

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor N.J. Hitchin, Mathematical Institute,
 University of Oxford, 24–29 St Giles, Oxford OX1 3LB, United Kingdom

The titles below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

- 46 *p*-adic Analysis: a short course on recent work, N. KOBLITZ
- 59 Applicable differential geometry, M. CRAMPIN & F.A.E. PIRANI
- 66 Several complex variables and complex manifolds II, M.J. FIELD
- 86 Topological topics, I.M. JAMES (ed)
- 87 Surveys in set theory, A.R.D. MATHIAS (ed)
- 88 FPF ring theory, C. FAITH & S. PAGE
- 90 Polytopes and symmetry, S.A. ROBERTSON
- 92 Representations of rings over skew fields, A.H. SCHOFIELD
- 93 Aspects of topology, I.M. JAMES & E.H. KRONHEIMER (eds)
- 96 Diophantine equations over function fields, R.C. MASON
- 97 Varieties of constructive mathematics, D.S. BRIDGES & F. RICHMAN
- 99 Methods of differential geometry in algebraic topology, M. KAROUBI & C. LERUSTE
- 100 Stopping time techniques for analysts and probabilists, L. EGGHE
- 104 Elliptic structures on 3-manifolds, C.B. THOMAS
- 105 A local spectral theory for closed operators, I. ERDELYI & WANG SHENGWANG
- 107 Compactification of Siegel moduli schemes, C.-L. CHAI
- 109 Diophantine analysis, J. LOXTON & A. VAN DER POORTEN (eds)
- 113 Lectures on the asymptotic theory of ideals, D. REES
- 114 Lectures on Bochner-Riesz means, K.M. DAVIS & Y.-C. CHANG
- 116 Representations of algebras, P.J. WEBB (ed)
- 119 Triangulated categories in the representation theory of finite-dimensional algebras, D. HAPPEL
- 121 Proceedings of *Groups - St Andrews 1985*, E. ROBERTSON & C. CAMPBELL (eds)
- 128 Descriptive set theory and the structure of sets of uniqueness, A.S. KECHRIS & A. LOUVEAU
- 130 Model theory and modules, M. PREST
- 131 Algebraic, extremal & metric combinatorics, M.-M. DEZA, P. FRANKL & I.G. ROSENBERG (eds)
- 132 Whitehead groups of finite groups, ROBERT OLIVER
- 138 Analysis at Urbana, II, E. BERKSON, T. PECK, & J. UHL (eds)
- 139 Advances in homotopy theory, S. SALAMON, B. STEER & W. SUTHERLAND (eds)
- 140 Geometric aspects of Banach spaces, E.M. PEINADOR & A. RODES (eds)
- 141 Surveys in combinatorics 1989, J. SIEMONS (ed)
- 144 Introduction to uniform spaces, I.M. JAMES
- 146 Cohen-Macaulay modules over Cohen-Macaulay rings, Y. YOSHINO
- 148 Helices and vector bundles, A.N. RUDAKOV *et al*
- 149 Solitons, nonlinear evolution equations and inverse scattering, M. ABLOWITZ & P. CLARKSON
- 150 Geometry of low-dimensional manifolds 1, S. DONALDSON & C.B. THOMAS (eds)
- 151 Geometry of low-dimensional manifolds 2, S. DONALDSON & C.B. THOMAS (eds)
- 152 Oligomorphic permutation groups, P. CAMERON
- 153 L-functions and arithmetic, J. COATES & M.J. TAYLOR (eds)
- 155 Classification theories of polarized varieties, TAKAO FUJITA
- 156 Twistors in mathematics and physics, T.N. BAILEY & R.J. BASTON (eds)
- 158 Geometry of Banach spaces, P.F.X. MÜLLER & W. SCHACHERMAYER (eds)
- 159 Groups St Andrews 1989 volume 1, C.M. CAMPBELL & E.F. ROBERTSON (eds)
- 160 Groups St Andrews 1989 volume 2, C.M. CAMPBELL & E.F. ROBERTSON (eds)
- 161 Lectures on block theory, BURKHARD KÜLSHAMMER
- 162 Harmonic analysis and representation theory, A. FIGA-TALAMANCA & C. NEBBIA
- 163 Topics in varieties of group representations, S.M. VOVSİ
- 164 Quasi-symmetric designs, M.S. SHRIKANDE & S.S. SANE
- 166 Surveys in combinatorics, 1991, A.D. KEEDWELL (ed)
- 168 Representations of algebras, H. TACHIKAWA & S. BRENNER (eds)
- 169 Boolean function complexity, M.S. PATERSON (ed)
- 170 Manifolds with singularities and the Adams-Novikov spectral sequence, B. BOTVINNIK
- 171 Squares, A.R. RAJWADE
- 172 Algebraic varieties, GEORGE R. KEMPF
- 173 Discrete groups and geometry, W.J. HARVEY & C. MACLACHLAN (eds)
- 174 Lectures on mechanics, J.E. MARSDEN
- 175 Adams memorial symposium on algebraic topology 1, N. RAY & G. WALKER (eds)
- 176 Adams memorial symposium on algebraic topology 2, N. RAY & G. WALKER (eds)
- 177 Applications of categories in computer science, M. FOURMAN, P. JOHNSTONE & A. PITTS (eds)
- 178 Lower K- and L-theory, A. RANICKI
- 179 Complex projective geometry, G. ELLINGSRUD *et al*
- 180 Lectures on ergodic theory and Pesin theory on compact manifolds, M. POLLICOTT
- 181 Geometric group theory I, G.A. NIBLO & M.A. ROLLER (eds)
- 182 Geometric group theory II, G.A. NIBLO & M.A. ROLLER (eds)
- 183 Shintani zeta functions, A. YUKIE
- 184 Arithmetical functions, W. SCHWARZ & J. SPILKER
- 185 Representations of solvable groups, O. MANZ & T.R. WOLF
- 186 Complexity: knots, colourings and counting, D.J.A. WELSH
- 187 Surveys in combinatorics, 1993, K. WALKER (ed)
- 188 Local analysis for the odd order theorem, H. BENDER & G. GLAUBERMAN
- 189 Locally presentable and accessible categories, J. ADAMEK & J. ROSICKY
- 190 Polynomial invariants of finite groups, D.J. BENSON

