1. Record Nr. UNINA9910789850303321

Titolo	Computational aspects of modular forms and Galois representations [[electronic resource]] : how one can compute in polynomial time the value of Ramanujan's tau at a prime / / edited by Jean-Marc Couveignes and Bas Edixhoven
Pubbl/distr/stampa	Princeton, N.J., : Princeton University Press, c2011
ISBN	1-283-05180-X 9786613051806 1-4008-3900-9
Edizione	[Course Book]
Descrizione fisica	1 online resource (438 p.)
Collana	Annals of mathematics studies ; ; 176
Classificazione	MAT001000MAT012010
Altri autori (Persone)	EdixhovenB <1962-> (Bas) CouveignesJean-Marc
Disciplina	512/.32
Soggetti	Galois modules (Algebra) Class field theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front matter -- Contents -- Preface -- Acknowledgments -- Author information -- Dependencies between the chapters -- Chapter 1. Introduction, main results, context / Edixhoven, Bas -- Chapter 2. Modular curves, modular forms, lattices, Galois representations / Edixhoven, Bas -- Chapter 3. First description of the algorithms / Couveignes, Jean-Marc / Edixhoven, Bas -- Chapter 4. Short introduction to heights and Arakelov theory / Edixhoven, Bas / de Jong, Robin -- Chapter 5. Computing complex zeros of polynomials and power series / Couveignes, Jean-Marc -- Chapter 6. Computations with modular forms and Galois representations / Bosman, Johan -- Chapter 7. Polynomials for projective representations of level one forms / Bosman, Johan -- Chapter 8. Description of X1(5l) / Edixhoven, Bas -- Chapter 9. Applying Arakelov theory / Edixhoven, Bas / de Jong, Robin -- Chapter 10. An upper bound for Green functions on Riemann surfaces / Merkl, Franz -- Chapter 11. Bounds for Arakelov invariants of modular curves / Edixhoven, B. / de Jong, R. -- Chapter 12. Approximating Vf over the complex numbers / Couveignes, Jean-Marc

-- Chapter 13. Computing Vf modulo p / Couveignes, Jean-Marc -- Chapter 14. Computing the residual Galois representations / Edixhoven, Bas -- Chapter 15. Computing coefficients of modular forms / Edixhoven, Bas -- Epilogue -- Bibliography -- Index

Sommario/riassunto

"Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices. Their Fourier coefficients, with Ramanujan's tau-function as a typical example, have deep arithmetic significance. Prior to this book, the fastest known algorithms for computing these Fourier coefficients took exponential time, except in some special cases. The case of elliptic curves (Schoof's algorithm) was at the birth of elliptic curve cryptography around 1985. This book gives an algorithm for computing coefficients of modular forms of level one in polynomial time. For example, Ramanujan's tau of a prime number P can be computed in time bounded by a fixed power of the logarithm of P. Such fast computation of Fourier coefficients is itself based on the main result of the book: the computation, in polynomial time, of Galois representations over finite fields attached to modular forms by the Langlands program. Because these Galois representations typically have a nonsolvable image, this result is a major step forward from explicit class field theory, and it could be described as the start of the explicit Langlands program. The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves. The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties. Exact computations involving systems of polynomial equations in many variables take exponential time. This is avoided by numerical approximations with a precision that suffices to derive exact results from them. Bounds for the required precision--in other words, bounds for the height of the rational numbers that describe the Galois representation to be computed--are obtained from Arakelov theory. Two types of approximations are treated: one using complex uniformization and another one using geometry over finite fields. The book begins with a concise and concrete introduction that makes its accessible to readers without an extensive background in arithmetic geometry. And the book includes a chapter that describes actual computations"--
"This book represents a major step forward from explicit class field theory, and it could be described as the start of the 'explicit Langlands program'"--