Create account Log in

Article Talk Read Edit View history Search

WIKIPEDIA
The Free Encyclopedia

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia
- Wikipedia store

Interaction
- Help
- About Wikipedia
- Community portal
- Recent changes
- Contact page

Tools
- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Page information
- Wikidata item
- Cite this page

Print/export
- Create a book
- Download as PDF
- Printable version

Languages
- Español
- Français
- Italiano
- 日本語
- Português
- Русский
- Українська

Edit links

Sieve of Sundaram

From Wikipedia, the free encyclopedia

In mathematics, the **sieve of Sundaram** is a simple deterministic algorithm for finding all prime numbers up to a specified integer. It was discovered by Indian mathematician S. P. Sundaram in 1934.[1][2]

Contents [hide]

Algorithm [edit]

Start with a list of the integers from 1 to *n*. From this list, remove all numbers of the form $i + j + 2ij$ where:

- $i, j \in \mathbb{N},\ 1 \le i \le j$
- $i + j + 2ij \le n$

The remaining numbers are doubled and incremented by one, giving a list of the odd prime numbers (i.e., all primes except 2) below $2n + 2$.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

i + j + 2ij

List of Primes

Sieve of Sundaram: algorithm steps for primes below 202 (unoptimized).

The sieve of Sundaram sieves out the composite numbers just as sieve of Eratosthenes does, but even numbers are not considered; the work of "crossing out" the multiples of 2 is done by the final double-and-increment step. Whenever Eratosthenes' method would cross out *k* different multiples of a prime $2i+1$, Sundaram's method crosses out $i + j(2i+1)$ for $1 \le j \le \lfloor k/2 \rfloor$.

Correctness [edit]

If we start with integers from 1 to n, the final list contains only odd integers from 3 to $2n + 1$. From this final list, some odd integers have been excluded: we must show these are precisely the *composite* odd integers less than $2n + 2$.

Let q be an odd integer of the form $2k + 1$. Then, q is excluded if and only if k is of the form $i + j + 2ij$, that is $q = 2(i + j + 2ij) + 1$. Then we have:

$$q = 2(i + j + 2ij) + 1$$
$$= 2i + 2j + 4ij + 1$$
$$= (2i + 1)(2j + 1).$$

So, an odd integer is excluded from the final list if and only if it has a factorization of the form $(2i + 1)(2j + 1)$ — which is to say, if it has a non-trivial odd factor. Therefore the list must be composed of exactly the set of odd *prime* numbers less than or equal to $2n + 2$.

See also [edit]

- Sieve of Eratosthenes
- Sieve of Atkin
- Sieve theory

References [edit]

1. ^ V. Ramaswami Aiyar (1934). "Sundaram's Sieve for Prime Numbers". *The Mathematics Student* **2** (2): 73. ISSN 0025-5742.
2. ^ G. (1941). "Curiosa 81. A New Sieve for Prime Numbers". *Scripta Mathematica* **8** (3): 164.

- Ogilvy, C. Stanley; John T. Anderson (1988). *Excursions in Number Theory*. Dover Publications, 1988 (reprint from Oxford University Press, 1966). pp. 98–100, 158. ISBN 0-486-25778-9.
- Honsberger, Ross (1970). *Ingenuity in Mathematics*. New Mathematical Library #23. Mathematical Association of America. p. 75. ISBN 0-394-70923-3.
- A new "sieve" for primes, an excerpt from Kordemski, Boris A. (1974). *Köpfchen, Köpfchen! Mathematik zur Unterhaltung*. MSB Nr. 78. Urania Verlag. p. 200. (translation of Russian book Кордемский, Борис Анастасьевич (1958). *Математическая смекалка*. М.: ГИФМЛ.)
- Movshovitz-Hadar, N. (1988). "Stimulating Presentations of Theorems Followed by Responsive Proofs". *For the Learning of Mathematics* **8** (2): 12–19.
- Ferrando, Elisabetta (2005). "Abductive processes in conjecturing and proving" (PDF). *Ph.D. theses*. Purdue University. pp. 70–72.
- Baxter, Andrew. "Sundaram's Sieve". *Topics from the History of Cryptography* (MU Department of Mathematics).

External links [edit]

- A C99 implementation of the Sieve of Sundaram using bitarrays

v · t · e	Number-theoretic algorithms [hide]
Primality tests	AKS test · APR test · Baillie–PSW · ECPP test · Elliptic curve · Pocklington · Fermat · Lucas · *Lucas–Lehmer* · *Lucas–Lehmer–Riesel* · *Proth's theorem* · *Pépin's* · Quadratic Frobenius test · Solovay–Strassen · Miller–Rabin
Prime-generating	Sieve of Atkin · Sieve of Eratosthenes · **Sieve of Sundaram** · Wheel factorization
Integer factorization	Continued fraction (CFRAC) · Dixon's · Lenstra elliptic curve (ECM) · Euler's · Pollard's rho · $p-1$ · $p+1$ · Quadratic sieve (QS) · General number field sieve (GNFS) · *Special number field sieve (SNFS)* · Rational sieve · Fermat's · Shanks' square forms · Trial division · Shor's
Multiplication	Ancient Egyptian · Long · Karatsuba · Toom–Cook · Schönhage–Strassen · Fürer's
Discrete logarithm	Baby-step giant-step · Pollard rho · Pollard kangaroo · Pohlig–Hellman · Index calculus · Function field sieve
Greatest common divisor	Binary · Euclidean · Extended Euclidean · Lehmer's
Modular square root	Cipolla · Pocklington's · Tonelli–Shanks
Other algorithms	Chakravala · Cornacchia · Integer relation · Integer square root · Modular exponentiation · Schoof's
Italics indicate that algorithm is for numbers of special forms · Smallcaps indicate a deterministic algorithm	

Categories: Primality tests