## 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

$$
x_{j}=f\left(x_{j-1}\right) \quad(\bmod n), \quad z_{j}=f\left(f\left(z_{j-1}\right)\right) \quad(\bmod n), \quad G C D\left(z_{j}-x_{j}, n\right)
$$

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

$$
x_{k}=x_{k-1}^{k} \quad(\bmod n) \text { and } G C D\left(x_{k}-1, n\right) .
$$

