algorithm as described above finds r in the k-th step, where $k < 4k_0$. (Strictly speaking, it could happen that $x_k - x_j$ has a larger g.c.d. with n, i.e., $g.c.d.((x_k - x_j)/r,\ n/r) > 1$; but the chance of a random integer having nontrivial g.c.d. with n/r is small, especially if n is a product of a small number of large primes. So we shall neglect this possibility, which at worse would have the effect of requiring a slightly larger constant C in the proposition.)

Thus, the number of bit operations needed to find r is bounded by $4k_0(C_1 log^3 n + C_2 log^2 n)$. According to Proposition V.2.1, the probability that k_0 is greater than $1 + \sqrt{2\lambda r}$ is less than $e^{-\lambda}$. If k_0 is not greater than $1 + \sqrt{2\lambda r}$, then the number of bit operations needed to find r is bounded by (here we use the fact that $r < \sqrt{n}$):

$$4(1 + \sqrt{2\lambda r})(C_1 log^3 n + C_2 log^2 n) < 4(1 + \sqrt{2}\sqrt{\lambda}\sqrt[4]{n})(C_1 log^3 n + C_2 log^2 n).$$

If we choose C slightly greater than $4\sqrt{2}(C_1 + C_2)$ (so as to take care of the added 1), we conclude, as claimed, that the factor r will be found in $C\sqrt{\lambda}\sqrt[4]{n}\, log^3 n$ bit operations, unless we made an unfortunate choice of $(f,\ x_0)$, of which the likelihood is less than $e^{-\lambda}$.

Remarks. 1. The basic assumption underlying the rho method is that polynomials can be found which behave like random maps in the sense of Proposition V.2.1. This has not been proved. However, practical experience factoring numbers by the rho method suggests that the "average" polynomial behaves like the "average" map, and that some very simple polynomials (the most popular one being $f(x) = x^2 + 1$) have this "average" property.

2. According to Proposition V.2.2, if we choose λ large enough to have confidence in success — for example, $e^{-\lambda}$ is only about 0.0001 for $\lambda = 9$ — then we know that for an average pair $(f,\ x_0)$ we are almost certain to factor n in $3C\sqrt[4]{n}\, log^3 n$ bit operations.

Exercises

In Exercises 1–4, use the rho method with the indicated $f(x)$ and x_0 to factor the given n. In each case compare x_k only with the x_j for which $j = 2^h - 1$ (where k is an $(h+1)$-bit integer).

1. $x^2 - 1,\ x_0 = 2,\ n = 91$.
2. $x^2 + 1,\ x_0 = 1,\ n = 8051$.
3. $x^2 - 1,\ x_0 = 5,\ n = 7031$.
4. $x^3 + x + 1,\ x_0 = 1,\ n = 2701$.
5. Let S be a set containing r elements, and let the maps f in the pairs $(f,\ x_0)$ range over all *bijections* of the set S to itself (i.e., f is a 1-to-1 correspondence between S and itself — no two x's have the same $f(x)$). As before, let $x_{j+1} = f(x_j)$ for $j = 0, 1, 2, \ldots$. For each pair