Review of the book

"Elliptic Curves – Number Theory and Cryptography (Second Edition)"
by Lawrence C. Washington
CRC Press, Taylor & Francis Group, 2008

ISBN: 978-1-4200-7146-7

Vincent C. Immler
Horst Görtz Institute for IT-Security

1 What the book is about

The book is about elliptic curves and introduces several applications for them.

Starting with a basic introduction to the subject (chapters 1,2,3,4), the book then splits up into three different parts:

I) **Cryptography Track:** Chapters 5, 6, 7, 11 ,13.

II) **Number Theory Track:** Chapters 8, 9, 10, 11, 12, 14, 15.

III) **Complex Track:** Chapters 9 and 10, plus Section 12.1.

The first chapter is an introduction, leading to an equation to describe an elliptic curve. After creating a basic understanding for elliptic curves, the author introduces the basic theory of elliptic curves in the second chapter, namely: the Weierstrass equations, the group law and the point at infinity. Furthermore, other equations and different coordinate systems are given to describe elliptic curves. This section on different coordinate systems was added to the second edition of the book and is a very useful addition to it. Further topics in the second chapter are: the j-invariant, endomorphisms, singular curves, elliptic curves in characteristic 2 and finally, elliptic curves mod n. The third chapter is about torsions points, which includes a section on Weil pairings which need to be understood for later proofs. After that, the fourth chapter deals with elliptic curves over finite fields and defines such things as: the Frobenius endomorphism, determining the group order and Schoof's algorithm.

Cryptography Track: This part concentrates on elliptic curves from a cryptographer's perspective. Starting with the discrete logarithm problem and general attacks, leading over to attacks based on pairings and various other attacks (e.g. on anomalous curves), followed by the description of different protocols like Diffie-Hellman key exchange and ElGamal based on elliptic curves. Chapter 6 additionally features signature algorithms and a cryptosystem based on the Weil pairing. Other applications like factoring and primality testing are introduced in chapter 7. Chapter 11 deals with divisors and chapter 13 with hyperelliptic curves.

Number Theory Track: The track more appealing to mathematicians concentrating on number theory, starts with chapter 8 on elliptic curves over the rational numbers and includes the complex track, that deals with elliptic curves over the complex numbers (chapters 9 and 10). Followed by a new chapter on isogenies, a chapter on zeta functions and a final chapter on Fermat's last theorem.

The appendix contains amongst theorems on number theory, groups and fields, a brief introduction on computer algebra packages (Pari, Magma, SAGE) to do computations on elliptic curves. Each chapter ends with exercises to solve. Unfortunately, the book does not contain solutions to these exercises.

Throughout the book, references are given for the even more interested and sophisticated reader. By now, there is only a very short but needed errata list on the author's website.[1]

2 What is the book like

As seen, the book is well structured and does not waste the readers time in dividing cryptography from number theory only information. This enables the reader just to pick the desired information. Even though, it is a very comprehensive guide on the theory of elliptic curves.

The book starts with good and easily understandable examples. After the first four chapters the book suffers from missing a little explanation. Sometimes it will be necessary to look up some basic information on a topic to get a first idea, what the whole thing is about (e.g. torsion points). After doing so, the reader is able to enjoy a precise description of the specific topic.

Later on in the book, chapters do not start with an abstract anymore. That is a pity, as this gives the reader a feeling of being lost. I would suggest to extend the existing chapter abstracts and add them, where they are missing. They create connections between chapters and give a nice red thread to follow.

Exercises are really valuable and let the reader reconsider the most important aspects of the section.

The writing style is always mathematical and the reader should be quite used to it. In that case, it should be possible to understand most topics in an appropriate time. The book is definitely not intended as a book to read right through.

A good distinction has been made in proofs that are necessary and those, that are better being referenced.

Not covered in this book are implementation related problems and solutions. A nice way to play with elliptic curves is to use one of the proposed computer algebra packages in the appendix.

To further enhance the book, adding a nomenclature would be a good idea.

3 Would you recommend this book?

I can recommend this book for both cryptographers and mathematicians doing either their Ph.D. or Master, because the book assumes some previous knowledge in number theory as well as cryptography. Therefore, the book only partially qualifies for self-study. Sometimes the given exercises are very easy to solve, but some could deserve a hint or even a solution. Undergraduates will probably only need the first five or six chapters of the book and will have more luck with more easily accessible books on elliptic curves, that have a little more explanation.

It is not necessary to have any previous knowledge on elliptic curves.

The book is not suited for engineers that want to have a more practical approach to elliptic curves, as implementation issues are not covered. In addition to that, the writing style might be too mathematical for them.

However, I enjoyed reading and studying this book and will be glad to have it as a future reference.

The reviewer is a student of IT-Security at the Ruhr-University Bochum (Germany).

[1] `http://www-users.math.umd.edu/~lcw/ECerrata2.pdf`.