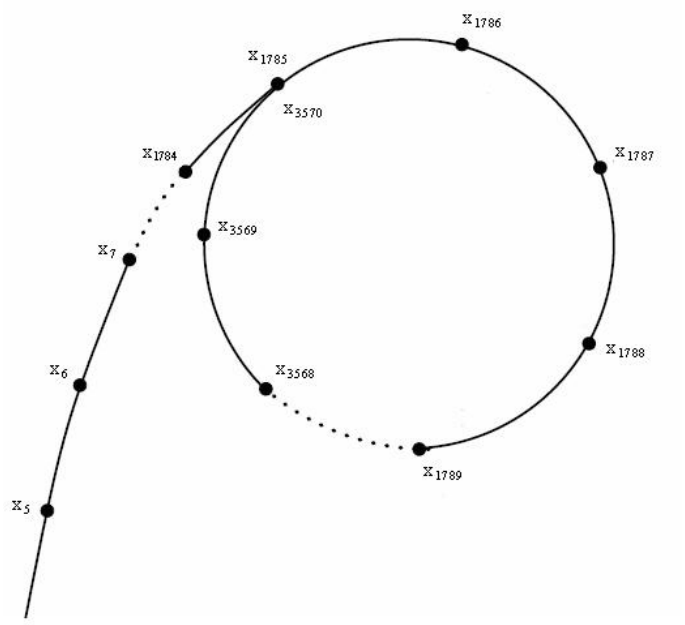
- $f(x) = x^2 + 1, \quad x_k = f(x_{k-1}) \pmod N$
- con $N = 82123, x_0 = 631$ si ha
- $x_1 = 69760, x_2 = 28986, x_3 = 69907$
- $x_4 = 13166, x_5 = 64027, x_6 = 40816,$
- $x_7 = 80802, x_8 = 20459, x_9 = 71874,$
- $x_{10} = 6685, x_{11} = 14314, x_{12} = 75835$
- si ha $(x_3 - x_{10}, N) = 41$ e $N = 41 \cdot 2003$
- nota che anche $(x_4 - x_{11}, N) = 41, (x_5 - x_{12}, N) = 41 \ldots$
- cosa succede considerando la successione

$$x_0, x_1, x_2, \ldots, x_{10}, x_{11}, x_{12} \ldots \pmod{41}?$$

ρ di Pollard



- se $x_h \equiv x_k \pmod{p}$,
- allora $x_{h+1} = f(x_h) \equiv f(x_k) = x_{k+1} \pmod{p}$

metodo di Floyd

- per ridurre il numero di MCD da calcolare, si usa il metodo di Floyd per la ricerca di un ciclo
- nella successione $x_0, x_1, x_2, \ldots, x_{10}, x_{11}, x_{12} \ldots$
- si considerano solo le coppie della forma (x_i, x_{2i}) $i = 1, 2, \ldots$
- e si calcolano solo i MCD$(x_i - x_{2i}, N)$ $i = 1, 2, \ldots$
- si può mostrare che questo è un metodo efficiente per trovare una collisione
- nell'esempio precedente la prima collisione si ha con (x_7, x_{14})
- al settimo passo - senza questo metodo, per trovare la prima collisione (x_3, x_{10}) servono $\binom{10}{2}$ confronti.