

6.2	Phase 2: Distinct-degree factorization	50
6.3	Phase 3: Finding irreducible factors of degree i	51

II

Quadratic Equations in Two Variables

7	Primality Testing: Before 2002	55
7.1	Fermat and Mersenne primes	55
7.1.1	Primes of the form $2^n + 1$	55
7.1.2	Primes of the form $2^n - 1$	56
7.2	Testing Fermat's little theorem	56
7.3	Fibonacci and Lucas pseudoprimality tests	57
7.4	The Miller-Rabin Test	58
7.4.1	Analysis of time complexity	59
7.4.2	Analysis of correctness probability	59
8	The Integer Factoring Problem	61
8.1	Trial Division and Fermat's Method	61
8.2	Pollard rho Algorithm	61
8.3	Dixon's Algorithm	63
9	Primality Testing: The AKS algorithm	67
9.1	A Polynomial Identity	67
9.2	The Algorithm	67
9.2.1	Running Time:	68
9.3	Correctness	68
9.3.1	The Proof Strategy	69
9.3.2	The Proof	69