Cambridge University Press

0521653746 - Elliptic Curves in Cryptography

I. F. Blake, G. Seroussi and N. P. Smart

Frontmatter

[More information](#)

- 191 Finite geometry and combinatorics, F. DE CLERCK *et al*
 192 Symplectic geometry, D. SALAMON (ed)
 194 Independent random variables and rearrangement invariant spaces, M. BRAVERMAN
 195 Arithmetic of blowup algebras, WOLMER VASCONCELOS
 196 Microlocal analysis for differential operators, A. GRIGIS & J. SJÖSTRAND
 197 Two-dimensional homotopy and combinatorial group theory, C. HOG-ANGELONI *et al*
 198 The algebraic characterization of geometric 4-manifolds, J.A. HILLMAN
 199 Invariant potential theory in the unit ball of \mathbb{C}^n , MANFRED STOLL
 200 The Grothendieck theory of dessins d'enfant, L. SCHNEPS (ed)
 201 Singularities, JEAN-PAUL BRASSELET (ed)
 202 The technique of pseudodifferential operators, H.O. CORDES
 203 Hochschild cohomology of von Neumann algebras, A. SINCLAIR & R. SMITH
 204 Combinatorial and geometric group theory, A.J. DUNCAN, N.D. GILBERT & J. HOWIE (eds)
 205 Ergodic theory and its connections with harmonic analysis, K. PETERSEN & I. SALAMA (eds)
 207 Groups of Lie type and their geometries, W.M. KANTOR & L. DI MARTINO (eds)
 208 Vector bundles in algebraic geometry, N.J. HITCHIN, P. NEWSTEAD & W.M. OXBURY (eds)
 209 Arithmetic of diagonal hypersurfaces over finite fields, F.Q. GOUVÊA & N. YUI
 210 Hilbert \mathbb{C}^* -modules, E.C. LANCE
 211 Groups 93 Galway / St Andrews I, C.M. CAMPBELL *et al* (eds)
 212 Groups 93 Galway / St Andrews II, C.M. CAMPBELL *et al* (eds)
 214 Generalised Euler-Jacobi inversion formula and asymptotics beyond all orders, V. KOWALENKO *et al*
 215 Number theory 1992–93, S. DAVID (ed)
 216 Stochastic partial differential equations, A. ETHERIDGE (ed)
 217 Quadratic forms with applications to algebraic geometry and topology, A. PFISTER
 218 Surveys in combinatorics, 1995, PETER ROWLINSON (ed)
 220 Algebraic set theory, A. JOYAL & I. MOERDIJK
 221 Harmonic approximation, S.J. GARDINER
 222 Advances in linear logic, J.-Y. GIRARD, Y. LAFONT & L. REGNIER (eds)
 223 Analytic semigroups and semilinear initial boundary value problems, KAZUAKI TAIRA
 224 Computability, enumerability, unsolvability, S.B. COOPER, T.A. SLAMAN & S.S. WAINER (eds)
 225 A mathematical introduction to string theory, S. ALBEVERIO, J. JOST, S. PAYCHA, S. SCARLATTI
 226 Novikov conjectures, index theorems and rigidity I, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
 227 Novikov conjectures, index theorems and rigidity II, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
 228 Ergodic theory of \mathbb{Z}^d actions, M. POLLICOTT & K. SCHMIDT (eds)
 229 Ergodicity for infinite dimensional systems, G. DA PRATO & J. ZABCZYK
 230 Prolegomena to a middlebrow arithmetic of curves of genus 2, J.W.S. CASSELS & E.V. FLYNN
