MATH 467, Pollard rho and p-1

Algorithm Pollard rho.

1. Choose a polynomial f with integer coefficients which is irreducible over \mathbb{Q} , such as $f(x) = x^2 + 1$.

- **2.** Pick an integer x_0 at random and take $z_0 = x_0$.
- **3.** For $j = 1, 2, 3, \ldots$, given x_{j-1}, z_{j-1} compute

 $x_j = f(x_{j-1}) \pmod{n}, \quad z_j = f(f(z_{j-1})) \pmod{n}, \quad GCD(z_j - x_j, n).$

4. If after a certain amount of time this does not produce a non-trivial factor of n start over with a different polynomial f.

Algorithm Pollard p-1.

- **1.** Pick some large positive integer K.
- **2.** Pick some a with (a, n) = 1.
- **3.** Let $x_0 = a$ and for $k = 1, \ldots, K$ successively compute

 $x_k = x_{k-1}^k \pmod{n}$ and $GCD(x_k - 1, n)$.