Integer Factorization

Diana Gren
Jonas Carlsson

DD2440 Advanced Algorithms
Stefan Nilsson

Contents

Chapter 1

Background

1.1 Algorithms

1.1.1 Pollard Rho

1.1.2 Quadratic Sieve

Chapter 2

Approach

2.1 Pollard Rho

2.1.1 Implementation

2.1.2 Problems

2.2 Pollard Rho with Brent

2.2.1 Implementation

2.2.2 Problems

Chapter 3

Results

Chapter 4

Conclusion

Appendix A

Pollard Rho source code