Many Rational Points: Coding Theory and Algebraic Geometry

By N. E. Hurt

Springer. Hardcover. Book Condition: New. Hardcover. 346 pages. Dimensions: 9.7in. x 6.6in. x 0.8in.2 Triangle Groups: An Introduction 279 3 Elementary Shimura Curves 281 4 Examples of Shimura Curves 282 5 Congruence Zeta Functions 283 6 Diophantine Properties of Shimura Curves 284 7 Klein Quartic 285 8 Supersingular Points 289 Towers of Elkies 9 289 7. CRYPTOGRAPHY AND APPLICATIONS 291 1 Introduction 291 Discrete Logarithm Problem 2 291 Curves for Public-Key Cryptosystems 3 295 Hyperelliptic Curve Cryptosystems 4 297 CM-Method 5 299 6 Cryptographic Exponent 300 7 Constructive Descent 302 8 Gaudry and Harley Algorithm 306 9 Picard Jacobians 307 Drinfeld Module Based Public Key Cryptosystems 10 308 11 Drinfeld Modules and One Way Functions 308 12 Shimuras Map 309 13 Modular Jacobians of Genus 2 Curves 310 Modular Jacobian Surfaces 14 312 15 Modular Curves of Genus Two 313 16 Hecke Operators 314 8. REFERENCES 317 345 Index Xll Preface The history of counting points on curves over finite fields is very ex tensive, starting with the work of Gauss in 1801 and continuing with the work of Artin, Schmidt, Hasse and Weil in their study of curves and the related zeta functions $Z_X(t)$, where m $Z_X(t)$ exp (2:...

READ ONLINE
[7.08 MB]