the value at some integer m of an irreducible monic integer polynomial of degree d:

$$n = f(m) = m^d + a_{d-1}m^{d-1} + a_{d-2}m^{d-2} + \cdots + a_1 m + a_0,$$

where m and the a_k are integers that are $O(n^{1/d})$. One way to find such a polynomial is to let m be the integer part of the d-th root of n and then expand n to the base m. For 125-digit numbers an analysis of the algorithm suggests that d should be 5, so that m and the coefficients will have about 25 digits.

The number field sieve then searches (by a sieving process similar to the quadratic sieve) for as many pairs (a, b) as possible such that both $a + bm$ and also

$$b^d f(-a/b) = (-a)^d + a_{d-1}(-a)^{d-1}b + a_{d-2}(-a)^{d-2}b^2 + \cdots - a_1 a b^{d-1} + a_0 b^d$$

are smooth over a given factor base (i.e., are divisible only by primes in the factor base). The details of how this is done and how this leads to a factorization of n can be found in the book *The Development of the Number Field Sieve* cited in the references below. In order for this procedure to succeed, the proportion of smooth numbers among values of the polynomial f should be approximately the same as the proportion of smooth numbers among all numbers of the same size. Although this is likely to be true, and is true in all examples that have been computed, it seems to be a very hard assertion to prove. Since the estimate of running time depends on this unproved conjecture, it is a heuristic estimate. While perhaps of little consequence in practice for factoring actual numbers, this circumstance points to some important open problems in the analysis of the theoretical asymptotic complexity of factoring.

The author would like to thank Joe Buhler for providing the above brief summary of the number field sieve for this book.

Exercises

1. In the example, find all linear dependence relations mod 2 between the rows of the matrix, and show that if $P = 50$ and $A \leq 499$ one cannot get a nontrivial factorization of 1042387 by this method.
2. Let $n \longrightarrow \infty$, and suppose that P and A are always chosen to have the same order of magnitude (for example, suppose that there are positive constants c_1 and c_2 such that $c_1 \leq \log A / \log P \leq c_2$). Asymptotically, what is the most time-consuming part of steps 1)-7) in the above version of the quadratic sieve? Give a big-O estimate for the number of bit operations required by that step.
3. Use the method in this section with $P = 50$ and $A = 500$ to factor: (a) 1046603, (b) 1059691, and (c) 998771.