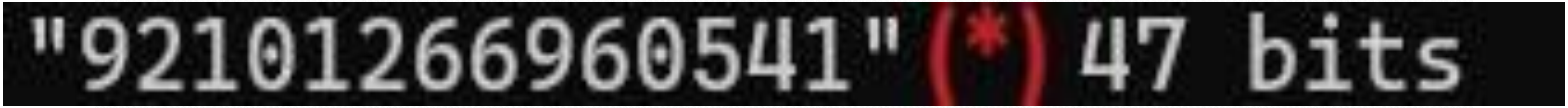
PRIMALITY TEST MADE WITH THE PRIMORIAL

Revision B
Treviglio, November, 11th 2023
Author: Vincenzo Sambito

This prime number (*) is for sale …



```
"92101266960541"(*)47 bits
```

(*) This number can be a “deterministically proved” prime number if the “VincS conjecture about prime numbers generative algorithm” will be confirmed true. This number represents just an example but the proposal is true!!!

What? … how can a number be sold?

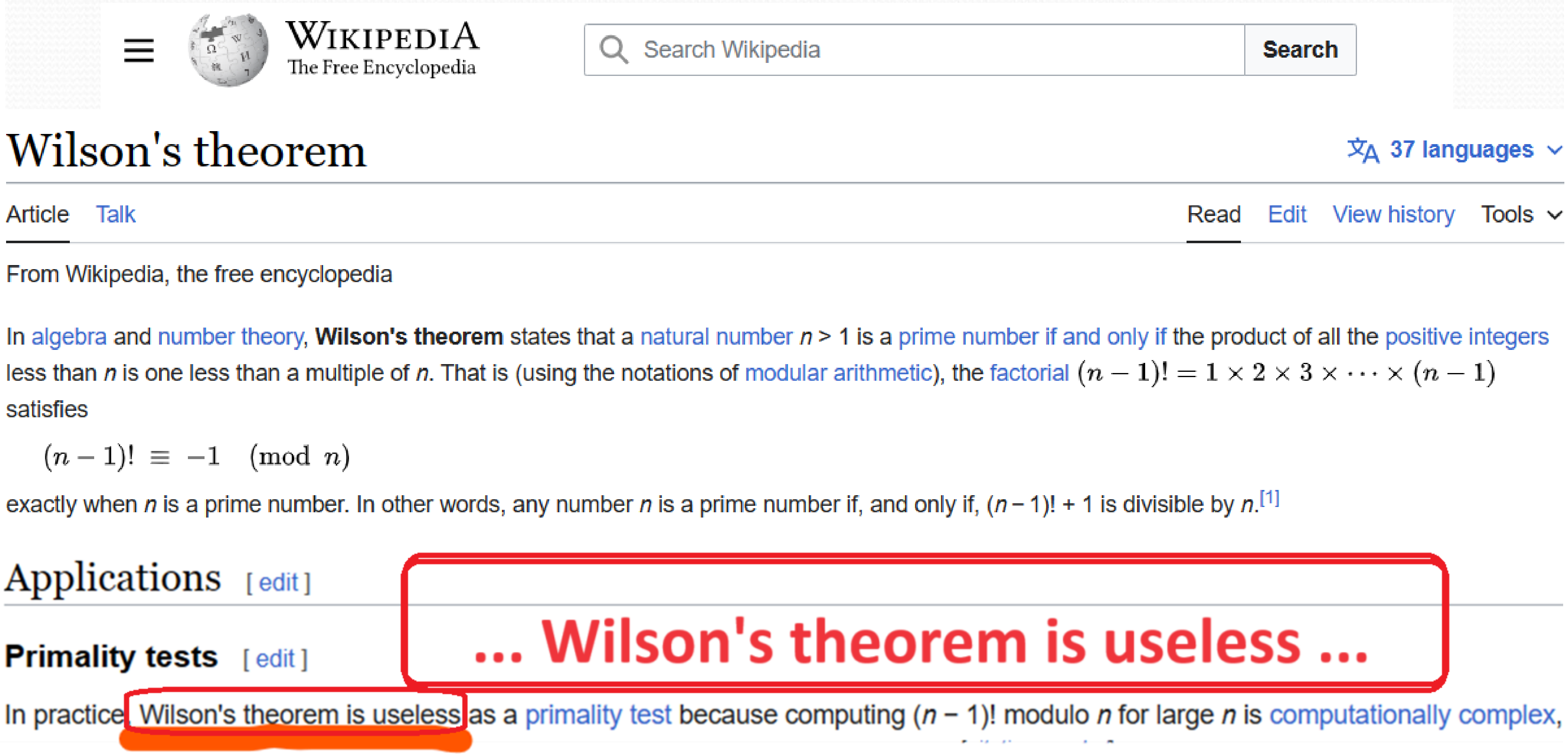
*Nowadays, **prime numbers** are widely known as of great importance for cybersecurity. Please read till the end to understand why this kind of huge prime numbers can be sold.*

Q: *How do we know if a certain number is definitely prime?*

A: *One of the few foolproof methods is Wilson's theorem!*

(… *but* …)

