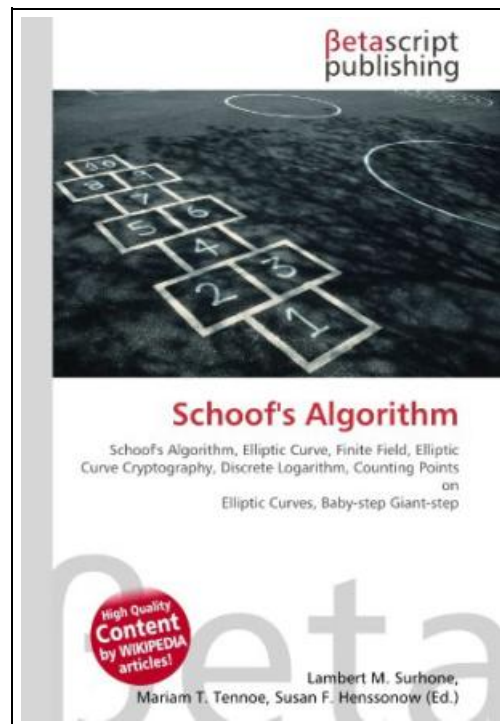


## Schoof's Algorithm



Filesize: 5.64 MB

### **Reviews**

*Very beneficial to all category of folks. We have study and that i am sure that i will planning to go through yet again again in the future. Its been printed in an extremely straightforward way in fact it is just soon after i finished reading this pdf where actually changed me, alter the way i really believe.*

*(Emmett Mann)*

## SCHOOF'S ALGORITHM



Betascript Publishers Jan 2010, 2010. Taschenbuch. Book Condition: Neu. 220x150x5 mm. Neuware - High Quality Content by WIKIPEDIA articles! Schoof's Algorithm is an efficient algorithm to count points on elliptic curves over finite fields. The algorithm has applications in elliptic curve cryptography where it is important to know the number of points to judge the difficulty of solving the discrete logarithm problem in the group of points on an elliptic curve. The algorithm was published by René Schoof in 1985 and it was a theoretical breakthrough, as it was the first deterministic polynomial time algorithm for counting points on elliptic curves. Before Schoof's algorithm, approaches to counting points on elliptic curves such as the naive and baby-step giant-step algorithms were, for the most part, tedious and had an exponential running time. This article explains Schoof's approach, laying emphasis on the mathematical ideas underlying the structure of the algorithm. 80 pp. Englisch.



[Read Schoof's Algorithm Online](#)



[Download PDF Schoof's Algorithm](#)

## Relevant Books

---



### Psychologisches Testverfahren

Reference Series Books LLC Nov 2011, 2011. Taschenbuch. Book Condition: Neu. 249x191x7 mm. This item is printed on demand - Print on Demand Neuware - Quelle: Wikipedia. Seiten: 100. Kapitel: Myers-Briggs-Typindikator, Keirsey Temperament Sorter, DISG,...

[Read eBook](#)

»



### Programming in D

Ali Cehreli Dez 2015, 2015. Buch. Book Condition: Neu. 264x182x53 mm. This item is printed on demand - Print on Demand Neuware - The main aim of this book is to teach D to readers...

[Read eBook](#)

»



### Adobe Indesign CS/Cs2 Breakthroughs

Peachpit Press, 2005. Softcover. Book Condition: Neu. Gebrauch - Sehr gut Unbenutzt. Schnelle Lieferung, Kartonverpackung. Abzugsfähige Rechnung. Bei Mehrfachbestellung werden die Versandkosten anteilig erstattet. - Adobe InDesign is taking the publishing world by storm and...

[Read eBook](#)

»



### The Preschool Inclusion Toolbox: How to Build and Lead a High-Quality Program

Brookes Publishing Co, United States, 2015. Paperback. Book Condition: New. 274 x 213 mm. Language: English . Brand New Book. Filled with tips, tools, and strategies, this book is the comprehensive, practical toolbox preschool administrators...

[Read eBook](#)

»



### Cool Cars: Set 12: Non-Fiction

Pearson Education Limited. Paperback. Book Condition: new. BRAND NEW, Cool Cars: Set 12: Non-Fiction, Emma Lynch, This title is part of Phonics Bug - the first Phonics programme to bring together research-based teaching methods with...

[Read eBook](#)

»