$(f,\ x_0)$, let k denote the first index such that there exists $j < k$ for which $f(x_k) = f(x_j)$. Prove that
(a) k is at most r, and for each value from 1 to r there is a $1/r$ probability that k is that value;
(b) the average value of k is $(r+1)/2$ (where the average is taken over all pairs $(f,\ x_0)$ with f a bijection).

6. Using Exercise 5, explain why a linear polynomial $ax+b$ should *never* be chosen for $f(x)$ in the rho method.
7. Suppose that you are using the rho method to factor a number which has a prime divisor r. You decide to choose $f(x) = x^2$ as your function to be iterated. (This is a bad choice of $f(x)$, as will become clear below.) We are interested in determining the first value of k such that $x_k \equiv x_\ell \ mod\ r$ for some $\ell < k$, i.e., the first value of k such that $x_0, x_1, \ldots, x_k$ are *not* all distinct modulo r. Suppose that you happen to choose x_0 which is a generator of $(\mathbf{Z}/r\mathbf{Z})^*$. Set $r-1 = 2^s t$, where t is odd.

(a) Write a congruence modulo $r-1$ which is equivalent to $x_k = x_\ell$ (equality means congruence modulo r).
(b) Find the first values of k and ℓ for which the condition in (a) holds, expressing them in terms of s and the binary expansion of the fraction $1/t$.
(c) Roughly how large is k compared to r? Why is $f(x)$ a bad choice of function for the rho method?

References for § V.2

1. W. D. Blair, C. B. Lacampagne and J. L. Selfridge, "Factoring large numbers on a pocket calculator," *American Math. Monthly* **93** (1986), 802–808.
2. R. P. Brent, "An improved Monte Carlo factorization algorithm," *BIT* **20** (1980), 176–184.
3. R. P. Brent and J. M. Pollard, "Factorization of the eighth Fermat number," *Math. Comp.* **36** (1981), 627–630.
4. R. K. Guy, "How to factor a number," *Proc. 5th Manitoba Conference on Numerical Mathematics* (1975), 49–89.
5. J. M. Pollard, "A Monte Carlo method for factorization," *BIT* **15** (1975), 331–334.

3 Fermat factorization and factor bases

Fermat factorization. As we saw earlier (see Exercise 3 of § I.2 and Exercise 4 of § IV.2), there's a way to factor a composite number n that is efficient if