Pollard's Rho ρ Algo

Try random nos. Prob. of picking one no. is $= \frac{2}{n}$

factor n ?

$n = 221 = 13 \times 17$

(1) $\{2, 220\} \rightarrow 219$ nos — search space. Only 2 nos divide 221

Now

$13 \times 1 = 13$
$13 \times 2 = 26$
$13 \times 3 = 39$
$\vdots$
$13 \times 16 = 208$

16 multiples of 13

and

$17 \times 1 = 17$
$17 \times 2 = 34$
$17 \times 3 = 51$
$\vdots$
$17 \times 12 = 204$

12 multiples of 17

They have one thing common

— They all share a common factor with 221

— $\therefore$ having found a no. that has a comm. factor with our n, then that comm. factor will be a factor of n.

(2) $\therefore$ Instead of looking 2 no.s between 2 & 221 why not look for one of the 28 (16+12) no.s which share a comm. factor.

$\therefore$ we have improved a chance by >14 times

(3) What is the prob. if we pick 2 no.s between 1 & 221 & the difference between them has a common factor with 221?

\# No. of ways of picking 2 nos $= (221)^2$
$= 48,841$

- Out of 48,841 poss. combinations there are over 6000 of them which results in the diff. between ~~th~~ the no's having a factor in comm. with 221.

- $\forall$ no. 1 & 221 there are 28 no.s that go with it for which the diff. is $\times$ of either 13 or 17. for eg:

14, 18, 27, 35, 40, 52, 53, 66, 69, 79, 86, 92, 103, 105, 118, 220, 131, 137, 144, 154, 157, 170, 171, 183, 188, 188, 196, 205 & 209.

⇒ If you were to pick 2 (different) no s between 1 & 221, there is a ~~great~~ greater ~~chance~~ than one in 8 chance that the difference between those no's would have a common factor in comm with 221

$\boxed{\rho\text{- factoring algo}}$

$x_0 = \text{random}(0, n-1)$

$x_i = f(x_{i-1}) \pmod n$, $i = 1, 2, 3, \ldots$

$x_0 \rightarrow$ random starting value
$n \rightarrow$ no. to be factored

$f \in \mathbb{Z}[x]$ poly. with integer coff.

usually , $f(x) = x^2 \pm a$, $a \neq -2, 0$

— If p is a prime seq $\{x_i \pmod p\}_{i>0}$ must eventually repeat.

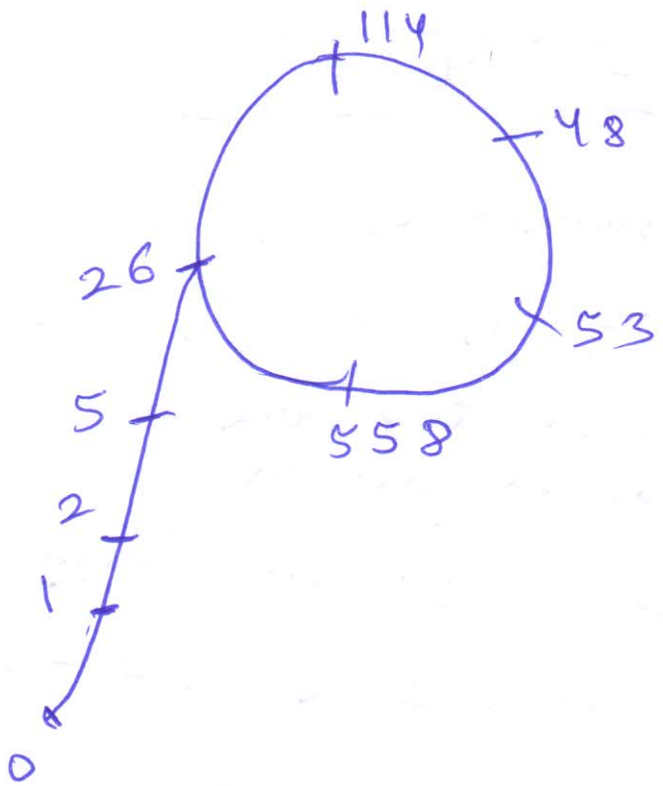
<u>Ex.</u> $f(x) = x^2 + 1$, $x_0 = 0$ & $p = 563$

