The first step in the rho method is to choose an easily evaluated map from $\mathbf{Z}/n\mathbf{Z}$ to itself, namely, a fairly simple polynomial with integer coefficients, such as $f(x) = x^2 + 1$. Next, one chooses some particular value $x = x_0$ (perhaps $x_0 = 1$ or 2, or perhaps it is a randomly generated integer) and computes the successive iterates of f: $x_1 = f(x_0)$, $x_2 = f(f(x_0))$, $x_3 = f(f(f(x_0)))$, etc. That is, we define

$$x_{j+1} = f(x_j), \qquad j = 0, 1, 2, \ldots .$$

Then we make comparisons between different x_j's, hoping to find two which are in different residue classes modulo n but in the same residue class modulo some divisor of n. Once we find such x_j, x_k, we have $g.c.d.(x_j - x_k, n)$ equal to a proper divisor of n, and we are done.

Example 1. Let us factor 91 by choosing $f(x) = x^2 + 1$, $x_0 = 1$. Then we have $x_1 = 2$, $x_2 = 5$, $x_3 = 26$, etc. We find that $g.c.d.(x_3 - x_2, n) = g.c.d.(21, 91) = 7$, so 7 is a factor. Of course, this is a trivial example: we could have found the factor 7 faster by trial division.

In the rho method it is important to choose a polynomial $f(x)$ which maps $\mathbf{Z}/n\mathbf{Z}$ to itself in a rather disjointed, "random" way. For example, we shall later see that $f(x)$ must not be a linear polynomial, and in fact, should not give a 1-to-1 map.

Let us suppose that $f(x)$ is a "random" map from $\mathbf{Z}/n\mathbf{Z}$ to itself, and compute how long we expect to have to wait before we have two iterations x_j and x_k such that $x_j - x_k$ has a nontrivial common factor with n. We do this by finding for a fixed divisor r of n (which, in practice, is not yet known to us) the *average* (taken over all maps from $\mathbf{Z}/n\mathbf{Z}$ to itself and over all values x_0) of the first index k such that there exists $j < k$ with $x_j \equiv x_k \bmod r$. In other words, we regard $f(x)$ as a map from $\mathbf{Z}/r\mathbf{Z}$ to itself and ask how many iterations are required before we encounter the first repetition of values $x_k = x_j$ in $\mathbf{Z}/r\mathbf{Z}$.

Proposition V.2.1. *Let S be a set of r elements. Given a map f from S to S and an element $x_0 \in S$, let $x_{j+1} = f(x_j)$ for $j = 0, 1, 2, \ldots$. Let λ be a positive real number, and let $\ell = 1 + \left[\sqrt{2\lambda r}\,\right]$. Then the proportion of pairs $(f,\ x_0)$ for which $x_0, x_1, \ldots, x_\ell$ are distinct, where f runs over all maps from S to S and x_0 runs over all elements of S, is less than $e^{-\lambda}$.*

Proof. The total number of pairs is r^{r+1}, because there are r choices of x_0, and for each of the r different $x \in S$ there are r choices of $f(x)$. How many pairs $(f,\ x_0)$ are there for which $x_0, x_1, \ldots, x_\ell$ are distinct? There are r choices for x_0, there are $r - 1$ choices for $f(x_0) = x_1$ (since this cannot equal x_0), there are $r - 2$ choices for $f(x_1) = x_2$, and so on, until $f(x)$ has been defined for $x = x_0, x_1, \ldots, x_{\ell-1}$. Then the value of $f(x)$ for each of the $r - \ell$ remaining x is arbitrary, i.e., there are $r^{r-\ell}$ possibilities for those values. Hence, the total number of possible ways of choosing x_0 and assigning the values $f(x)$ so that $x_0, \ldots, x_\ell$ are distinct is: