [1987]
2. The derivative of a polynomial-time computable analytic function is also computable in polynomial time.Ker-I. KO [1982]
3. The integral of a polynomial-time computable analytic function is also computable in polynomial time. Ker-I Ko [1988]

Initial Transformation using the Error Function

- Transform the function $f(x)$ using the error function to obtain $g(x) = 1 - \mathrm{erf}(a \cdot f(x)^2)$ ($g(x) := 1 - \frac{f(x)}{f(x)+\frac{1}{a}}$ is also a way). This ensures that $g(x)$ approaches zero for most values of x except near the zeros of $f(x)$, where it will have sharp peaks approaching 1.
- Choose a large value for the parameter a. The choice of a affects the sharpness of the peaks in the transformed function. This problem will be shown late

Remark

In this particular case we could use

$$f(x) := \cos^2(\frac{\pi t}{x}) + \cos^2(\pi x)$$

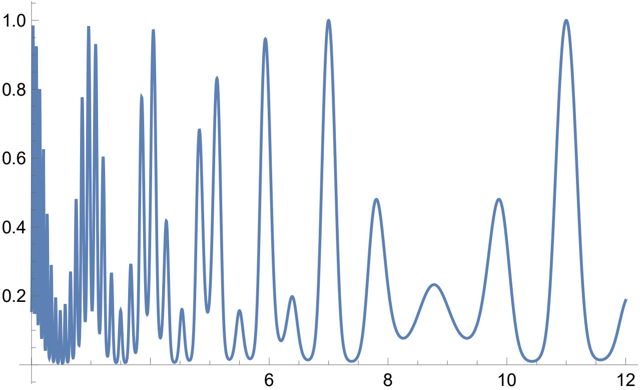
as

$$(1/2(\cos^2(\frac{\pi t}{x}) + \cos^2(\pi x)))^a$$

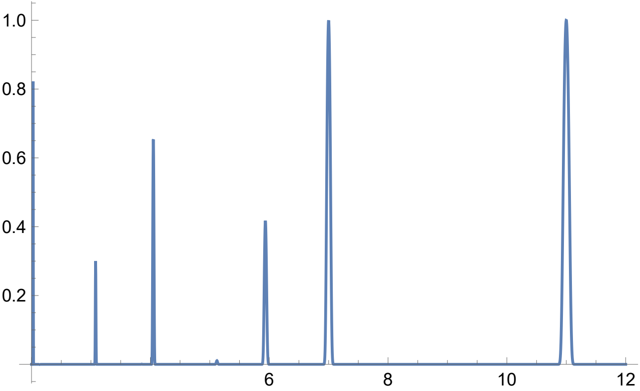
instead of

$$f(x) := 1 - \mathrm{erf}(a * (\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)))$$

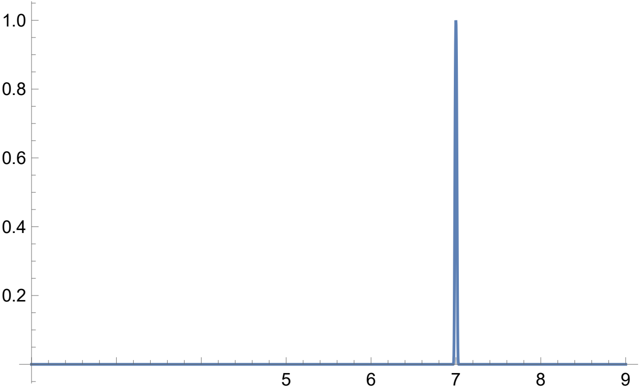
$$f(x) := 1 - \mathrm{erf}(\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x))$$



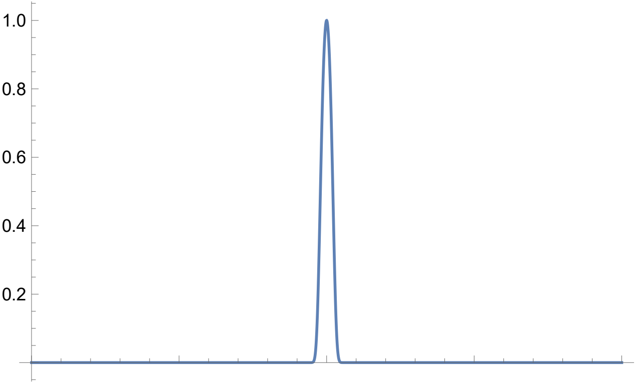
$$f(x) := 1 - \mathrm{erf}(12(\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)))$$



$$f(x) := 1 - \operatorname{erf}(77(\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)))$$



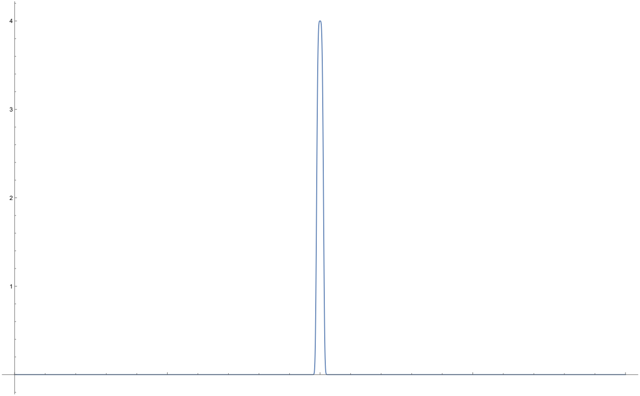
$$f(x) := 1 - \operatorname{erf}(77(\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)))$$



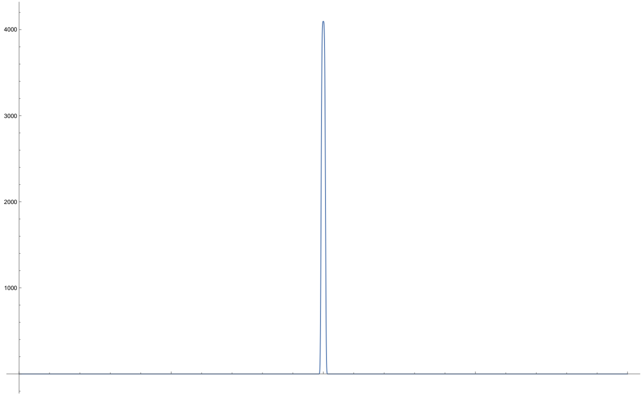
Modulation of the Transformed Function

- Apply the modulation to $g(x)$ using the function $h(x) = -\cos(\pi(g(x)+1)^b)$. This aims to ensure that the integral of the resulting function forms a "ladder" pattern, with distinct steps corresponding to the zeros of $f(x)$.
- Choose a suitable value for the parameter b for the modulation function. The value of b influences the shape of the modulation.

$$f(x) := (-\cos(1 - \operatorname{erf}(77(\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)))))^2$$



$$f(x) := (-\cos(1-\operatorname{erf}(77(\sin^2(\frac{\pi t}{x})+\sin^2(\pi x)))))^{12}$$



Integration and Binary Search

- Compute the integral of the modulated function, $H(x) = \int h(g(x))\,dx$. The integral is expected to have a step-like pattern.
- Perform a binary search on $H(x)$ within a suitable interval to detect the zeros of $f(x)$.

Refinement and Precision Handling

- Address numerical precision issues, particularly near the steep regions of $g(x)$.
- Refine the detected zeros using a root-finding algorithm like Newton's method for higher accuracy if needed.

Overview

- The complexity of the method could depend on the parameters a and b
- In this case a depend on the fact, how close false zeros are to 0

N. Müller. Taylor series. https://ub-deposit.fernuni-hagen.de/rsc/viewer/mir_derivate_00001451/Mueller_Taylor_Series_1987.pdf?page=17, 1987. Accessed: [put the date you accessed the PDF].

Harvey FRIEDMAN Ker-I. KO. Computational complexity of real functions. *Theoretical Computer Science*, 1982. Accessed: 2024-01-18.

Harvey Friedman Ker-I Ko. Computing power series in polynomial time. *ADVANCES IN APPLIED MATHFMATICS 9*, 9(9):40, 1988. doi: 10.1016/0196-8858(88)90006-1. URL https://www.sciencedirect.com/science/article/pii/0196885888900061. Accessed: 2024-01-18.