
Contents

Preface	ix
Acknowledgments	x
Author information	xi
Dependencies between the chapters	xii
Chapter 1. Introduction, main results, context by <i>B. Edixhoven</i>	1
1.1 Statement of the main results	1
1.2 Historical context: Schoof's algorithm	7
1.3 Schoof's algorithm described in terms of étale cohomology	9
1.4 Some natural new directions	12
1.5 More historical context: congruences for Ramanujan's τ -function	16
1.6 Comparison with p -adic methods	26
Chapter 2. Modular curves, modular forms, lattices, Galois representations by <i>B. Edixhoven</i>	29
2.1 Modular curves	29
2.2 Modular forms	34
2.3 Lattices and modular forms	42
2.4 Galois representations attached to eigenforms	46
2.5 Galois representations over finite fields, and reduction to torsion in Jacobians	55
Chapter 3. First description of the algorithms by <i>J.-M. Couveignes and B. Edixhoven</i>	69
Chapter 4. Short introduction to heights and Arakelov theory by <i>B. Edixhoven and R. de Jong</i>	79

4.1	Heights on \mathbb{Q} and $\overline{\mathbb{Q}}$	79
4.2	Heights on projective spaces and on varieties	81
4.3	The Arakelov perspective on height functions	86
4.4	Arithmetic surfaces, intersection theory, and arithmetic Riemann-Roch	88
Chapter 5. Computing complex zeros of polynomials and power series by <i>J.-M. Couveignes</i>		95
5.1	Polynomial time complexity classes	96
5.2	Computing the square root of a positive real number	101
5.3	Computing the complex roots of a polynomial	107
5.4	Computing the zeros of a power series	115
Chapter 6. Computations with modular forms and Galois representations by <i>J. Bosman</i>		129
6.1	Modular symbols	129
6.2	Intermezzo: Atkin-Lehner operators	138
6.3	Basic numerical evaluations	140
6.4	Numerical calculations and Galois representations	150
Chapter 7. Polynomials for projective representations of level one forms by <i>J. Bosman</i>		159
7.1	Introduction	159
7.2	Galois representations	161
7.3	Proof of the theorem	166
7.4	Proof of the corollary	167
7.5	The table of polynomials	170
Chapter 8. Description of $X_1(5l)$ by <i>B. Edixhoven</i>		173
8.1	Construction of a suitable cuspidal divisor on $X_1(5l)$	173
8.2	The exact setup for the level one case	178
Chapter 9. Applying Arakelov theory by <i>B. Edixhoven and R. de Jong</i>		187
9.1	Relating heights to intersection numbers	187
9.2	Controlling $D_x - D_0$	195
Chapter 10. An upper bound for Green functions on Riemann surfaces by <i>F. Merkl</i>		203
Chapter 11. Bounds for Arakelov invariants of modular curves		

by <i>B. Edixhoven and R. de Jong</i>	217
11.1 Bounding the height of $X_1(pl)$	217
11.2 Bounding the theta function on $\text{Pic}^{g-1}(X_1(pl))$	225
11.3 Upper bounds for Arakelov Green functions on the curves $X_1(pl)$	232
11.4 Bounds for intersection numbers on $X_1(pl)$	241
11.5 A bound for $h(x'_i(Q))$ in terms of $h(b_i(Q))$	244
11.6 An integral over $X_1(5l)$	246
11.7 Final estimates of the Arakelov contribution	249
Chapter 12. Approximating V_f over the complex numbers	
by <i>J.-M. Couveignes</i>	257
12.1 Points, divisors, and coordinates on X	260
12.2 The lattice of periods	263
12.3 Modular functions	266
12.4 Power series	279
12.5 Jacobian and Wronskian determinants of series	286
12.6 A simple quantitative study of the Jacobi map	292
12.7 Equivalence of various norms	297
12.8 An elementary operation in the Jacobian variety	303
12.9 Arithmetic operations in the Jacobian variety	306
12.10 The inverse Jacobi problem	307
12.11 The algebraic conditioning	313
12.12 Heights	319
12.13 Bounding the error in X^g	323
12.14 Final result of this chapter	334
Chapter 13. Computing V_f modulo p	
by <i>J.-M. Couveignes</i>	337
13.1 Basic algorithms for plane curves	338
13.2 A first approach to picking random divisors	346
13.3 Pairings	350
13.4 Divisible groups	354
13.5 The Kummer map	359
13.6 Linearization of torsion classes	362
13.7 Computing V_f modulo p	366
Chapter 14. Computing the residual Galois representations	
by <i>B. Edixhoven</i>	371
14.1 Main result	371
14.2 Reduction to irreducible representations	372

14.3	Reduction to torsion in Jacobians	373
14.4	Computing the $\mathbb{Q}(\zeta_l)$ -algebra corresponding to V	374
14.5	Computing the vector space structure	378
14.6	Descent to \mathbb{Q}	379
14.7	Extracting the Galois representation	379
14.8	A probabilistic variant	380
Chapter 15. Computing coefficients of modular forms		
	by <i>B. Edixhoven</i>	383
15.1	Computing $\tau(p)$ in time polynomial in $\log p$	383
15.2	Computing T_n for large n and large weight	385
15.3	An application to quadratic forms	397
	Epilogue	399
	Bibliography	403
	Index	423