$\{x_i \bmod p\}_{i>0}$ given as

$x_0 = 0$
$x_1 = x_0^2 + 1 = 1$
$x_2 = x_1^2 + 1 = 2$
$x_3 = x_2^2 + 1 = 5$
$x_4 = x_3^2 + 1 = \underline{26}$
$x_5 = x_4^2 + 1 = 114$
$x_6 = x_5^2 + 1 = 48$
$x_7 = x_6^2 + 1 = 53$
$x_8 = x_7^2 + 1 = 558$
$x_9 = x_8^2 + 1 = \underline{26}$

i.e. $0, 1, 2, 5, \overline{26, 114, 48, 53, 558}$

- Fig ρ



Verify! ρ cycle mod 1951 using $f(x) = x^2+1$ & $x_0 = 0$

To factor $n = 1098413 = 563 \cdot 1951$

we perform (gen. two seqs) $\{x_i\}$, $\{y_i\}$ mod n (= 1098413)

$\gcd(x_i - y_i, n)$

$y_i = x_{2i}$

$x_0 = \underline{0}$

$x_1 = x_0^2+1 = \underline{1}$

$x_2 = x_1^2+1 = \underline{2}$ $\quad y_1 = x_2 = 2 \quad \gcd(1-2, n) = 1$

$x_3 = x_2^2+1 = \underline{5}$

$x_4 = x_3^2+1 = \underline{26}$ $\quad y_2 = x_4 = 26, \ \gcd(2-26, n) = 1$

$x_5 = x_4^2+1 = \cancel{667}\ 677 \equiv \underline{114}$

$x_6 = x_5^2+1 = 458330 \equiv \underline{48}$ $\quad y_3 = x_6 = 458330$

$\gcd(5 - 458330, n) = 1$

$x_7 = x_6^2 + 1 = 394716$
$\equiv \underline{53}$

$x_8 = x_7^2 + 1 = 722324$ $\quad y_4 = x_8 = 722324$
$\equiv \underline{558}$ $\quad \gcd(26 - 722324, n) = 1$

$x_9 = x_8^2 + 1 = 293912$
$\equiv \underline{26}$

$x_{10} = x_9^2 + 1 = 671773$ $\quad y_5 = x_{10} = 671773$
$\equiv \underline{114}$ $\quad \gcd(677 - 671773, n)$
$= \underline{563}$

$\therefore$ factor found.

$\boxed{\text{Brent - Pollard's } \rho \text{- Method}}$

__Algo:__ n (composite $\mathbb{Z}$) > 1

Algo finds a non trivial factor d of n which is small compared with $\sqrt{n}$. suppose for $f(x) = x^2 + 1$

① $\boxed{\text{Initialization}}$ _ Choose a seed $x_0 = 2$

- $f(x) = x^2 + 1 \pmod{n}$
- Choose a value t not much bigger than $\sqrt{d}$ perhaps $t < 100\sqrt{d}$

② $\boxed{\text{Iteration \& Computation}}$

Compute $\{x_i\}$ & $\{y_i\}$ as follows:

$x_1 = f(x_0)$
$x_2 = f(f(x_0)) = f(x_1)$
$x_3 = f(f(f(x_0))) = f(f(x_1)) = f(x_2)$
$\vdots$
$x_i = f(x_{i-1})$,

$$y_1 = x_2 = f(x_1) = f(f(x_0)) = f(f(y_0))$$
$$y_2 = x_4 = f(x_3) = f(f(x_2)) = f(f(y_1))$$
$$y_3 = x_6 = f(x_5) = f(f(x_4)) = f(f(y_2))$$
$$\vdots$$
$$y_i = x_{2i} = f(f(y_{i-1}))$$

and simultanously compare x_i & y_i by computing $d = \gcd(x_i - y_i, n)$

(3) $\boxed{\text{(factor found?)}}$ If $1 < d < n$ then d is a non-trival factor of n, print d and go to ~~set~~ step (5)

(4) (Another search?) If $x_i \equiv y_i \pmod{n}$ for some i or $i \geq \sqrt{k}$ then go to step (1) to choose a new seed & a new gen. & repeat

(5) $\boxed{\text{Exit}}$ Terminate the algo.

$\boxed{\text{Conjecture}}$ p (prime) $| n$ & $p = O(\sqrt{k})$

then ρ-also has expected runn. time

$$O(\sqrt{p}) = O(\sqrt{p}\,(\log n)^2) = O(n^{1/4}(\log n)^2)$$

to find prime factor p of n