 231 Semigroup theory and its applications, K.H. HOFMANN & M.W. MISLOVE (eds)
 232 The descriptive set theory of Polish group actions, H. BECKER & A.S. KECHRIS
 233 Finite fields and applications, S. COHEN & H. NIEDERREITER (eds)
 234 Introduction to subfactors, V. JONES & V.S. SUNDER
 235 Number theory 1993–94, S. DAVID (ed)
 236 The James forest, H. FETTER & B. GAMBOA DE BUEN
 237 Sieve methods, exponential sums, and their applications in number theory, G.R.H. GREAVES *et al*
 238 Representation theory and algebraic geometry, A. MARTSINKOVSKY & G. TODOROV (eds)
 239 Clifford algebras and spinors, P. LOUNESTO
 240 Stable groups, FRANK O. WAGNER
 241 Surveys in combinatorics, 1997, R.A. BAILEY (ed)
 242 Geometric Galois actions I, L. SCHNEPS & P. LOCHAK (eds)
 243 Geometric Galois actions II, L. SCHNEPS & P. LOCHAK (eds)
 244 Model theory of groups and automorphism groups, D. EVANS (ed)
 245 Geometry, combinatorial designs and related structures, J.W.P. HIRSCHFELD *et al*
 246 p -Automorphisms of finite p -groups, E.I. KHUKHRO
 247 Analytic number theory, Y. MOTOHASHI (ed)
 248 Tame topology and o-minimal structures, LOU VAN DEN DRIES
 249 The atlas of finite groups: ten years on, ROBERT CURTIS & ROBERT WILSON (eds)
 250 Characters and blocks of finite groups, G. NAVARRO
 251 Gröbner bases and applications, B. BUCHBERGER & F. WINKLER (eds)
 252 Geometry and cohomology in group theory, P. KROPHOLLER, G. NIBLO, R. STÖHR (eds)
 253 The q -Schur algebra, S. DONKIN
 254 Galois representations in arithmetic algebraic geometry, A.J. SCHOLL & R.L. TAYLOR (eds)
 255 Symmetries and integrability of difference equations, P.A. CLARKSON & F.W. NIJHOFF (eds)
 256 Aspects of Galois theory, HELMUT VÖLKLEIN *et al*
 257 An introduction to noncommutative differential geometry and its physical applications 2ed, J. MADORE
 258 Sets and proofs, S.B. COOPER & J. TRUSS (eds)
 259 Models and computability, S.B. COOPER & J. TRUSS (eds)
 260 Groups St Andrews 1997 in Bath, I, C.M. CAMPBELL *et al*
 261 Groups St Andrews 1997 in Bath, II, C.M. CAMPBELL *et al*
 263 Singularity theory, BILL BRUCE & DAVID MOND (eds)
 264 New trends in algebraic geometry, K. HULEK, F. CATANESE, C. PETERS & M. REID (eds)
 265 Elliptic curves in cryptography, I. BLAKE, G. SEROUSSI & N. SMART
 267 Surveys in combinatorics, 1999, J.D. LAMB & D.A. PREECE (eds)
 268 Spectral asymptotics in the semi-classical limit, M. DIMASSI & J. SJÖSTRAND
 269 Ergodic theory and topological dynamics, M. B. BEKKA & M. MAYER
 270 Analysis on Lie Groups, N. T. VAROPOULOS & S. MUSTAPHA
 271 Singular perturbations of differential operators, S. ALBERVERIO & P. KURASOV
 272 Character theory for the odd order function, T. PETERFALVI
 273 Spectral theory and geometry, E. B. DAVIES & Y. SAFAROV (eds)
 274 The Mandelbrot set: theme and variation, TAN LEI (ed)

Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Frontmatter
[More information](#)

London Mathematical Society Lecture Note Series. 265

Elliptic Curves in Cryptography

I. F. Blake
Hewlett-Packard Laboratories, Palo Alto

G. Seroussi
Hewlett-Packard Laboratories, Palo Alto

N. P. Smart
Hewlett-Packard Laboratories, Bristol



Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Frontmatter
[More information](#)

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521653749

© I.F. Blake, G. Seroussi, N.P. Smart 1999

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 1999
Reprinted 2000 (three times), 2001, 2002, 2004

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

Blake Ian F.

Elliptic Curves in Cryptography / I.F. Blake, G. Seroussi, N.P. Smart
p. cm. – (London Mathematical Society Lecture Note Series; 265)

Includes bibliographical references and index.

ISBN 0 521 65374 6 (pbk.)

1. Computer security. 2. Cryptography. 3. Curves, Elliptic—Data processing.

I. Seroussi, G. (Gadiel), 1955 - II. Smart, Nigel P. (Nigel Paul), 1967 -.

III. Title. IV. Series.

QA76.9.A25.B27 1999

005.8'.2—dc21 99—19696 CIP

ISBN-13 978-0-521-65374-9 paperback

ISBN-10 0-521-65374-6 paperback

Transferred to digital printing 2006

Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Frontmatter
[More information](#)

To

Elizabeth, Lauren and Michael,

Lidia, Ariel and Dahlia,

Maggie, Ellie and Oliver.

Contents

Preface	xi
Abbreviations and Standard Notation	xiii
Chapter I. Introduction	1
I.1. Cryptography Based on Groups	2
I.2. What Types of Group are Used	6
I.3. What it Means in Practice	8
Chapter II. Finite Field Arithmetic	11
II.1. Fields of Odd Characteristic	11
II.2. Fields of Characteristic Two	19
Chapter III. Arithmetic on an Elliptic Curve	29
III.1. General Elliptic Curves	30
III.2. The Group Law	31
III.3. Elliptic Curves over Finite Fields	34
III.4. The Division Polynomials	39
III.5. The Weil Pairing	42
III.6. Isogenies, Endomorphisms and Torsion	44
III.7. Various Functions and q -Expansions	46
III.8. Modular Polynomials and Variants	50
Chapter IV. Efficient Implementation of Elliptic Curves	57
IV.1. Point Addition	57
IV.2. Point Multiplication	62
IV.3. Frobenius Expansions	73
IV.4. Point Compression	76
Chapter V. The Elliptic Curve Discrete Logarithm Problem	79
V.1. The Simplification of Pohlig and Hellman	80
V.2. The MOV Attack	82
V.3. The Anomalous Attack	88
V.4. Baby Step/Giant Step	91
V.5. Methods based on Random Walks	93
V.6. Index Calculus Methods	97
V.7. Summary	98

viii	CONTENTS	
Chapter VI.	Determining the Group Order	101
VI.1.	Main Approaches	101
VI.2.	Checking the Group Order	103
VI.3.	The Method of Shanks and Mestre	104
VI.4.	Subfield Curves	104
VI.5.	Searching for Good Curves	106
Chapter VII.	Schoof's Algorithm and Extensions	109
VII.1.	Schoof's Algorithm	109
VII.2.	Beyond Schoof	114
VII.3.	More on the Modular Polynomials	118
VII.4.	Finding Factors of Division Polynomials through Isogenies: Odd Characteristic	122
VII.5.	Finding Factors of Division Polynomials through Isogenies: Characteristic Two	133
VII.6.	Determining the Trace Modulo a Prime Power	138
VII.7.	The Elkies Procedure	139
VII.8.	The Atkin Procedure	140
VII.9.	Combining the Information from Elkies and Atkin Primes	142
VII.10.	Examples	144
VII.11.	Further Discussion	147
Chapter VIII.	Generating Curves using Complex Multiplication	149
VIII.1.	The Theory of Complex Multiplication	149
VIII.2.	Generating Curves over Large Prime Fields using CM	151
VIII.3.	Weber Polynomials	155
VIII.4.	Further Discussion	157
Chapter IX.	Other Applications of Elliptic Curves	159
IX.1.	Factoring Using Elliptic Curves	159
IX.2.	The Pocklington–Lehmer Primality Test	162
IX.3.	The ECPP Algorithm	164
IX.4.	Equivalence between DLP and DHP	166
Chapter X.	Hyperelliptic Cryptosystems	171
X.1.	Arithmetic of Hyperelliptic Curves	171
X.2.	Generating Suitable Curves	173
X.3.	The Hyperelliptic Discrete Logarithm Problem	176
Appendix A.	Curve Examples	181
A.1.	Odd Characteristic	181
A.2.	Characteristic Two	186
	Bibliography	191
	Author Index	199

Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Frontmatter
[More information](#)

CONTENTS

Subject Index

ix

201

Preface

Much attention has recently been focused on the use of elliptic curves in public key cryptography, first proposed in the work of Koblitz [62] and Miller [103]. The motivation for this is the fact that there is no known sub-exponential algorithm to solve the discrete logarithm problem on a general elliptic curve. In addition, as will be discussed in Chapter I, the standard protocols in cryptography which make use of the discrete logarithm problem in finite fields, such as Diffie–Hellman key exchange, ElGamal encryption and digital signature, Massey–Omura encryption and the Digital Signature Algorithm (DSA), all have analogues in the elliptic curve case.

Cryptosystems based on elliptic curves are an exciting technology because for the same level of security as systems such as RSA [134], using the current knowledge of algorithms in the two cases, they offer the benefits of smaller key sizes and hence of smaller memory and processor requirements. This makes them ideal for use in smart cards and other environments where resources such as storage, time, or power are at a premium.

Some researchers have expressed concern that the basic problem on which elliptic curve systems are based has not been looked at in as much detail as, say, the factoring problem, on which systems such as RSA are based. However, all such systems based on the perceived difficulty of a mathematical problem live in fear of a dramatic breakthrough to some extent, and this issue is not addressed further in this work.

This book discusses various issues surrounding the use of elliptic curves in cryptography, including:

- The basic arithmetic operations, not only on the curves but also over finite fields.
- Ways of efficiently implementing the basic operation of adding a point to itself a large number of times (point multiplication).
- Known attacks on systems based on elliptic curves.
- A large section devoted to computing the number of rational points on elliptic curves over finite fields.
- A discussion on the generalization of elliptic curve systems to hyperelliptic systems.

The book is written for a wide audience ranging from the mathematician who knows about elliptic curves (or has been acquainted with them) and who wants a quick survey of the main results pertaining to cryptography, to an

implementer who requires some knowledge of elliptic curve mathematics for use in a practical cryptosystem. Clearly, aiming for such diverse audiences is hard, and not all parts of the book will be of the same level of interest to all readers. However, most of the important points such as implementation issues, security issues and point counting issues can be acquired with only a moderate understanding of the underlying mathematics.

We try and give a flavour of the mathematics involved for those who are interested. We decided however not to include most proofs since that not only would dramatically increase the size of the book but also would not serve its main purpose. It is hoped that the numerous references cited and the extensive bibliography provided will direct the interested reader to appropriate sources for all the missing details. In fact, much of the necessary mathematical background can be found in the books by Silverman, [147] and [148].

Some of the topics covered in the book by Menezes [97] are expanded upon. In particular the improvements made to the algorithm of Schoof [141] for determining the number of rational points on an elliptic curve are explained, and the method of finding curves using the theory of complex multiplication is discussed. This latter method has other applications when one uses elliptic curves to construct proofs of primality. We also give the first treatment in book form of such methods as point compression (including x -coordinate compression), the attack on anomalous curves and the generalization of the MOV attack to curves such as those with the trace of Frobenius equal to two. Two chapters are devoted to implementation issues. One covers finite fields while the second covers the various techniques available for point multiplication. In addition, the chapter on Schoof's algorithm and its improvements provides algorithmic summaries intended to facilitate the implementation of these point counting techniques.

