

1. Record Nr.	UNINA9910458424203321
Autore	Schertz Reinhard <1943->
Titolo	Complex multiplication // Reinhard Schertz [[electronic resource]]
Pubbl/distr/stampa	Cambridge : , : Cambridge University Press, , 2010
ISBN	1-107-20891-2 1-139-63666-9 1-282-65186-2 9786612651861 0-511-77543-1 0-511-77619-5 0-511-77361-7 0-511-77254-8 0-511-77689-6 0-511-77467-2
Descrizione fisica	1 online resource (xiii, 361 pages) : digital, PDF file(s)
Collana	New mathematical monographs ; ; 15
Disciplina	516.3/52
Soggetti	Multiplication, Complex
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from publisher's bibliographic system (viewed on 05 Oct 2015).
Nota di contenuto	Preface -- 1. Elliptic functions -- 2. Modular functions -- 3. Basic facts from number theory -- 4. Factorisation of singular values -- 5. The reciprocity law -- 6. Generation of ring class fields and ray class fields -- 7. Integral basis in ray class fields -- 8. Galois module structure -- 9. Berwick's congruences -- 10. Cryptographically relevant elliptic curves -- 11. The class number formulas of Curt Meyer -- 12. Arithmetic interpretation of class number formulas -- References -- Index of notation -- Index.
Sommario/riassunto	This is a self-contained 2010 account of the state of the art in classical complex multiplication that includes recent results on rings of integers and applications to cryptography using elliptic curves. The author is exhaustive in his treatment, giving a thorough development of the theory of elliptic functions, modular functions and quadratic number fields and providing a concise summary of the results from class field

theory. The main results are accompanied by numerical examples, equipping any reader with all the tools and formulas they need. Topics covered include: the construction of class fields over quadratic imaginary number fields by singular values of the modular invariant  $j$  and Weber's tau-function; explicit construction of rings of integers in ray class fields and Galois module structure; the construction of cryptographically relevant elliptic curves over finite fields; proof of Berwick's congruences using division values of the Weierstrass  $p$ -function; relations between elliptic units and class numbers.

---