From Wikipedia…



Wilson's theorem

From Wikipedia, the free encyclopedia

In algebra and number theory, **Wilson's theorem** states that a natural number *n* > 1 is a prime number if and only if the product of all the positive integers less than *n* is one less than a multiple of *n*. That is (using the notations of modular arithmetic), the factorial $(n-1)! = 1 \times 2 \times 3 \times \cdots \times (n-1)$ satisfies

$$(n-1)! \equiv -1 \pmod{n}$$

exactly when *n* is a prime number. In other words, any number *n* is a prime number if, and only if, $(n-1)! + 1$ is divisible by *n*.[1]

Applications [edit]

Primality tests [edit]

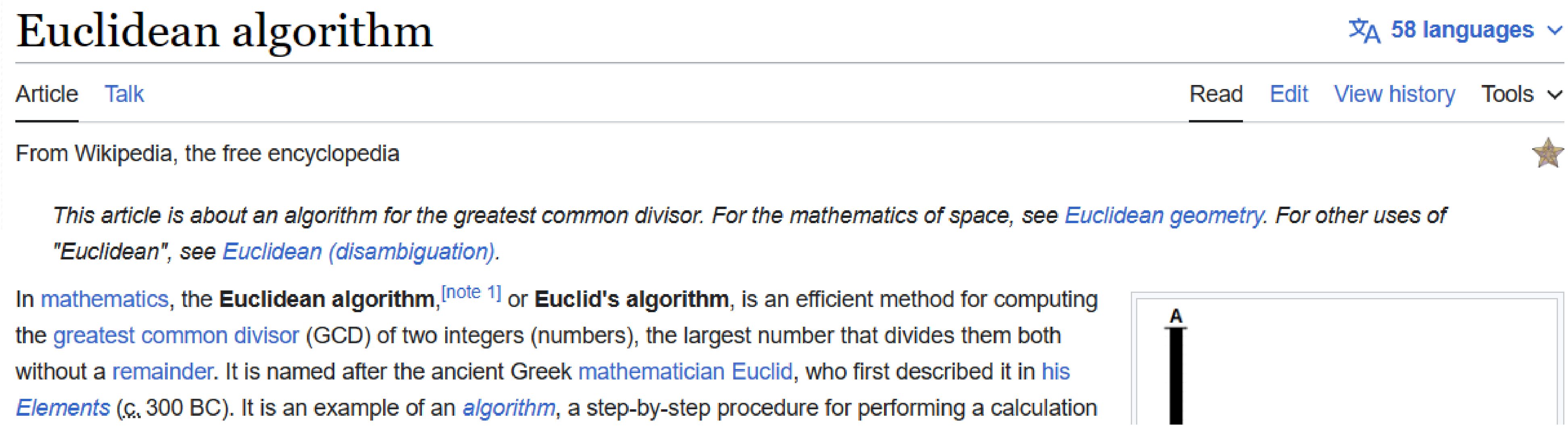
In practice, Wilson's theorem is useless as a primality test because computing $(n-1)!$ modulo *n* for large *n* is computationally complex,

... Wilson's theorem is useless ...

Can something similar be theorized so that it can be useful?

In reality, an USABLE algorithm is ready since about 2300 years…

From Wikipedia…

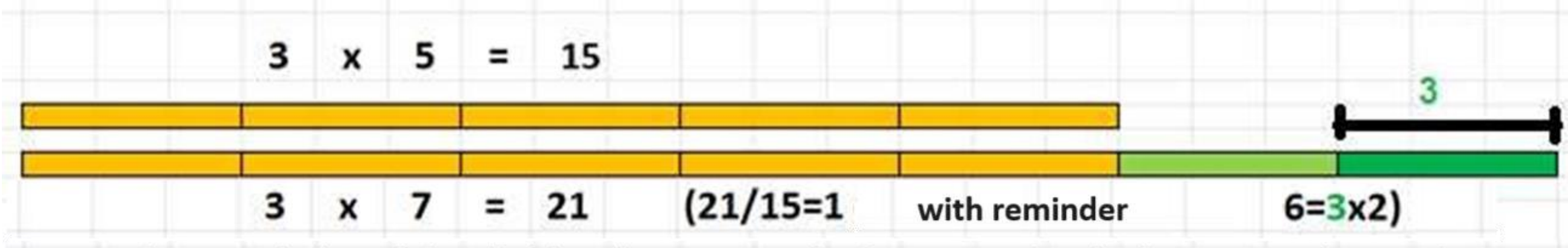


Euclidean algorithm

From Wikipedia, the free encyclopedia

This article is about an algorithm for the greatest common divisor. For the mathematics of space, see Euclidean geometry. For other uses of "Euclidean", see Euclidean (disambiguation).

In mathematics, the **Euclidean algorithm**,[note 1] or **Euclid's algorithm**, is an efficient method for computing the greatest common divisor (GCD) of two integers (numbers), the largest number that divides them both without a remainder. It is named after the ancient Greek mathematician Euclid, who first described it in his *Elements* (c. 300 BC). It is an example of an *algorithm*, a step-by-step procedure for performing a calculation



3 x 5 = 15

3 x 7 = 21 (21/15=1 with reminder 6=3x2)

… so, the remainder of the division, has, among its factors, 3 that is the G.C.D. of 15 and 21.

"The remainder of the division between two integers contains, among its factors, the Greatest Common Divisor of the two numbers."

Idea!

To use the Euclid's algorithm with the primorial instead of the Wilson's theorem with the factorial!

Why not apply Euclid's theorem between the primorial of the number-1 and the number itself, whose primality we want to test? The remainder of the division between the primorial and the number (modulus) will contain the information to determine whether the number is prime or not.

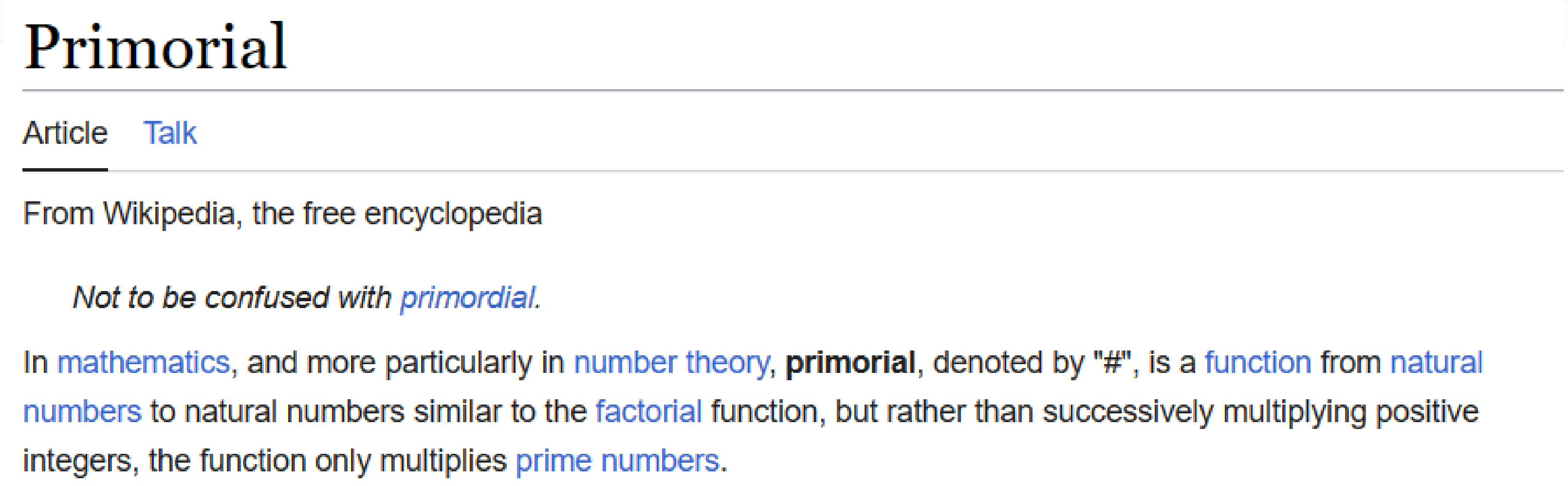
... while (by evident parallel) ...

Wilson's theorem states that the remainder of the division between the factorial of the number-1 and the number itself, whose primality we want to test, will contain the information to determine whether the number is prime (remainder=-1) or not (remainder =0).

Primorial … whoo?!?!

While the factorial is quite well known, the primorial is not so known.

From Wikipedia …



Primorial

Article Talk

From Wikipedia, the free encyclopedia

Not to be confused with primordial.

In mathematics, and more particularly in number theory, **primorial**, denoted by "#", is a function from natural numbers to natural numbers similar to the factorial function, but rather than successively multiplying positive integers, the function only multiplies prime numbers.

Yet the primorial was used by Eratosthenes to demonstrate that prime numbers are infinite through the popular sieve.

Demonstration

Even if the feasibility of a primality test with the primorial can be demonstrated through Euclid's theorem on G.C.D., ... another original demonstration of the application is described in a separate document (click below) ...

www.VincS.it

NEPRIMES PROJECT

Never Ending Primes

Primes factory

New New New New

…….. 982451581 ……. 982451609 ……. 982451629 ……. 982451653 …..∞?

Project goal

Create an original website (nothing like this currently exists) that deterministically generates prime numbers 24 hours a day and stores them in a database.

Imagine having a window on the site page where the last prime number generated by the deterministic algorithm will be perpetually displayed.

What already exists is just a static database (which therefore does not grow automatically), maintained in ... https://primes.utm.edu/lists/small/millions/

The generating algorithm

The generating algorithm is simply based on the use of a sieve similar to the famous one of Eratosthenes.

This sieve, instead of using a binary map with the subsequent exclusion of the primes already found, uses the product of the same primes: this product is called primorial.

Advantages of the primorial

- The *primorial* of a given number is the most efficient packet of information for determining whether the next number *is prime or not*..
- The enormous *primorial* of large numbers can easily be preserved, broken down, into relatively small parts (hence the neologism *primorialets* – *primorialini* in italian). By exploiting the invariant property of the multiplicative operation on the module, it is possible to organize the verification of very large prime numbers with distributed computing techniques.

Some remarks …

- EVERYTHING THAT CAN BE DONE WITH THE FACTORIAL (Wilson) CAN BE DONE WITH THE PRIMORIAL (Vinc.S.)
- THE FACTORIAL GROWS EXPONENTIALLY, INSTEAD, THE PRIMORIAL GROWS PROPORTIONALLY WITH THE NATURAL LOGARITHM
- ONCE THE PRIMORIALET HAS BEEN CALCULATED (OR DOWNLOADED), IT CAN REMAIN RESIDENT ON THE VOLUNTARY PARTICIPANT'S COMPUTER (AT LEAST AS LONG AS THE VOLUNTEER IS ONLINE)
- THAT VOLUNTEER WILL ALWAYS TEST THAT FIELD OF PRIME NUMBERS AS POTENTIAL FACTORS OF THE CANDIDATES THAT WILL BE PROPOSED TO IT
- IT IS SUFFICIENT TO COMMUNICATE TO IT:
  - THAT WE HAVE INCREASED BY 1 (OR 2 – IF WE CONSIIDER ONLY ODDs) THE NUMBER FOR THE INCREMENTAL SEARCH OF PRIME NUMBERS (AS IN THE CASE OF OUR NEPRIMES PROJECT)... OR ...
  - THE NUMBER WE WANT TO TEST FOR PRIMALITY

Some remarks … (follows) …

- WITH THE "DISTRIBUTED" PRIMORIAL YOU CAN CREATE THE MOST EFFICIENT SIEVE EVER CONCEIVED (ERATOSTHENE'S MAP OF THE PRIMES WILL FALL INTO OBLIGION)

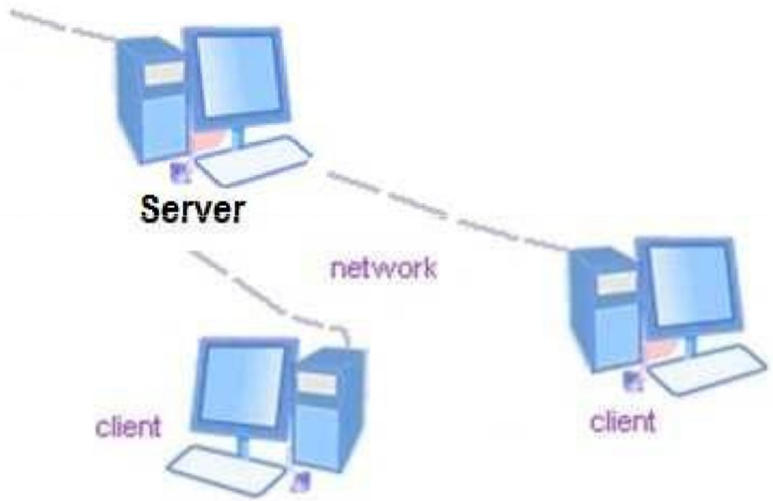
- THE PRIMORIAL CAN BE CONSIDERED THE "ZIPPED" VERSION OF ERATOSTHENE'S MAP OF THE PRIMES

- THE PRIMORIAL IS IMPLICITLY "FAULT TOLERANT": IF, IN FACT, YOU USE PROBABILISTIC METHODS (msec x each generated prime), TO CREATE IT OR TO ENLARGE IT, IT WILL NOT GENERATE ERRORS IN THE DETERMINISTIC PRIMALITY TESTS THAT WILL USE IT (AT THE LIMIT IT WILL ONLY BE A A LITTLE LARGER) AS IF IT WILL BE USED FOR SIEVING

- THE TURN-OVER, WHICH IS NOT PREDICTABLE WHEN IT’S DUE TO CONNECTIONS TERMINATED WITHOUT ADVICE OF THE VOLUNTEER PARTICIPANTS IN DISTRIBUTED COMPUTING, IS MANAGED WITH REDUNDANCY TECHNIQUES AND/OR BACKUP FROM A CENTRAL SERVER

Distributed computing

Therefore, the peculiarity of the project is the fact that it's particularly well suitable to parallel computing structures due to the possibility of distributing well-defined asynchronous tasks with a minimum exchange of data to and from the server (minimum bandwidth occupation).



Powerful “full time” dedicated computers?
***No!**... a simple Calculator!*

The tool used to achieve this result is intended to be a simple software (Open Source in Java language) that simulates a calculator whose main characteristic is working with large integers.

This calculator relies on a software library universally known by those who work in this field because it is probably integrated into the microchips of ATMs, credit cards, password access systems, computer browsers, etc. etc..

