But despite our good fortune in finding a set of mod 2 linearly dependent rows so quickly, it turns out that we are not so lucky after all: the two numbers being squared in the above congruence are both $\equiv 111078 \pmod{1042387}$, so we get only the trivial factorization. As we continue down the matrix, we find some other sets of dependent rows, which also fail to give us a nontrivial factorization. Finally, when we are about to give up — and start over again with a larger A — we notice that the last row — corresponding to our very last value of t — is dependent on the earlier rows. More precisely, it is equal modulo 2 to the fifth row. This gives us $(1112 \cdot 1520)^2 \equiv (3^3 \cdot 17 \cdot 23 \cdot 47)^2 \pmod{1042387}$, i.e., $647853^2 \equiv 496179^2 \pmod{1042387}$, and we obtain the nontrivial factor $g.c.d.(647853 - 496179, 1042387) = 1487$.

Based on some plausible conjectures, one can show that the expected running time of the quadratic sieve factoring method is asymptotically

$$O\left(e^{(1+\epsilon)\sqrt{\log n \log\log n}}\right)$$

for any $\epsilon > 0$. There is a fairly large space requirement, also of the form $\exp(C\sqrt{\log n \log\log n})$. For a detailed discussion of time and space requirements for the quadratic sieve (and several other) factoring algorithms, see Pomerance's article in the volume *Computation Methods in Number Theory*.

The number field sieve. Until recently, all of the contenders for the best general purpose factoring algorithm had running time of the form

$$\exp\big(O(\sqrt{\log n \log\log n})\big).$$

Some people even thought that this function of n might be a natural lower bound on the running time. However, during the last few years a new method — called the *number field sieve* — has been developed that has a heuristic running time that is much better (asymptotically), namely:

$$\exp\big(O((\log n)^{1/3}(\log\log n)^{2/3})\big).$$

In practice, it appears to be the fastest method for factoring numbers that are at or beyond the current (1994) upper limits of what can be factored, i.e., > 150 digits.

In some respects, the number field sieve factoring algorithm is similar to the earlier algorithms that attempt to combine congruences so as to obtain a relation of the form $x^2 \equiv y^2 \pmod{n}$. However, one uses a "factor base" in the ring of integers of a suitably chosen algebraic number field. Thus, along with the basic machinery of the quadratic sieve, this factoring method uses algebraic number theory. It is perhaps the most complicated factoring algorithm known. We shall give only an overview.

The basic requirements of the algorithm can be briefly described as follows. Given an integer n to be factored, choose a degree d and find n as