Pollard’s rho algorithm

[intro]

Pollard’s rho algorithm is an algorithm for integer factorization.

[core idea]

[pseudo code]

x ← 2

y ← 2

d ← 1

**while** d = 1:

x ← g(x)

y ← g(g(y))

d ← gcd(|x - y|, n)

**if** d = n:

**return failure**

**else**:

**return** d

[ref]

[Pollard's rho algorithm - Wikipedia](https://en.wikipedia.org/wiki/Pollard's_rho_algorithm)