We would like to thank D. Boneh, S. Galbraith, A.J. Menezes, K. Paterson, M. Rubinstein, E. Scheafer, R. Schoof and S. Zaba who have looked over various portions of the manuscript and given us their comments. All of the remaining mistakes and problems are our own and we apologize in advance for any you may find. The authors would also like to thank Dan Boneh, Johannes Buchmann, Markus Maurer and Volker Müller for many discussions on elliptic curves, their assistance with the implementation of point counting algorithms and the prompt answering of many queries. Thanks are due also to John Cremona for his \LaTeX algorithm template which we modified to produce the algorithms in this book.

Finally thanks are due to Hewlett-Packard Company and our colleagues and managers there for their support, assistance and encouragement during the writing of this book.

Abbreviations and Standard Notation

Abbreviations

The following abbreviations of standard phrases are used throughout the book:

AES	Advanced Encryption Standard
BSGS	baby step/giant step method
CM	Complex multiplication
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DHP	Diffie–Hellman problem
DLP	Discrete logarithm problem
DSA	Digital Signature Algorithm
ECDLP	Elliptic curve discrete logarithm problem
ECM	Elliptic curve factoring method
ECPP	Elliptic curve primality proving method
GCD	Greatest common divisor
LCM	Least common multiple
MOV	Menezes–Okamoto–Vanstone attack
NAF	Non-adjacent form
NFS	Number field sieve
ONB	Optimal normal basis
RNS	Residue number system
RSA	Rivest–Shamir–Adleman encryption scheme
SD	Signed digit
SEA	Schoof–Elkies–Atkin algorithm

Standard notation

The following standard notation is used throughout the book, often without further definition. Other notation is defined locally near its first use.

K^*, K^+, \bar{K}	for a field K , the multiplicative group, additive group, and algebraic closure, respectively
$\text{Gal}(K/F)$	Galois group of K over F
$\text{Aut}(G)$	Automorphism group of G
$\text{char}(K)$	characteristic of K
$\text{gcd}(f, g), \text{lcm}(f, g)$	GCD, LCM of f and g
$\text{deg}(f)$	degree of a polynomial f
$\text{ord}(g)$	order of an element g in a group
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	integers, rationals, reals and complex numbers
$\mathbb{Z}_{>k}$	integers greater than k ; similarly for $\geq, <, \leq$
$\mathbb{Z}/n\mathbb{Z}$	integers modulo n
$\mathbb{Z}_p, \mathbb{Q}_p$	p -adic integers and numbers, respectively
\mathbb{F}_q	finite field with q elements
$\text{Tr}_{q/p}(x)$	trace of $x \in \mathbb{F}_q$ over $\mathbb{F}_p, q = p^n$
$\langle g \rangle$	cyclic group generated by g
$\#S$	cardinality of the set S
E	elliptic curve (equation)
$E(K)$	group of K -rational points on E
$[m]P$	multiplication-by- m map applied to the point P
$E[m]$	group of m -torsion points on the elliptic curve E
$\text{End}(E)$	Endomorphism ring of E
\mathcal{O}	point at infinity (on an elliptic curve)
\wp	Weierstrass ‘pay’ function
φ	Frobenius map
ϕ_{Eul}	Euler totient function
$GL_2(R)$	general linear group over the ring R : 2×2 matrices over R with determinant a unit in R
$PGL_2(K)$	projective general linear group over the field K , with scalar multiples identified
$SL_2(\mathbb{Z})$	special linear group of 2×2 matrices over \mathbb{Z} with determinant one
$\left(\frac{\cdot}{p}\right)$	Legendre symbol
$\text{Re}(z), \text{Im}(z)$	real and imaginary parts of $z \in \mathbb{C}$, respectively
\mathcal{H}	Poincaré half-plane $\text{Im}(z) > 0$
$O(f(n))$	function $g(n)$ such that $ g(n) \leq c f(n) $ for some constant $c > 0$ and all sufficiently large n
$o(f(n))$	function $g(n)$ such that $\lim_{n \rightarrow \infty} (g(n)/f(n)) = 0$
$\log_b x$	logarithm to base b of x ; natural log if b omitted

Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Frontmatter
[More information](#)

ABBREVIATIONS AND STANDARD NOTATION

xv

Often we will need to present binary, hexadecimal or decimal numbers which are too long to fit on one line. We shall use the standard convention of breaking the number into multiple lines, with a backslash at the end of a line indicating that the number is continued in the next line. For example

$$\begin{aligned} p &= 2^{230} + 67 \\ &= 17254365866976409468586889655692563631127772430425\backslash \\ &\quad 96638790631055949891. \end{aligned}$$