Lecture Notes in Mathematics 1512

Editors:
A. Dold, Heidelberg
B. Eckmann, Zürich
F. Takens, Groningen

Leonard M. Adleman   Ming-Deh A. Huang

Primality Testing and Abelian Varieties Over Finite Fields

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Authors

Leonard M. Adleman
Ming-Deh A. Huang
Department of Computer Science
University of Southern California
Los Angeles, CA 90089-0782, USA

Adleman's research supported by NSF through grant CCR 8519296.
Huang's research supported by NSF through grant CCR 8701541 and USC Faculty Research Award.

Mathematics Subject Classification (1991): 10-XX, 10D25, 14G15, 14K15, 68-XX, 68C25

ISBN 3-540-55308-8 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-55308-8 Springer-Verlag New York Berlin Heidelberg

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1992
Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
46/3140-543210 - Printed on acid-free paper

To my wife Chen Yu.

To my parents Herman and Jeanne Adleman.

The problem of distinguishing prime numbers from composites, and of resolving composite numbers into their prime factors, is one of the most important and useful in all of arithmetic.... The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated.
Carl Friedrich Gauss
Disquisitiones Arithmeticae
ART. 329 (1801) (translation from [Kn])

ABSTRACT

The existence of a random polynomial time algorithm for the set of primes is proved. The techniques used are from algebraic geometry, algebraic number theory and analytic number theory. Particular use is made of the theory of two dimensional Abelian varieties over finite fields. The result complements the well known result of Solovay and Strassen that there exists a random polynomial time algorithm for the set of composites.

Contents

1 Introduction 1

2 Acknowledgement 4

3 Overview Of The Algorithm And The Proof Of The Main Theorem 5
3.1 Overview Of The Algorithm . . . 5
3.2 Overview Of The Proof Of The Main Theorem . . . 8
3.2.1 Overview Of Section 5 - Proof Of Proposition 1 . . . 8
3.2.2 Overview Of Section 6 - Proof Of Proposition 2 . . . 13
3.2.3 Overview Of Section 7 - Proof Of Proposition 3 . . . 14

4 Reduction Of Main Theorem To Three Propositions 15
4.1 Three Propositions . . . 15
4.2 The Algorithm . . . 16
4.3 Reduction Of The Main Theorem . . . 17

5 Proof Of Proposition 1 21
5.1 Preliminaries - Basic Results, Definitions And Notations . . . 21
5.1.1 Curves And Jacobians . . . 21
5.1.2 Weil Numbers . . . 22
5.1.3 Rings . . . 27
5.1.4 Complex Multiplication . . . 37
5.2 On The Density Of Good Weil Numbers . . . 42
5.3 Principally Polarized Abelian Varieties With Given Endomorphism Rings In Characteristic 0 . . . 46
5.4 Principally Polarized Abelian Varieties With Given Endomorphism Rings Over Finite Fields . . . 52
5.5 Principally Polarized Abelian Varieties With Given Endomorphism Rings Over Prime Fields . . . 58
5.6 Ideal Classes And Isomorphism Classes . . . 61
5.7 Class Field Theoretic Estimates . . . 67
5.8 Local Estimates . . . 73
5.9 Analytic Estimates . . . 91
5.10 Jacobian Varieties Associated With Good Weil Numbers . . . 95
5.11 Counting Affine Representatives . . . 101
5.12 Demonstration Of Proposition 1 . . . 105

6 Proof Of Proposition 2 110
6.1 Preliminaries . . . 110
6.2 l-Torsion . . . 112
6.3 Number Of Rational Points On The Jacobian . . . 120
6.4 Demonstration Of Proposition 2 . . . 123

7 Proof Of Proposition 3 126

References 137

Index 140