This is the BigInteger library available for various languages and therefore also for Java, for which you can find documentation in:

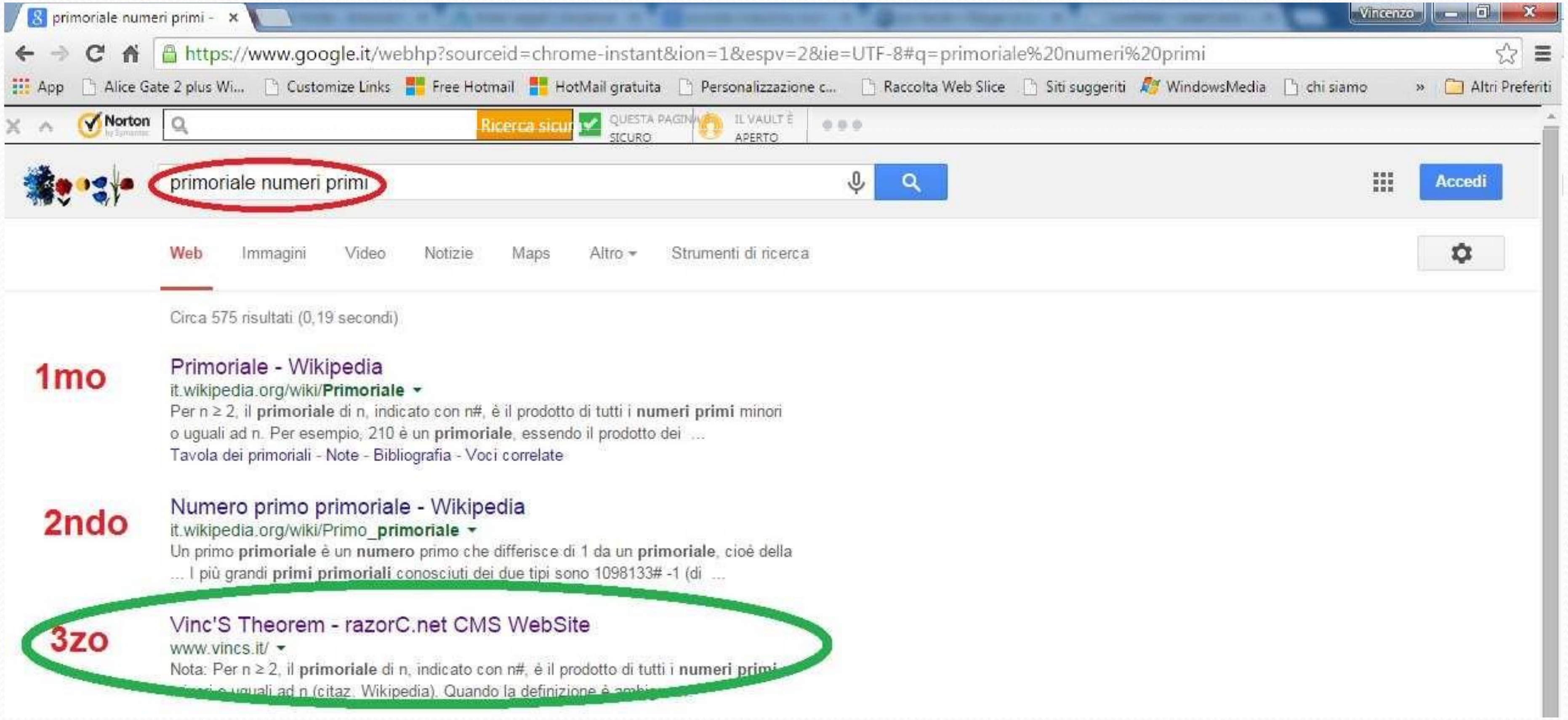
http://docs.oracle.com/javase/1.5.0/docs/api/java/math/BigInteger.html

VincSCalc key Features:

- One of the few calculators with resizable window (up to full screen) in order to allow a wide input/output field for huge numbers (horizontal) and deeply nested calculation (vertical).
- Nesting of calculation kept shown in calculation area that may become vertically scrollable for deeply nested calculation.
- Input/Output operand fields horizontally scrollable to allow arbitrary hugeness of integers (as huge as your hardware will allow)
- Numeric Keyboard disabled automatically when data is consistent to avoid involuntary overwrite (only operators or "clears" buttons are accepted)
- 5 "Memories Absolute«
- 5 "Memories Editable«
- Calculations can be performed "run time", for a quick response, or also postponed to the "=" operator request to keep track and double check (RunTm checkbox is "run time" by default). - In case of postponed operations, the user could also eventually go back (cBkS button) in order to correct his input.
- Integer calculations can be performed in Modulo (settable directly in its field) allowing experiments with modular arithmetic.
- Integers primality test in probabilistic and deterministic methods.
- Integers HowManyPrimes precise functions to test the Gauss formulas (logarithmic, Integral Logarithmic) or the Riemann's derived formulas; among with this total. it will be possible to calculate how many primes are in the form m*k+/-n
- Numeric/Operators Pad of computer keyboard can be used for fast input by maniacs
- A dedicated primorial calculation button (x#).
- 4 Data Types (Double, BigInt[eger], XXLInt[eger], Ar[bitrary]Prec[ision])
- 4 numeric bases/radix + custom (only for integer types - decimal, octal, hexdecimal, binary)

- Calculations can be performed "run time", for a quick response, or also postponed to the "=" operator request to keep track and double check (RunTm checkbox is "run time" by default). - In case of postponed operations, the user could also eventually go back (cBkS button) in order to correct his input.

