that we want to factor, it will fail every single primality test we apply to it, and the primality tests will not help us find a factor.

References for § V.1

1. L. M. Adleman, C. Pomerance, and R. S. Rumely, "On distinguishing prime numbers from composite numbers," *Annals of Math.* **117** (1983), 173–206.
2. H. Cohen and H. W. Lenstra, Jr., "Primality testing and Jacobi sums," *Math. Comp.* **42** (1984), 297–330.
3. J. D. Dixon, "Factorization and primality tests," *American Math. Monthly* **91** (1984), 333–352.
4. E. Kranakis, *Primality and Cryptography*, John Wiley & Sons, 1986.
5. A. Lenstra, "Primality testing," *Cryptology and Computational Number Theory, Proc. Symp. Appl. Math.* **42** (1990), 13–25.
6. G. L. Miller, "Riemann's hypothesis and tests for primality," *Proc. 7th Annual ACM Symposium on the Theory of Computing*, 234–239.
7. C. Pomerance, "Recent developments in primality testing," *The Math . Intelligencer* **3** (1981), 97–105.
8. C. Pomerance, "The search for prime numbers," *Scientific American* **247** (1982), 136–147.
9. M. O. Rabin, "Probabilistic algorithms for testing primality," *J. Number Theory* **12** (1980), 128–138.
10. R. Solovay and V. Strassen, "A fast Monte Carlo test for primality," *SIAM J. Computing* **6** (1977), 84–85 and *erratum*, **7** (1978), 118.
11. S. Wagon, "Primality testing," *The Math. Intelligencer* **8**, No. 3 (1986), 58–61.

2 The rho method

Suppose we know that a certain large odd integer n is composite; for example, we found that it fails one of the primality tests in §1. As mentioned before, this does not mean that we have any idea of what a factor of n might be. Of the methods we have encountered for testing primality, only the very slowest — trying to divide by the successive primes less than $\sqrt{n}$ — actually gives us a prime factor at the same time as it tells us that n is composite. All of the faster primality test algorithms are more indirect: they tell us that n must have proper factors, but not what they are.

The method of trial division by primes $< \sqrt{n}$ can take more than $O(\sqrt{n})$ bit operations. The simplest algorithm which is substantially faster than this is J. M. Pollard's "rho method" (also called the "Monte Carlo" method) of factorization.