

CONTENTS

The number field sieve: an annotated bibliography	1
<i>H. W. Lenstra, Jr.</i>	
Factoring with cubic integers	4
<i>J. M. Pollard</i>	
Introduction	4
Properties of the set S	5
Operations on the integers of S	6
Factorisation of F_7	7
Computer and program details	9
Example of an A -solution	10
References	10
The number field sieve	11
<i>A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard</i>	
1. Introduction	11
2. The algorithm	14
3. Finding generators	20
4. Sieving	25
5. Finding the unit contribution	29
6. Run time analysis	30
7. Additional remarks	33
8. Examples	34
9. Generalization	38
References	40
The lattice sieve	43
<i>J. M. Pollard</i>	
Object of the lattice sieve	43
Operation of the sieve	45
More factorisations of F_7 !	46
Some programming notes	48
Numerical example from the factorisation of F_7	49
References	49
Factoring integers with the number field sieve	50
<i>J. P. Buhler, H. W. Lenstra, Jr., Carl Pomerance</i>	
1. Introduction	50
2. The idea of the number field sieve	52
3. Finding a polynomial	54
4. The rational sieve	55
5. The algebraic sieve	57
6. Four obstructions	60

7. Algebraic interlude	63
8. Quadratic characters	67
9. Finding square roots	70
10. Analytic interlude	76
11. Summary of the number field sieve and a heuristic analysis	80
12. Homogeneous polynomials	84
References	92
Computing a square root for the number field sieve	95
<i>Jean-Marc Couveignes</i>	
1. Introduction	95
2. Description and analysis of the method	98
References	102
A general number field sieve implementation	103
<i>Daniel J. Bernstein, A. K. Lenstra</i>	
1. Introduction	103
2. Outline of the implementation	104
3. Choosing the polynomial	104
4. Searching for a polynomial	107
5. Computing bases	108
6. Sieving	108
7. Trial dividing	114
8. Constructing the matrix	115
9. Reducing the matrix	116
10. Computing the square root	116
11. Proof that the square root works	118
12. Examples	120
13. Future directions	124
References	125
The illustration on the front cover	127
Index	129