MATH 343, REVIEW SHEET FOR THE SECOND HOUR EXAM

ANDREW J. BLUMBERG

1. Things to know

(1) Smooth numbers and the quadratic sieve.
(2) RSA signatures.
(3) Collision algorithms for discrete log. (You must understand the probabilistic analysis, at least roughly.)
(4) Pollards ρ algorithm.
(5) Elliptic curves (including the idea of $\mathbb{F}_p$ points).
(6) The addition law on an elliptic curve.
(7) Finite fields of order p^q.
(8) The Frobenius and its use in elliptic curve cryptography.