

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 1 |
| 1.1 | Development of the results | 1 |
| 1.2 | Structure of the thesis | 3 |
| 2 | Prime numbers | 5 |
| 2.1 | The distribution of primes | 5 |
| 2.2 | More on analytic number theory | 12 |
| 2.3 | Counting other classes of integers | 22 |
| 3 | Algorithmic number theory | 27 |
| 3.1 | Basic algorithms | 27 |
| 3.2 | Newton: Recognizing perfect powers | 37 |
| 3.3 | Primality testing | 39 |
| 3.4 | Factoring algorithms by sieving | 51 |
| 3.5 | Factoring algorithms using elliptic curves | 57 |
| 4 | Differential addition in Edwards form | 69 |
| 4.1 | State of the art | 69 |
| 4.2 | Edwards form | 72 |
| 4.3 | Representing points in Edwards form | 72 |
| 4.4 | A tripling formula | 75 |
| 4.5 | Recovering the x -coordinate | 76 |
| 4.6 | A parametrization using squares only | 78 |
| 5 | Public key cryptography | 81 |
| 5.1 | Diffie and Hellman: New directions in cryptography | 81 |
| 5.2 | Doing it: RSA | 82 |
| 5.3 | The ubiquity of grained integers | 83 |
| 6 | Coarse-grained integers | 85 |
| 6.1 | The recursion | 88 |
| 6.2 | Using estimates | 90 |

| | | |
|-----------|--|------------|
| 6.3 | Approximations | 93 |
| 6.4 | Solving the recursion for $\tilde{\lambda}^k$ | 96 |
| 6.5 | Estimating the estimate $\hat{\lambda}^k$ | 110 |
| 6.6 | Reestimating $\hat{\lambda}^k$ without Riemann | 114 |
| 6.7 | Improvements | 116 |
| 6.8 | Non-squarefree numbers are negligible | 120 |
| 6.9 | Results on coarse-grained integers | 122 |
| 6.10 | Numeric evaluation | 125 |
| 7 | Hardware for the GNFS | 129 |
| 7.1 | Framework | 129 |
| 7.2 | Modelling the cluster system | 130 |
| 7.3 | Concrete statistical analyses | 134 |
| 7.4 | Generalizations to an arbitrary number of clusters | 137 |
| 7.5 | Connection to the theoretical results | 139 |
| 8 | RSA integers | 141 |
| 8.1 | Framework | 141 |
| 8.2 | RSA integers in general | 143 |
| 8.3 | Toolbox | 146 |
| 8.4 | Some common definitions for RSA integers | 156 |
| 8.5 | Arbitrary notions | 162 |
| 8.6 | Complexity theoretic considerations | 166 |
| 9 | Generalized RSA integers | 171 |
| 9.1 | Framework and toolbox | 172 |
| 9.2 | Some results | 173 |
| 10 | Standards for RSA integers | 177 |
| 10.1 | Generating RSA integers properly | 177 |
| 10.2 | Output entropy | 182 |
| 10.3 | Information-theoretical efficiency | 185 |
| 10.4 | Impact on standards and implementations | 186 |
| 11 | Future work and open problems | 195 |
| | Bibliography | 197 |
| | Players | 213 |
| | Index | 221 |