Increasing popularity of the primorial



primoriale numeri primi

Circa 575 risultati (0,19 secondi)

1mo

Primoriale - Wikipedia
it.wikipedia.org/wiki/**Primoriale**
Per n ≥ 2, il **primoriale** di n, indicato con n#, è il prodotto di tutti i **numeri primi** minori o uguali ad n. Per esempio, 210 è un **primoriale**, essendo il prodotto dei ...
Tavola dei primoriali - Note - Bibliografia - Voci correlate

2ndo

Numero primo primoriale - Wikipedia
it.wikipedia.org/wiki/Primo_**primoriale**
Un primo **primoriale** è un **numero** primo che differisce di 1 da un **primoriale**, cioè della ... I più grandi **primi primoriali** conosciuti dei due tipi sono 1098133# -1 (di ...

3zo

Vinc'S Theorem - razorC.net CMS WebSite
www.vincs.it/
Nota: Per n ≥ 2, il **primoriale** di n, indicato con n#, è il prodotto di tutti i **numeri primi** minori e uguali ad n (citaz. Wikipedia). Quando la definizione è ambi

The VincS primes generator algorithm

After having proved the VincS Theorem, with some improvements and optimizations, that need yet to be proved and validated, now the project is ready to generate forever potential huge prime numbers. With a cheap home laptop, the algorithm is able to generate 47 bits size potential prime numbers in just one day of sieving.

Some proposals for financing the VincS prime numbers research and the NeverEndingPrimes project

What follows is not a proposal of investment, not a promise of earnings, not a proposal to become a shareholder, etc.:

It's just a sale (truly not yet a sale – since it is a non-binding pre-order) of an abstract object and what it represents, with its support (whatever could be the meaning – paper, informatic storage, etc): as it would be a painting that is sold together with its canvas. The worth is not in the canvas.

A proposal for financing the VincS prime numbers research and the NeverEndingPrimes project; first stage – to sell “certificates”

The idea is borrowed from those weird agencies that sell “stars”: of course not “real” stars but the chance for the buyer to link his/her name to a specific and unique star. In our case, to sell a “certificate” (not in the financial meaning) that represents the genuineness of the “potential prime number” coming from the VincS generating algorithm. This “certificate” will be uniquely tied to that potentially prime number. Vincenzo Sambito (a.k.a.VincS) undertakes, through the sales contract, that there will be no other registered owner of the same "potentially prime number“ in his organization. Of course, we know that the certificate owner will never be able to forbid the use of that number, for any purpose, by anyone that would need or would like to do. Unless he went crazy and the fact that he bought this certificate is a madness principle. The estimation of value for the certificate is 5$.

A proposal for financing the VincS prime numbers research and the NeverEndingPrimes project; first stage bis – to sell “merchandising” (1)

The basic «certificate» would be a jpeg with a hidden encrypted watermark. This «certificate», of course, will have printed on the name of the owner and any other text he/she would like to put on it (e.g. a dedication for a gift to a beloved person). This «certificate» will be simply sent by mail or downloadable from a website. It will be possible, for the customer, to order some merchandising like the printed version of the «certificate» on a parchment, a T-shirt with the number printed on, a milk cup, a cap, etcetera.

A proposal for financing the VincS prime numbers research and the NeverEndingPrimes project; first stage bis – to sell "merchandising" (2)

This can be seen as a modern formula of "Offer me a beer" or "Give Me Five" campaigns. The proven capability of the algorithm to generate "potential prime numbers" is unmatched, in speed, by any other algorithm.

A proposal for financing the VincS prime numbers research and the NeverEndingPrimes project: second stage – to sell NFTs

When the size, in bits, of the generated potential prime number will be greater than any generated prime number created with other methods, could be interesting to propose selling the property of an NFT representing a certificate of genuineness of the tied “potential prime number”, coming from the VincS generating algorithm. The NFT, differently from a paper/pdf certificate, can be sold conveniently through a blockchain attesting the property.

This NFT will be uniquely tied to that potential prime number. Vincenzo Sambito (a.k.a.VincS) undertakes, through the sales contract, that there will be not other registered owner of the same "potential prime number“ in his organization.

The proven capability of the algorithm to generate “potential prime numbers” are unmatched by any other algorithm, in speed and now also in size. This can give a pbig otential worth to the NFT since it will be, in the future, witness of the birth of a new branch of Numbers Theory, as a kind of early “modern artwork”.

A proposal for financing the VincS prime numbers research and the NeverEndingPrimes project: third stage – crowdfunding campaigns

Crowdfunding campaigns will be launched in popular platform as:

Kickstarter: Kickstarter is a crowdfunding platform that focuses on creative projects, such as film, music, art, design, and technology. The platform was founded in 2009 and has been used to fund over 200,000 projects, with a total of over $6 billion in funding[1].

Indiegogo: Indiegogo is a crowdfunding platform that allows people to raise funds for a wide range of projects, including technology, art, design, film, and much more. The platform was founded in 2008 and has been used to fund over 800,000 projects worldwide[1].

