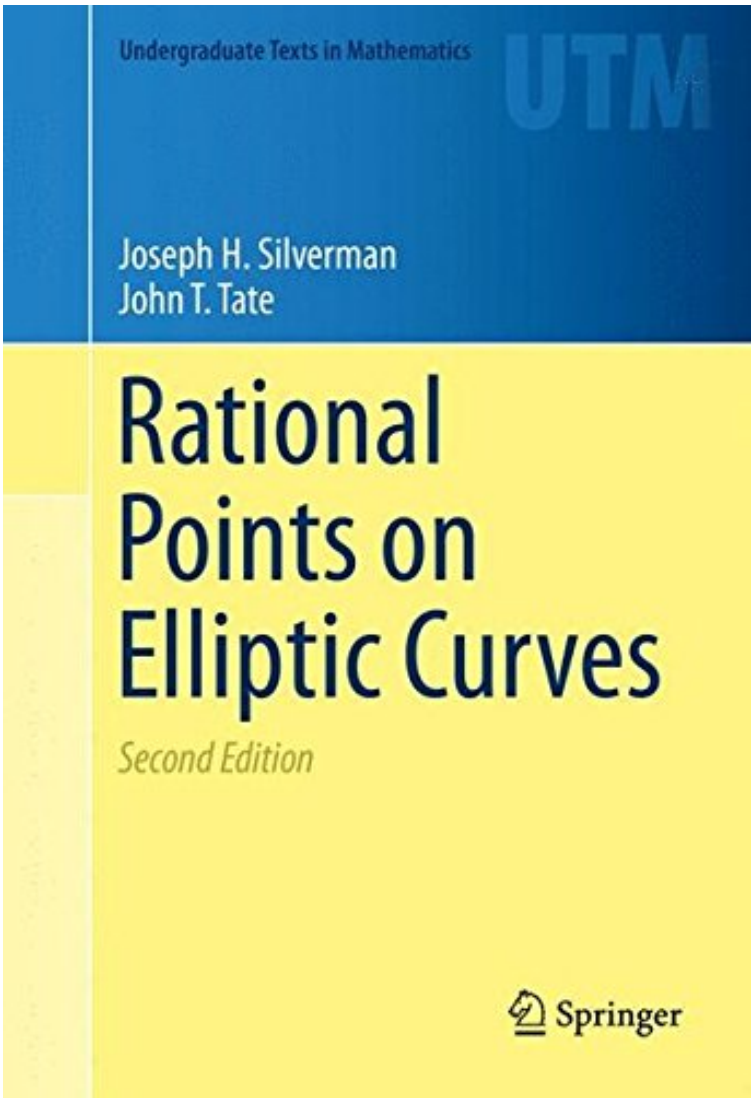
Rational Points on Elliptic Curves (Undergraduate Texts in Mathematics)

Joseph H. Silverman, John T. Tate
**Download PDF | ePub | DOC | audiobook | ebooks*



#815286 in Books 2015-06-03Original language:EnglishPDF # 1 9.21 x .81 x 6.14l, 1.40 #File Name: 331918587X332 pages | File size: 23.Mb

Joseph H. Silverman, John T. Tate : Rational Points on Elliptic Curves (Undergraduate Texts in Mathematics) before purchasing it in order to gage whether or not it would be worth my time, and all praised Rational Points on Elliptic Curves (Undergraduate Texts in Mathematics):

2 of 2 people found the following review helpful. A book with modest prerequisteBy CustomerThis book is well written, and to be honest, it is very easy to understand. Usually an author of a math book likes to say: "the prerequisite is very modest..." but later you will find that this is only true for Chapter 1. This book is different. It tries to omit some

technical details but still provides useful information. The 2015 new edition adds Fermat theorem and cryptology. Highly recommended to anyone interested in Number Theory.5 of 6 people found the following review helpful. Great entry ticket into the subject matter for the non-graduate level mathematicianBy RKLIn theory, I should be pretty good at math... but I chose CS as my calling instead of math. Alas, given the importance of elliptic curve cryptography, I thought it is about time that I read up on the subject. Not having gone into any graduate level math of any type, this subject proved quite challenging -- until I discovered this book. OK, so it isn't rigorous in terms of proving everything. But for the reader interested in self-study and looking for an entry ticket, this book is the answer. When I finish, I will decide whether to pursue a more rigorous treatment. But to get started, this is a great "intro". (I put that in quotes because it still requires quite an investment.)1 of 1 people found the following review helpful. Interesting material well-doneBy bachpianohackInteresting material, carefully put together, and readable.

