1. **Introduction:** John Pollard invented the Rho factorization algorithm in 1975. It does a fairly fast job for numbers with small prime factors, even if those numbers themselves are big, and it has a very small memory footprint, so it’s a useful tool to do some initial probing.

2. **Idea:** Given some \( n \in \mathbb{Z} \), suppose \( p \) is an unknown factor of \( n \). The goal is to find integers \( x_0, x_1, ..., x_s \) which are distinct mod \( n \) but not mod \( p \). Once we have done this then we have some \( i, j \) with \( x_j \equiv x_i \pmod{n} \) and \( x_j \equiv x_i \pmod{p} \). At this point note that \( p | (x_j - x_i) \) and \( p | n \). Consider now that \( \gcd(x_j - x_i, n) \) is a divisor of \( n \) but is greater than or equal to \( p \) since \( p | (x_j - x_i) \) and \( p | n \).

To find such \( x_i \) and \( x_j \) we pick an initial \( x_0 \) and define \( f(x) = x^2 + 1 \). We then take \( x_1 = f(x_0) \) reduced \( \pmod{n} \), \( x_2 = f(x_1) \) reduced \( \pmod{n} \), and so on. This basically generates a list of pseudorandom numbers mod \( n \). Since we’re examining differences mod \( n \) and mod \( p \), and since \( p \) is assumed to be quite small, it’s sensible that we might obtain \( x_i \) and \( x_j \) which are congruent mod \( p \) fairly quickly while still being incongruent mod \( n \).

However it’s still not reasonable to check all possible \( x_i \) and \( x_j \) as we go. Consider our sequence \( x_0, x_1, x_2, ... \) taken mod \( p \). We know for a fact that eventually \( x_j \equiv x_i \pmod{p} \) for \( j > i \) because eventually we run out of options mod \( p \). At this point the numbers repeat mod \( p \) every \( j - i \) steps. in other words \( x_\alpha \equiv x_\beta \pmod{p} \) when \( (j - i) | (\alpha - \beta) \) and \( \alpha, \beta \geq i \).

Suppose \( s \) is the smallest multiple of \( j - i \) with \( s \geq i \) then observe that \( x_{2s} \equiv x_s \pmod{p} \) because \( (j - i) | (2s - s) \) and \( 2s, s \geq i \).

The practical result of this is that we assign \( x_0 \) and calculate \( x_1, x_2, x_3, ... \) but only check \( x_{2s} \) and \( x_s \) when possible.

3. **Pollard’s Rho Method:** Given an integer \( n \) which we assume has a small factor we choose some \( x_0 \) (often \( x_0 = 2 \)), and we choose \( f(x) = x^2 + 1 \) (this is typical). We generate \( x_1 = f(x_0) \) reduced \( \pmod{n} \), \( x_2 = f(x_1) \) reduced \( \pmod{n} \), and so on. At each even subscript \( x_{2s} \) we calculate \( \gcd(x_{2s} - x_s, n) \) and immediately upon obtaining a number greater than 1 we are done.

**Note:** The gcd we find is not necessarily our hypothesized \( p \), however \( p \) is a divisor of it, and it is not uncommon to actually obtain a prime.

**Example:** Let’s factor \( n = 1111 \). We set \( x_0 = 2 \) and \( f(x) = x^2 + 1 \). We then calculate:

\[
\begin{align*}
x_1 &= 5 \\
x_2 &= 26 \quad \gcd(26 - 5, 1111) = 1 \\
x_3 &= 677 \\
x_4 &= 598 \quad \gcd(598 - 26, 1111) = 11
\end{align*}
\]

We know 11 is a factor and we’re done.
Example: Let’s factor \( n = 1189 \). We set \( x_0 = 2 \) and \( f(x) = x^2 + 1 \). We then calculate:

\[
\begin{align*}
    x_1 &= 5 \\
    x_2 &= 26 & \text{gcd} (26 - 5, 1189) &= 1 \\
    x_3 &= 677 \\
    x_4 &= 565 & \text{gcd} (565 - 26, 1189) &= 1 \\
    x_5 &= 574 \\
    x_6 &= 124 & \text{gcd} (124 - 677, 1189) &= 1 \\
    x_7 &= 1109 \\
    x_8 &= 456 & \text{gcd} (456 - 565, 1189) &= 1 \\
    x_9 &= 1051 \\
    x_{10} &= 21 & \text{gcd} (21 - 574, 1189) &= 1 \\
    x_{11} &= 442 \\
    x_{12} &= 369 & \text{gcd} (369 - 124, 1189) &= 1 \\
    x_{13} &= 616 \\
    x_{14} &= 166 & \text{gcd} (166 - 1109, 1189) &= 41 \\
\end{align*}
\]

We know 41 is a factor and we’re done.

4. **Nomenclature:** The reason that this is called the Rho method is that when we obtain \( x_{2s} \equiv x_s \mod p \) we have found \( x_j \equiv x_i \mod p \) and we have a cycle. In the previous example \( x_{14} \equiv x_7 \mod 41 \) and hence because of the cyclic nature we have \( x_{15} \equiv x_8 \mod 41, x_{16} \equiv x_9 \mod 41 \) and so on. Our sequence of \( x_i \), taken mod \( p \), form the shape of the Greek letter \( \rho \).