GoFundMe: GoFundMe is a crowdfunding platform that allows people to raise funds for a wide range of personal causes, including medical expenses, family emergencies, education, and much more. The platform was founded in 2010 and has been used to raise over $10 billion in funding[1].

Patreon: Patreon is a crowdfunding platform that allows content creators to earn money from their fans. Fans can support their favorite creators with monthly donations or per-content donations. The platform was founded in 2013 and has been used by over 200,000 content creators worldwide[2].

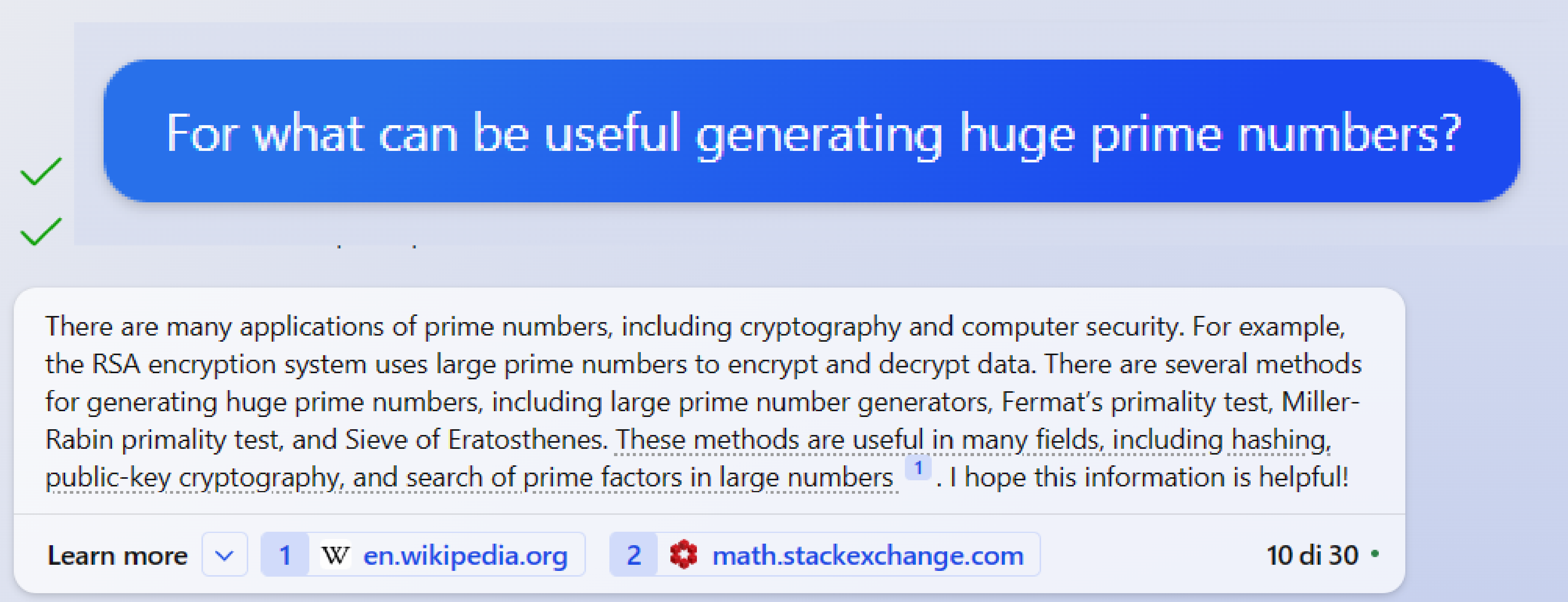
Etcetera

A proposal for financing the VincS prime numbers research and the NeverEndingPrimes project: fourth and last stage – begin to sell "huge prime nubers"

Once all the conjectures are proven, the VincS hypothesis will be demonstrated, selling "huge prime numbers" will be really possible. The interest will no longer be just for fun. A company can be established. Those who helped, will be remembered.

In Numbers Theory is well known that huge prime numbers are used to create uncorruptible (at the current "state of the art") crypto-keys. If these huge prime numbers are deterministically proven, cryptography is more secure.

Don’t you trust me? Ask AI !



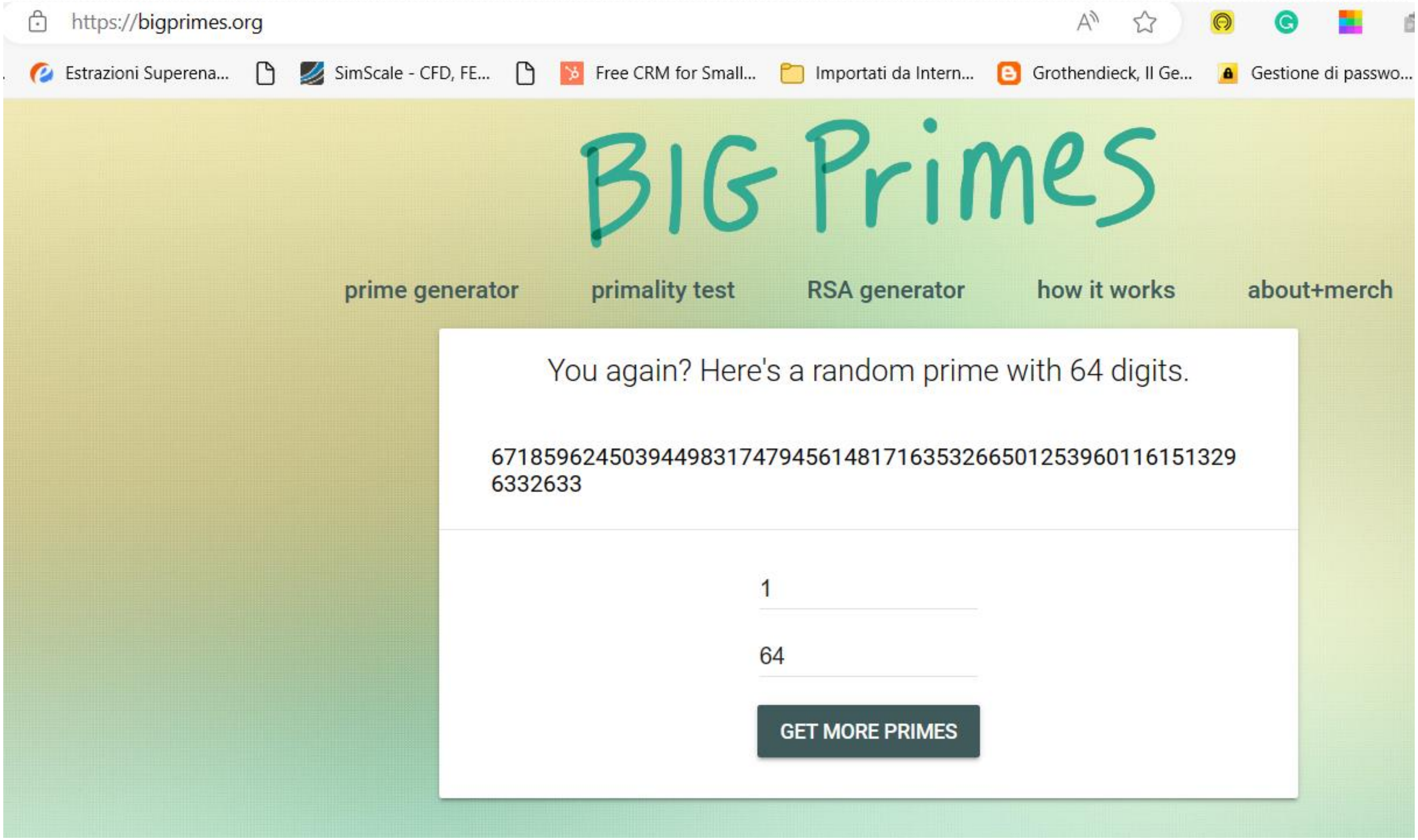
For what can be useful generating huge prime numbers?

✓

✓

There are many applications of prime numbers, including cryptography and computer security. For example, the RSA encryption system uses large prime numbers to encrypt and decrypt data. There are several methods for generating huge prime numbers, including large prime number generators, Fermat’s primality test, Miller-Rabin primality test, and Sieve of Eratosthenes. These methods are useful in many fields, including hashing, public-key cryptography, and search of prime factors in large numbers [1]. I hope this information is helpful!

It’s true! The matter is hot!! A competitor … https://bigprimes.org/



You again? Here's a random prime with 64 digits.

6718596245039449831747945614817163532665012539601161513296332633

1

64

Comparing with competitors

The methods: *As well described in the Big Number Generator website, the primality test behind it* ***is not deterministic*** *for numbers greater than 64 bit size. Our advantage is that, after overcoming the 64 bit barrier, and proven the "VincS hypothesis" is true,* ***our huge generated prime number will be deterministically proven****.*

WE ARE REALLY CLOSE TO 64 BITS, AFTER JUST ONE DAY OF SIEVING!!!

The speed: *This feature is* ***unmatched*** *by any other method at* ***our speed****!!! And it will be crucial for cryptosecurity.*

A call for interest

*What above is **not to be considered binding** neither for Vincenzo Sambito (a.k.a. VincS) nor for the persons that will manifest a will of interest or a will to book a certificate/NFT. Vincenzo Sambito, right now, subscribes and signs only that everything is **genuine**. When the collection of interest is big enough, the proposal will be well-defined and people who have subscribed early will be served earlier for the sales.*

*This is just an early call for smart people. This is just the beginning of something that will change forever the branch of mathematics named «Theory of numbers». **Be a part of it!***

Stay tuned with the top records of our Huge Prime Numbers Generator!!!

Click on the below permanent link in order to access to our updated top records!!!

Huge Prime Numbers Generation «State of the Art»

Thanks for your attention!

- For more information about the status of the project ...
- To voluntarily contribute to the project (even simply by installing a copy of the freely distributed calculator VincSCalc) ...
- To help in writing Java code ...
- To book a prime number "certificate" / NFT / merchandising (without any purchase obligation) …
- For any interest in partnership …

vincscalc@gmail.com