The theory of elliptic curves involves a pleasing blend of algebra, geometry, analysis, and number theory. This volume stresses this interplay as it develops the basic theory, thereby providing an opportunity for advanced undergraduates to appreciate the unity of modern mathematics. At the same time, every effort has been made to use only methods and results commonly included in the undergraduate curriculum. This accessibility, the informal writing style, and a wealth of exercises make Rational Points on Elliptic Curves an ideal introduction for students at all levels who are interested in learning about Diophantine equations and arithmetic geometry.Most concretely, an elliptic curve is the set of zeroes of a cubic polynomial in two variables. If the polynomial has rational coefficients, then one can ask for a description of those zeroes whose coordinates are either integers or rational numbers. It is this number theoretic question that is the main subject of Rational Points on Elliptic Curves. Topics covered include the geometry and group structure of elliptic curves, the NagellLutz theorem describing points of finite order, the MordellWeil theorem on the finite generation of the group of rational points, the ThueSiegel theorem on the finiteness of the set of integer points, theorems on counting points with coordinates in finite fields, Lenstra's elliptic curve factorization algorithm, and a discussion of complex multiplication and the Galois representations associated to torsion points. Additional topics new to the second edition include an introduction to elliptic curve cryptography and a brief discussion of the stunning proof of Fermat's Last Theorem by Wiles et al. via the use of elliptic curves.

The two main changes for this edition are a new section on elliptic curve cryptography and an explanation of how elliptic curves played a role in the proof of Fermats Last Theorem. the best place to start learning about elliptic curves. (Fernando Q. Gouva, MAA s, maa.org, April, 2016)The book is an excellent introduction to elliptic curves over the rational numbers and ideal textbook for an undergraduate course. This book is highly recommended to students and researches interested in elliptic curves and their applications. It provides a natural step to a more advanced treatment of the subject. (Andrej Dujella, zbMATH 1346.11001, 2016)From the Back CoverThe theory of elliptic curves involves a pleasing blend of algebra, geometry, analysis, and number theory. This book stresses this interplay as it develops the basic theory, thereby providing an opportunity for advanced undergraduates to appreciate the unity of modern mathematics. At the same time, every effort has been made to use only methods and results commonly included in the undergraduate curriculum. This accessibility, the informal writing style, and a wealth of exercises make Rational Points on Elliptic Curves an ideal introduction for students at all levels who are interested in learning about Diophantine equations and arithmetic geometry.Most concretely, an elliptic curve is the set of zeroes of a cubic polynomial in two variables. If the polynomial has rational coefficients, then one can ask for a description of those zeroes whose coordinates are either integers or rational numbers. It is this number theoretic question that is the main subject of this book. Topics covered include the geometry and group structure of elliptic curves, the NagellLutz theorem describing points of finite order, the MordellWeil theorem on the finite generation of the group of rational points, the ThueSiegel theorem on the finiteness of the set of integer points, theorems on counting points with coordinates in finite fields, Lenstras elliptic curve factorization algorithm, and a discussion of complex multiplication and the Galois representations associated to torsion points. Additional topics new to the second edition include an introduction to elliptic curve cryptography and a brief discussion of the stunning proof of Fermats Last Theorem by Wiles et al. via the use of elliptic curves.About the AuthorJoseph H. Silverman is Professor of Mathematics at Brown University. He is the author of over 100 research articles and numerous books on elliptic curves, diophantine geometry, cryptography, and arithmetic dynamical systems.John T. Tate is Professor Emeritus of Mathematics at The University of Texas at Austin and at Harvard University. For his seminal contributions to number theory, he was awarded the 2010 Abel Prize.