4. In the continued fraction algorithm explain why there is no need to include in the factor base B any primes p such that $(\frac{n}{p}) = -1$.
5. Following Examples 2 and 3, use the continued fraction algorithm to factor the following numbers: (a) 9509; (b) 13561; (c) 8777; (d) 14429; (e) 12403; (f) 14527; (g) 10123; (h) 12449; (i) 9353; (j) 25511; (k) 17873.

References for § V.4

1. H. Davenport, *The Higher Arithmetic*, 5th ed., Cambridge Univ. Press, 1982.
2. D. Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, 1973.
3. D. H. Lehmer and R. E. Powers, "On factoring large numbers," *Bull. Amer. Math. Soc.* **37** (1931), 770–776.
4. M. A. Morrison and J. Brillhart, "A method of factoring and the factorization of F_7," *Math. Comp.* **29** (1975), 183–205.
5. C. Pomerance and S. S. Wagstaff, Jr., "Implementation of the continued fraction integer factoring algorithm," *Proc. 12th Winnipeg Conference on Numerical Methods and Computing*, 1983.
6. M. C. Wunderlich, "A running time analysis of Brillhart's continued fraction factoring method," *Number Theory, Carbondale 1979*, Springer Lecture Notes Vol. 751 (1979), 328–342.
7. M. C. Wunderlich, "Implementing the continued fraction factoring algorithm on parallel machines," *Math. Comp.* **44** (1985), 251–260.

5 The quadratic sieve method

The quadratic sieve method for factoring large integers, developed by Pomerance in the early 1980's, for a long time was more successful than any other method in factoring integers n of general type which have no prime factor of order of magnitude significantly less than $\sqrt{n}$. (For integers n having a special form there may be special purpose methods which are faster, and for n divisible by a prime much smaller than $\sqrt{n}$ the elliptic curve factorization method in §VI.4 is faster. Also see the discussion of the number field sieve at the end of the section.)

The quadratic sieve is a variant of the factor base approach discussed in §3. As our factor base B we take the set of all primes $p \leq P$ (where P is some bound to be chosen in some optimal way) such that n is a quadratic residue mod p, i.e., $\left(\frac{n}{p}\right) = 1$ for p odd, and $p = 2$ is always included in B. The set of integers S in which we look for B-numbers (recall that a B-number is an integer divisible only by primes in B) will be the same set that we used in Fermat factorization (see §3), namely: