$$S = \{t^2 - n \mid [\sqrt{n}] + 1 \leq t \leq [\sqrt{n}] + A\}$$

for some suitably chosen bound A.

The main idea of the method is that, instead of taking each $s \in S$ one by one and dividing it by the primes $p \in B$ to see if it is a B-number, we take each $p \in B$ one by one and examine divisibility by p (and powers of p) simultaneously for all of the $s \in S$. The word "sieve" refers to this idea. Here we should recall the "sieve of Eratosthenes," which one can use to make a list of all primes $p \leq A$. For example, to list the primes ≤ 1000 one takes the list of all integers ≤ 1000 and then for each $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ one discards all multiples of p greater than p — one "lets them fall through a sieve which has holes spaced a distance p apart" — after which the numbers that remain are the primes.

We shall give an outline of a procedure to carry out the method, and then give an example. The particular version described below is only one possible variant, and it is not necessarily the most efficient one. Moreover, our example of a number n to be factored (and also the numbers to be factored in the exercises at the end of the section) will be chosen in the range $\approx 10^6$, so as to avoid having to work with large matrices. However, such n are far too small to illustrate the time advantage of the sieve in finding a large set of B-numbers.

Thus, suppose we have an odd composite integer n.

1. Choose bounds P and A, both of order of magnitude roughly

$$e^{\sqrt{\log n \log\log n}}.$$

Generally, A should be larger than P, but not larger than a fairly small power of P, e.g., $P < A < P^2$.

This function $\exp(\sqrt{\log n \log\log n})$, which we encountered before in this chapter and which is traditionally denoted $L(n)$, has an order of magnitude intermediate between polynomial in $\log n$ and polynomial in n. If $n \approx 10^6$, then $L(n) \approx 400$. In the examples below, we shall choose $P = 50$, $A = 500$.

2. For $t = [\sqrt{n}] + 1,\ [\sqrt{n}] + 2, \ldots, [\sqrt{n}] + A$, make a column listing the integers $t^2 - n$.

3. For each odd prime $p \leq P$, first check that $\left(\frac{n}{p}\right) = 1$ (see §II.2); if not, then throw that p out of the factor base.

4. Assuming that p is an odd prime such that n is a quadratic residue mod p (we'll treat the case $p = 2$ separately), solve the equation $t^2 \equiv n \ (mod\ p^\beta)$ for $\beta = 1, 2, \ldots$, using the method in Exercise 20 of §II.2. Take increasing values of β until you find that there is no solution t which is congruent modulo p^β to any integer in the range $[\sqrt{n}] + 1 \leq t \leq [\sqrt{n}] + A$. Let β be the largest integer such that there is some t in this range for which $t^2 \equiv n \ (mod\ p^\beta)$. Let t_1 and t_2 be two solutions of $t^2 \equiv n \ (mod\ p^\beta)$ with